# CyberSmart

## CYBER AWARENESS GUIDE

*Your trusted guide to cyber security resources from industry leaders*

eplus.com/security

eplus-security@eplus.com

The rate of cyber crimes has increased exponentially this year – and data is more at risk than it has ever been. According to Cybersecurity Ventures, the damage related to cybercrime is projected to hit $6 trillion annually by 2021. More sophisticated attacks combined with a huge increase in the number of employees working from home or in other remote capacities has created a wealth of opportunities for cyber criminals to gain unauthorized access to information.

The good news is that with so many resources at your fingertips, there's no reason to be cyber-spooked about your data being compromised. Creating a security-aware culture in your organization is a good foundational step to protecting every facet of your data and network. Awareness of the threats that exist around you – as well as how to search for them, detect them, identify them, remediate and prevent them – will keep you from having to navigate a scary situation.

# Table of Contents

Contact ePlus for any questions about these technologies, or to discuss your security program.

**eplus.com/security**
**eplus-security@eplus.com**

# Identity and Access Management (IAM)

Identity and Access Management (IAM) is a framework of policies that dictate the identities of exactly who is permitted to be on your network, and exactly what data they can access. Implementing an IAM framework is an important foundational step to building a robust and pervasive security program at your organization. Relatively easy to implement, IAM is a fairly quick way to noticeably improve your organization's security posture. There has been significantly more importance placed on IAM solutions as workforces become more distributed.

The resources in this section are available to help you understand the importance of implementing an Identity program, the components of doing so, and the measurable impact that can have across your organization.

okta

Modernizing IT Whitepaper

Read now

Contact ePlus for any questions about these technologies, or to discuss your security program.

**eplus.com/security**
**eplus-security@eplus.com**

# Modernizing IT

## Identity is a Key Tool to Facilitate IT Modernization

## Executive Summary

Many enterprises are saddled with an IT architecture that has evolved organically over time. The realities of competing priorities, limited staffing and budgets often mean that systems and strategies remain in place far longer than originally intended. This often results in a significant burden of cost and complexity, and can compromise a business's agility.

Recognizing this reality, many organizations have embraced modernization initiatives. Approaches vary between an incremental "two speed" model and the more ambitious "greenfield" method. Under either approach, a modern cloud-based identity management strategy is a critical catalyst in speeding the transformation process and ensuring systems and processes work together seamlessly.

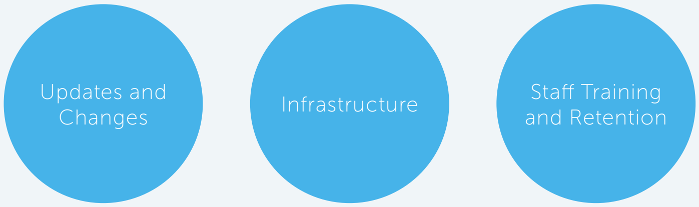
Such an identity strategy helps businesses increase agility by deploying a single identity architecture, and facilitating change through automating many IT lifecycles. Businesses that embrace this change are able to decrease costs, increase efficient and accelerate growth.

## The Challenge: Aging IT

If there is any constant in modern business and IT, it's change. Mergers, acquisitions, changing priorities, new applications, services and platforms create a huge amount of flux in IT infrastructure.

Compounding reality is the fact that IT organizations are constantly being asked to do more with less. To provide value from shareholders, IT organizations push for efficiency, which often means making tough prioritization choices. When it comes time to choose between rolling out new business services and updating legacy technology, new services almost always win out.

But the long term impacts of these decisions add up over time. Maintenance creates a tax on IT. Updates and changes monopolize cycles, infrastructure to support legacy applications strains capital budgets, and staff training and retention becomes a critical priority.



Updates and Changes

Infrastructure

Staff Training and Retention

*The cost of aging IT*

Left unchecked these impacts become a massive burden

- 71% of the IT budget for US federal civilian agencies is spent on maintaining legacy systems[1]
- 65% of enterprise IT spend is on "run the business"[2]

## Two Approaches to Transformation

Recognizing the need to pay down this technical debt, many organizations are embracing IT modernization initiatives. Since no two businesses are the same, two distinct models for transformation are emerging[3], each with its own pros and cons:

1. The "**two-speed**" model focuses on improvements in specific areas of the IT architecture, while leaving some areas undisturbed
2. The "**greenfield**" model seeks to make broad, sweeping changes across the IT architecture

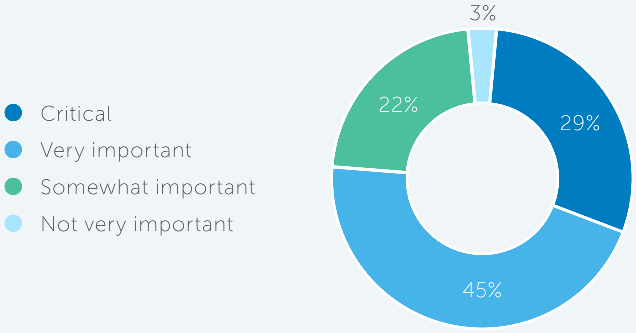
The two-speed model is often appealing to organizations that wish to minimize disruption and operational risks. It identifies a prioritized set of focused projects and changes, and can be useful where budget constraints might preclude larger efforts. To be successful, the two-speed model also assumes there are no issues with existing integrations and that current architectural complexity is manageable.

By contrast, the greenfield model seeks to make broad, sweeping change to maximize the return on investment of the modernization initiative. It takes a longer term view on budget, recognizing that sweeping change will take time, and that business benefits will accrue over the following years. At times, this model is chosen out of necessity, when an overly complex, "spaghetti" architecture is hindering business growth.

[1] WSJ, 2/9/16, Protecting U.S. Innovation From Cyberthreats
[2] KPMG Research, 2014
[3] McKinsey & Company, 2015, "Two ways to modernize IT systems for the digital era"

## Identity Management is Key to IT Modernization

Under either approach, one of the biggest roadblocks to transformation is identity. 74% of enterprise executives surveyed believe IAM is critical or very important to digital business initiatives.



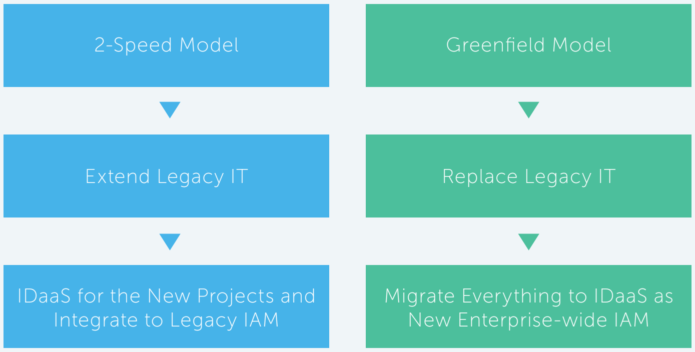
*Importance of IAM in Relation to Digital Business Initiatives*[4]

The reasons become clear when you examine several examples of the role identify plays in modernization projects:

- Migrating an enterprise application to the cloud. As seen in the massive adoption of Office 365, businesses are embracing cloud-based technology for agility and simplicity. But with the proliferation of services, integration with Active Directory can be complex, causing delays and frustration.
- Moving an HR Information System (HRIS) to the cloud. Cloud-based HRIS offers myriad advantages, and integration with IAM can drive efficiency by streamlining the onboarding, offboarding and change processes.
- Building a web or mobile app. Digital offering present a tremendous opportunity to provide value to customers, but if the user experience is poor, adoption suffers. Being able to support the latest identify protocols can be a critical usability differentiator.
- Opening developer access to business systems. Interoperability and integration is key to modern business, but can open access errors. A modern identity strategy can help businesses facilitate access while remaining secure.

## An Identity Strategy to Support Either Transformation Mode

Identity and Access Management strategies should be flexible enough to support either transformation mode, or a combination of the two.


2-Speed Model

Extend Legacy IT

IDaaS for the New Projects and Integrate to Legacy IAM

Greenfield Model

Replace Legacy IT

Migrate Everything to IDaaS as New Enterprise-wide IAM

*Identity as a core component of either type of modernization*

Under a two speed model, the goal is often to extend legacy IT. Mission critical projects that are reserved for future change need to continue to work with legacy IAM solutions. New projects, and other projects slated for immediate change, present an opportunity to work with a modern, more flexible IAM solution. In this case, cloud-based identity as a service (IDaaS) can act as a single management console—interfacing directly with some services and through legacy IAM solutions for others.

Under a greenfield model, replacing as much legacy IT as possible is the goal. This represents the chance to treat IAM as one of those legacy applications, migrating everything to a new, cloud-based IDaaS solution. The benefits of a single interface of identity remain, without the burden of having to support legacy IAM solutions.

Under either approach, businesses will experience enhanced value across three key pillars:

1. Decreased cost and enhanced efficiency
2. Enhanced agility to add and change IT services
3. Increased ability to deliver business value

## Why Okta?

Okta's modern approach to identity management is uniquely positioned to help businesses take control of identity to modernize IT across the three pillars of value.

[4] 2016 IDG/Okta Survey of 58 enterprise executives

### Decreased costs and enhanced efficiency

- A single solution for identity as a service. A single architecture and point of access means less cost and complexity architecture
- Cloud delivery means no hardware or on-premise software to maintain
- A simple administrative interface that makes administrators self-sufficient, and not reliant on customization
- Easy maintenance and automatic updates
- High availability deployment means a resilient infrastructure less prone to costly disruption

### Enhanced IT Agility

- Library of preconfigured integrations means faster changes and updates
- Simple integration to a directory (e.g., multiple domains) makes it easier to maintain a complex environment
- Easily integrate with existing and future on-premise, cloud and mobile applications, as well as new services
- Integrated multi-factor authentication eases the burden of delivering enhanced security

### Delivering enhanced business value

- Deploy web/mobile applications more quickly to provide enhanced customer value
- Programmatically federate with partners, or self-service registration for contractors, partners and customers to build stickier experiences
- Broad developer platform (e.g., APIs, SDKs) makes integration and for richer business context
- Faster change management lets business respond to needs in near real time

## Roadmap to Success

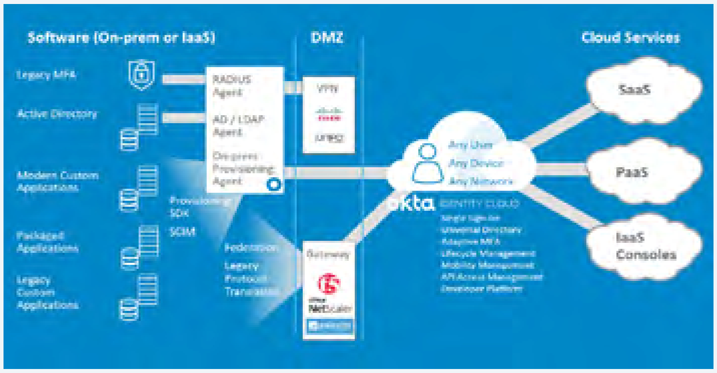
To recap, a modern, automated approach to identity helps take control of credentials to drastically reduce the risk of a data breach. Where should organizations start?

We recommend you focus on these key milestones:

1. Deploying a cloud-based identity platform with high availability and user store
2. Achieving simple integration as new access requirements are introduced
3. Ability to deploy multi-factor authentication
4. The capability to federate with partners, or self-service registration for contractors, partners and customers

## We are Here to Help

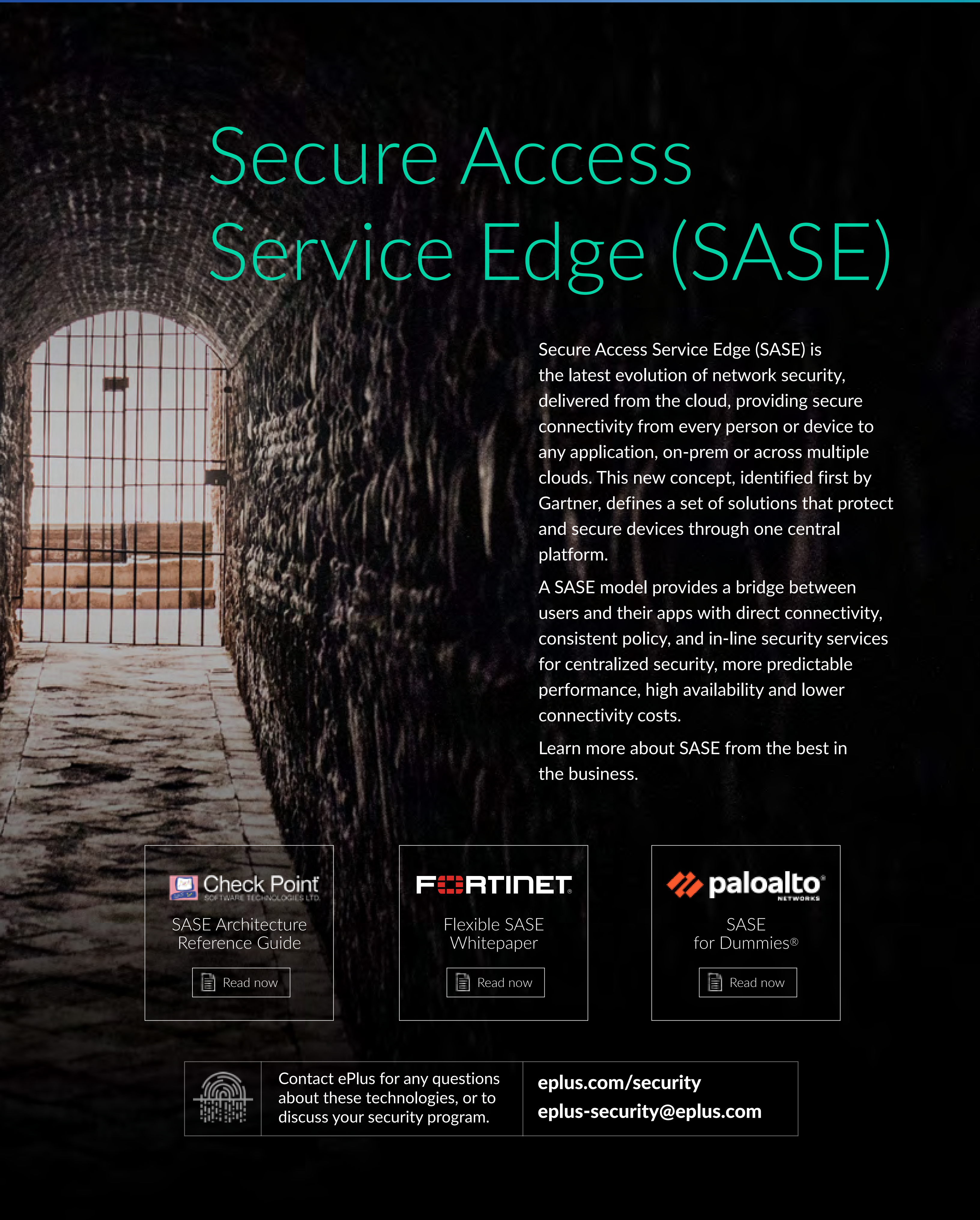
Okta provides an end-to-end suite for modern identity management. We connect with complex service infrastructures, enrich context by providing threat intelligence to deploy single sign-on, multi-factor authentication and automate lifecycle management. We do all of that by working with your existing security infrastructure to provide value.



*The Okta Identity Cloud Security Platform*

### About Okta

Okta is the foundation for secure connections between people and technology. Our IT products uniquely use identity information to grant people access to applications on any device at any time, while still enforcing strong security protections. Our platform securely connects companies to their customers and partners. Today, thousands of organizations trust Okta to help them fulfill their missions as quickly as possible.



# Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE) is the latest evolution of network security, delivered from the cloud, providing secure connectivity from every person or device to any application, on-prem or across multiple clouds. This new concept, identified first by Gartner, defines a set of solutions that protect and secure devices through one central platform.

A SASE model provides a bridge between users and their apps with direct connectivity, consistent policy, and in-line security services for centralized security, more predictable performance, high availability and lower connectivity costs.

Learn more about SASE from the best in the business.

Check Point SOFTWARE TECHNOLOGIES LTD.
SASE Architecture Reference Guide
Read now

FORTINET
Flexible SASE Whitepaper
Read now

paloalto NETWORKS
SASE for Dummies®
Read now

Contact ePlus for any questions about these technologies, or to discuss your security program.

**eplus.com/security**
**eplus-security@eplus.com**

# SASE Architecture

Architecture Reference Guide for the Implementation of Secure Access Service Edge

S.\SE
SECURE ACCESS SERVICE EDGE

Check Point
SOFTWARE TECHNOLOGIES LTD

[Internal Use] for Check Point employees

## ABSTRACT

As resources and applications shift to the cloud, on premise data centers are no longer the core of the network, users are no longer found only in corporate offices, and remote working becomes widely accepted with COVID-19 moving the world into a new paradigm.

To meet these needs and more, enterprises are seeking advice on how to re-architect their infrastructure.

This document provides a basic understanding of SASE architecture, explains how it solves different needs of evolving organizations, and best practices for deployment.

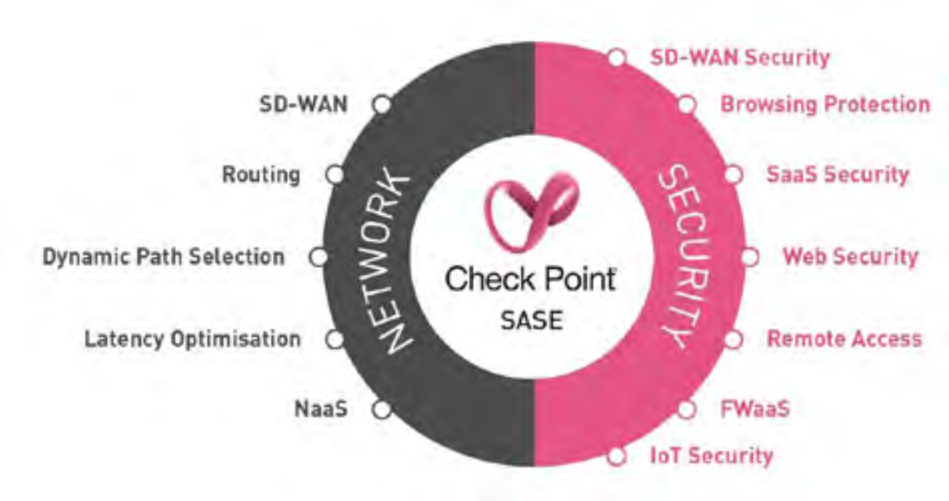
## AUDIENCE

This document is written for technical readers, IT security architects, and network specialists who are venturing out into cloud territory.

Readers should be familiar with basic concepts of virtualization, networks, and have a strong understanding of security design.

# TABLE OF CONTENTS

# INTRODUCTION TO SASE



The acronym SASE stands for Secure Access Service Edge.

SASE describes a change in architectural principles that moves away from a traditional on-premise Data Center and shifts to a decentralized architecture. When organizations adopt SASE principles, they distribute user access to corporate resources instead of consolidating them in one place.

We view SASE as an architectural methodology that converges network and security requirements into a single cloud-centric solution that allows cloud transformation.

It is an undeniable trend that more resources are moving from the traditional Data Center to the cloud.

This is the reason why instead of routing traffic from branch offices and remote users to the Data Center, where the internet egress point was typically located, SASE recommends that users and branches should all have a direct internet breakout.

The SASE model covers a wide range of functionalities, ranging from layer 3 in the OSI model up to the application layer, as depicted in the graphic on the left-hand side.

## SASE Main Components

**Security**

- SD-WAN Security: Sets companies dealing with a significant amount of legacy infrastructure in branch offices to stop backhauling all internet-bound traffic to the regional hub site without having to upgrade the legacy gateways, saving WAN costs without compromising security.
- Firewall as a Service (FWaaS): A cloud-based Next-Generation Firewall is a scalable, application-aware solution allowing enterprises to eliminate the challenges of legacy appliance-based solutions.
- Web Security: Secures Internet access to Web applications and resources leveraging unified Threat Prevention solutions, such as URL Filtering, Anti-Virus, IPS, Anti-Bot, and Zero-Day attack prevention.
- Browsing protection: a simple browser extension complements the cloud-based security controls and allows for full visibility into encrypted traffic, protecting against the loss of corporate data and mitigating modern-day malware such as ransomware, zero-day attacks, phishing, etc. so you can safely navigate today’s menacing threat landscape.
- Secure Remote Access to Corporate Resources: Replacing traditional remote access solutions where the VPN was terminated in an on-premise Data Center, SASE Remote access no longer requires the traffic to be backhauled, improving the user experience.
- SaaS Security: Secure access to SaaS applications like Office 365, Google suite, etc. using a Cloud Access Security Broker (CASB).

- IoT Security: SASE enables IoT devices to break out to the internet directly in a secure way.

**Network**

- SD-WAN: Optimizing access to the Internet and Data Centers by allowing branch offices and users to break out to the internet directly and securely, significantly improving the user experience.
- Elements like routing, dynamic path selection, NaaS, and latency optimization are all essential networking features of SD-WAN, laying the foundations on which security is built.

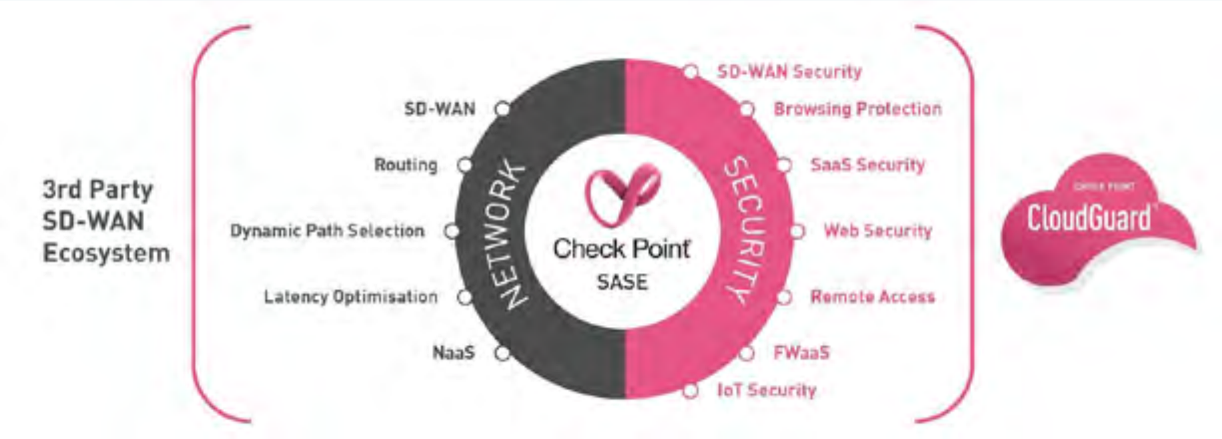
| Reasons to consider a SASE architecture | | |
|---|---|---|
| **Business Drivers** | **Reducing the operational burden and cost** | With network security as a service, maintenance and upgrades are included in the monthly cost. Upgrading multiple physical gateways is time-consuming and leaves security inconsistent and lagging; converting to an FWaaS architecture and managing the entire infrastructure from a single pane of glass saves time, resources, and training as well as reduced cost.<br>Reducing the Wide Area Network costs by retiring expensive MPLS circuits in favor of broadband internet links is a second important driver. |
| | **Cloud-centric architecture and technology** | Enterprises are looking for a zero-touch provisioning solution, which is centrally managed, easy to deploy, and scale.<br>We would expect the majority of SASE solutions to be delivered from the cloud, reducing the need for on-premise hardware and delivery times. |
| | **Ubiquitous access to corporate resources** | During the Covid-19, many enterprises allowed their workforce to work from home.<br>Many were pleasantly pandemic surprised to see that employee productivity went up. In a post-pandemic world, this new way of working will become the norm, and employees must be able to access any corporate resource securely and efficiently. When productivity goes up, business figures usually follow suit. |
| **Security and User Experience Drivers** | **Internet access optimization** | SD-WAN Dynamic link selection ensures the best path is always automatically chosen if multiple access circuits are present. |
| | **Improving security and reducing threats** | Increasing security to a level that can deal with Gen VI attacks, even with old EOL perimeter equipment. |
| | **Cloud adoption** | As enterprises rapidly move their data centers to the cloud, backhauling traffic to the hub site may not be the best option in terms of cost and/or latency for roaming users or for users in branch offices requiring access to (corporate) resources in the cloud. For instance, streaming audio or video is much more efficient in terms of WAN bandwidth consumption with a local breakout. |
| | **Zero Trust Network Access** | The same level of security should always be enforced, regardless of the location of the user. Whether they are in the office or roaming, a SASE architecture will constantly ensure complete session protection. |

# CHECK POINT SASE SOLUTION

SASE is an architectural model consisting of several products, whose goal is to allow users to access applications with the best possible user experience and the highest level of security, all depending on the user's identity.

Any user, regardless of their location, or asset should be able to access any application, either corporate or public, in a secure way. Versatility, scalability and user experience are of paramount importance.

The Check Point SASE model covers two aspects – network and security:



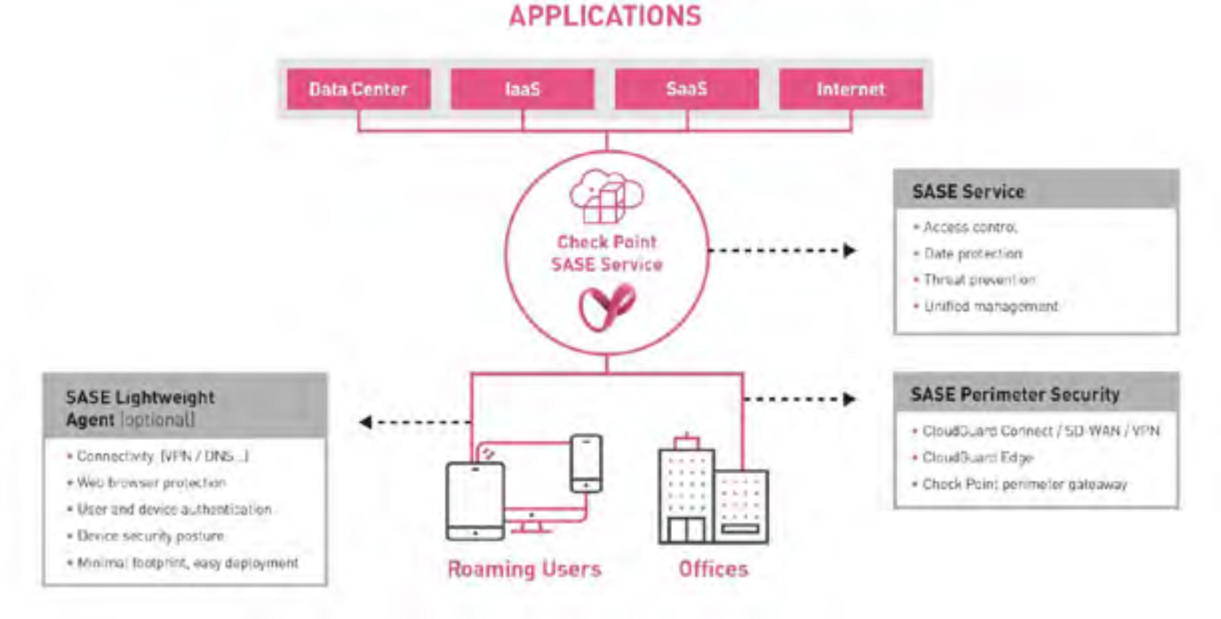
The network part serves as a transport layer for users and devices connecting to resources and applications on the corporate network and the internet.

Check Point has tight integration with most popular SD-WAN providers, establishing a best-of-breed SASE solution that provides efficient connectivity and comprehensive security capabilities.

vmware
silver peak
VERSA NETWORKS
Microsoft Azure
CISCO
CITRIX
aruba a Hewlett Packard Enterprise company
aryaka
HUAWEI
nuagenetworks

***Graphic:*** *Check Point's strategic SD-WAN partner ecosystem*

The security part is a unified solution based on Check Point CloudGuard products, the adjacency of those provides Check Point's SASE solution. All services are managed using Web UI Management, providing single pane of glass for the Administrator.



*The Check Point SASE solution*

The Check Point SASE solution places security as a service in the cloud in a distributed fashion instead of enforcing it the legacy way on gateways, on-premise Data Centers and branches. Access to corporate resources is possible directly without detours, and securely, for everyone.

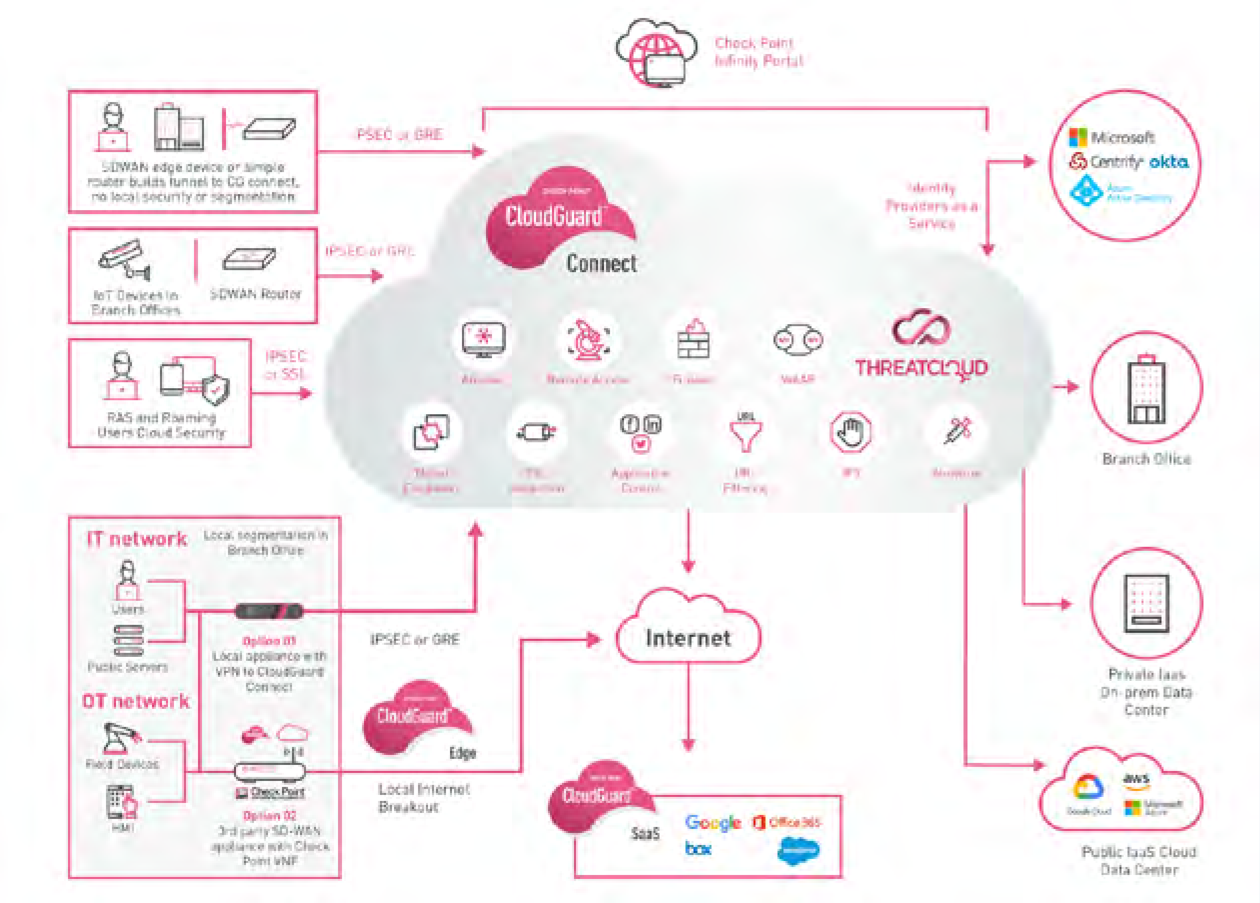
The service runs on top of the Amazon AWS and Azure infrastructure to ensure maximal availability and the best possible response times when accessing cloud resources.
This cloud-based solution does not burden IT staff with deploying or maintaining dedicated hardware and supports adding advanced threat prevention capabilities on top of existing routers or SD-WAN deployments. With a simple and easy setup process, network traffic from existing SD-WAN edge devices are tunneled to a primary cloud-based network security service at a near-by location. A second connection provides redundancy. This ensures branch offices stay connected and removes the operational overhead of deploying and maintaining security for hundreds and thousands of physical devices, reducing overall CAPEX and OPEX costs.

The SASE infrastructure is deployed in the cloud, fully managed by Check Point. The SASE functionalities in the cloud include the most sophisticated Next Generation Threat Prevention and zero-day protection mechanisms, ensuring the best possible protection against Gen V attacks, such as: Application Control and URL Filtering, Anti-Bit / Anti-Virus, IPS, Threat Emulation and Extraction along with SSL inspection capabilities and Remote Access VPN technologies.

All features of the service can be managed using a single pane of glass; either by Management as a Service (MaaS) leveraging the Infinity Web Portal or existing R80 Smart Center management system deployed on-premises.

# SASE ARCHITECTURE REFERENCE

The following graphic represents the recommended Check Point SASE architecture, with several use cases as outlined below.


Check Point Infinity Portal
SDWAN edge device or simple router builds tunnel to CG connect, no local security or segmentation
IPSEC or GRE
IoT Devices in Branch Offices
SDWAN Router
IPSEC or GRE
RAS and Roaming Users Cloud Security
IPSEC or SSL
CloudGuard Connect
Remote Access
Firewall
THREATCLOUD
Application Control
URL Filtering
IPS
Identity Providers as a Service
Microsoft
Centrify okta
Azure Active Directory
Branch Office
Private IaaS On-prem Data Center
Public IaaS Cloud Data Center
Internet
IT network
Local segmentation in Branch Office
Users
Public Servers
OT network
Field Devices
HMI
Option 01
Local appliance with VPN to CloudGuard Connect
Check Point
Option 02
3rd party SD-WAN appliance with Check Point VNF
IPSEC or GRE
CloudGuard Edge
Local Internet Breakout
CloudGuard SaaS
Google
Office 365
box

***Note:** some features and capabilities shown above, are part of Check Point short-term roadmap and will become available duiring the 2nd half of 2020, e.g.: remote access to an on-prem data center via the SASE cloud service, for users or branches; branch-to-branch communication; the use of external Identity Providers as a Service.*

## Use case: Security as a Service

- **Remote Access VPN to Data Center**
  Users can connect to the SASE cloud with a lightweight client, which connects to the SASE cloud over IPSEC or SSL. The traffic is secured and the user gets access to corporate resources either in an on-premise Data Center or in the public cloud. This is explained in more detail on page 15.
- **Clientless Access to Corporate Applications**
  Applications can be published to users directly thought the SASE cloud using only a browser. Assess is based on identity, which is typically provided by an Identity-as-a-Service provider. Applications will only be shown to users who have access to them, as they are hidden by default. This is explained in more detail on page 16.
- **Internet Web Access Security**
  When roaming users access the internet, they are secured by SASE cloud-based security controls, meaning these security controls do not need to be enforced locally. The lightweight agent routes all traffic to CloudGuard Connect in the SASE cloud where access control and threat prevention take place.

- **SandBlast browser extension**

  The browser extension secures all web traffic before it is SSL encrypted: direct visibility into the rendered browsing content allows for zero-day protection (threat emulation and extraction) and phishing protection.

  It also permits dynamical delegation of network security functions (URLF, phishing & malware prevention) to the endpoint allowing intelligent direct internet routing without compromising security.

- **SaaS Application Security**

  Roaming users connect to SaaS applications in the public cloud, like Office365. Check Point's SASE cloud solution secures *access* to applications. An key part of this access process is determining the identities (these originate from a 3rd party identity provider such as AzureAD) and risk level of users, as this information is used in the security policy that decides which applications users get access to. A second and equally important part is to provide data protection and threat prevention, both inline and out-of-band through the API integration Check Point has with SaaS providers.

## Use case: SD-WAN / Branch Office Security

- **SD-WAN device connected to Check Point SASE service**

  A branch office that is equipped with an existing SD-WAN device can connect to CloudGuard Connect using an IPSEC or GRE tunnel, set up between the on-premise SD-WAN device and the CloudGuard Connect infrastructure. All access control and threat prevention features are enforced in the SASE cloud before allowing the traffic to break out to the Internet or any (corporate) resource like SaaS applications, the on-premise Data Center or public cloud resources.
  The same setup can also be used if there is only a simple router present at the branch. As long as the on-premise device is capable of building a tunnel, the branch can be secured.

- **SD-WAN device running Check Point Virtual Machine (VNF)**

  Some of the SD-WAN vendors allow a Check Point VNF (virtual machine) to be run on routers. This allows for segmentation of the local network and inbound access to servers in a DMZ.

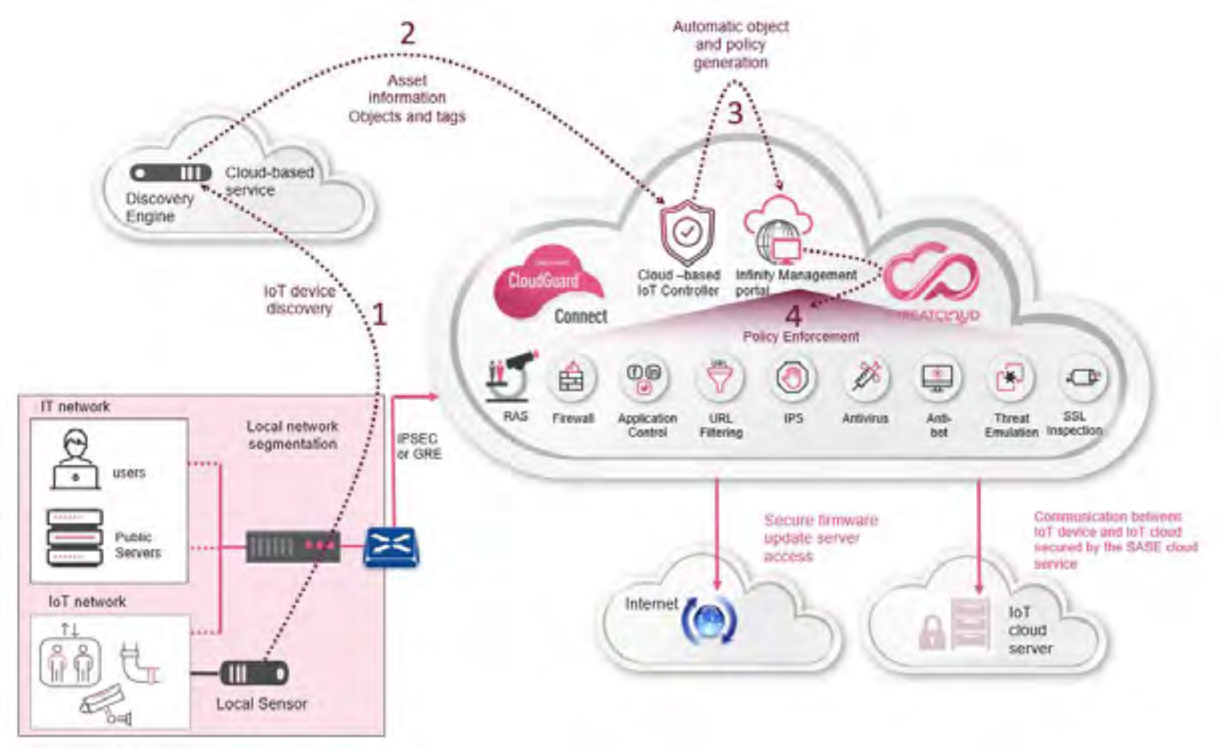
- **A Check Point gateway FW/IPS and an SD-WAN device**

  Some branch offices may have old Check Point equipment in place that is nearing its end of life, but upgrading is a time- consuming process. In these cases, advanced security features are disabled on the gateway because it is not powerful enough to run them. This leaves the branch exposed to modern-day malware. To fix this, the gateway can be kept for local segmentation purposes and the SD-WAN device can be used to build a tunnel to the SASE cloud, as in the previous example.

## Use case: IoT Security

SASE also secures machine-to-machine communication.
A branch office can have IoT devices that need to communicate with an IoT cloud service, where the data of all IoT devices is stored, for example, surveillance cameras uploading video clips to a public cloud video storage service. SASE allows the cameras to send the footage via a VPN tunnel between the branch and CloudGuard Connect to the public cloud storage, ensuring integrity, encryption, and authorization of the upload process.

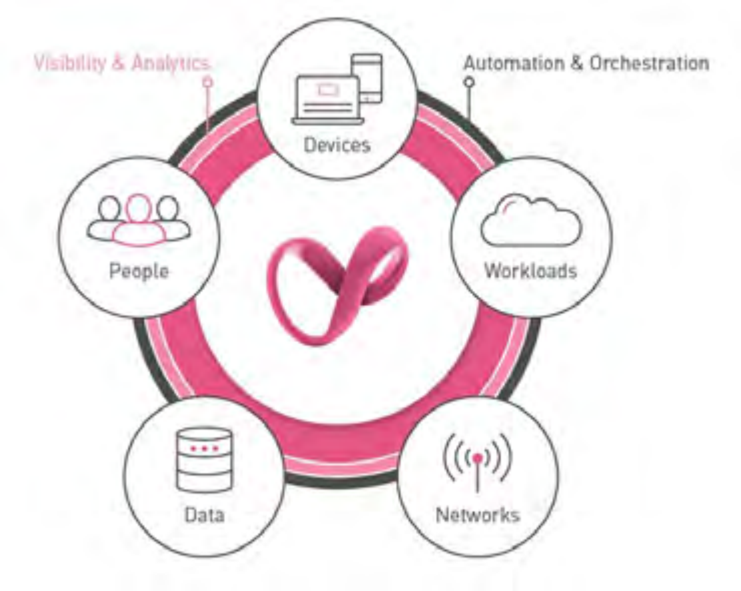
Conversely, SASE also allows for direct internet access for certain services. In the use case below: firmware updates for said IoT devices.



An additional advantage is that a local sensor in the branch office can be used to send the data it collects about IoT devices to a cloud-based 3rd party discovery engine (1), which in turn feeds this information to the Check Point cloud-based IoT controller (2). This Management-as-a-Service (MaaS) platform uses that data to automatically generate objects and policies based on the behavior and communication patterns of the IoT devices and feed them to the Infinity Management portal (3). After review by the security admin, the suggested policies can be enforced in the SASE cloud (4) or on on-premise gateways.

## Alignment with the Zero Trust Model

SASE secures the communication between resources, branches, users and devices in a way that is completely aligned with the key principles of Zero Trust Network Access. By identifying users and devices, regardless of their location, the resources they need to access are secured by user-centric policies.



- **Zero trust people:**
  Identity Awareness is an essential component of SASE. User-centric policies for CloudGuard SaaS ensure that the only the corporate applications a user is allowed access to, will be displayed. Identity awareness will also be used on both CloudGuard Connect and CloudGuard edge, for user-based access control as well as threat prevention.
- **Zero trust devices:**
  The full End Point client enables on-device security protection for all employee devices, to prevent zero-day malware, malicious app installations, phishing attacks, bot attacks, and more.
  BYOD and non-managed devices (i.e. from temps or contractors) can also be used to obtain access to web-based corporate applications in a clientless scenario.
- **Zero trust data:**
  The DLP blade can be enabled on CloudGuard Edge, and content awareness can be enabled on CloudGuard Connect. CloudGuard SaaS uses API's in the cloud to enforce DLP policies to protect corporate data in the cloud.
- **Zero trust workloads:**
  Enable access control and full threat prevention for all south-north communication between users, the branch and data center, IaaS assets, and SaaS applications. Only displaying the applications to which users are supposed to have access to, is a perfect example of both zero-trust workloads and zero-trust people.
- **Zero trust network:**
  In case inbound access is required, a local appliance or CloudGuard Edge can be used to segment the DMZ from the user's segment and apply the necessary security controls between segments. Either the local VNF, security gateway or the CloudGuard Connect instance will segment the branch from the next hop, protecting the corporate network from lateral malware movements.

# CHECK POINT SASE COMPONENTS

Check Point's SASE platform supports multiple security and network components, which are centrally managed using the Cloud Guard Connect management web application or console.

Check Point's SASE platform includes the following components:

- **Secure Web Gateway** – Check Point's cloud SWG is designed to protect your organization from known and unknown threats. It offers protection for users accessing the internet and SaaS applications in the office or remotely, and includes functionality of FWaaS.

  Security includes URL Filtering, application control, IPS, phishing and malicious download prevention using SandBlast technology to prevent zero-day attacks, and DLP.

- **Network Security as a Service –** Cloud-hosted network threat prevention service, on top of existing SD-WAN deployments. Solution delivers the latest and most comprehensive cyber security available, protecting branch offices from the latest generation of targeted and advanced cyber threats.

- **Secure Access to corporate resources –** provide safe access to remote employees to corporate resources, providing the same level of security as in the office.
  Corporate resources are protected by zero-trust access based on user-identity, endpoint security posture and session risk. Access is granted based on the Zero Trust policy as well as behavioral models for users and applications. Corporate resources are protected in the data center or in the private and public cloud.
  Corporate applications are also protected with advanced IPS and WAAP.

- **Anti-Bot and Anti-Virus** - Protects against malicious files, malware infested websites and more. Analysis uses real-time virus signatures and anomaly-based protections. Identifies and contains infections by blocking Command and Control traffic between infected hosts and a remote operator.

- **SaaS Applications Protection**

  A robust, native API based solution that provides zero-day threat protection from malicious links and attachments, anti-phishing, ID protection, and data leak prevention across cloud emails, office suites, and applications (e.g. Dropbox, Slack).

  - **Mail Security** - Check Point's Mail protection acts as the last line of defense, protecting your mailboxes from the vulnerabilities of built in Office 365 email security. Use artificial intelligence to detect malicious content heading for your email accounts and block sophisticated phishing schemes that bypass traditional email security solutions.

  - **DNS Security** – Check Point's solution prevents access to malicious domains, at the access level. DNS Security prevents DNS exploits and tunneling, over HTTP or HTTP integrated with Threat Cloud, solution provides malicious domain blocking, for newly-registered domains related to active threat campaigns, as well as prevention against zero-phishing.

  - **Browser extension -** endpoint-based browsing protection compliments network SWG functions with superior protections. Browser extension provides visibility ti encrypted traffic, and protection against zero-day phishing and malware attacks. Browser extension can be deployed independently, or as part of the SASE agent for PC.

  It is meant for those enterprises that need on-premises security for data privacy or data location requirements and can also be used to segment the local network.

## CloudGuard Connect / Edge

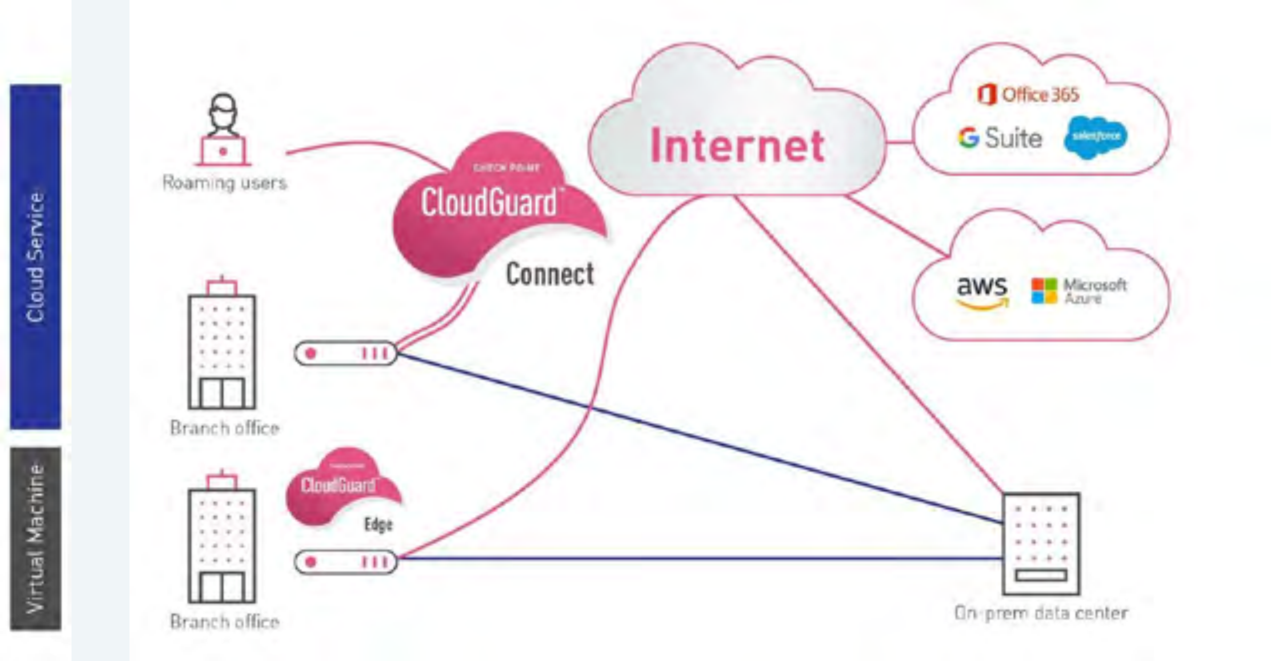
This chapter helps the reader choose between Check Point's **CloudGuard Connect** and **CloudGuard Edge** technologies and explains their ZTNA features.

Consider some of the following factors:

- The importance of owning a platform vs. using it as a service
- The necessity of inbound access to public servers in the branch
- The ability to use cloud services for security vs. having a strict policy restricted to on-premise solutions only

CloudGuard Connect is a native cloud service that requires no dedicated security hardware on-premise. It can also be used as an FWaaS solution for roaming users and also allow them to access resources in an on-prem Data center.

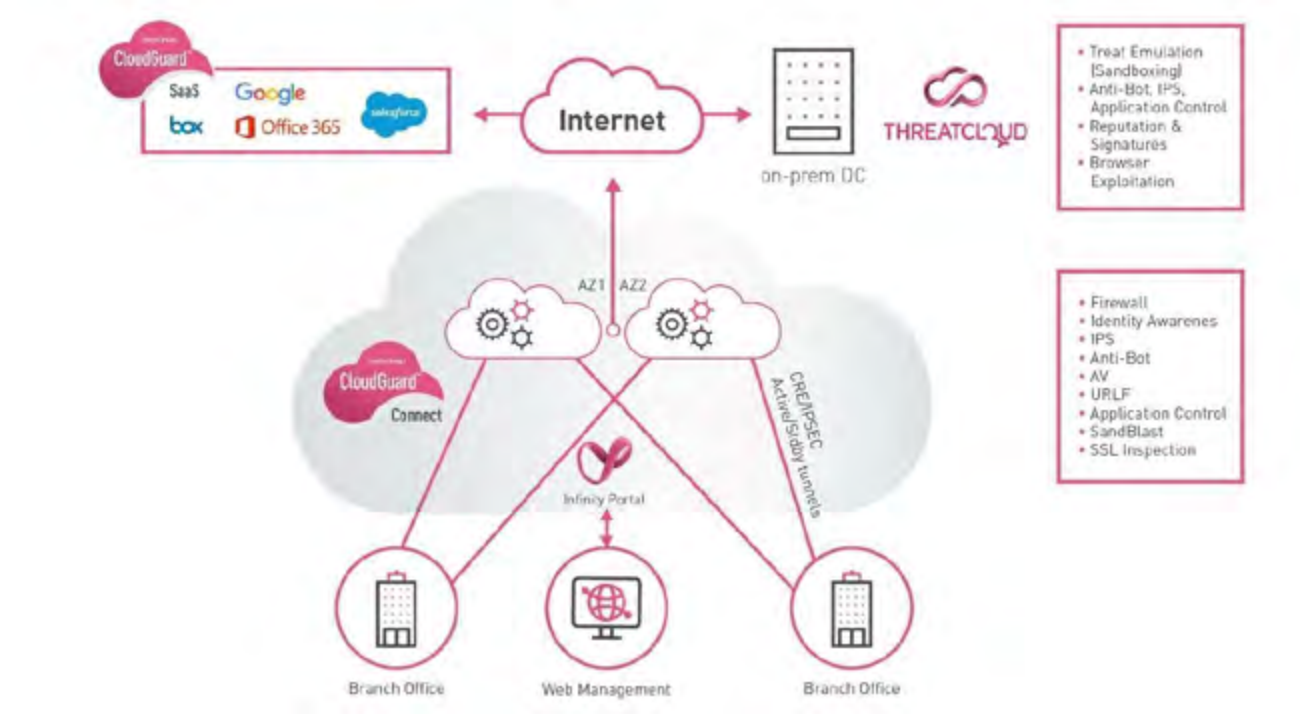
CloudGuard Edge is a Check Point VNF running on 3rd party SD-WAN hardware. Both solutions allow branch offices to break out to the internet without the need to backhaul the traffic back over the WAN to the hub site where the internet egress point would traditionally reside.



### When to Consider CloudGuard Connect

1. In cases where old security Customer Premise Equipment (CPE) in the branch cannot immediately be replaced with modern hardware, for any reason. There is a need for a local internet breakout in the branch, but the CPE is not powerful enough to enforce all required security controls typically enabled at the perimeter.
2. As long as the CPE is capable of building an IPsec or GRE tunnel to a Check Point CloudGuard Connect instance, all security controls can be enforced in the cloud instead of on the CPE, and the branch office obtains a secure local internet breakout.
3. The choice has been made for a specific 3rd party SD-WAN vendor and their products are not designed to run a Check Point VNF image on them. As in the previous case, the SD-WAN device only needs to build a tunnel to the CloudGuard connect instance and route all the traffic over the tunnel to obtain a secure local internet breakout.

4. CloudGuard Connect can also be used to provide roaming users with secure internet access without having to deploy a fat agent on their machines; a lightweight client will provide secure access to all resources, or even clientless for non-managed devices.



The CloudGuard Connect security as a service solution offers the following advantages:

- Auto scaling
- No operational hassle: no need to worry about upgrades and provisioning of hardware
- Cost reduction: the WAN costs will decrease as traditional expensive MPLS circuits are replaced by VPN over cheap broadband connections
- Better user experience for internet-bound traffic (i.e. SaaS) by eliminating additional latency caused by backhauling via the hub site

### Specifications:

Check Point's CloudGuard Connect is a cloud-hosted network threat prevention service offering a maintenance-free, comprehensive, affordable security solution for branch offices and roaming users. CloudGuard Connect seamlessly delivers the latest and most comprehensive cybersecurity available, protecting branch offices from the latest generation of targeted and advanced cyber threats.

CloudGuard Connect doesn't burden IT staff with deploying or maintaining dedicated hardware and supports adding advanced threat prevention capabilities on top of existing routers or SD-WAN deployments. With a simple and easy setup process, network traffic from existing SD-WAN edge devices is tunneled to a primary cloud-based network security service at a nearby location. A second connection provides redundancy, ensuring branch offices stay connected and removing the operational overhead of deploying and maintaining security for hundreds and thousands of physical devices, reducing overall CAPEX and OPEX costs.

| Cloud Services | |
|---|---|
| Branch-to-Site connection | IPsec IKEv1, IPsec IKEv2 or GRE tunnels |
| Availability regions | US South-East, US North-East, US South-West, US North-West, Canada, Germany, France, Sweden, Ireland, United Kingdom, Hong Kong, South Korea, Singapore, Japan, Australia, India, Brazil, Bahrain |

| Software | |
|---|---|
| Latency | Up to 50 milliseconds1 |

| Performance | |
|---|---|
| Single IPsec tunnel | Up to 870 Mbps per tunnel |

(1) The expected additional latency for a branch in the same CloudGuard Connect region

### When to Consider CloudGuard Edge

1. Local segmentation is a requirement: An example could be a manufacturing facility where the IT network needs to be segmented from the OT network
2. Inbound access to public servers is required at the branch office
3. There is a need for specific telco features on the SD-WAN hardware that are unavailable on Check Point solutions

The CloudGuard Edge product offers the following advantages:

- Hosting local public servers in the branch in a secure way
- Dynamic path selection: The SD-WAN appliance will choose the best circuit for any given session

### Specifications:

CloudGuard Edge is a lightweight virtual image of the Check Point Branch Office Security Gateway. Within a minute of powering on the virtual security gateway, your branch office is protected.

CloudGuard Edge security gateways are deployed through the SD-WAN management console. This tight integration reduces deployment time, effort, and costs. When CloudGuard Edge is deployed on SD-WAN or uCPE equipment, the CloudGuard Edge virtual security gateway is configured, automatically connected, and ready to be centrally managed and monitored by the customer’s domain in cloud-hosted SMP or the headquarters’ R80 Security Management.

| Software | |
|---|---|
| Security | • Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot,<br>• Antivirus and SandBlast Threat Emulation (sandboxing) |

| Performance | | | | | |
|---|---|---|---|---|---|
| VMware SD-WAN | Edge 520v | Edge 620 | Edge 640 | Edge 680 | Edge 840 |
| Threat Prevention | 100 Mbps | 100 Mbps | 350 Mbps | 500 Mbps | 550 Mbps |

**Note:** The VMware SD-WAN Edge image configuration is set to 2 cores

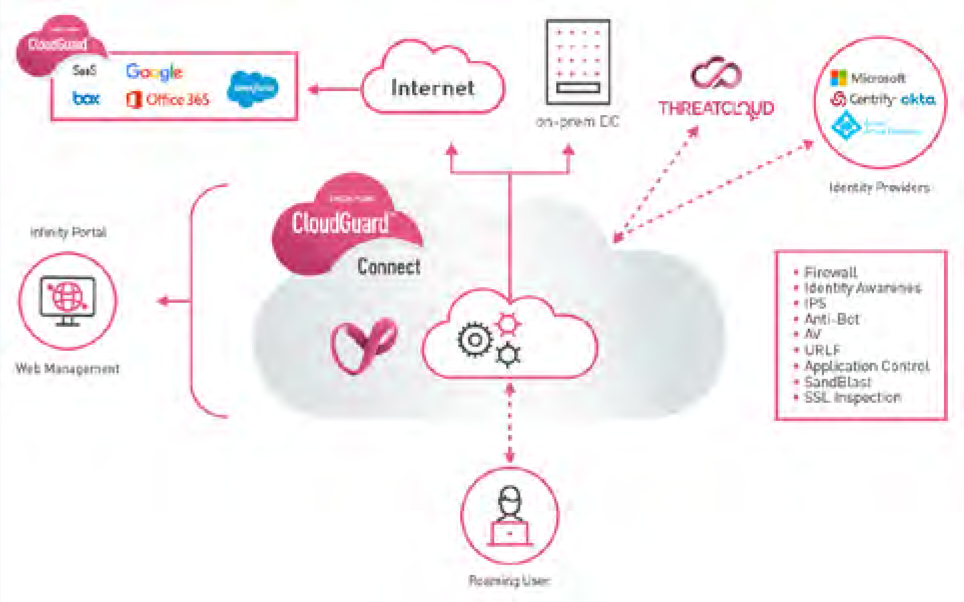
| Branch Edge Device | |
|---|---|
| VMware SD-WAN | Edge 520v, 620, 640, 680, 840 |
| Cisco Enterprise VNF | ENCS 5104, ENCS 5412 |

## Remote Access for Corporate Applications

Remote access to corporate applications is a primary need for all remote users. It has traditionally been done using VPN to data center/office perimeter GW from the client side. This solution may load the perimeter GW, will require an end point agent, and may give too wide permission to the users on the internal network, and all its resources.

The solution is to design the access based on the principles of Zero Trust Network Access, which is part of the overall SASE solution.

Zero Trust is a set of principles, that are implemented as part of an SDP (Software Defined Perimeter) application. SDP application, as part of the SASE solution, will provide corporate web applications access as a service. In other words, it will manage the access to corporate applications (in data centers), for all users, in a granular and flexible way.



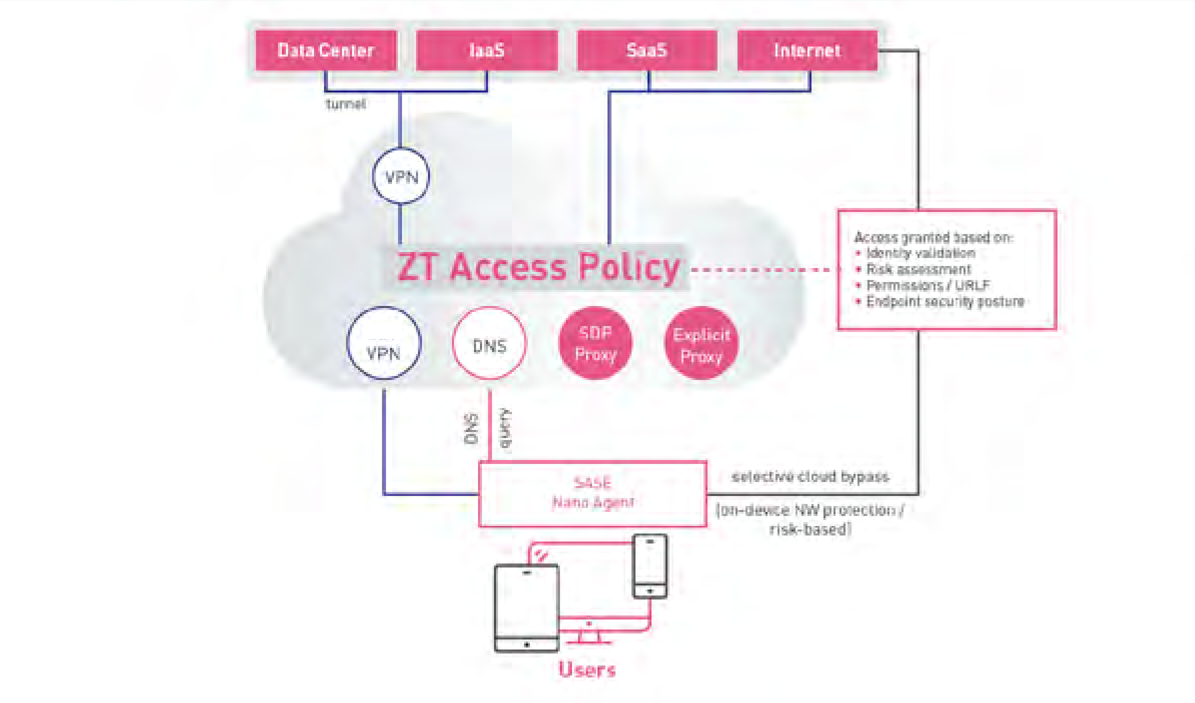
SASE ZTNA application will support the following features:

- Zero Trust access – minimum privileges to all users s default. Hiding all unauthorized applications and services from all users.
- Inspection and authentication in the application level (IP agnostic)
- Continuous authentication and authorization per user per application
- BYOD friendly - clientless access to corporate applications
- Secure the access using advanced threat prevention mechanisms and data protection engines

Corporate Access can be deployed in a clientless mode, or with a light agent.

## Lightweight Client

The lightweight agent routes all traffic to the closest CloudGuard Connect instance where all necessary security controls are enforced before the user is allowed to access any corporate resource or the internet, as with branch offices.



This means the endpoint, as well as the data and application, is protected but requires an agent to be installed. It ensures the same level of security for the users, regardless of their location. At the same time, the client also allows for a bypass path for specific types of traffic to break out to the internet directly, such as streaming services, thus avoiding a detour via the SASE cloud.

The lightweight Agent also adds an additional layer of DNS security to the ZTNA functionality.

**DNS security reroutes corporate DNS queries to Check Point, allowing the following:**

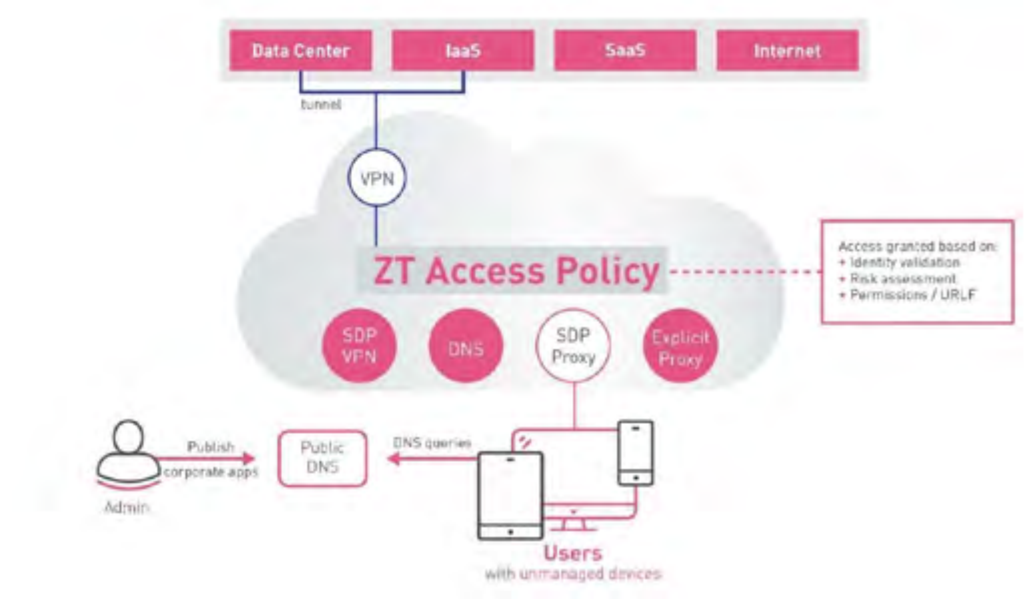
- Malicious domain prevention using Check Point's ThreatCloud
- DNS exploit prevention
- DNS tunneling prevention
- Prevention of infected hosts from communicating back to their command & control servers
- Check Point’s ThreatCloud proactively discovers and prevents access to newly-registered domains related to active threat campaigns and exploit kits
- Access control policy for domains using your own definitions as well as with 115 predefined categories by Check Point
- Zero phishing by defining domains of interest to prevent access to lookalike domains

## Clientless

In the clientless scenario, the emphasis lies mainly on protecting the resource and data users are trying to access, rather than protecting the endpoint. This product is designed to allow contractors, temps, or employees with a non-managed asset (BYOD) access to corporate resources. In this case, it is assumed the endpoint already has the required security controls in place and a posture check can be carried out to make sure the device is compliant before being allowed access to any corporate resource.

In clientless environments, users won't typically get the same level of trust an agent-based connection would get. This is why applications get published via a web portal, over RDP, VNC or SSH. Full layer-3 access is not desirable and these users would only manipulate data remotely and would not download it to their device.

The user browses to https://application.xyz.company.checkpoint.cloud where the admin publishes any corporate application, as depicted below:



It is also possible to use the SandBlast browser extension, preventing the download of malicious files, without the need for an agent to be installed. The functionality of the browser extension includes

- **Threat Emulation:**
  Detect malicious behavior by running files within a secure virtual environment.
- **Threat Extraction:**
  Obtain immediate and safe access to documents by removing potentially malicious elements or converting the downloaded file to PDF. Users can download the original file once Threat Emulation completes.
- **Phishing protection:**
  Zero Phishing is an innovative Anti-Phishing product, protecting corporate users and administrators from Zero-day phishing sites and Password / identity theft

## Data Loss Prevention (DLP)

When data is in motion, APIs allow inspection and potential leakage of data for corporate applications using the CloudGuard WAAP product and for SaaS applications, CloudGuard SaaS.

However, when corporate data residing on the endpoint itself is at rest, it needs protection as well.

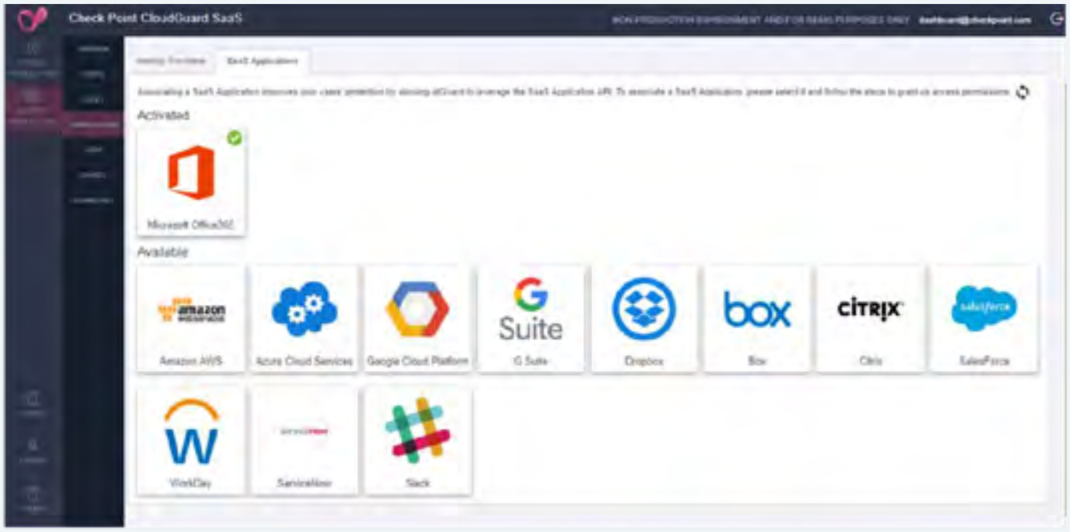
This is why a full endpoint agent on the roaming users' machines still makes sense as certain features cannot be enforced in the cloud (i.e. Full Disk Encryption). The same challenge arises when the machine is not connected to the internet. It can still be vulnerable in that scenario: removable media could potentially contain malware and harm the machine even offline. Having a full endpoint solution on the machine ensures it is always protected, regardless. In the future, the lightweight agent to connect to CloudGuard connect will become part of Check Point's full End Point Suite.

## CloudGuard SaaS security

The ability to access SaaS applications *directly* in a secure fashion combined with a satisfying user experience (without the additional latency caused by backhauling traffic through a Data Center) is a core business driver for adopting the SASE model.

### CloudGuard SaaS Apps

A brief overview of some of the applications that can be accessed safely are listed below (the list is not exhaustive):

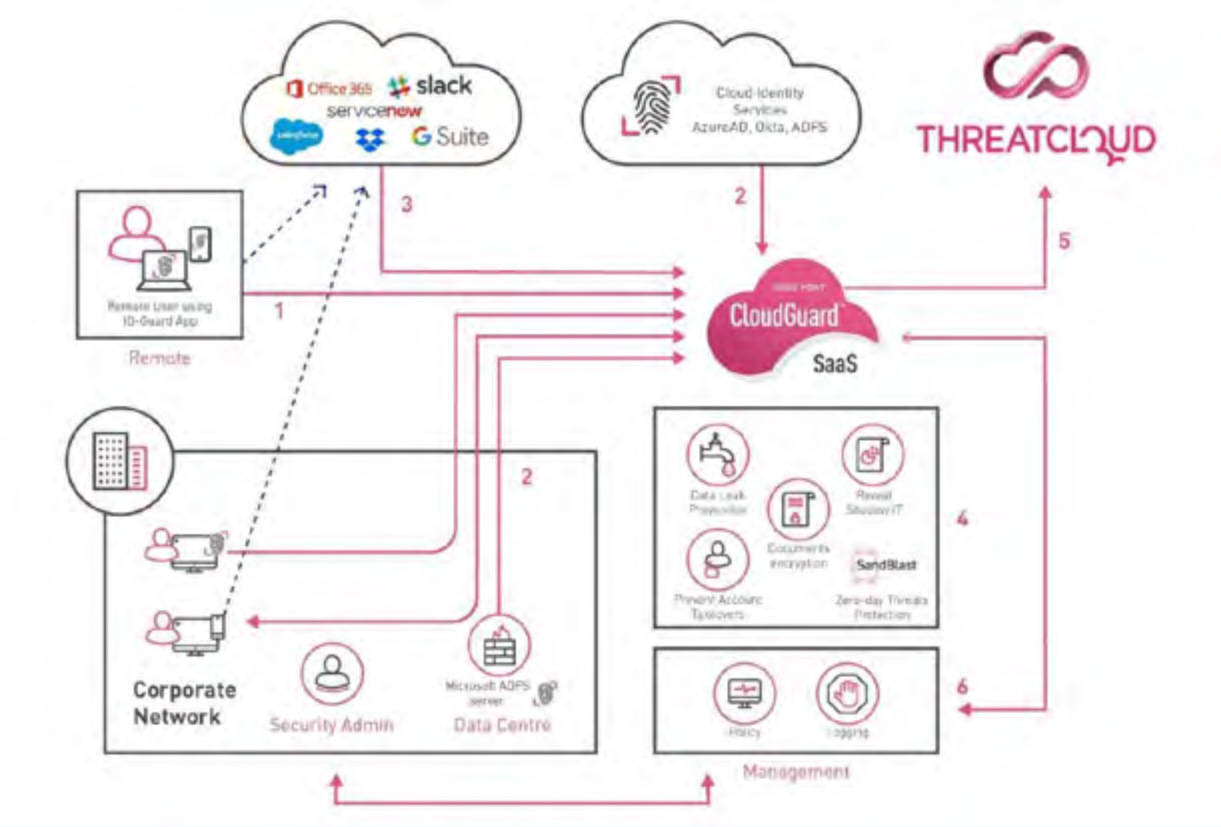


### CloudGuard SaaS Architecture

CloudGuard SaaS is a cloud-only, API-driven, Threat Prevention and Identity Protection platform leveraging several components to perform SaaS application security. This section breaks down the architecture to ensure the correct configuration is achieved.

The security services offered by Check Point SaaS can be split into two categories: Threat Prevention and Identity Protection. Upon configuration, all these services are available from the Check Point Portal.

The following graphic outlines the key components and their relationships:



*This graphic shows how the CloudGuard SaaS integrates with the cloud and device ID services*

- **Agent** or **Agentless** connections options:

  Agent-mode is a lightweight agent installed on all Windows machines allowing user-identity and connection-context to be shared with the CloudGuard SaaS platform. The CloudGuard SaaS is called ID-Guard and is mandatory if identity protection is required.

  Agentless-mode are one-time passwords sent to either the Check Point Sandblast mobile application, or by SMS, used to identify users. Agentless-mode also makes use of the connection context, such as source IP, time of connection, etc. to relay information to the platform.

- **Identity Providers**

  CloudGuard SaaS integrates with ADFS using a Check Point agent installed on the ADFS server. CloudGuard SaaS can also use cloud-based identity providers such as AzureAD.

- **Service Provider**

  CloudGuard SaaS essentially acts as the mediator between the Identity Provider and Service Provider. It is a service required by users.

- **CloudGuard Security Services**

  These Check Point services are available to the administrator once the SaaS application has authorized CloudGuard SaaS access.

- **Check Point Security Services Including Threat Cloud**

  CloudGuard SaaS is deployed into Check Point data centers (currently in the EMEA and USA), offering the same security services as CloudGuard Connect.

- **CloudGuard SaaS Portal**
  All admin is done using a web portal, including setting up the policy, logging, etc., and downloading the required agents.

### Putting identity at the core of SaaS application security

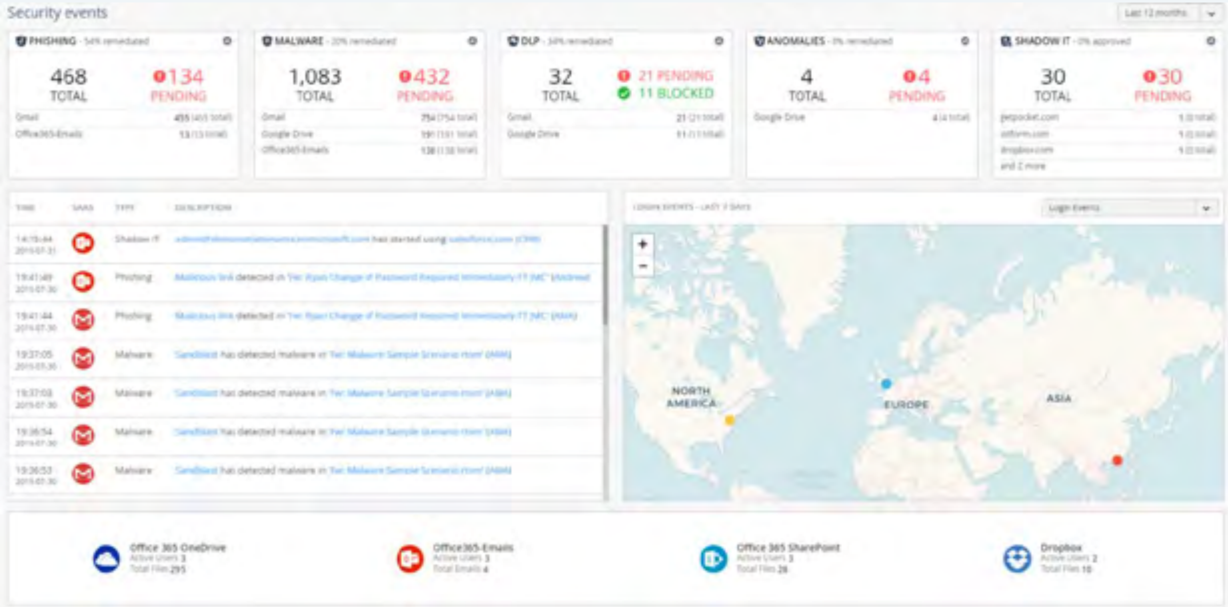
A key component of a modern security approach is the incorporation of user-identity into the security policy, security platform, and security posture. Label-based or identity-based security is more effective where mobility and agility are business requirements. Check Point has developed a unique Identity Protection engine, which integrates with any Identity Provider and SaaS Provider that supports the SAML 2.0 protocol.

# MANAGEMENT AND REPORTING

## CloudGuard SaaS Management

The management interface of the platform allows administrators to build the required security policy, download the various CloudGuard SaaS agents, and configure identity protection policies. Once configured, the SaaS portal can display logs and heat-maps to help identify the use of shadow IT. Currently, the management interface is cloud-only. In the future, the SaaS management interface will be merged with the CloudGuard Connect and Edge Management interface.

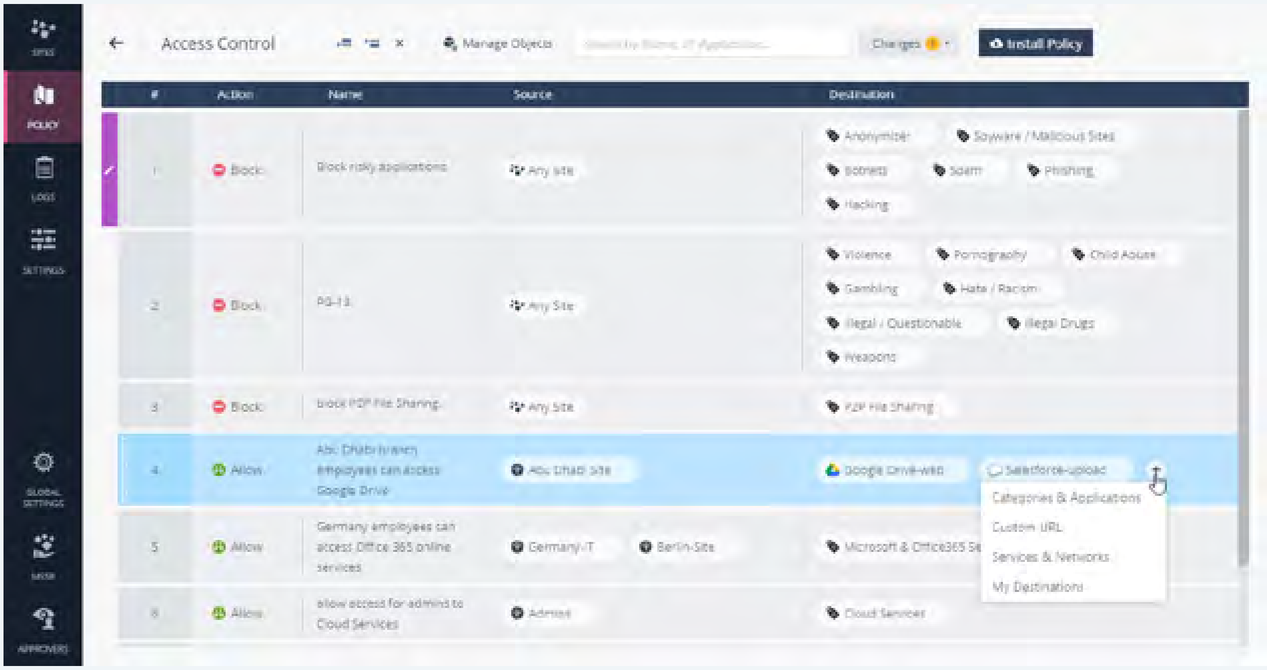
The screenshot below shows the Cloud Guard SaaS management portal. Please refer to the user manual for more details.



## CloudGuard Connect / Edge Management

CloudGuard Connect is managed via the Infinity Portal and with an R80.20 or the SmartCenter above.

The following is a screenshot of the Infinity Portal:

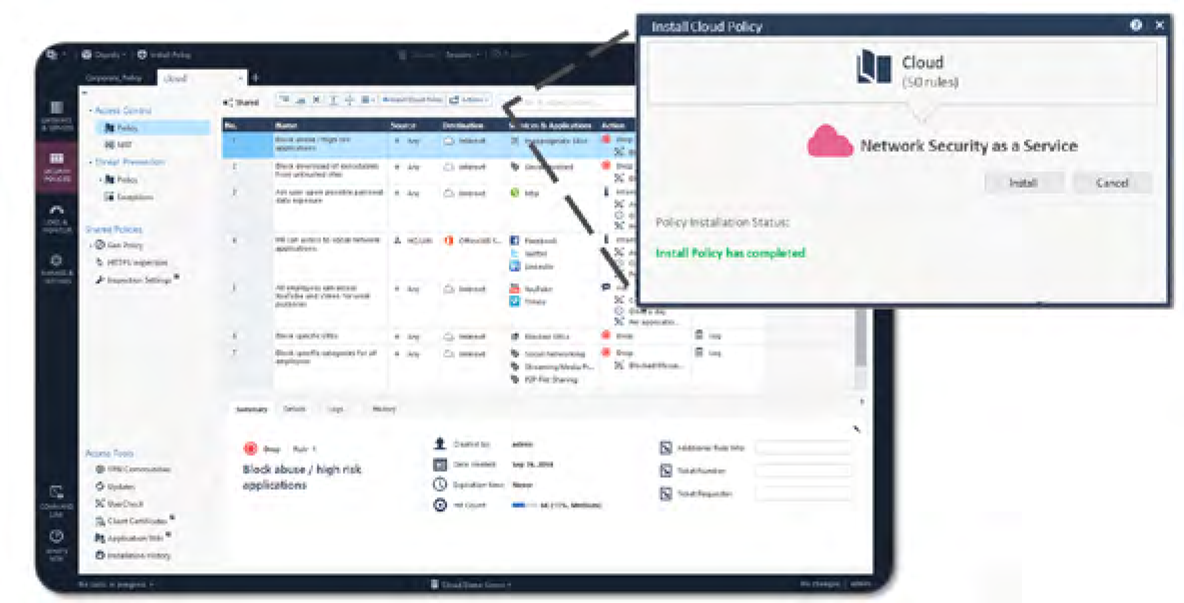


| # | Action | Name | Source | Destination |
|---|---|---|---|---|
| 1 | Block | Block risky applications | Any site | Anonymizer<br>Spyware / Malicious Sites<br>Botnets<br>Spam<br>Phishing<br>Hacking |
| 2 | Block | PG-13 | Any Site | Violence<br>Pornography<br>Child Abuse<br>Gambling<br>Hate / Racism<br>Illegal / Questionable<br>Illegal Drugs<br>Weapons |
| 3 | Block | block P2P File Sharing | Any Site | P2P File Sharing |
| 4 | Allow | Abu Dhabi branch employees can access Google Drive | Abu Dhabi Site | Google Drive-web<br>Salesforce-upload |
| 5 | Allow | Germany employees can access Office 365 online services | Germany-IT<br>Berlin-Site | Microsoft & Office365 Se |
| 6 | Allow | allow access for admins to Cloud Services | Admins | Cloud Services |

**Benefits for managing Internet policy within the Infinity Portal:**

- The destination column consolidates applications, custom IPs and custom URLs
- A single, unified policy for all branch offices ensures central management
- The first three predefined security policy rules in the security portal are out-of-the-box-defaults which secure branch offices with zero customization.

Another option is to manage the SD-WAN policy using an >R80.20 management station. This method is supported by both CloudGuard Edge and CloudGuard Connect.



Install Cloud Policy

Cloud
(50 rules)

Network Security as a Service

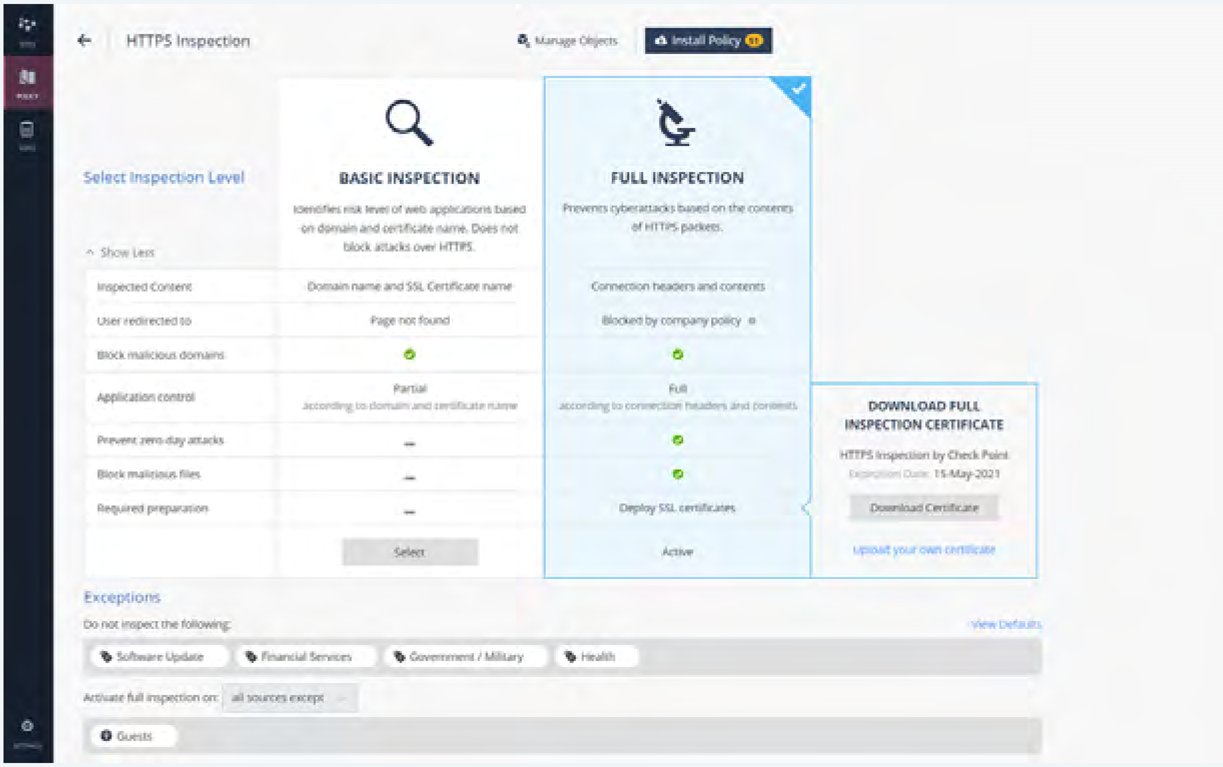
Install Cancel

Policy Installation Status:

Install Policy has completed

As CloudGuard Edge VNF is a gateway SMB image, it can be managed by the local web, SMP cloud web management, or by SmartConsole of any version that supports Check Point's Large-Scale Management (LSM), which is essentially any version except for R80.10.

Full HTTPS inspection is also supported:



HTTPS Inspection

Manage Objects | Install Policy

Select Inspection Level

| Show Less | BASIC INSPECTION<br>Identifies risk level of web applications based on domain and certificate name. Does not block attacks over HTTPS. | FULL INSPECTION<br>Prevents cyberattacks based on the contents of HTTPS packets. |
|---|---|---|
| Inspected Content | Domain name and SSL Certificate name | Connection headers and contents |
| User redirected to | Page not found | Blocked by company policy |
| Block malicious domains | ✓ | ✓ |
| Application control | Partial<br>according to domain and certificate name | Full<br>according to connection headers and contents |
| Prevent zero-day attacks | – | ✓ |
| Block malicious files | – | ✓ |
| Required preparation | – | Deploy SSL certificates |
| | Select | Active |

DOWNLOAD FULL INSPECTION CERTIFICATE

HTTPS Inspection by Check Point
Expiration Date: 15-May-2021

Download Certificate

Upload your own certificate

Exceptions

Do not inspect the following: View Defaults

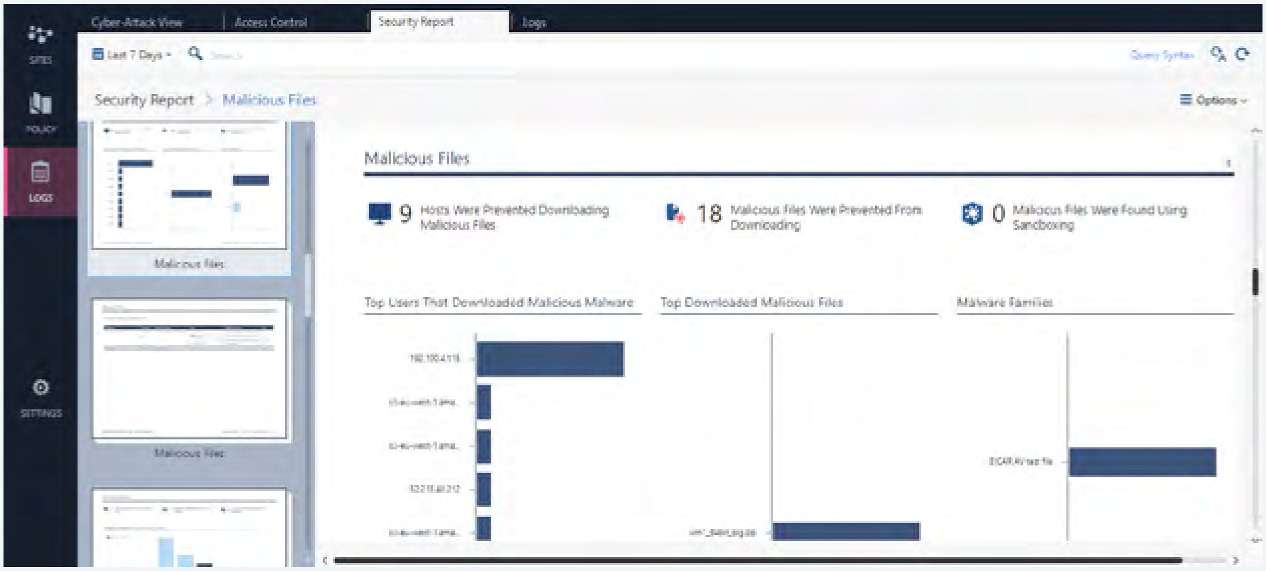
Software Update | Financial Services | Government / Military | Health

Activate full inspection on: all sources except

Guests

As can be seen at the bottom of the screenshot, HTTPS inspection can be bypassed for traffic originating from specific sources at the branch office.

Examples of a weekly threat report and logs:



Security Report > Malicious Files

Malicious Files

9 Hosts Were Prevented Downloading Malicious Files

18 Malicious Files Were Prevented From Downloading

0 Malicious Files Were Found Using Sandboxing

## CONCLUSION

SASE allows organizations to easily migrate from expensive on-premise, bare-metal-based networks to an OPEX-based and cloud-centric security architecture that is far more agile, cost-effective, and secure.

Check Point believes that SASE technology will gradually become more widely used and accepted and that eventually, most on-premise appliance-based security controls will be replaced with cloud-based alternatives.

SASE helps support SD-WAN technology, secure access to SaaS applications, and protect roaming users - while meeting the specific needs of each business and their unique infrastructure. All products discussed in this paper are part of the Check Point Infinity architecture and can be managed from a single pane of glass; the Infinity portal.

WHITE PAPER

# Fortinet Delivers the Most Flexible SASE Solution

FORTINET

## Executive Summary

Digital innovation, cloud adoption, and the recent widespread shift to remote work have fundamentally transformed the network. And with the increased reliance on cloud-based resources, such as Software-as-a-Service (SaaS) applications and data moving from the data center to multi-cloud environments, the need for a new approach to secure network access—especially the challenges of implicit trust inherent in legacy network architectures—has become clear.

Today's organizations require immediate, uninterrupted access to network and cloud-based resources and data, including business-critical applications, from any location, on any device, at any time. The challenge is that many of the issues resulting from digital innovation efforts, such as dynamically changing network configurations and the rapid expansion of the attack surface, mean that many traditional security solutions no longer provide the level of security and access control that organizations and users require.

> "Customer demands for simplicity, scalability, flexibility, low latency and pervasive security force convergence of the WAN edge and network security markets."[1]

Secure access service edge (SASE) is an emerging enterprise strategy that combines network security functions with WAN capabilities. SASE's goal is to support the dynamic, secure access needs of today's organizations—right in line with the security-driven networking strategy that Fortinet has been actively developing and promoting for years. SASE plays a critical role in ensuring that security can be delivered anywhere, including at the WAN edge, cloud edge, data-center (DC) edge, core edge, and endpoint devices used by today's heavily mobile remote workforce.

## Start by Accurately Defining SASE

As with any emerging technology category, there is still some uncertainty about a precise definition of a SASE solution. Is it strictly a cloud-based offering? Or does it include physical solutions as well? And what technologies are involved in a SASE solution?

While SASE is generally classified as a cloud-delivered service, there are common circumstances that may require a combination of physical and cloud-based solutions for SASE to be effectively integrated into the network. This may include combining SASE connectivity with network access controls and edge security devices for remote workers, supporting a physical software-defined wide-area networking (SD-WAN) device—especially one that contains a full stack of security—or even needing to integrate with technologies such as wireless local-area network (LAN) controllers or Wi-Fi access points at branch offices.

So, in addition to its essential cloud-based protections, a robust SASE solution also needs to support such things as network segmentation and compliance requirements that cloud-based security can't address without shuttling traffic out to the cloud for inspection. Because of this, Fortinet provides the most comprehensive and flexible solutions for SASE deployment, spanning both cloud and physical device integrations and deployments.

## SASE Is All About Secure Access

Conceptually, SASE is an attempt to address the security challenges created by SD-WAN vendors who may have delivered an innovative networking solution but failed to provide comprehensive and integrated security as part of their offering. Fortinet addressed this challenge head-on with a fully integrated Secure SD-WAN solution that provides a robust suite of both integrated networking and security features and functions that no other vendor has been able to achieve. These are all part of the security-driven networking and Security Fabric platform strategy we have been providing to customers for years.

Fortinet supports a fully integrated SASE solution with the broadest range of physical and cloud-based security solutions on the market. It starts with these essential security elements:

- **A fully functional SD-WAN solution.** As the heart of the SASE solution, SD-WAN needs to include such things as dynamic path selection, self-healing wide-area networking (WAN) capabilities, and consistent application and user experience for business applications.

- **A next-generation firewall (NGFW) (physical) or Firewall-as-a-Service (FWaaS) (cloud-based) firewall.** SASE also needs to include a full stack of security that spans both physical and cloud-based scenarios. For example, organizations with a remote worker strategy will require a combination of edge security and internal segmentation to prevent guest or Internet-of-Things (IoT) threats from crossing over to restricted corporate network resources, combined with cloud-based security for accessing resources located online or in the cloud. Physical, processor-enhanced hardware and scalable cloud-native security can deliver the same high performance at scale, enabling maximum flexibility and security for the organization.
- **Zero-Trust Network Access (ZTNA)** is used to identify users and devices and authenticate them to applications. Because ZTNA is more of a strategy than a product, it includes several technologies working together. Multi-factor authentication (MFA) identifies all users. On the physical side, ZTNA includes secure network access control (NAC), access policy enforcement, and integration with dynamic network segmentation to limit access to networked resources. And on the cloud side, ZTNA supports things like microsegmentation with traffic inspection for secure east-west communications between users, and always-on security for devices both on- and off-network. By combining physical and cloud-based ZTNA services, organizations can ensure secure access and the enforcement of policy, whether devices and users are on- or off-premises.
- **A Secure Web Gateway** is used to protect users and devices from online security threats by enforcing internet security and compliance policies and filtering out malicious internet traffic. It can also enforce acceptable use policies for web access, ensure compliance with regulations, and prevent data leakage.
- **A CASB** cloud-based service enables organizations to take control of their SaaS applications, including securing application access and eliminating Shadow IT challenges. This needs to be combined with on-premises DLP to ensure comprehensive data loss prevention.

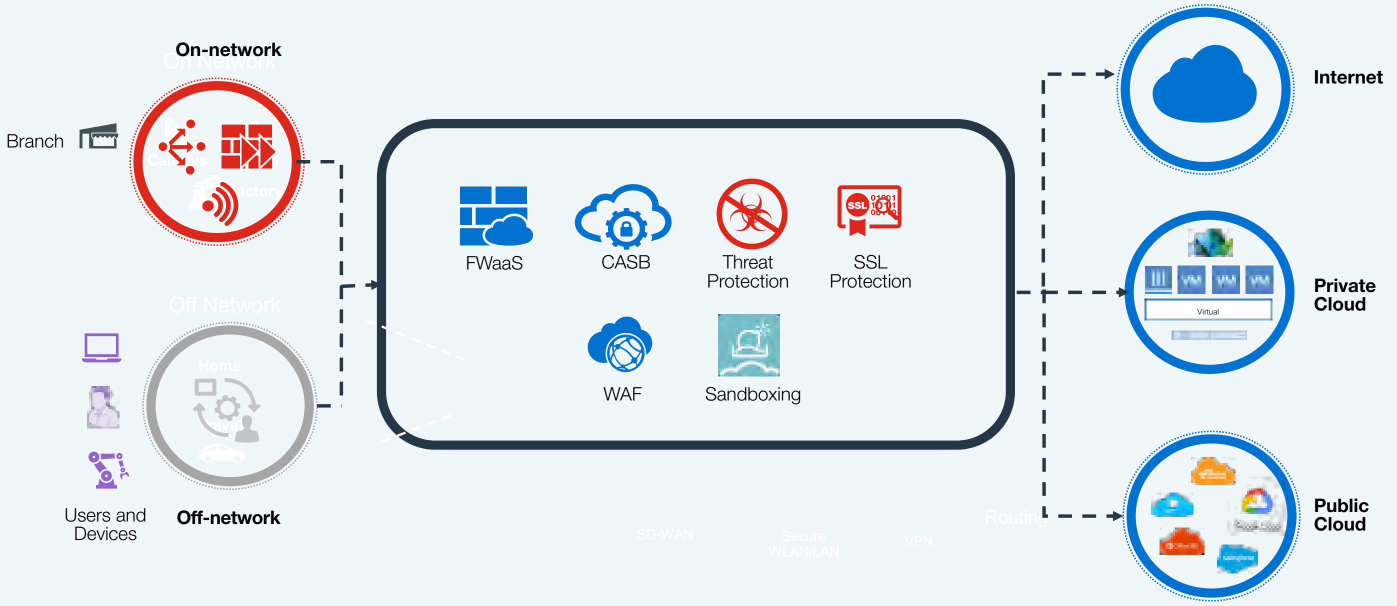


Figure 1: SASE diagram.

## Enhancing SASE with Additional Technologies

SASE is designed to enhance and support digital innovation, but without looking at a SASE approach holistically, organizations may also end up creating yet another isolated security solution that needs to be managed separately from the rest of the security architecture. This can severely limit both visibility and control across the network. So, in addition to providing the core elements any robust SASE solution requires, Fortinet also offers optional tools designed to extend and enhance the security of the users and devices utilizing the SASE solution. And they also ensure that the entire solution can be seamlessly integrated into the larger Security Fabric.

For example, endpoint security, such as endpoint protection (EPP) and endpoint detection and response (EDR) technologies, ensures that devices leveraging SASE are themselves secure. An advanced virtual private network (VPN) provides secure data transmission and transactions while managing the complexities that can quickly arise when hundreds or thousands of remote offices and users need to interconnect. And the addition of secure Wi-Fi and LAN controllers ensures that traffic leaving or entering the network receives an additional layer of inspection.

Every organization's needs are different, but it's illogical for organizations only to embrace those technologies considered "core" to SASE when a more comprehensive network and security solution provides a richer set of business outcomes.

## Lots of Potential and Too Few Qualified Vendors

While SASE is designed to address the access control and secure WAN challenges today's organizations face, the problem is that very few vendors are qualified to provide a complete SASE solution. For example, few if any of their tools—especially the security components—have been tested or certified. This means that consumers have no real way of knowing whether the security services they are purchasing will protect them in a real-world environment.

This is already a serious concern even within the highly specialized cybersecurity space, where vendors sometimes opt out of third-party testing and validation when their solutions cannot perform up to industry expectations. This problem is amplified when vendors provide SASE solutions with minimal or narrow security experience, but rush to take advantage of "SASE" as a buzzed-about marketing term.

## The Fortinet Advantage

At Fortinet, we are often asked, "What is your SASE strategy?" For SASE to work well, all of its components need to interoperate as a single integrated system—connectivity, networking, and security elements alike. Part of the reason that sounds so familiar to us at Fortinet is that we have been delivering the core SASE requirements—plus much more—for years as part of our integrated Security Platform and Security Fabric architecture. This creates true convergence of networking and security functions as part of a security-driven networking approach that further enables the rapid acceleration of digital innovation—without ever compromising protection. A number of our customers looking to implement SASE have found that, with minor adjustments, they already had a SASE solution in place thanks to the power of the Security Fabric.

SASE endeavors to solve a real problem. But it's the same sort of problem Fortinet has addressed before.

- We were the first major security vendor to fully integrate security into SD-WAN because we were able to combine years of security and networking experience into a single, unified solution.
- We then went a step further by developing the world's first SD-WAN processor designed to accelerate networking and security functionalities to provide the level of performance today's most demanding network environments require.
- We are proud that Fortinet security tools are the most tested, validated, and certified solutions in the industry today.

What this means is that delivering the kind of SASE solution your organization needs is already part of our approach to networking and security. And we can customize that solution with a range of advanced connectivity and security technologies, ensuring that your SASE solution is designed to adapt as your requirements evolve. The Fortinet Security Fabric can also integrate and connect with other solutions you deploy, whether on-premises or in the cloud. And all of these elements are covered by our single-pane-of-glass management system to ensure broad visibility and granular control across your entire network, including your SASE environment.

Fortinet is uniquely positioned to offer a complete SASE solution that ensures security is delivered consistently anywhere across the network—not just at the WAN and cloud edges, but at the DC edge, core network edge, and endpoint edge as well, to enable seamless connectivity, visibility, and control.

We're excited by the recent market momentum around SASE because it further validates our Security Fabric approach and underscores what we've been saying for years. In the era of cloud connectivity and digital innovation, networking and security must converge. There's no going back to outmoded and siloed architectures. Fortinet is engineered for the SASE era and so much more.

[1] Frank Marsala, "The Future of Network Security Is in the Cloud," Gartner, September 13, 2019.

FURTINET

www.fortinet.com

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

August 10, 2020 1:05 PM
Macintosh HD:Users:bhoulihan:Downloads:wp-FA-fortinet-delivers-the-most-flexible-sase-solution-7312020:wp-FA-fortinet-delivers-the-most-flexible-sase-solution-7312020

Palo Alto Networks Special Edition

# Secure Access Service Edge (SASE)

for dummies®
A Wiley Brand

Reduce networking and security complexity

Stop cyberattacks with consistent security

Increase business speed and agility

Brought to you by

paloalto® NETWORKS

## About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit **www.paloaltonetworks.com.**

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Secure Access Service Edge (SASE)

Palo Alto Networks Special Edition

**by Lawrence Miller**

for dummies®
A Wiley Brand

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Secure Access Service Edge (SASE) For Dummies®, Palo Alto Networks Special Edition

Published by
**John Wiley & Sons, Inc.**
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2020 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-69602-5 (pbk); ISBN 978-1-119-69608-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Editor:** Elizabeth Kuball

**Associate Publisher:** Katie Mohr

**Editorial Manager:** Rev Mengle

**Business Development Representative:** Karen Hattan

**Production Editor:** Tamilmani Varadharaj

**Special Help:** Shannon Bonfiglio, Carmine Clementelli, Matt De Vincentis, Rachna Srivastava

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Table of Contents

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Introduction

With increasing numbers of mobile users, branch offices, data, and services located outside the protections of traditional network security appliances, organizations are struggling to keep pace and ensure the security, privacy, and integrity of their networks and, more important, their customers.

Today, many of the current network security technologies on the market were not designed to handle all of the types of traffic and security threats that a modern organization has to deal with. This forces organizations to adopt multiple point products to handle different requirements, such as secure web gateways, firewalls, secure virtual private network (VPN) remote access, and software-defined wide area networks (SD-WANs). For every product, there is an architecture to deploy, a set of policies to configure, an interface to manage, as well as its own set of logs. This creates an administrative burden that introduces cost, complexity, and gaps in security posture.

To address these challenges, secure access service edge (SASE) has emerged. Originally defined by Gartner, a SASE (pronounced "sassy") solution is designed to help organizations embrace cloud and mobility by providing network and network security services from a common cloud-delivered architecture. A SASE solution must provide consistent security services and access to all types of cloud applications — for example, public cloud, private cloud, and software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) — delivered through a common framework. By removing multiple point products and adopting a single cloud-delivered SASE solution, organizations can reduce complexity while saving significant technical, human, and financial resources.

In *SASE For Dummies*, you'll learn about this new approach to networking and security, including its core capabilities and key benefits for organizations in the modern digital workplace.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## About This Book

*Secure Access Service Edge (SASE) For Dummies* consists of five chapters that explore the following:

- Modern trends and their impact on the evolution of networking architectures (Chapter 1)
- SASE use cases (Chapter 2)
- Networking capabilities in SASE (Chapter 3)
- Security capabilities in SASE (Chapter 4)
- Key SASE benefits (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backward).

There's also a glossary in case you get stumped on any acronyms or terms.

## Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you work in an organization that is looking for a better way to simplify your approach to networking and security services. Perhaps you're an IT executive or manager such as a chief information officer (CIO), chief technology officer (CTO), or chief information security officer (CISO). Or perhaps you're a network or security architect or engineer.

As such, this book is written for technical readers with a general understanding of cloud, networking, and security concepts and technologies.

If any of these assumptions describes you, then this is the book for you. If none of these assumptions describes you, keep reading anyway — it's a great book and you'll learn quite a bit about SASE.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

TIP

Tips are appreciated, never expected — and I sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

## Beyond the Book

There's only so much I can cover in 64 short pages, so if you find yourself at the end of this book, thinking, "Gosh, this was an amazing book! Where can I learn more?," check out `www.paloaltonetworks.com/prisma/access`.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**IN THIS CHAPTER**

- » Understanding the role of the cloud in digital transformation strategies
- » Untethering users with mobile computing
- » Evolving the network architecture
- » Discovering a new approach to enterprise networking and security
- » Addressing networking and security challenges with SASE

# Chapter 1 The Evolution of Networking

In this chapter, you learn how cloud and mobile computing trends have changed enterprise networking and how a secure access service edge (SASE, pronounced "sassy") can help your organization address its modern networking and security requirements.

## The Journey to the Cloud — And Beyond

We live in an age of cloud and digital transformation. Users and applications are moving outside the traditional network perimeter, accessing an ever-increasing number of applications — including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) application workloads in the public cloud. Organizations face the challenge of proactively protecting their users, applications, and data from security threats, without compromising user experience.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The *2019 RightScale State of the Cloud Report* from Flexera found that public cloud adoption among organizations has grown to 91 percent and companies now run a majority of their workloads in the cloud (38 percent of their workloads run in public cloud and 41 percent run in private cloud). Companies are also using SaaS, PaaS, and IaaS offerings from multiple cloud providers — nearly five clouds on average.

As cloud computing continues to play an integral role in digital transformation, the enterprise network must evolve to support new technologies and business initiatives.

## The Rise of Mobile Computing

The proliferation of mobile devices in our everyday lives is indisputable. According to the June 2019 *Ericsson Mobility Report*, there are now nearly 8 billion mobile subscriptions worldwide. By the end of 2024, Ericsson predicts that 95 percent of all subscriptions will be mobile broadband. Many smartphones now contain more computing power than the average desktop computer. People are increasingly using smartphones to access the Internet and SaaS apps, not only for personal computing needs, but also for work purposes.

At the same time, public Wi-Fi hotspots are now available practically everywhere. This ubiquitous connectivity enables users to work on their laptops, tablets, and smartphones from practically anywhere.

Organizations are increasingly taking advantage of these trends by implementing bring your own device (BYOD) policies and embracing remote working as a new norm in the modern digital workplace. Remote working increases productivity and, ironically, promotes a work-life balance that many employees prefer instead of commuting to an office and “clocking in and out” every day.

Mobile and remote computing introduce new networking and security challenges that traditional remote access connectivity is not designed to address.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## THE TOP FIVE MOBILE SECURITY THREATS

Mobile devices have emerged in recent years as the leading platform for cybercrime and cybersecurity threats against organizations. However, organizations are still working on ways to protect these mobile devices, especially because they often contain a mixture of business and personal data and operate both on and off the enterprise network.

Here are some of the top mobile security threats today:

- **Phishing:** In the past, phishing attacks largely took place by email. Today, they're primarily happening through mobile channels, such as text messaging, Facebook Messenger, WhatsApp, and phony websites that look legitimate.
- **Mobile malware:** Every website visited or link clicked has the potential to infect mobile devices with malware, such as spyware, ransomware, Trojan viruses, adware, and others. This risk of infection by malware on mobile devices is often higher than on desktop or laptop computers because most mobile users don't install anti-malware software on their smartphones and tablets and don't recognize the threat.
- **Fake public Wi-Fi networks:** Many mobile workers today use public Wi-Fi networks at coffee shops, airports, restaurants, and other locations whenever they're working outside the office. Cybercriminals are aware of this trend and often leverage these networks to trick mobile users into connecting to fake Wi-Fi networks, thereby potentially compromising sensitive data.
- **Malicious apps:** The world is full of software applications that can be used over the Internet or downloaded from websites (including the Apple App Store and Google Play Store). Many of these applications are legitimate and safe to use, but there are also thousands that aren't. Thus, downloading an app or granting an app permission to access functions on a mobile device may expose the user's company to a host of security and privacy risks. Some apps even collect data without asking the user for permission.

*(continued)*

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

*(continued)*

- **Data leaks:** Data leaks occur with any unauthorized or unintentional transfer of data from inside an organization to an external party or destination. These leaks can range from someone inside a company accidentally transferring confidential or sensitive data to an unsanctioned/unapproved cloud application or oversharing confidential or sensitive data on cloud sharing apps or public cloud storage, all the way to an attacker or a disgruntled employee deliberately stealing the company's data. Mobile devices, which often contain both business and personal data, make it even easier to blur the boundaries either inadvertently or maliciously.

## The Impact on Branch Networking and WAN Architectures

In the early 2000s, multiprotocol label switching (MPLS) networks began to replace traditional asynchronous transfer mode (ATM) and private leased line hub-and-spoke WAN architectures. Over the next decade, MPLS became the prevalent enterprise WAN architecture. MPLS networks provided a simple network connection between branch offices and central headquarters or data center sites. This design worked well because, at the time, most network traffic was between client desktop computers located in headquarters and branch offices and business applications hosted on servers in the on-premises data center. Internet traffic volume was relatively low and generally consisted of email and static web page browsing. Any Internet-bound traffic — including traffic from the branch offices, which traversed the MPLS connection to the central headquarters or data center sites — was sent through the perimeter firewall for security protection. All network traffic could be inspected, and a centralized security policy could be enforced by the perimeter firewall.

As Internet usage increased, many branch offices began to experience performance issues and latency as their Internet traffic was being backhauled across the MPLS connection and inspected by the perimeter firewall, which was becoming a bottleneck. The growing congestion on the MPLS network negatively impacted both Internet traffic and data center traffic. The rapid adoption of cloud-based SaaS applications amplified this problem

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

exponentially and essentially put the final nail in the MPLS coffin. Organizations began to provision direct Internet access (DIA) connections, such as broadband, for their branch offices from local Internet service providers (ISPs) to alleviate some of this congestion.

Adding DIA connections at branch offices alleviated some of the network congestion issues but introduced a whole new set of challenges. On the networking side, these challenges include

- **Routing complexity:** Routers need to be configured to send traffic over the appropriate network link (for example, data center traffic over the MPLS link and Internet traffic over the DIA link). In most cases, the simplest solution is to configure static routes, which provide only limited resiliency.
- **Inefficient bandwidth usage:** It may be possible in certain cases to configure some basic round-robin load balancing between multiple Internet connections, but more advanced algorithms that take distance, cost, load, or other weighted factors into account are generally not available. As a result, there may be times when the DIA link is congested, but the MPLS link — which could otherwise be used to backhaul Internet traffic through the headquarters or data center Internet connection — is relatively idle.
- **Management complexity:** In many cases the local Internet service provider (ISP) provides a commodity router for the DIA link and does not give the customer management access. Even if the customer has management access, the ISP routers likely won't be the same type as the MPLS routers. This means different management interfaces, different operating systems, and different remote administration tools — multiplied by the number of different remote locations, different ISPs, and different router models that you need to manage.

On the security side, challenges created by this evolved WAN architecture include

- **Loss of visibility and control:** With most network traffic traversing the DIA connection at remote offices destined for the cloud and the Internet, enterprise security teams are no longer able to see the traffic and apply security policies from a centralized perimeter firewall in the data center, thereby significantly increasing risk.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Lack of integration and interoperability:** To address the loss of visibility and control, many organizations deploy firewalls, intrusion prevention systems (IPSs), web content filters, data loss prevention (DLP), and other point security solutions in their remote offices. These solutions often come from different vendors and have only limited or no integration capabilities. This makes it more difficult for security teams to correlate events and implement a cohesive enterprise security strategy.
- **Management complexity:** Different security solutions from different vendors means different management interfaces, different operating systems, and different remote administration tools — multiplied by the number of different remote locations that you need to manage. This management complexity challenge is exponentially more difficult on the security side (compared to the networking side), because of the volume and types of security information that must be analyzed on a daily basis from these different tools.

## The SASE Vision

In order to address the shift in networking and security requirements, a new architecture is needed. Gartner writes about a model known as the *secure access service edge* (SASE, pronounced "sassy").

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 1-1) that includes the following:

- **Networking**
  - Software-defined wide area networks (SD-WANs)
  - Virtual private networks (VPNs)
  - Zero Trust network access (ZTNA)
  - Quality of service (QoS)
- **Security**
  - Firewall as a service (FWaaS)
  - Domain Name System (DNS) security

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Threat prevention
- Secure web gateway (SWG)
- Data loss prevention (DLP)
- Cloud access security broker (CASB)

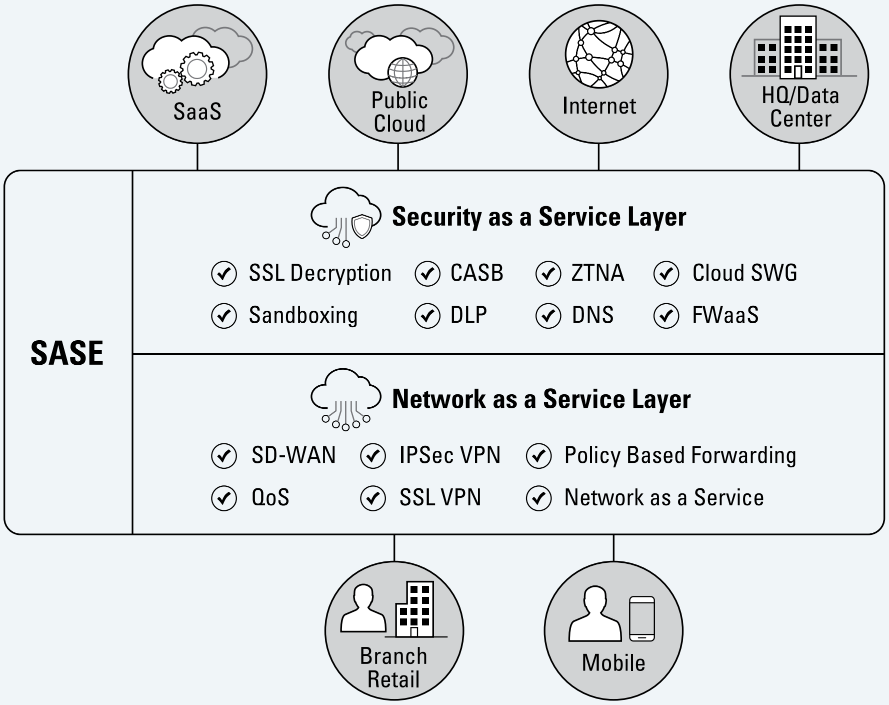


**FIGURE 1-1:** SASE delivers advanced network and security capabilities in a converged cloud-delivered solution.

## Modern Networking and Security Challenges Revisited with SASE

With networking and security functions unified in a single, multifunction cloud-delivered solution, the challenges of modern networking and security are solved by SASE in the following ways:

- **Lower capital costs:** SASE requires relatively lower capital investments than other approaches. SASE delivers networking and security capabilities in the cloud, with minimal hardware or software required on-site or on the users' device.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Full visibility and control:** SASE provides full visibility and control with cloud-delivered capabilities including FWaaS, SWG, DLP, and SaaS security via CASB functionality.
- **Less complexity:** All management functions for the cloud service can be centrally managed in the cloud from an intuitive single-pane-of-glass management interface. This means network and security teams no longer need to learn, configure, and manage multiple systems from different vendors.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- » Enabling mobile and remote users
- » Connecting and securing branch and retail locations

# Chapter 2
# SASE Use Cases

In this chapter, you learn about some of the most common use cases today for a secure access service edge (SASE).

## Mobile and Remote Users

Securing mobile users with traditional types of network security can be a challenge, especially when users work in areas where you don't have IT staff or it's cost-prohibitive to have IT staff in many locations. For years, the standard tool for connecting mobile users into a corporate network was remote-access virtual private networks (VPNs). In fact, for many people, *remote access* and *VPN* are synonymous.

However, with the number of applications and workloads moving to the cloud, the need for remote access is diminishing. In addition, it's apparent that organizations need more than remote access — they need secure access to cloud applications and the Internet as well.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## The limitations of traditional remote access VPNs

Remote access VPNs are primarily built to do one thing: Allow users outside the perimeter firewall to access resources inside the corporate network.

Remote-access VPNs use a hub-and-spoke architecture (see Figure 2-1), with users connected by tunnels of various lengths depending on their distance from the data center. Nearby users may enjoy high performance, but distance degrades performance, introducing issues with speed, bandwidth, and latency. Nevertheless, this is the optimal architecture for data center applications because the goal is to reach the "hub" where your internal applications and data are located.

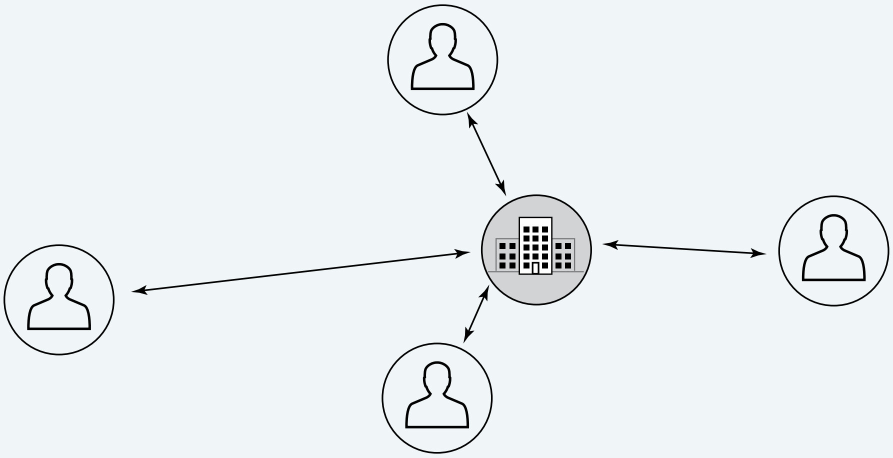


**FIGURE 2-1:** Traditional remote-access VPN architecture.

The model breaks down when a mixture of cloud applications is involved. With remote-access VPN, traffic always goes to the VPN gateway first, even if the application is hosted in the cloud (see Figure 2-2). As a result, the traffic goes to the VPN gateway at the corporate headquarters or data center and then egresses from the perimeter firewall to the Internet, with the application response going back to headquarters or the data center before it returns to the user. With cloud applications, this traffic essentially follows a "trombone" path, making a lengthy (and slow!) trip to reach an Internet-accessible location. This is sensible from a security perspective, but it doesn't make sense for network optimization.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

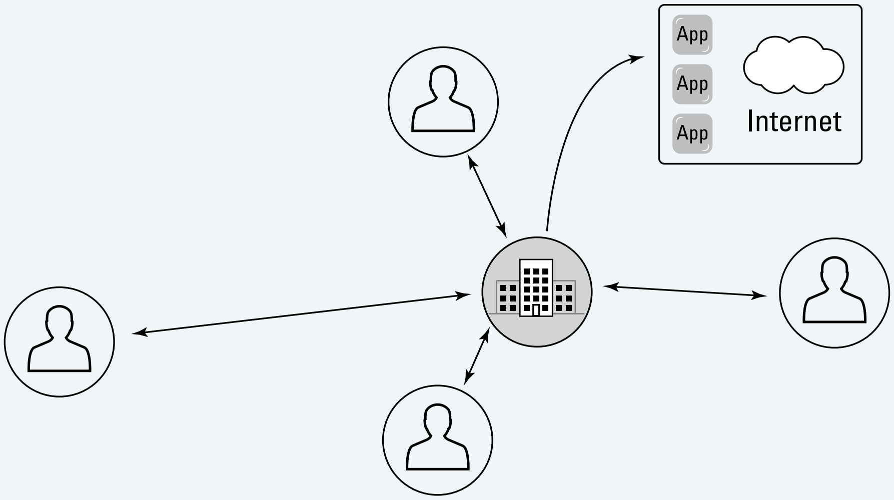


**FIGURE 2-2:** Traditional remote-access VPN backhauling traffic to reach the cloud.

Using cloud applications over remote-access VPN can hurt the user experience, and as a result, end users tend to avoid using remote-access VPN whenever possible. They tend to connect when they need access to the internal data center and disconnect when they don't, which leads to multiple issues. When users are disconnected, their organizations lose visibility into application usage, control over access to unsanctioned applications, and the ability to enforce security policies.

## Unsatisfactory compromises

To compensate for the networking problems with remote-access VPN, IT teams typically introduce a number of compromises with certain security implications:

- **User-initiated tunnel:** A common remote-access VPN deployment model is to let users initiate the tunnel as needed. Typically, they connect for a short time, complete their work with a given application, and disconnect. When disconnected, they have direct access to the Internet with no traffic inspection.
- **Split-tunnel VPN:** A common yet insecure method of deploying remote access VPN is to set up a policy that permits split tunneling. In this model, traffic bound for the corporate domain goes over the VPN tunnel, and everything else goes directly to the Internet. The improvements in network performance come at a cost, though: There is no traffic inspection for Internet and cloud traffic.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Web proxy/secure web gateway:** To compensate for scenarios when users are not connected to the VPN, many organizations have tried alternative network security measures, such as using a proxy for the web browser when users are off-network. However, by definition, a web proxy doesn't fully inspect network traffic. Even worse, the traffic inspection the proxy does perform will be fundamentally different from the inspection that's happening at headquarters, with inconsistent results depending on users' locations.

With the rapid growth of mobile workforces and cloud-based applications, organizations are finding that their remote access VPN is neither optimized for the cloud nor secure. A new approach is necessary to account for today's application mix.

## A modern architecture for the mobile workforce

The mobile workforce needs access to the data center and the Internet, as well as applications in the public cloud. A proper architecture should optimize access to all applications, wherever they or your users are located. A SASE solution provides a cloud-delivered networking and security infrastructure that makes it possible for an organization to connect users automatically to a nearby cloud gateway, enable secure access to all applications, and maintain full visibility and inspection of traffic across all ports and protocols (see Figure 2-3).

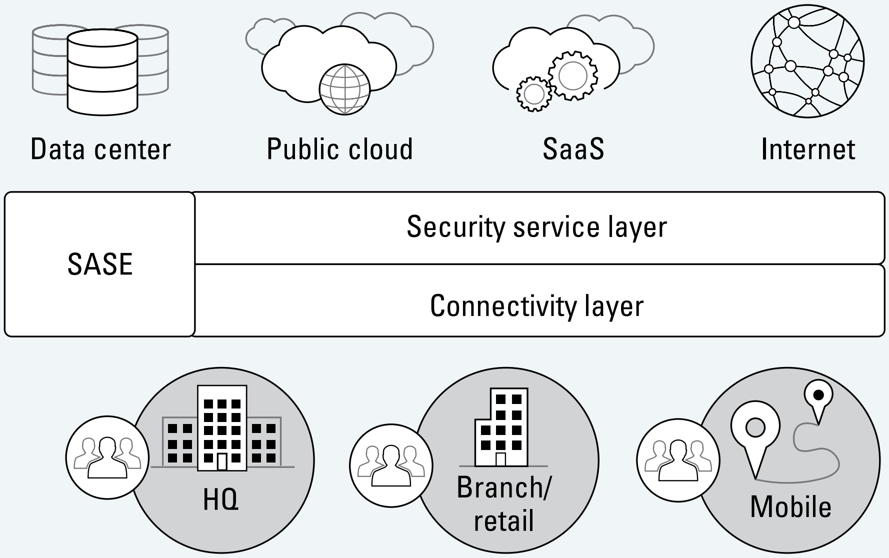


**FIGURE 2-3:** Easy access to the connectivity layer, wherever your users are.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

For managed devices:

- Users with managed devices have a SASE client app installed on their laptops, mobile phones, or tablets. The app connects to the SASE platform automatically whenever Internet access is available, without requiring any user interaction.
- Users can access all their applications, whether in the cloud or the data center. The connectivity layer connects applications in different locations, making it possible to establish secure access (based on application and user identification policies) to public cloud, software as a service (SaaS), and data center applications.
- SASE delivers protection through the security service layer, such as protections against known and unknown malware, exploits, command-and-control (C2) traffic, and credential-based attacks.

For unmanaged devices:

- Users with BYOD devices can access applications without an app installed by using a clientless VPN.
- Clientless VPN also enables secure access to web-based and SaaS applications from unmanaged devices with inline protections by using Security Assertion Markup Language (SAML) proxy integration.

## Branch and Retail

Cloud adoption is doing more than changing user mobility strategies. It’s affecting branch and retail networking strategies, too. With the growing number of applications in the cloud, it doesn’t make sense to carry all of an enterprise network’s traffic back to headquarters over expensive multiprotocol label switching (MPLS) connections. As a result, many organizations are adopting new strategies to redesign their wide area networks (WANs) to enable branch offices and retail stores to go directly to the cloud. With the drive to reduce the IT footprint at the branch in order to cut operational costs and reduce complexity, organizations are also looking for ways to reduce the amount of hardware that needs to be physically installed and managed at each location.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## The challenges of traditional branch/retail networking

The traditional standard for branch/retail networking uses an MPLS circuit between each remote site and headquarters in a hub-and-spoke topology. This makes sense when the remote site largely uses applications hosted in an internal data center or when bandwidth requirements are not very high. For example, a company that sells machine parts may host an inventory application in its internal data center, and stores across the region might query the database to get real-time information on warehouse inventory. The application does not require significant bandwidth, but the connection must be reliable because any downtime or performance issues could lead to lost business.

Many applications have now moved out of the internal data center and into the public cloud. As a result, hub-and-spoke networking is no longer ideal because traffic passes over the MPLS connection, egresses the perimeter firewall, connects to the cloud-based host, and follows the reverse path back to the user. The MPLS link is a bottleneck because the traffic makes an unnecessary trip to headquarters over a relatively slow connection and adds cost and complexity associated with the additional MPLS resources required to hairpin traffic.

Compounding this issue even further, employees at branch or remote locations need access to more bandwidth-intensive applications than ever before, driving up bandwidth requirements. It's common to see branch offices and retail stores adopt new applications, such as:

- Employee training applications, often including streaming video and audio content
- Digital marketing in retail stores to provide product information, personalized shopping tools (for example, gift registries and customization tools), and online catalogs
- In-store guest Internet

As a result, the transformation to enable direct Internet access at the branch is a necessity for businesses to compete today. However, the options for how it's done can be overwhelming when you consider the need for bandwidth capacity, reliability, operational efficiency, and security.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Augmenting MPLS with direct Internet access

As organizations embark on their cloud journey, traditional connectivity options of private links from branch to data center just don't work. Many organizations augment their private links with Internet connections for direct cloud access. Providing branch locations with direct Internet connections requires IT teams to consider many factors. Plenty of options are available, with most major cities having a range of providers for low-cost, high-speed business-class Internet. However, the top speed of the service is typically not the sole concern. Businesses need to consider the reliability and security of the service as well, and those issues aren't always easy to address.

Several different strategies for augmenting MPLS with direct Internet access can come into play including the following:

- **MPLS offloading:** MPLS offloading strategies typically don't try to eliminate the MPLS circuit; instead, they reduce the amount of traffic it must carry. For example, many organizations supplement the MPLS circuit with a direct-to-Internet connection so that Internet traffic doesn't have to be backhauled to headquarters.
- **MPLS replacement with direct to Internet:** In some scenarios, it might make sense to replace the MPLS circuit entirely and implement direct-to-Internet access from the branch. In direct-to-Internet scenarios, the networking requirements can be considerable depending on the topology of the site-to-site VPN connections.
- **MPLS offloading or replacement with SD-WAN:** Whether you're offloading or replacing MPLS, one of the strategies that you can also adopt is the use of SD-WAN. SD-WAN provides the intelligence to optimize networking decisions based on the applications, networking, and bandwidth requirements that are available, automates complex networking tasks (such as policy-based routing), and provides a common interface to manage networking across branch locations. However, no SD-WAN solution is complete without a natively integrated, robust security system.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## A modern architecture for branch transformation

Branch offices need access to all applications, including those in the data center; on the Internet; in SaaS applications; and in public clouds. In other words, the proper architecture should optimize access to all applications, wherever the applications or the users are located.

SASE provides cloud-delivered networking and security infrastructure that makes it possible to connect branch offices to a nearby cloud gateway, enabling secure access to all applications together with full visibility and inspection of traffic across all ports and protocols.

With this architecture, organizations don't have to manage separate on-premises networking and security appliances. Instead of using specialized networking or security hardware, your organization can repurpose an existing branch router or firewall at the branch site, an SD-WAN edge device, or any other Internet Protocol Security (IPSec)–compatible device to connect to the SASE platform. Policies are applied to traffic destined for the cloud, to the Internet, back to corporate headquarters, and even over a full-mesh VPN for branch-to-branch applications.

This immediately eliminates operational expenses, such as the shipping, installation, and ongoing maintenance of extra IT equipment at remote sites. Staffing can focus on operations and protecting the organization from a central location rather than handling the enforcement at the branch network edge.

TIP

In Chapters 3 and 4, you'll learn about the core networking and security capabilities, respectively, that support mobile and remote users and branch/retail use cases in a SASE platform.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- » Defining the need for SD-WANs
- » Getting real about VPNs
- » Implementing ZTNA
- » Ensuring service quality with QoS

# Chapter 3 SASE Networking Capabilities

In this chapter, you learn about the core networking capabilities of a SASE solution.

## Software-Defined Wide-Area Network

Wide area networks (WANs) use links such as multiprotocol label switching (MPLS), wireless, broadband, virtual private networks (VPNs), and the Internet to give users in remote offices access to corporate applications, services, and resources, allowing them to carry out daily functions regardless of location. Traditional WANs rely on physical routers to connect remote or branch users to applications hosted in data centers. Each router has a data plane (which holds the information) and a control plane (which tells the data where to go). Where the data flows is typically determined by a network engineer or administrator who creates rules and policies, often manually, for each router on the network — a process that can be time-consuming and prone to errors.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Software-defined WAN (SD-WAN) allows enterprises to leverage a wide combination of WAN transport services including MPLS, Long-Term Evolution (LTE), and commodity broadband, to securely connect branches and users to applications both in the cloud and data center.

SD-WAN separates the control and management processes from the underlying networking hardware, making them available as software that can be easily configured and deployed. A centralized control plane means network administrators can create new rules and policies, and then configure and deploy them across an entire network at once.

As cloud applications become mainstream, the traditional approach of a private WAN link backhauling traffic to a data center does not work, because the traffic has to then be sent out to the cloud from the data center. Backhauling traffic to data centers was a suitable WAN architecture when all applications were hosted in data centers. Now that most applications are cloud/software as a service (SaaS) based, it doesn't make sense to backhaul traffic to the data center on its way to the Internet. It's better to go directly to the Internet from the branch (direct Internet access) for cloud/SaaS and back to the data center only for apps hosted there. SD-WAN makes this possible.

Compared to traditional WANs, SD-WANs can intelligently manage multiple types of connections, including MPLS, broadband, Long-Term Evolution (LTE), and others, as well as support applications hosted in data centers, public and private clouds, and SaaS services. SD-WAN can route application traffic over the most optimal path based on performance (that is, latency, jitter, packet loss, and availability), in real time, by intelligently load balancing across multiple links. Prior to SD-WAN, organizations would have to manually configure multiple links to behave a certain way using policy-based routes, for example, to determine what application should take which link.

REMEMBER

Companies are embracing SD-WAN to connect branch offices to the corporate network and provide local Internet breakout for better performance and user experience.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

SD-WAN offers geographically distributed organizations and companies with multiple branches a number of benefits, including

- **Simplicity:** SD-WAN enables centralized management and simplified configuration rules. In addition, combining SD-WAN with zero-touch provisioning — a feature that helps automate the deployment and configuration processes — organizations can further reduce the complexity, resources, and operating expenses required to turn up new sites.
- **Greater flexibility and agility:** With SD-WAN, organizations have more connectivity options, such as broadband Internet, which is faster to provision than MPLS. Configuring, deploying, and managing MPLS is time-consuming for most organizations. It can sometimes take a service provider up to three months to install a new MPLS circuit, and MPLS isn't readily available in all areas. SD-WAN remediates this challenge because it separates control of the network services from transport, letting organizations securely use any available Internet connection (such as broadband or LTE) in a given region without being limited to the coverage provided by the MPLS carrier.
- **Improved user experience:** Without SD-WAN, connecting branch offices to cloud applications is expensive. Traditional WANs must backhaul traffic to the headquarters or corporate data center, usually over MPLS (see Figure 3-1). This can lead to inefficient use of resources and poor performance. By enabling efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better overall user experience that leads to less frustration, higher productivity, and better collaboration.
- **Efficient use of resources:** SD-WAN can lead to greater efficiency in the following ways:
  - *Acquisition of hardware, software, and support:* According to industry research, companies can save up to 40 percent over five years.
  - *Personnel to manage, troubleshoot, and provision WAN equipment.*
  - *Network expenses:* Because SD-WAN supplements or substitutes MPLS with broadband or other Internet connectivity, traffic can be routed based on the best option for cost versus performance.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

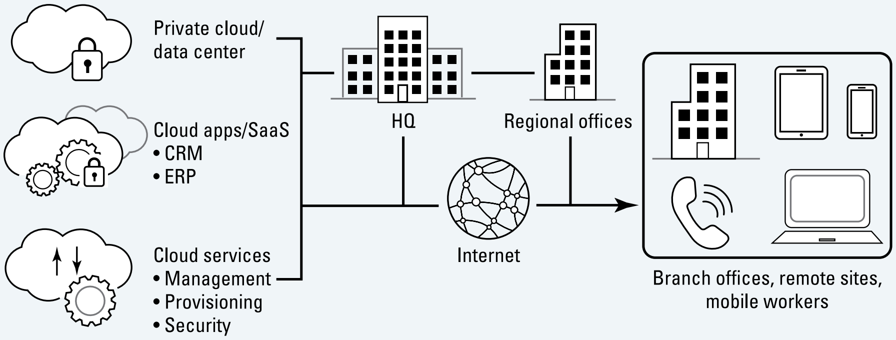


**FIGURE 3-1:** Efficient SD-WAN traffic routing.

WARNING

When adopting SD-WAN, however, decision-makers often prioritize connectivity and cost benefits over security. This can put your network at risk.

Although SD-WAN offers many benefits, it also brings many challenges, including new security risks, unreliable performance, and increased complexity resulting from the need for multiple overlays. When security is an afterthought, it tends to be bolted on, introducing management complexity and subpar protection. Moreover, network performance becomes less reliable because organizations use the congested public Internet as the WAN middle mile. Organizations sometimes try to address these challenges by building their own SD-WAN hub and interconnect infrastructures, which results in more complexity.

In a SASE solution, SD-WAN edge devices can be connected to a cloud-based infrastructure, rather than physical SD-WAN hubs located in data center or colocation facilities. This enables the interconnectivity between branch offices without the complexity of deploying and managing physical SD-WAN hubs.

TIP

SD-WAN should be something you're already considering or you've already adopted into your organization's network infrastructure as a way to securely connect and control access to branch offices and remote employees. SASE creates a unified framework for SD-WAN and security services to connect to, providing a single point of view and simplified management solution to protect your network.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Virtual Private Network

A VPN uses a public network, such as the Internet, to enable remote users and sites to connect securely to the corporate network. Two types of VPNs are a remote-access VPN and a site-to-site VPN. Corporate networks are sometimes built on site-to-site VPNs, where the local area network (LAN) of each location can be connected to the data center via a secure WAN on which company resources can be shared. Remote-access VPNs allow individual users to connect to the corporate network remotely.

On VPNs, data travels over the Internet securely through a tunneling protocol, where it's encrypted using Internet Protocol Security (IPSec) or Secure Sockets Layer (SSL). The tunneling protocol also *encapsulates* (wraps) the data with routing information for the receiving user.

Organizations rely on VPNs to provide a secure encrypted connection for mobile users and branch offices to access corporate data, applications, and Internet access. VPNs are not optimized for access to the cloud, however, resulting in no security or access control when users disconnect to reach cloud apps or services (see Figure 3-2).

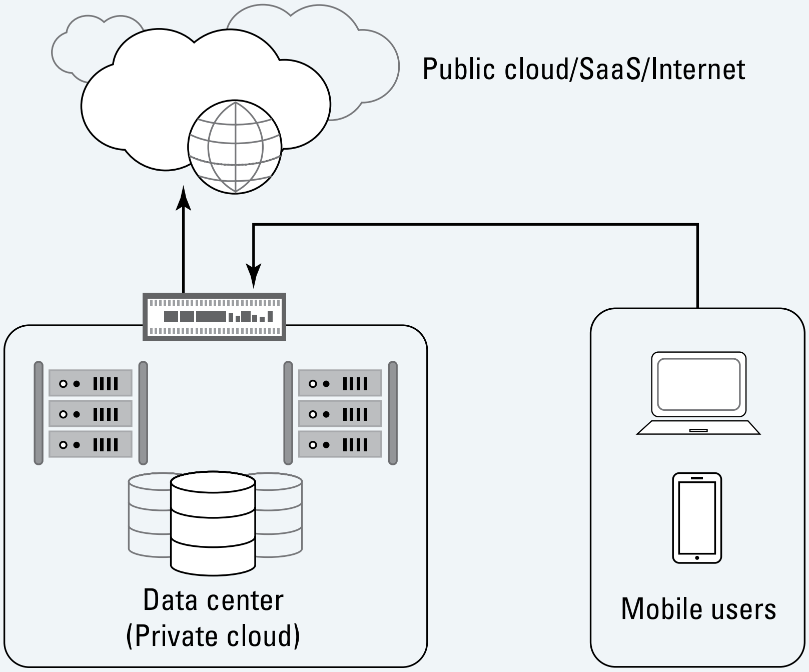


**FIGURE 3-2:** Remote-access VPN is not designed to support cloud applications.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

A SASE solution encompasses VPN services and enhances the capabilities to operate in a cloud-based infrastructure in order to securely route traffic to public cloud services including SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS), as well as Internet and private cloud apps and services. In an IPSec VPN example, you can create a site-to-site connection to a cloud-based infrastructure from any IPSec-compatible device located at a branch or retail location via a branch router, wireless access point, SD-WAN edge device, or firewall (see Figure 3-3). Mobile users employ an always-on IPSec or SSL VPN connection between their endpoint or mobile device, and a SASE solution ensures consistent traffic encryption and threat prevention.

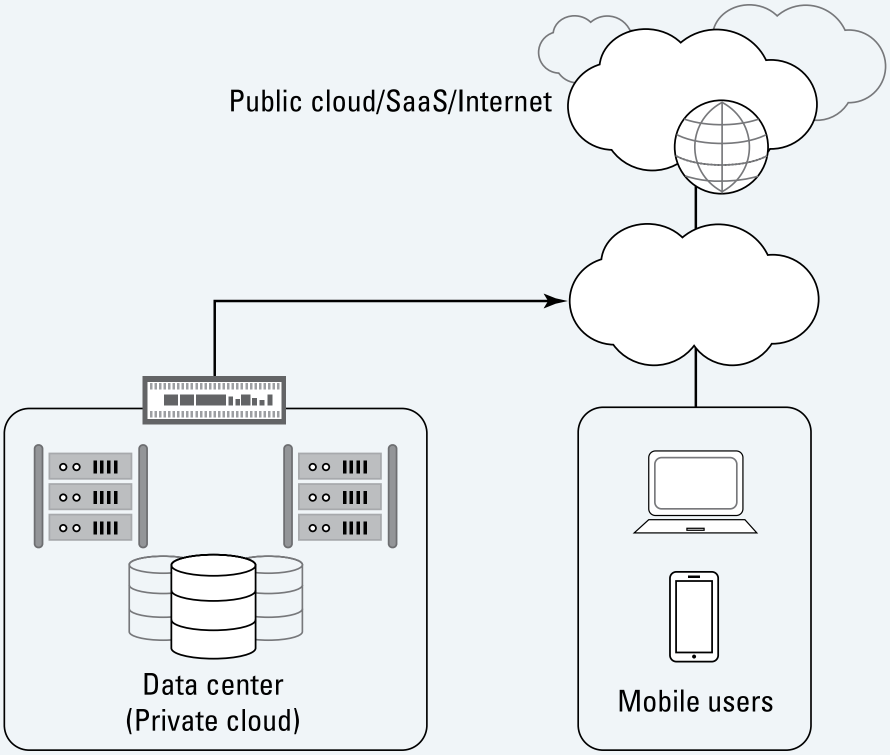


**FIGURE 3-3:** SASE uses cloud infrastructure to connect users to both cloud apps and the data center.

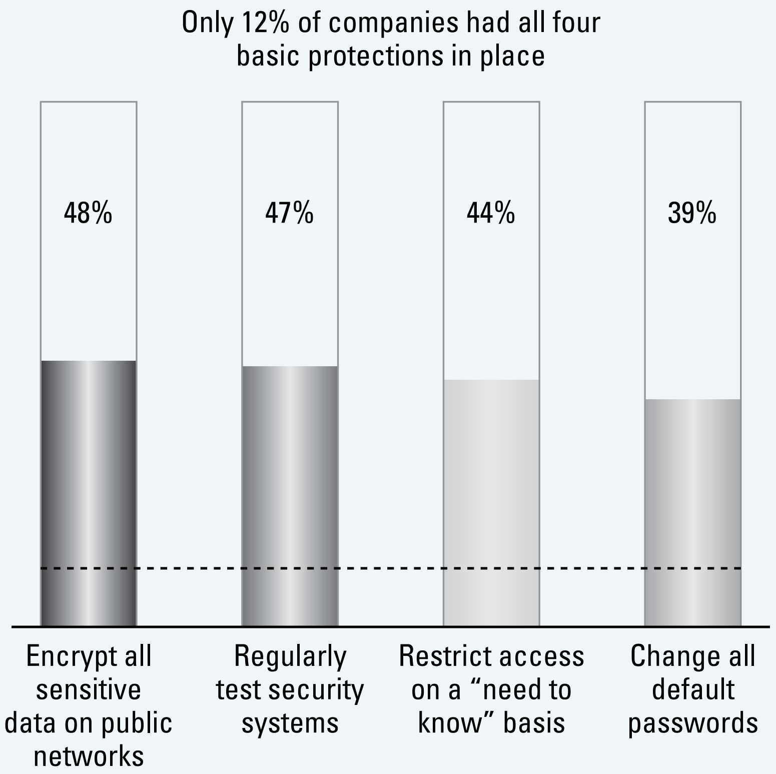
REMEMBER

No matter which type of VPN service you use in your organization, a SASE solution provides a unified cloud infrastructure to connect to, instead of backhauling to a VPN gateway at corporate headquarters. This dramatically simplifies the management and policy control needed to enforce least-privilege access rules.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Zero Trust Network Access

As shown in Figure 3-4, companies still lack the necessary security protections and policies needed to adequately protect their users and data. Zero Trust network access (ZTNA) is a key part of the Zero Trust philosophy of "never trust, always verify," developed by Forrester Research. ZTNA requires users who want to connect to the cloud to authenticate and have their traffic inspected up through Layer 7 via a gateway prior to gaining access to the applications they need. This provides an IT admin with the ability to identify users and create policies to restrict access, minimize data loss, and quickly mitigate any issues or threats that may arise. Many ZTNA products are based on micro-perimeter architectures, which do not provide content inspection, thus creating a discrepancy in the types of protection available for each application. In terms of consistent protection, the organization must build additional controls on top of the ZTNA model and establish inspection for all traffic across all applications.



*Source: Verizon Mobile Security Index 2019 report*

**FIGURE 3-4:** Which of the following match your organization's security policies?

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Layer 7 inspection and control are imperative to Zero Trust.

SASE builds upon the key principles of ZTNA and applies them across all the other services within a SASE solution. By identifying users, devices, and applications, no matter where they're connecting from, policy creation and management is simplified. SASE removes the complexity of connecting to a gateway, by incorporating the networking services into a single unified cloud infrastructure.

REMEMBER

A SASE solution should support ZTNA capabilities for protecting applications, as well as apply other security services for the consistent enforcement of data loss prevention (DLP) and threat prevention policies. This is necessary because access controls, in and of themselves, are useful for establishing who the person is, but other security controls are also necessary to make sure their behaviors and actions are not harmful to the organization and its data. It's also necessary to apply the same controls across access to all applications.

## WHAT IS ZERO TRUST?

Zero Trust is a cybersecurity strategy that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

Zero Trust was created by John Kindervag at Forrester Research, based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted. Under this broken trust model, it's assumed that a user's identity is not compromised and that all users act responsibly and can be trusted. The Zero Trust model recognizes that trust is a vulnerability. Once on the network, users — including threat actors and malicious insiders — are free to move laterally and access or exfiltrate whatever data they aren't limited to. ***Remember:*** The point of infiltration of an attack is often not the target location.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Quality of Service

As organizations transition from MPLS to SD-WAN using direct Internet access (DIA) links, they're finding that the service quality varies. Quality of service (QoS) establishes bandwidth allocation assigned to particular apps and services. Businesses rely on QoS to ensure that their critical apps and services (for example, medical equipment or credit card processing services) perform adequately. If these systems were to get bogged down due to a lack of available bandwidth caused by network congestion (for example, non-business-related streaming video), this would severely impact business operations and sales (as shown in Figure 3-5).

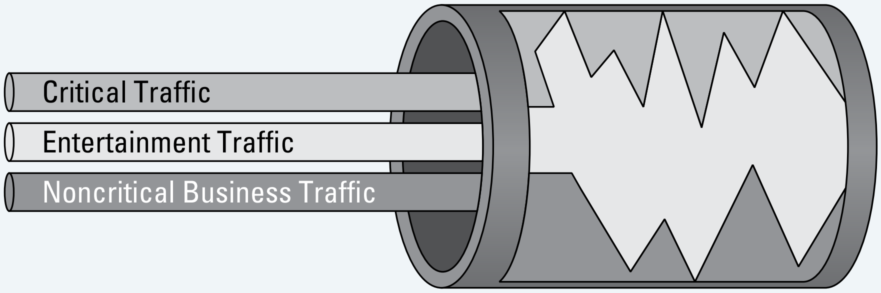


**FIGURE 3-5:** Bandwidth without QoS control.

WARNING

Broadband Internet is a "best effort" service that doesn't provide a consistent bandwidth level. For this reason, QoS isn't supported on broadband Internet links. If you have QoS configured for your network, your broadband Internet service provider (ISP) will ignore QoS tagging on its routers.

QoS prioritizes business-critical apps, based on a ranking system, so you can choose which apps and services take precedence over others (see Figure 3-6). QoS is an important step when you begin migrating from MPLS. A SASE solution incorporates QoS services in the cloud, allowing you to easily mark sensitive applications, such as voice over IP (VoIP), as high priority over general Internet and entertainment sites and apps.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

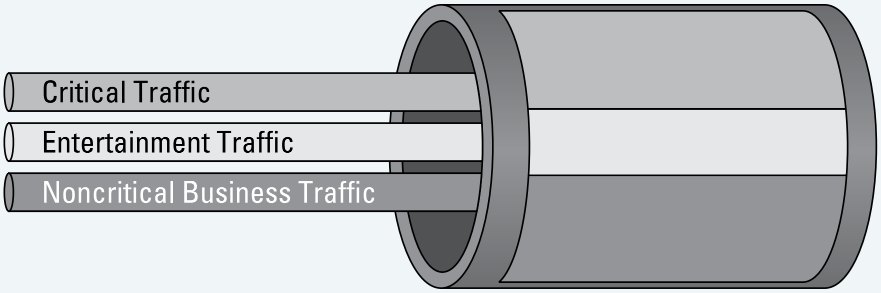


**FIGURE 3-6:** Bandwidth with QoS control.

REMEMBER

QoS is immensely important for businesses of any size, especially as they migrate from MPLS to direct to Internet. Managing the QoS traffic and allocation doesn't need to be difficult. A good SASE solution will enable you to dynamically shape traffic based on the policies that prioritize critical application requirements.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**IN THIS CHAPTER**

- » Deploying a next-generation firewall "as a service"
- » Securing DNS resolution
- » Leveraging threat prevention tools
- » Blocking malicious websites with an SWG
- » Preventing sensitive data loss and ensuring regulatory compliance
- » Identifying and securing access to SaaS apps

# Chapter 4 SASE Security Capabilities

n this chapter you learn about the core security capabilities in a SASE solution.

## Firewall as a Service

Firewalls were originally designed to protect on-site company networks, but as more companies moved their applications and data to the cloud, firewalls had to evolve. Now, firewall as a service (FWaaS) enables firewalls to be delivered as a cloud service.

In the past, organizations ran all their applications and data in on-site data centers and used a perimeter-based defense to secure their networks, with on-premises firewalls serving as the main security checkpoints. However, as companies moved to the cloud, added more company- and employee-owned mobile devices to their networks, and began using more software as a service (SaaS)

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

applications and data hosted on third-party infrastructure, they quickly discovered they no longer had clearly defined network perimeters.

They also found that because many of their applications and data were now being run and managed on third-party infrastructure, they no longer had full visibility into, or control over, their entire networks. This problem was further exacerbated by the proliferation of third-party point products that had to be separately managed.

This forced many organizations to completely rethink their approach to security. FWaaS is a deployment method for delivering a firewall as a cloud-based service. FWaaS has the same features of a next-generation firewall, but it's implemented in the cloud. By moving the firewall to the cloud, organizations can benefit from cost savings by eliminating the need to install or maintain security hardware or software across their entire organization.

The FWaaS approach enables organizations to:

- Aggregate all traffic from multiple sources (for example, on-site data centers, branch offices, mobile users, cloud infrastructure) into the cloud
- Consistently apply and enforce security policies (fewer error-prone, manual configurations) across all locations and users
- Gain complete visibility into and control over their networks without having to deploy physical appliances, thereby reducing support costs

TIP

A company with 500 employees can expect to save 37 percent, on average, by using FWaaS solutions versus traditional hardware, according to Secure Data.

A SASE solution incorporates FWaaS into its unified platform, providing the same services as a next-generation firewall but as a cloud-delivered service. By encompassing the FWaaS service model within a SASE framework, organizations can easily manage their deployments from a single platform.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

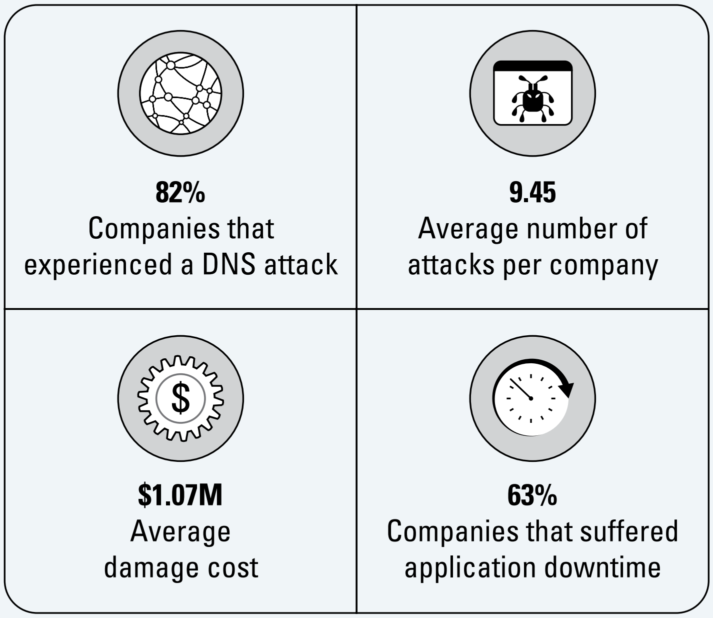
REMEMBER

A SASE solution should enable FWaaS capabilities in order to provide the protection of a next-generation firewall by implementing network security policy in the cloud. It's important to ensure your SASE solution doesn't only provide basic port blocking or minimal firewall protections. You need the capabilities of a next-generation firewall, as well as cloud-based security services, such as threat prevention services and Domain Name System (DNS) security.

## Domain Name System Security

Each device connected to the Internet has an Internet Protocol (IP) address. The DNS is a protocol that translates a user-friendly domain name, such as `www.paloaltonetworks.com`, to an IP address — in this case, 199.167.52.137. DNS is ubiquitous across the Internet. Without it, we'd have to memorize random strings of numbers, which our brains aren't equipped to do very well.

DNS is an open service, and by default it doesn't have a way to detect DNS-based threats. As a result, malicious activity within DNS can be used to propagate an attack causing costly damage and downtime (see Figure 4-1).



*Source: IDC 2019 Global DNS Threat Report*

**FIGURE 4-1:** DNS attacks are prevalent and result in costly damage and application downtime for organizations.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

DNS is a massive and often overlooked attack surface present in every organization. According to the Palo Alto Networks Unit 42 threat research team, almost 80 percent of malware uses DNS to initiate command-and-control (C2) communications (see the "DNS-based attacks: OilRig" sidebar in this chapter). Unfortunately, security teams often lack basic visibility into how threats use DNS to maintain control of infected devices. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack, including reliable C2.

Security teams struggle to keep up with new malicious domains and enforce consistent protections for millions of emerging domains at once. It's impossible for enterprise network and security teams to keep up with the high volume of malicious domains, let alone advanced tactics like DNS tunneling for stealthy data theft.

## DNS-BASED ATTACKS: OilRig

OilRig is an active, organized threat group first discovered by the Palo Alto Networks Unit 42 threat research team. Operating primarily in the Middle East, OilRig carefully targets organizations to further its regional strategic goals across multiple industries, including supply-chain-based attacks. As part of its adversary playbook, the group employs sophisticated, custom DNS tunneling for C2 and data exfiltration. The use of tunneling includes

- **ALMA Communicator Trojan,** which uses DNS tunneling to receive commands from the adversary and exfiltrate data. The malware employs specially crafted subdomains to send data to the C2 server and specific Internet Protocol version 4 (IPv4) addresses to transmit data from the C2 to the Trojan over DNS requests.
- **Helminth PowerShell-based Trojan,** which can obtain files from a C2 server using a series of DNS text (TXT) queries repeated every 50 milliseconds, essentially building malware on victim systems through hard-to-detect increments sent over DNS.

OilRig's use of DNS tunneling allows the group to establish reliable C2 that can potentially evade existing defenses to carry out further stages of the attack.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

DNS security protects users by detecting and blocking malicious domains while neutralizing threats. A SASE solution embraces DNS security features by providing consistent security across the network and users, no matter their location, with advanced capabilities that include enabling organizations to:

- **Automatically protect against tens of millions of malicious domains identified with real-time analysis and continuously growing, global threat intelligence:** Protection continues to grow with data from a large, expanding threat intelligence sharing community. A malicious domain database is created from multiple sources, including the following:
  - *Malware prevention* to find new C2 domains, file download source domains, and domains in malicious email links
  - *URL filtering* to continuously crawl newfound or uncategorized sites for threat indicators
  - *Passive DNS and device telemetry* to understand domain resolution history
  - *Threat research* to provide human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots
  - *Third-party threat intelligence* sources
- **Predict and stop malicious domains from domain generation algorithm-based malware with instant enforcement.** Malware's use of domain generation algorithms (DGAs) continues to grow, limiting the effectiveness of blocking known malicious domains alone. DGA malware uses a list of randomly generated domains for C2, which can overwhelm the signature capability of traditional security approaches. DNS security deals with DGA malware by using:
  - *Machine learning* to detect new and never-before-seen DGA domains by analyzing DNS queries as they're performed.
  - *Easy-to-set policy* for dynamic action to block DGA domains or sinkhole DNS queries.
  - *Threat attribution and context* to identify the malware family with machine learning for faster investigation efforts.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Your SASE solution should provide DNS security delivered within the cloud environment as part of the network access. DNS security should be built in, rather than bolted on, to the solution your branch offices and mobile users use to connect to the Internet. The DNS security provided in your SASE solution should leverage a combination of predictive analytics, machine learning, and automation to combat threats in DNS traffic.

## Threat Prevention

The dynamic nature of public cloud usage and user mobility requires security teams to adapt and embrace a new approach to threat prevention. According to respondents in a recent ESG survey, threat detection and response is more difficult today than ever before because:

- The volume and/or sophistication of threats has increased (34 percent).
- The threat detection/response workload has increased (17 percent).
- The attack surface has grown (16 percent).
- Threat detection/response is dependent on many manual processes within the organization (11 percent).
- The organization uses numerous disparate threat detection/response tools (11 percent).
- The organization doesn't have the skills or appropriately sized cybersecurity staff (8 percent).

In today's world of small- and large-scale breaches, threat prevention is key to protecting your organization's data and employees. There are a variety of threat prevention tools out there, from anti-malware and intrusion prevention to SSL decryption and file blocking, providing organizations ways to block threats. However, these point products require separate solutions, making management and integration difficult.

Within a SASE solution, all these point products and services are integrated into a single cloud platform. This provides simplified management and oversight of all threats and vulnerabilities across your network and cloud environments.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Stopping exploits and malware by using the latest threat intelligence is crucial to protecting your employees and data. Your SASE solution should incorporate threat prevention tools into its service so you can react quickly and effectively to remediate threats. Be sure to check the quality of threat intelligence that is being provided by the vendor. The vendor should be gathering and sharing data from various sources, including customers, vendors, and other relevant thought leaders, to provide continuous protection from unknown threats.

REMEMBER

Continuous and effective threat prevention, detection, and automated response across your environment requires the following:

- Granular visibility into your users, apps, and data
- Advanced threat prevention over the network
- Threat detection and analysis by correlating risky configurations, anomalous user and network activity, host vulnerabilities, and threat intelligence gathered from multiple data sources
- Automated response to simplify security event triage
- Cloud context to expedite security investigations

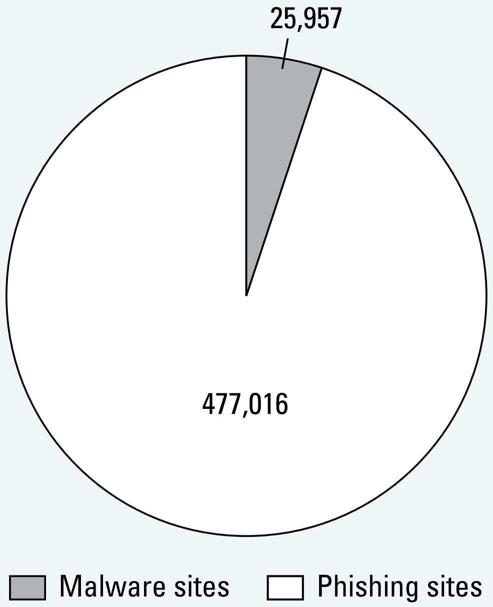
## Secure Web Gateway

In recent years, the emergence of secure web gateways (SWGs) has provided one approach to the problem of securing web traffic from a branch or mobile user's endpoint (discussed in Chapters 2 and 3).

Instead of performing full inspection of all network traffic, a web gateway examines traffic from a web browser and blocks websites and known malware. Organizations looking for a better solution, as opposed to no inspection, may use this approach without having to deploy a hardware appliance at the branch.

Many organizations rely on an SWG to protect employees and devices from accessing malicious websites. According to the *Google Transparency Safe Browsing Report*, more than 500,000 unsafe websites were detected by Google in July 2019 (see Figure 4-2).

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



*Source: Google Transparency Safe Browsing Report*

**FIGURE 4-2:** More than 500,000 unsafe websites were detected by Google in July 2019.

SWG can be used to block inappropriate content (for example, pornography and gambling) or websites that businesses simply don't want users accessing while at work, such as streaming services like Netflix. Additionally, SWG can be used to enforce an acceptable use policy (AUP) before Internet access is granted.

WARNING

Web gateways are not a substitute for a firewall. Partially inspecting traffic means the remaining traffic passes through uninspected, or else the application breaks. The organization remains blind to applications that legitimately use alternative ports, as well as those intentionally evading inspection. Security is compromised because there is no inspection of non-browser traffic and no protection against other stages of the attack life cycle (see the "Know your enemy: Modern cyberattack strategy" sidebar), such as secondary malware payloads or ongoing C2 traffic with a compromised endpoint.

SWG is just one of the many security services that a SASE solution must provide. As organizations grow and add more and more remote users, coverage and protection becomes more difficult. A SASE solution moves SWG into the cloud, providing protection in the cloud through a unified platform for complete visibility and control over the entire network.

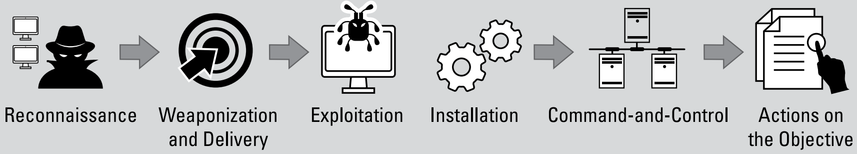
These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

A SASE solution includes the same security services in an SWG, allowing organizations to control access to the web and enforce security policies that protect users from hostile websites. Remember that SWG is just one service of the SASE solution. Other security services like FWaaS, DNS security, threat prevention, data loss prevention (DLP), and cloud access security broker (CASB) are also necessary.

## KNOW YOUR ENEMY: MODERN CYBERATTACK STRATEGY

Modern cyberattack strategy employs a patient, multistep, covert process that blends exploits, malware, and evasion in a coordinated attack. The cyberattack life cycle (see the figure) is a sequence of events that an attacker goes through to successfully infiltrate an organization's network and steal data.



Here are the steps of the cyberattack life cycle:

1. **Reconnaissance.** Like common criminals, cybercriminals carefully study their victims and plan their attacks, often using social engineering, phishing, email address harvesting, and other tactics to research, identify, and select targets. They also use various tools to scan networks (and SaaS applications) for vulnerabilities, services, and applications that can be exploited.
2. **Weaponization and delivery.** Next, the attacker determines the malware payload and the method that will be used to deliver it. For example, data files or web pages can be weaponized with exploits that are used to target the victim's vulnerable software and delivered via an email attachment or drive-by-download.
3. **Exploitation.** The attacker generally has two options for exploitation: social engineering or software exploits. *Social engineering* is a relatively simple technique used to lure someone into clicking on

*(continued)*

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

*(continued)*

a bad link or opening a malicious executable file, for example. *Software exploits* are a more sophisticated technique because they essentially trick the operating system (OS), browser, or other third-party software into running an attacker's code. This means the attacker has to craft an exploit to target specific vulnerable software on the endpoint. When exploitation has succeeded, an advanced malware payload can be installed.

4. **Installation.** When a target endpoint has been infiltrated, the attacker needs to ensure *persistence* (resilience or survivability). Various types of advanced malware are used for this purpose, including anti-AV software, backdoors, bootkits, and rootkits.
5. **Command-and-control (C2).** Communication is the life blood of a successful attack. Attackers must be able to communicate with infected systems to enable C2, and to extract stolen data from a target system or network. This communication can also be used by the attacker to move laterally, targeting other systems on the victim's network. C2 communications must be stealthy and can't raise any suspicion on the network.
6. **Actions on the objective.** Attackers have many different motives for an attack, including data theft, destruction of critical infrastructure, hacktivism, or cyberterrorism. This final phase of the attack often lasts months or even years, particularly when the objective is data theft, because the attacker uses a low-and-slow attack strategy to avoid detection.

## Data Loss Prevention

Companies are processing massive amounts of data in more places than ever (for example, in their offices, in the cloud, in multiple SaaS applications and cloud storage environments, and so on). In addition, with cloud and mobile computing technologies, employees now have the ability to directly access applications and data anytime, anywhere, and from any device.

The challenge is:

- Most companies don't have much visibility into where their sensitive and regulated data is, and how and where their employees access it, use it, or share it with others. In cloud environments, all of the above is especially true.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- SaaS and public cloud providers may offer some data protection capabilities, which can lead to ineffective and inconsistent security.
- The number of data breaches by insider threats continues to increase.

To overcome these challenges, it's crucial for companies to put a solid data protection strategy in place.

DLP protects sensitive data (for example, intellectual property, financial data, identities, regulated data, and so on) from loss and theft.

REMEMBER

DLP allows a company to

- Discover all their sensitive data consistently across different repositories and communication vectors, such as Office 365, Box, Slack, corporate devices, network traffic, and so on.
- Monitor usage of sensitive data.
- Protect sensitive data and proactively prevent data leakage.

TIP

For DLP to be effective, companies must

- Protect their data across their networks, clouds, and users, including SaaS applications, cloud storage, and network traffic.
- Optimize their DLP deployment and management efforts.
- Discover, classify, monitor, and protect all their sensitive data, such as personally identifiable information (PII) and intellectual property (IP).
- Clearly define and enforce policies in order to accurately detect data exposure and violations.
- Ensure that their data is being stored, accessed, and used in a way that complies with regulations and privacy laws, such as the European Union General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), U.S. Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS), and so on.

DLP is traditionally a composite solution that monitors data within the environments where it's deployed (such as network, endpoints, and cloud). With SASE, DLP becomes a single

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

cloud-delivered solution centered around the data itself. Policies are consistently applied to sensitive data at rest, in motion, and in use, regardless of its location. With SASE, organizations can finally enable a comprehensive data protection solution that relies on a scalable and simple architecture and allows effective machine learning by leveraging access to all the organization's traffic and data.

REMEMBER

DLP is a necessary tool to protect sensitive data and ensure compliance throughout the organization. With SASE, DLP is an embedded, cloud-delivered service used to accurately and consistently identify, monitor, and protect sensitive data across networks, clouds, and users.

## Cloud Access Security Broker

SaaS applications (like Office 365, Box, Slack, and Salesforce) offer companies, employees, and customers many operational benefits.

However, for each positive, there is also a negative when it comes to information security (see Table 4-1).

**TABLE 4-1** The Pros and Cons of SaaS Adoption

| Pros | Cons |
|---|---|
| SaaS apps can be deployed quickly. As a software solution, the installation and configuration of SaaS apps are quick and painless. By utilizing the cloud, the apps are easily accessible directly to all users. | Anyone with a credit card can start using almost any cloud service. Cloud services are typically set up without IT and security oversight. Users are able to access the application from anywhere and on any device — secure or not. |
| Large amounts of data can be stored in the cloud with a low total cost of ownership (TCO) for the organization. Data in the cloud is easily shareable among users within the organization and with external third parties. | Data stored in SaaS applications is practically invisible to IT and can be excessively shared and exposed to more users and threats. When such data is sensitive, it's a huge risk for breaches and noncompliance. |

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

| Pros | Cons |
|---|---|
| They're simple to maintain. Instead of having your IT department manually upgrade the app, that responsibility falls to the SaaS vendors, saving you IT resources. | Maintenance isn't always for the purpose of increasing uptime. SaaS vendors do an amazing job releasing new features and functionality, but this frequent pace of change also makes it difficult for IT and security teams to keep tabs on configurations and risk. |
| Because SaaS apps live in the cloud, they're scalable, no matter the size of your organization, and remote users can access SaaS apps no matter their location. | Most Tier 1 SaaS apps are designed to be infinitely scalable in theory. The downside is that unsanctioned apps will grow virally in your organization. |

Given the ease of use inherent to SaaS apps, the volume and sensitivity of data being transferred, stored, and shared in SaaS cloud environments continues to increase. Simultaneously, users are constantly moving to different physical locations, using multiple devices, operating systems, and application versions to access the data they need.

As a result, some undesirable security tradeoffs have emerged:

- **Lack of visibility** (and therefore protection) into data uploaded and created in the cloud.
- **Direct access to applications and data from any device** (including unmanaged devices and bring your own device, or BYOD, personal devices) and from anywhere (including unsafe public Wi-Fi in coffee shops or at home).
- **Shadow IT,** in which employees use and access unsanctioned applications to get their work done as a workaround to sanctioned IT if they aren't provided with the tools that they need. Shadow IT introduces security risk and potentially exposes sensitive corporate data.

REMEMBER

*Shadow IT* refers to IT applications and services that are acquired and operated by end users without explicit organizational approval and often without organizational IT knowledge or support.

Many organizations depend on SaaS security, like cloud access security brokers (CASBs), to gain visibility into SaaS application usage (both sanctioned and shadow IT), understand where their

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

sensitive data resides, enforce company policies for user access, and protect their data from threat actors. CASBs are cloud-based security policy enforcement points that provide a gateway for your SaaS provider and your employees.

However, legacy CASB approaches to securing SaaS applications use a standalone proxy designed to perform a limited amount of inline inspection capabilities. There are different deployment modes by which a CASB can deliver its functions, including network inline, Security Assertion Markup Language (SAML) proxy, agent, and application programming interface (API) based (or introspection). And although CASB can also be used for API-based controls, it often has a limited set of ties to contextual policies about which specific users or devices have access to particular data. Despite multiple options for deployment, there are shortcomings with traditional implementation methods, and many enterprise CASB projects have struggled to get off the ground because of it.

TIP

SaaS security functionality is integrated into SASE as a core capability providing SaaS application and data security in a single platform. A SASE solution helps you understand which SaaS apps are being used and where data is going, no matter where users are located. Specific capabilities should include the following:

- **SaaS visibility**
  - Discovery of shadow IT
  - App discovery
  - App usage reporting
  - App risk assessment
  - Configuration assessment
- **Control and compliance**
  - App access control
  - Data discovery and classification
  - Compliance reporting and remediation
  - Unmanaged device access control
- **SaaS protection**
  - Threat protection
  - Data protection

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Encryption
- Rights management
- User anomaly detection
- Workflow integration

A SASE solution should incorporate both in-line and API-based SaaS controls for governance, access controls, and data protection. Also called a multi-mode CASB, the combination of in-line and API-based SaaS security capabilities provide superior visibility, management, security, and zero-day protection against emerging threats.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- **Getting full visibility and control of users, data, and apps**
- **Simplifying monitoring and reporting**
- **Protecting mobile and remote users and enabling consistent security**
- **Reducing costs and integration nightmares**
- **Improving performance and aligning networking and security**

# Chapter 5 Ten Benefits of SASE

Here are ten important business and technical benefits of deploying secure access service edge (SASE) in your organization.

## Complete Visibility across Hybrid Environments

SASE enables complete visibility of hybrid enterprise network environments that connect data centers, headquarters, branch and retail locations, public and private cloud, and mobile users.

The combination of firewall as a service (FWaaS), secure web gateway (SWG), data loss prevention (DLP), and cloud access security broker (CASB) capabilities and functions in SASE empower enterprise security teams with full visibility into all network activity in the environment, including users, data, and apps.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Control of Users, Data, and Apps

Users are increasingly leveraging a variety of applications — including SaaS applications from multiple devices and locations — for work-related (as well as personal) purposes. Many applications, such as instant messaging (IM), peer-to-peer (P2P) file sharing, and Voice over Internet Protocol (VoIP), are capable of operating on nonstandard ports or hopping ports. Some of these applications are sanctioned by the organization, others are tolerated, and others are unsanctioned. Users are increasingly savvy enough to force applications to run over nonstandard ports through protocols such as Remote Desktop Protocol (RDP) and Secure Shell (SSH), regardless of the organization's policy regarding various applications (sanctioned, tolerated, unsanctioned).

SASE can classify traffic by application on all ports, by default — and it doesn't create an administrative burden by requiring you to research which applications use which ports in order to configure appropriate policies and rules. SASE provides complete visibility into application usage along with capabilities to understand and control their use (see Figure 5-1).

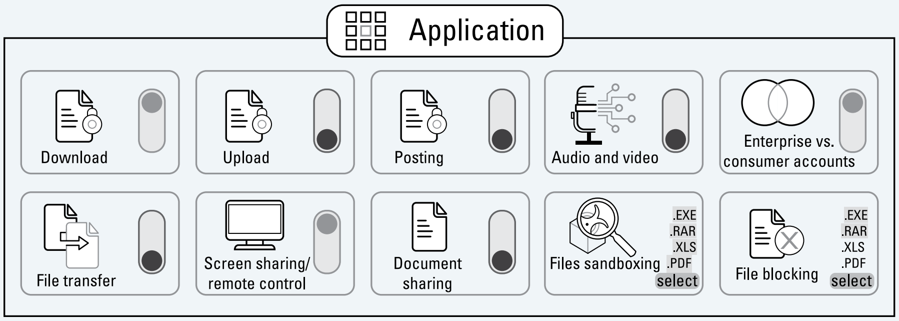


**FIGURE 5-1:** Control application usage in policy.

# Monitoring and Reporting

SASE eliminates the need to monitor multiple consoles across different networking and security products and creating separate reports for key metrics. Monitoring and reporting can be done from a "single pane of glass" in SASE, which also helps networking and security teams correlate events and alerts to simplify troubleshooting and accelerate incident response.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Less Complexity

SASE enables your business to simplify networking and security by

- Eliminating unnecessary, limited use of siloed point security solutions
- Operating from the cloud to cut operational complexity and cost
- Avoiding logistical issues with shipping, installing, and upgrading multiple networking and security hardware devices to remote branch (or retail) locations

## Consistent Data Protection Everywhere

In a traditional multiprotocol label switching (MPLS) wide area network (WAN), all traffic from branch and retail locations is backhauled to a headquarters or data center location — typically, a headquarters office or on-premises data center. This includes data center and Internet traffic. This basic design architecture eliminates the need for firewalls at branch and retail locations because all traffic can be inspected and a centralized security policy can be enforced by the perimeter firewall at the headquarters or data center location. Of course, this also means that the perimeter firewall can become a bottleneck for the entire enterprise with all traffic flowing through the headquarters or data center.

Consistent data protection is about consolidating data protection policies across every environment and data communication vector. No more disjointed data protection policy and configurations for different SaaS apps, for on-premises repositories, and so on, which cause security blind spots, complex manageability, policy inconsistency, shadow IT, and shadow data. SASE enables a consistent DLP protection policy across every environment where data lives and flows, regardless of its location. New security services and applications with specific security policies can also be rapidly and easily deployed from the cloud to branch and retail locations, instead of having to be individually managed at each location.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Reducing Costs

Organizations may choose to invest in commodity point networking and security products. Although this may initially seem to be a less expensive solution, administrative costs will quickly grow out of control as limited networking and security staff resources must learn different management consoles and operating systems — many of which will potentially have very limited remote management capabilities.

SASE enables organizations to extend the networking and security stack to all their locations in a cost-effective manner via a converged, cloud-delivered solution that fully integrates networking and security capabilities and functions.

## Lower Administrative Time and Effort

Managing multiple point networking and security products from different vendors in a large number of locations is an administrative burden that few organizations can afford. The cost to train and retain networking and security staff on a multitude of point networking and security products will quickly exceed the organization's capital investments for these products.

SASE enables single-pane-of-glass management of networking and security functions for all your locations in a consistent manner, which reduces the administrative burden and helps to lower training and retention costs.

## Reducing Need for Integration

SASE combines multiple networking and security capabilities and functions in a unified cloud-delivered solution, thereby eliminating the need for complex integrations between multiple point networking and security products from different vendors. See Chapter 1 to learn more about the core networking and security capabilities in SASE.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

## Better Network Performance and Reliability

SASE helps organizations improve network performance and reliability for all users and locations by delivering SD-WAN capabilities that enable multiple links from different sources — including MPLS, broadband, Long-Term Evolution (LTE), satellite, and more — to be load balanced, aggregated, and or configured for failover. This helps reduce congestion and latency associated with backhauling Internet traffic across MPLS connections or routing traffic across a connection that is experiencing high utilization or performance issues.

## Greater Agility

Instead of waiting months for MPLS links to be installed, organizations can rapidly connect branch locations using any available Internet connection — such as broadband or LTE — from a local Internet service provider (ISP) with the networking and security capabilities in SASE.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

# Glossary

**acceptable use policy (AUP):** An information security policy that defines appropriate and inappropriate user behavior with respect to content in applications such as web browsing, email, and mobile devices.

**Active Directory (AD):** A directory service developed by Microsoft for identifying and authenticating users on a Microsoft Windows network or application.

**application programming interface (API):** A set of protocols, routines, and tools used to develop and integrate applications.

**asynchronous transfer mode (ATM):** A high-speed, low-latency, packet-switched communications protocol.

**bring your own device (BYOD):** A mobile device policy that permits employees to use their personal mobile devices in the workplace for work-related and personal business.

**California Consumer Privacy Act (CCPA):** A privacy rights and consumer protection statute for residents of California that was enacted in 2018 and became effective on January 1, 2020.

**cloud access security broker (CASB):** Software that monitors activity and enforces security policies on traffic between an organization's users and cloud-based applications and services.

**command-and-control (C2):** Communications traffic between malware and/or compromised systems and an attacker's remote server infrastructure used to send and receive malicious commands or exfiltrate data.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**data loss prevention (DLP):** A data protection strategy to detect the unauthorized storage or transmission of sensitive data.

**direct Internet access (DIA):** A networking strategy to provide broadband Internet access to a remote site. Direct to Internet complements or replaces conventional MPLS hub and spoke topologies. *See also* multiprotocol label switching (MPLS).

**DNS hijacking:** An attack technique that incorrectly resolves DNS queries to redirect victims to malicious sites. Also known as DNS redirection. *See also* Domain Name System (DNS).

**DNS resolver:** A server that relays requests for IP addresses to root and top-level domain servers. *See also* DNS root server, top-level domain (TLD), *and* Domain Name System (DNS).

**DNS root server:** An authoritative name server for a specific TLD in the DNS root zone of the Internet. *See also* top-level domain (TLD) *and* Domain Name System (DNS).

**DNS tunneling:** An attack technique that exploits the DNS protocol to tunnel malware and other data through a network. *See also* Domain Name System (DNS).

**domain generation algorithm (DGA):** A program developed by attackers that generates semi-random domain names so that malware can quickly generate a list of domains that it can use for C2 communications. *See also* command-and-control (C2).

**Domain Name System (DNS):** A hierarchical, decentralized directory service database that converts domain names to IP addresses for computers, services, and other computing resources connected to a network or the Internet.

**exploit:** Software or code that takes advantage of a vulnerability in an operating system or application, and causes unintended behavior in the operating system or application, such as privilege escalation, remote control, or a denial of service.

**Extensible Markup Language (XML):** A human- and machine-readable markup language.

**firewall as a service (FWaaS):** A firewall platform provided as a service offering in a cloud environment.

**General Data Protection Regulation (GDPR):** A European Union law on data protection and privacy for all individuals within the EU and the European Economic Area. The GDPR supersedes the Data Protection Directive (95/46/EC) and became enforceable in 2018.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**Health Insurance Portability and Accountability Act (HIPAA):** U.S. legislation passed in 1996 that, among other things, protects the confidentiality and privacy of protected health information (PHI). *See also* protected health information (PHI).

**hybrid cloud:** An environment that combines a private cloud (internal data center) with resources in the public cloud. *See also* private cloud *and* public cloud.

**infrastructure as a service (IaaS):** A category of cloud computing services in which the customer manages operating systems, applications, compute, storage, and networking, but the underlying physical cloud infrastructure is maintained by the service provider.

**instant messaging (IM):** A type of real-time online chat over the Internet.

**intellectual property (IP):** Includes patents, trademarks, copyrights, and trade secrets.

**Internet Engineering Task Force (IETF):** An international, membership-based, nonprofit organization that develops and promotes voluntary Internet standards.

**Internet Protocol (IP):** The OSI Layer 3 protocol that's the basis of the modern Internet. *See also* Open Systems Interconnection (OSI) model.

**Internet Protocol Security (IPSec):** An IETF open-standard VPN protocol for secure communications over IP-based public and private networks. *See also* Internet Engineering Task Force *and* virtual private network.

**Internet service provider (ISP):** A telecommunications company that provides access to the Internet.

**intrusion prevention system (IPS):** A hardware or software application that both detects and blocks exploits and malicious activity such as C2 traffic. *See also* command-and-control (C2).

**Lightweight Directory Access Protocol (LDAP):** A protocol for accessing directory services, typically used to identify and authenticate users.

**local area network (LAN):** A computer network that connects computers in a relatively small area, such as an office building, warehouse, or residence.

**Long-Term Evolution (LTE):** A type of 4G cellular connection that provides fast connectivity primarily for mobile Internet use.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**malware:** Malicious software or code that typically damages or disables, takes control of, or steals information from a computer system.

**man-in-the-middle attack:** A type of attack where the attacker impersonates a legitimate service in order to intercept and sometimes modify communications.

**mobile device management (MDM):** Software used to manage the administration of mobile devices such as smartphones and tablets.

**multi-cloud:** An environment that consists of multiple types of clouds (such as a public and private cloud, more commonly known as a hybrid cloud), or multiple vendors of the same type of cloud (such as using Amazon Web Services, Google, and Microsoft for public cloud applications). *See also* hybrid cloud, private cloud, *and* public cloud.

**multiprotocol label switching (MPLS):** A method of forwarding packets through a network by using labels inserted between Layer 2 and Layer 3 headers in the packet.

**Open Systems Interconnection (OSI) model:** The seven-layer reference model for networks. The layers are Physical, Data Link, Network, Transport, Session, Presentation, and Application.

**Payment Card Industry Data Security Standard (PCI DSS):** A proprietary information security standard mandated for organizations that handle American Express, Discover, JCB, MasterCard, or Visa payment cards.

**peer-to-peer (P2P):** A distributed application architecture that enables sharing between nodes.

**Personal Information Protection and Electronic Documents Act (PIPEDA):** A Canadian data privacy law that governs how private-sector organizations collect, use, and disclose personal information in the course of conducting commercial business.

**personally identifiable information (PII):** Data (such as name, address, Social Security number, birthdate, place of employment, and so on) that can be used on its own or with other information to identify, contact, or locate a person.

**phishing:** A social engineering cyberattack technique widely used in identity theft crimes. An email, purportedly from a known legitimate business (typically financial institutions, online auction sites, retail stores, and so on), requests the recipient to verify personal information online at a forged or hijacked website.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**platform as a service (PaaS):** A category of cloud computing services in which the customer is provided access to a platform for deploying applications and can manage limited configuration settings, but the operating system, compute, storage, networking, and underlying physical cloud infrastructure is maintained by the service provider.

**private cloud:** A cloud computing deployment model that consists of a cloud infrastructure that is used exclusively by a single organization.

**protected health information (PHI):** Any information about health status, healthcare, or healthcare payments that can be associated with a specific, identifiable individual.

**public cloud:** A cloud computing deployment model that consists of a cloud infrastructure that is open to use by the general public.

**quality of service (QoS):** The ability to prioritize traffic based on operational needs and importance.

**Remote Authentication Dial-in User Service (RADIUS):** An open-source, UDP-based client–server protocol used to authenticate remote users. *See also* User Datagram Protocol (UDP).

**Remote Desktop Protocol (RDP):** A proprietary Microsoft protocol that provides remote access to a computer. RDP uses TCP port 3389 and UDP port 3389 by default. *See also* Transmission Control Protocol (TCP) *and* User Datagram Protocol (UDP).

**secure access service edge (SASE):** Defined by Gartner as "an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FwaaS, and ZTNA) to support the dynamic secure access needs of digital enterprises". *See also* wide-area network (WAN), secure web gateway (SWG), cloud access security broker (CASB), firewall as a service (FWaaS), *and* Zero Trust network access (ZTNA).

**Secure Shell (SSH):** A cryptographic network protocol that provides secure access to a remote computer.

**Secure Sockets Layer (SSL):** A transport layer protocol that provides session-based encryption and authentication for secure communication between clients and servers on the Internet.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**secure web gateway (SWG):** A security platform or service that is designed to maintain visibility in web traffic. Additional functionality may include web content filtering.

**Security Assertion Markup Language (SAML):** An XML-based, open-standard data format for exchanging authentication and authorization credentials between organizations. *See also* Extensible Markup Language (XML).

**service-level agreement (SLA):** Formal minimum performance standards for systems, applications, networks, or services.

**shadow IT:** IT applications and services that are acquired by end users without explicit organizational approval and often without organizational IT knowledge or support.

**social engineering:** A technique for hacking that uses deception to trick the victim into performing an action or revealing sensitive information.

**software as a service (SaaS):** A category of cloud computing services in which the customer is provided access to a hosted application that is maintained by the service provider.

**software-defined perimeter (SDP):** A software-defined perimeter extends access to private applications (either in the data center or the public cloud).

**software-defined wide-area network (SD-WAN):** A newer approach to wide area networking that separates the network control and management processes from the underlying hardware, and makes them available as software.

**top-level domain (TLD):** A domain at the highest (root) level of the DNS of the Internet. Some examples include `.com`, `.edu`, `.gov`, `.net`, `.org`, as well as country code TLDs such as `.us` and `.ca`.

**Transmission Control Protocol (TCP):** A connection-oriented protocol responsible for establishing a connection between two hosts and guaranteeing the delivery of data and packets in the correct order.

**unified threat management (UTM):** A security appliance that combines a number of services such as firewall, anti-malware, and intrusion prevention capabilities into a single platform.

**Uniform Resource Locator (URL):** Commonly known as a *web address.* The unique identifier for any resource connected to the web.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

**User Datagram Protocol (UDP):** A network protocol that doesn't guarantee packet delivery or the order of packet delivery over a network.

**virtual private network (VPN):** An encrypted tunnel that extends a private network over a public network (such as the Internet).

**Voice over Internet Protocol (VoIP):** Telephony protocols that are designed to transport voice communications over TCP/IP networks.

**vulnerability:** A bug or flaw in software that creates a security risk that may be exploited by an attacker.

**wide area network (WAN):** A computer network that spans a wide geographical area and may connect multiple local area networks. *See also* local area network (LAN).

**Zero Trust network access (ZTNA):** A "never trust, always verify" security approach that ensures proper user context through authentication and attribute verification before allowing access to apps and data in the cloud or data center.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Consistent security, everywhere that you need it

You shouldn't have to compromise between speed and security.

Prisma Access by Palo Alto Networks provides the industry's most comprehensive Secure Access Service Edge (SASE), enabling you to securely embrace cloud and mobility.

Learn how Prisma Access provides connectivity and consistent security to mobile users, branch offices and retail locations, with a personal online demonstration.

**https://www.paloaltonetworks.com/company/request-demo**

paloalto® NETWORKS | PRISMA

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

With digital transformation initiatives driving cloud adoption, mobility, and software-defined wide area networks (SD-WANs), the ability for organizations to remain secure and prevent data breaches is becoming difficult. This is especially true when considering that traditional security solutions weren't designed with the cloud in mind, which creates problems with complexity, administrative effort, and incomplete protection. A secure access service edge (SASE) provides connectivity and consistent security to mobile users, branch offices, and retail locations, anywhere in the world.

## Inside…

- Learn what a SASE solution is
- Discover ways to reduce costs and integration nightmares
- Understand how to gain full visibility and control over users, apps, and data
- Identify ways to improve performance and align networking and security
- See how a SASE solution can simplify monitoring and reporting

**Lawrence Miller** served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 150 *For Dummies* books on numerous technology and security topics.

**Go to Dummies.com™**
**for videos, step-by-step photos, how-to articles, or to shop!**

ISBN: 978-1-119-69602-5
Not for resale

9 781119 696025

## WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.

# Managed Detection and Response (MDR)

Managed Detection and Response (MDR) technologies provide continuous threat monitoring, intelligence and threat remediation. As a managed service, MDR experts can quickly identify destructive cyber threats before they cause real damage, providing organizations with real-time access to information on risk, vulnerabilities, remediation activities, configuration exposures, and compliance status.

The information in this section has been created and curated to provide resources around MDR, how it works and how it can help your organization.

CISCO
MDR Whitepaper
Read now

ALERT LOGIC
Bloor Spotlight: MDR Services
Read now

CRITICALSTART
Guide to MDR
Read now

PROFICIO
MDR Checklist
Read now

Contact ePlus for any questions about these technologies, or to discuss your security program.

**eplus.com/security**
**eplus-security@eplus.com**

Cisco
Customer Experience

# Protect what matters most with the best in cybersecurity

Advance your security operations capabilities by reducing mean time to detect and contain threats with Cisco Managed Detection and Response.

Every day we connect more desktops, devices, and things, creating new opportunities for service delivery and business growth. To take advantage of these opportunities, businesses must contend with a growing attack surface and an increasing number of cyberthreats, putting their privacy, data, and reputations on the line.

While these risks can be managed and mitigated with the right expertise, there is currently a significant cybersecurity skills shortage globally that adds to the challenge organizations face.

In fact, by 2021, it is projected there will be 3.5 million vacant cybersecurity positions around the world[1].

The key to minimizing the impact of a data breach is reducing time to detection. Without a focused detection capability, breaches can go undetected for months, by which time your organization’s critical data is likely compromised.

With Cisco® Managed Detection and Response (MDR), you can reduce breach detection and response times and shield yourself from the high costs of security breaches.

## Cybersecurity, managed for you by experts.

Cisco MDR, a managed security service, monitors and detects threats in the network, cloud, and at endpoints with the world's best cybersecurity experts, including:

- **A stronger security posture**, with access to advanced capabilities and experts who understand the expanding attack surface.
- **Greater confidence**, thanks to proven threat intelligence and automation.
- **Faster threat detection** and a more consistent response based on defined investigation and response playbooks supported by Cisco Talos® research.
- **Greater visibility** via integrated security architecture with 24x7x365 threat detection and response, drastically reducing mean time to detect and respond to threats.

## Every 14 seconds

a business falls prey to ransomware[2].

While an overwhelming number of alerts come from security monitoring systems, nearly half of the alerts organizations receive go uninvestigated[3].

With more device usage and greater connectivity than ever before, the attack surface expands and evolves rapidly, meaning the frequency of threats will only increase.

## Faster detection has results

The faster a data breach can be identified and contained, the lower the costs. Breaches with a lifecycle of less than 200 days are, on average, $1.22 million less costly than breaches with a lifecycle of more than 200 days[3].

## 0% cybersecurity unemployment rate

The current cybersecurity unemployment rate is zero percent[1].

The demand for cybersecurity professionals is growing at a faster rate than the supply of qualified candidates. In fact, the lack of cybersecurity skills has been identified by IT professionals (53%) as the most problematic skills shortage in organizations today[4]. As such, recruiting, retaining, and affording high-quality security expertise is among the biggest challenges organizations grapple with today.

# Advance security operations with leading detection and response capabilities

Cisco MDR is delivered by a team of elite researchers, investigators, and responders, and supported by threat intelligence from Cisco Talos Intelligence Group, the largest non-governmental threat intelligence research team in the world.

The service leverages Cisco's world-class, integrated security architecture to advance your security capabilities, providing greater visibility across the network, cloud, and endpoints.

Organizations increase operational capabilities, advancing the security operations center (SOC) by monitoring multi-cloud, network, and endpoints. The service delivers relevant and prioritized actions with expert guidance and effective automated response to protect your business.

## Cisco MDR provides:

- **Detection**, using an integrated cloud security ecosystem that improves mean time to detect and contain security threats. The service delivers relevant, high-confidence and consistent results using proven methodologies, unique intelligence and an experienced team.
- **Analysis** through the enrichment of alerts, including Talos threat intelligence. MDR provides attacker attributes and tactics to analysts with the critical context needed to prioritize the impact and urgency of a threat to a business.
- **Investigation** of identified threats utilizing defined investigation playbooks, which provide added context. When malware, ransomware, bot-net, bad actors and other such bad behavior occurs, we make data-driven decisions that establish relevant, meaningful and prioritized response actions.
- **Response**, which utilizes security orchestration and automated response (SOAR) and case management to execute defined response playbooks and provide detailed threat analysis, including recommended response actions.

# Your security operations with and without Cisco MDR

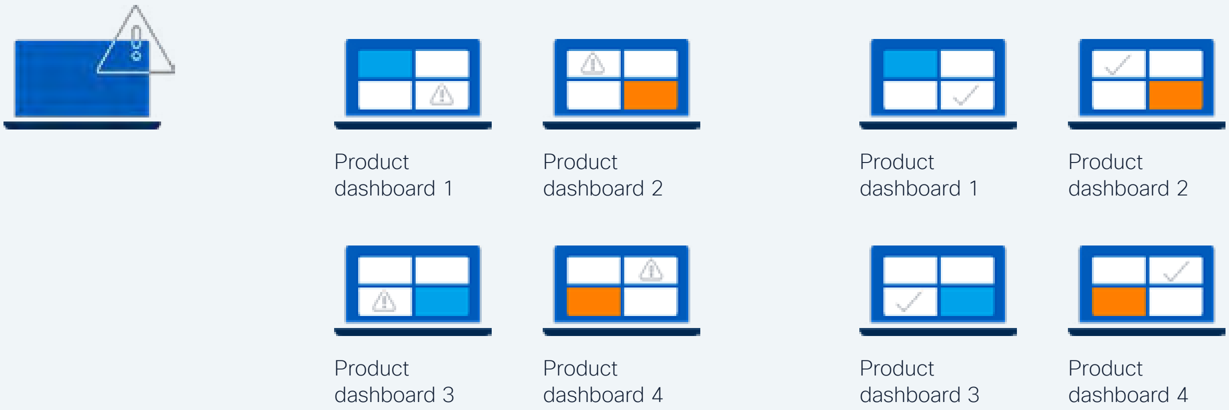
## Before Cisco MDR

Inefficient, error-prone process required manual threat correlation, and performing complex tasks across multiple systems, which could result in missed threats and delayed responses.

1. Alert triggered

2. Investigation in multiple consoles

3. Response/remediation



Product dashboard 1

Product dashboard 2

Product dashboard 3

Product dashboard 4

Product dashboard 1

Product dashboard 2

Product dashboard 3

Product dashboard 4

Industry average time to detect a threat: 206 days[3]

## With Cisco MDR

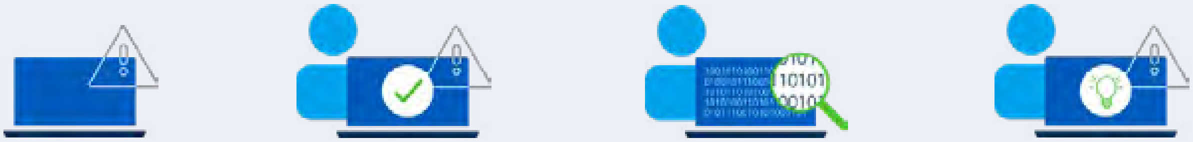
Accelerate detection and response to security threats provided by an integrated security ecosystem, unique threat intelligence, proven case management, deined playbooks, and response recommendations by an elite team of security experts.

1. Alert Triggered

2. Analysis

3. Investigation

4. Response Actions



MDR can reduce the time to detect and respond from months to hours

## MDR leverages Cisco's world-class integrated security architecture

The MDR security architecture consists of Cisco Stealthwatch® Cloud, Advanced Malware Protection (AMP) for Endpoints, Threat Grid, and Umbrella™.

- **Stealthwatch Cloud** applies the latest threat intelligence and analytics capabilities to proactively protect your cloud resources, internal network, and even encrypted traffic against new threats.
- **AMP for Endpoints** correlates Talos threat data against your environment's telemetry data and known behavior, linking your defenses into a single, cohesive shield against emerging malware threats. It continually evolves your endpoint defenses with deep malware analysis, preventing malicious files from spreading.
- **Threat Grid** combines advanced sandboxing with a robust, context-rich malware knowledge base to determine the risk new malware poses to your specific environment and helps prioritize proactive defenses.
- **Cisco Umbrella** enforces security at the DNS and IP layers, blocking threats before they reach the network or endpoints. Under one umbrella, you can extend protection to devices, remote users, and distributed locations anywhere in minutes.

## Healthcare industry example use case

### Challenge

The increasing transition from paper to digital healthcare record-keeping puts patient information and medical records at risk.

### Solution

MDR detects ransomware that can bypass traditional anti-virus defenses, spread laterally, and cripple a hospital's network.

Cisco's expert investigators research the suspicious file access activity and lateral movement attempts throughout the hospital's network.

MDR responds by isolating the host, cleaning the infection, and blocking external command and control servers to prevent any other hosts from being infected.

### Outcomes

The threat is identified early in the kill chain, contained and eliminated within the hospital's network to minimize any potential impact and prevent the threat from successfully performing its objectives.

Advanced security analytics and automation are utilized to deliver alerts with correlated insights and actionable next steps tailored to the hospital's security operational policies.

## Stay protected with Cisco MDR

To protect and grow your business in an increasingly connected world, it is critical to detect security risks and protect your assets. Cisco MDR puts the best in cybersecurity on guard for you 24 hours a day, providing advanced detection and response capabilities with expert resources that understand the expanding and evolving attack landscape.

MDR helps you improve your organization's security posture and advance security operations efficiency with an expert team and industry-leading threat research.

Protect what matters most. Secure your organization today.

1. The 2019 Official Annual Cybersecurity Jobs Report, Cybersecurity Ventures, 2019
2. Ransomware Report, Cybersecurity Ventures, 2017
3. IBM Security and Ponemon Institute 2019 Cost of a Data Breach Study
4. Enterprise Strategy Group Survey, 2018 - 2019

Learn more

cisco.com/go/mdr

## Get in touch.

Contact your Cisco sales representative, partner or visit cisco.com/go/mdr

cisco

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Copyright © 2020, Cisco Systems, Inc. All rights reserved.

Bloor

Spotlight

**Spotlight** Paper by Bloor
Author **Fran Howarth**
Publish date **January 2020**

# Managed detection and response services
## *…key to winning today's security battles*

> “Managed detection and response services will help to bridge security gaps, providing access to advanced technology and skilled resources as and when needed to ensure that organisations can achieve their objectives.”

# Executive summary

Cybersecurity is reliant on a combination of people, processes and technology. Processes are essential for good governance, ensuring that business objectives can be met, risk is adequately managed, and that legal and regulatory requirements are fulfilled. Technology provides the means to ensure that those objectives can be met, and helps the organisation to protect itself from the harm caused by security threats and incidents. People are essential for the smooth operation of that technology.

But, as the threats that we face become ever more sophisticated and complex, the technology deployed to counter those threats has evolved rapidly to the point where it is similarly sophisticated and complex. Many organisations are struggling to make the best use of such technology, hampered by a lack of experienced staff to deploy the technology to its full potential. For many, managed detection and response services will help to bridge that gap, providing access to advanced technology and skilled resources as and when needed to ensure that organisations can achieve their objectives.

This document is intended for security and risk management leaders, and executive decision makers who are looking for the best way to improve their security posture and defeat determined adversaries. It describes how services can help to achieve security goals. A complementary document ***MDR market guide ...reducing the costs and risks of cybersecurity investments*** is available that describes the types of offerings available, features to look for and what best suits your organisation, referring to some of the leading players in this emerging market.

> **“Many organisations are struggling to make the best use of such technology, hampered by a lack of experienced staff to deploy the technology to its full potential.”**

# Introduction

> **Over the past couple of years it has become apparent that organisations are looking for a much higher level of hands-on guidance to augment the capabilities of the security tools that they invest in.**

Virtually every security executive these days laments the situation of facing too many threats, but of having too many disparate tools and not enough people to effectively deal with them. Threats are becoming ever more complex – as are the tools that have been developed to stop them. This is especially true given that it is an uphill struggle to protect networks from threats. It is now widely accepted that threat prevention cannot be guaranteed and the onus has shifted from prevention to detecting threats that have made their way onto the network, where they can cause real damage, and to finding a way to efficiently respond to incidents that have occurred.

## The shift from products to services

These factors – escalating threats, complexity and a shortage of skilled security practitioners – is leading to a shift in the way that security defences are delivered. Technology vendors can no longer just deliver security products to organisations and let them get on with it, albeit with some level of professional help in terms of implementation and tuning, which can alternatively be provided by consultants. Over the past couple of years it has become apparent that organisations are looking for a much higher level of hands-on guidance to augment the capabilities of the security tools that they invest in.

According to Forrester, spending on cybersecurity services outpaced all other investments for the first time in 2018. Today, it estimates that four times more budget is being directed to cybersecurity services than anything else. Gartner estimates that spending on security services will account for 50% of cybersecurity budgets in 2020, estimating that $64.2 billion was spent on security services in 2019. This will not only continue, but rates of spending on security services will grow at rates in the double figures.

## The rise of managed detection and response (MDR) services

Given the challenges that they face, one area in which organisations are particularly looking for help is in detecting and responding to threats—hence, the burgeoning market for managed detection and response services. The 2019 cost of a data breach report from the Ponemon Institute estimates that the average time taken for an organisation to identify and contain a breach on their network is 279 days, which is 4.9% longer than the average for 2018. The longer it takes before a breach can be contained, the greater the potential for damage and the higher the total associated cost. Where the breach is the result of malicious or criminal activity, it takes even longer to identify and contain the threat at an average of 314 days, which adds to costs even further.

In recent research conducted by ESG, 82% of security professionals surveyed agreed that improving threat detection and response is a high priority, yet 76% state this is more difficult to achieve than it was just two years ago owing to the factors stated above. As a result, Gartner estimates that 25% of all organisations will be using MDR services by 2024, up from less than 5% in 2019. IDC estimates that take up is currently greatest among large organisations, finding that 41% of large organisations with more than 5,000 employees are looking to outsource advanced threat detection and response to third parties. However, it also sees an increasing opportunity for midmarket organisations to benefit from such services—especially those that have less mature security operations centres or that lack 24x7 staff coverage to manage complex detection tools. This is echoed by Garter, which estimates that 40% of midmarket organisations will choose MDR as the only managed security services that they use.

# Why should you care?

The World Economic Forum polls private sector organisations worldwide annually to gauge what executives believe to be the greatest risks that they face. In the 2019 report, cyber attacks were cited as the second biggest risk that they face, coming behind only fiscal crises. In the 2018 poll, cyber attacks were seen as just the fifth biggest risk facing business, showing how big and fast growing the problem is becoming.

Digging deeper into the results, cyber attacks are seen in 2019 as the most pressing risk for CEOs in Europe and North America, including six of the ten largest economies in the world. These represent regions that are highly dependent on the use of technology to run their economies and businesses and have also been subject to multiple and notable cybersecurity incidents over the past year, including ransomware that was used to attack prominent industrial and manufacturing companies, as well as breaches of digitised public services. With growing digitisation, cyber attacks are becoming more lucrative for attackers who use an increasing array of sophisticated tools, and more dangerous for victims. The World Economic Forum cautions that detecting, defending against and deterring new cybercrimes is as important as managing known threats.

## A matter for the board

Such are the magnitude of cyber risks that no business can afford to rest on its laurels. Every organisation faces risk, including financial, reputational, operational, environmental, regulatory and legal risks. Now more than ever, security risks need to be added to that list. It needs to be given the same weighting as all other risks and therefore the same level of operational oversight. Cybersecurity risk is not just an IT issue. It needs to be firmly on the agenda of board executives so that it is given the attention that it deserves, security programmes are adequately funded and a culture of security can be driven throughout the organisation. By adequately managing cybersecurity risks, the magnitude of damage can be reduced.

In order to do this, executives with cybersecurity management skills must be hired and given the prominence in the organisation that is needed. This is essential for guiding organisations in the switch in thinking that is required. Such executives will understand that security is more than a compliance tool. Cybersecurity tools can literally save a business – but only if they are operated and managed effectively. The landscape is shifting and savvy business leaders are needed who can help the organisation to move with the times and respond to threats in a quick and efficient manner. They must recognise the change from just investing in tools to procuring expert services that can keep their businesses safe.

## The expanding attack surface and increasing complexity

As businesses are increasingly being driven by technology, control over that technology is being lost. As little as ten years ago, most technology was deployed within the walls – and control – of organisations. The walls of the organisation were once a hardened perimeter where access could be tightly controlled, but that is no longer the case. Organisational networks are increasingly hybrid in nature, bridging in-house technology with the use of public and private cloud services, mobile endpoints and increasingly interconnected tools, such as those that make up industrial networks. This greatly increases the available attack surface for adversaries.

The adoption of new technologies is essential to maintain competitiveness and for digital transformation initiatives that aim to take advantage of the power of digital technologies. But it is not just organisations that are looking to take advantage of the latest advanced technologies. Attackers are increasingly using artificial intelligence and machine learning algorithms to make their attacks more successful, along with increased use of bots to automate their tasks. Organisations need to make use of such technologies themselves and provide greater resilience.

> “…cyber attacks are seen in 2019 as the most pressing risk for CEOs in Europe and North America, including six of the ten largest economies in the world.”

The fear of being hit by a cyber attack or actually experiencing one can galvanise an organisation into action, providing the awareness that is needed for increasing investment in cybersecurity tools. But it also leads to a scramble to invest in point products to solve particular pain points. As many security practitioners will attest, this leaves them struggling to manage too many tools that are often not integrated, preventing them from having visibility over their security posture.

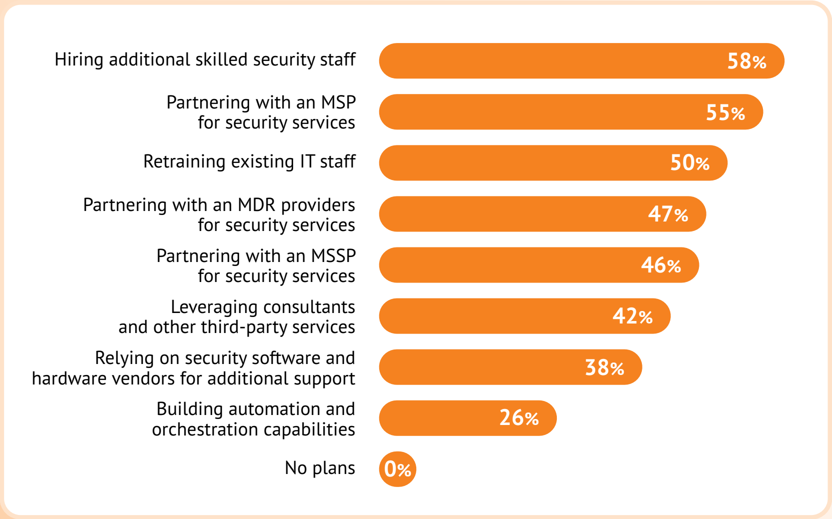


*Figure 1: How are you bridging the skills gap? (Source: 451 Group)*

Given the nature and volume of the threats that they face and the need to adopt new technologies to drive digital transformation, many of the tools that organisations must purchase to bolster security are extremely complex in nature, often needing more knowledge and expertise to handle than the standard tools that were traditionally available and that are no longer sufficient. According to Trend Micro, the security tools that are available today must be able to contextualise and analyse indicators of compromise to dig deeper into what really happened and how. Such technologies must be learnt, deployed, integrated and optimised to be effective, yet 47% of organisations surveyed by FireMon report that they are unable to learn or utilise complex new technologies to their full potential. Technology can only add real value if it can be used effectively.

Many such tools are also expensive to procure, draining already tight budgets. Fairly recently, endpoint detection and response (EDR) technologies have come onto the market to help organisations better detect and respond to threats impacting endpoints, which are a favourite target for attackers. Yet, research by Sophos has found that organisations have struggled to use such tools, with 54% saying that they are unable to get the full benefit from their investments, a figure that cuts across organisations of all sizes.

## Skills shortages a drain on investments

Organisations report that they are finding it a challenge to hire and retain experienced security personnel who understand the new technologies that they wish to implement in order to elevate their cyber defences. Estimates of the global shortfall in skilled security personnel vary, but ISC2 has recently estimated that the number of unfilled security practitioner positions is as high as four million. According to research by the 451 Group, 78% of organisations are facing a skills and expertise gap in security. This is impacting organisations of all sizes, even among the largest enterprises. At the midmarket level, many firms have just a director of security and perhaps one or two security analysts, leaving them with no capacity to deal with alerts, even though this sector tends to see highly targeted attacks.

The ways that organisations are trying to resolve this situation are shown in *Figure 1*, which indicates that many are looking to outsource security functions. However, 58% are still relying on hiring new staff, which is unlikely to lead to a positive change in their circumstances.

Given this situation, is outsourcing security functions a good idea? Will the service provider not be facing the same staffing problems?

According to Trend Micro, skilled incident responders find it more exciting to work for a services firm such as an MDR provider that does hundreds of investigations per year. This is echoed by Cynet, which states that it has no difficulty recruiting staff, but that its customers – especially in financial services, manufacturing, energy and retail sectors – experience great difficulty doing so. F-Secure provides it staff with ample opportunities to spend time on research, leading to a better career path and skills development for them.

> **Organisations report that they are finding it a challenge to hire and retain experienced security personnel who understand the new technologies that they wish to implement in order to elevate their cyber defences.**

### How and why MDR services have evolved

The ability to detect threats hidden deep in networks depends on detailed analysis of log and event data from a wide variety of sources—endpoint, network, cloud and systems attached to the network.

Many organisations have become dependent on security incident and event management (SIEM) systems, but found that they had many limitations in terms of data that it could ingest and therefore analyse, including insider threats and those using remote endpoints as an attack vector.

Advanced analytics and machine learning techniques enable a deeper level of insight to be gained from event data, greatly enhancing the capabilities of such tools. This has led to the development of complementary technologies, including endpoint detection and response (EDR), security orchestration, automation and response (SOAR), user and entity behavioural analytics (UEBA) and network flow analysis. But this also adds greatly to the complexity that organisations must manage.

This complexity, along with the demands placed on short-staffed security operations teams, has meant that not all organisations were able to realise the value of their investments in security tools.

MDR services not only relieve the burdens on organisations, but ensure that they are better able to face up to the threats that they face in an efficient and effective manner. They will help organisations to close security gaps and prevent them from becoming the next salacious headline.

# Why not just go with an MSSP?

The use of managed service providers has been growing rapidly since they came to prominence in the 1990s and continues to grow. It is a form of outsourcing that enables organisations to improve their operations through access to external skills and resources in order to cut expenses. Among the key factors for considering the use of managed service provider are cost, quality of service and avoidance of risk.

Managed security service providers (MSSPs) are used by organisations of all sizes, providing a systematic approach to managing their security needs. They provide services such as round-the-clock monitoring and management in areas that include remote firewall configuration and administration, log management and analytics.

However, the use of MSSPs has its limitations as many of the services offered are generic in nature, being generally limited to the monitoring of security infrastructure. Although many offer a stable of technologies that they can manage on behalf of customers, they are rarely focused on the specific needs of the customer and its particular environment. As such, they are generally unable to offer services such as extensive, tailored forensics, threat research and analytics, being rather focused on detecting known threats such as vulnerability exploits and high volume attacks. They are able to alert customers to anomalies that are detected, but are not able to help customers with prioritising and investigating alerts for anomalies that are uncovered. According to MDR provider Expel, MSSPs offer just another alert feed for organisations that already receive more alerts than they know what to do with.

> “MDR services are designed to go above and beyond the services offered by traditional MSSPs.”

## Enter MDR services

MDR services are designed to go above and beyond the services offered by traditional MSSPs. MSSPs are primarily focused on preventive controls; MDR services are designed to offer proactive detection to enable threats to be more quickly identified and remediation advice and recommendations, providing a much higher level of guidance for organisations for their security needs. Whilst they do provide the 24x7 continuous monitoring of IT assets that MSSPs have traditionally offered, they provide a more specialised level of service that includes alert prioritisation, incident investigation and offensive threat hunting across feeds from endpoint, network, server and cloud data, including the detection of lateral movement across the ecosystem that indicates that a threat has gained a foothold.

A key factor differentiating MDR providers from traditional MSSPs is in the use of the word *“services”.* MDR providers provide organisations with access to advanced technology, whether that be their own, that provided by a partner or controls that an organisation has already invested in, combined with access to a range of expert security professionals that can offer services tailored to an organisation’s specific security needs in the areas of detection and response through direct interaction with the organisation. This is essential for organisations that face difficulties hiring and retaining experienced security practitioners. Through direct interaction with the organisation, an MDR provider’s staff can provide services that are tailored directly to the organisation’s needs, often with a dedicated person assigned to that particular organisation. With this, they provide a high touch, people first approach.

© 2020 Bloor

### What constitutes MDR services?

MDR refers to a threat monitoring, detection, incident analysis and response service. It acts as an extension of an organisation's security operations team, whether as a virtual SOC or auxiliary expertise. MDR services can help an organisation to get the best out of existing technology investments, or help with the deployment and use of best of breed technologies.

MDR services collect telemetry from an organisation's environment, including its network, endpoints, cloud services and user activity, and correlates and analyses it in conjunction with threat intelligence services. Working not only in a reactive mode, threat hunting services can use offensive security techniques to proactively uncover hidden and unknown threats.

Experts from the service provider can then help the organisation to define and execute the best response to threats, events and incidents uncovered. Automation and orchestration capabilities are required for the most efficient and effective response. Other aspects that are routinely part of MDR services include machine learning, user behaviour and big data analytics.

> **“Through direct interaction with the organisation, an MDR provider's staff can provide services that are tailored directly to the organisation's needs, often with a dedicated person assigned to that particular organisation.”**

# Benefits of MDR services

Many of the technology tools that have been developed for dealing with complex, sophisticated security threats and incidents are expensive to purchase, implement and maintain, and require customisation to meet the specific requirements of an organisation. This requires advanced skills that most organisations do not have at their disposal.

MDR services provide access to a team of experts at a price that organisations can afford and enable them not only to better detect and analyse threats, but to stop them in their tracks before extensive damage can be done. They will provide much greater peace of mind for organisations that are struggling to keep their houses in order, offering a cost-effective adjunct to in-house capabilities to help improve the security posture of any organisation.

> “MDR services provide access to a team of experts at a price that organisations can afford and enable them not only to better detect and analyse threats, but to stop them in their tracks before extensive damage can be done.”

© 2020 Bloor

# Summary

Today's sophisticated and complex security threats require a swift, coordinated response by their victims. For many years, organisations have relied on an arsenal of technology in order to outgun their adversaries. As those tools multiply and deploy ever more advanced techniques in an effort to stay ahead, many organisations are finding themselves playing a game of catch up with the limited resources that they have at their disposal to handle them. MDR services provide an attractive alternative, giving access to expertise as and when needed to stack the odds in their favour in terms of detecting and responding to threats. Whatever the size or needs of an organisation are, MDR services could provide the lifeline that they need to stay afloat.

> **“Whatever the size or needs of an organisation are, MDR services could provide the lifeline that they need to stay afloat.”**

**FURTHER INFORMATION**
Further information about this subject is available from
***https://www.bloorresearch.com/2020/03/what-is-mdr-and-why-is-it-needed/***

## About the author

**FRAN HOWARTH**
**Practice Leader, Security**

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including ***Silicon***, ***Computer Weekly***, ***Computer Reseller News***, ***IT-Analysis*** and ***Computing Magazine***. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of ***InfoToday***.

© 2020 Bloor

## Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of ***Mutable*** business Evolution is Essential to your success.

***We'll show you the future and help you deliver it.***

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

## Copyright and disclaimer

This document is copyright **© 2020 Bloor**. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

tel: **+44 (0)1494 291 992**
web: **www.Bloorresearch.com**
email: **info@Bloorresearch.com**

CRITICALSTART™

# Guide to Managed Detection & Response

## Deploy an MDR Platform That Can Protect Any Business

CRITICALSTART

# Executive Summary

Managed Detection and Response is reinventing information security. In this paper, you will learn how it provides far better visibility into threats and enables an active, real-time response to mitigate any impact. We'll discuss what to look for in an MDR provider and—most importantly—why every alert matters.

## Topics Include:

- The business case for managed services
- How MDR provides better protection in today's environment
- The right questions to ask an MDR service provider
- How to know if the MDR you're considering is really MDR
- Why every alert should be treated equally
- What kind of real-world results can you expect through a solid approach to MDR

CRITICALSTART

© 2020 CRITICALSTART. All rights reserved.

# The Imperative for Managed Services

Our world is increasingly digital. Ten years ago, just under 30 percent of the population was online. In June 2020, that number stood at almost 60 percent. And as 2020 witnesses a dramatic shift to a remote workforce, the prevalence of online attacks is ever present. According to the 2020 Cost of a Data Breach Report, 76% of respondents at organizations that shifted to remote work expect that working from home could increase the time it takes to identify and contain a data breach. 70% of respondents expect remote working could increase the cost of a data breach.

## But Here's the Real Challenge:

The same report found that remote work could result in costs that were nearly $137,000 higher than the global average of $3.86 million and respondents estimated that the shortage of security skills increased costs by an average of $257,000.

Contributing to this cost is the effort and expense of deploying a Security Operations Center (SOC). If an organization tries to respond to threats by building this capability internally, an internal SOC can cost a minimum of $750,000 in employee salaries alone.

## Calculating the Cost of Digital Security

Need to determine the cost of security analysts to protect your infrastructure? Consider the following:

An average endpoint generates **5000** security alerts per year

+

2000 endpoints generate **10,000,000 alerts annually**

+

A security analyst takes an average **15-30 minutes to investigate one alert**

+

Investigating only the alerts classified as “high” or “critical” would require **hiring 21-22 analysts**

=

An average analyst's salary is $35/hr., so those 21-22 analysts would require an investment of over **$1.5 million annually.**

For more information on calculating the cost of your own SOC, review our Total Cost of Ownership eBook.

CRITICALSTART

© 2020 CRITICALSTART. All rights reserved.

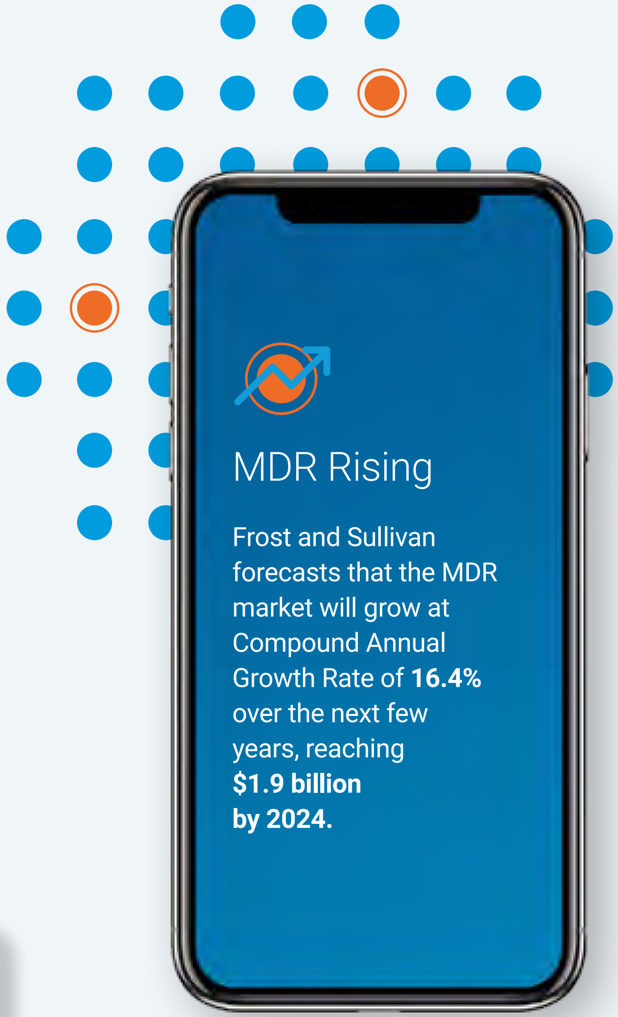
# MDR Lifts the Security Burden

Managed Detection and Response (MDR) is where many firms are turning to protect their business and alleviate staffing and technology concerns. By working with a security partner that utilizes their own analysts, tools, threat identification strategies and procedures to be proactive in responding to cyberattacks, damage from these attacks can be effectively mitigated for far less cost than an internal solution.

## First, is the Consideration of Tools

MDR often utilizes artificial intelligence (AI) to prioritize alerts, consolidating everything onto one platform to provide comprehensive visibility to the SOC. Analysts can then decide on the alerts that represent a security threat and respond with direct action, such as isolating an endpoint, changing passwords, or whatever action in necessary to prevent the attack from moving within the network.

MDR is the latest evolution to protect organizations from a highly-diverse, multifaceted threat environment, including everything from individual hackers to nation states. But perhaps its most important benefit is that a company can access the latest security expertise without hiring internally, and available resources can grow with the business without the need to add additional personnel.



### MDR Rising

Frost and Sullivan forecasts that the MDR market will grow at Compound Annual Growth Rate of **16.4%** over the next few years, reaching **$1.9 billion by 2024.**

For more information on calculating the  cost on your own SOC, review our Total Cost of Ownership eBook.

© 2020 CRITICALSTART. All rights reserved.

# How to Select an MDR Partner

The essential key in selecting an MDR vendor is to realize that not all are created equal. Consider asking a potential vendor these questions as indicators of how they will perform when your organization is facing a threat:

How long does your team take to respond to alerts? Are there contractual obligations around this?

Will my company have access to your SOC as needed or is that an additional charge?

Is there any hardware associated with this tool?

If my company grows quickly can the MDR tool you're using scale quickly?

Can this tool help me respond to both SIEM and EDR from one console?

Can we investigate and respond to alerts natively from our phones?

## Key Takeaway

The last two questions are particularly important, as they can determine what kind of control and visibility you will have in determining the direction of your new security environment. Information on alerts needs to be accessible in one platform on any device you use to do business. It should be accessible at any time and place to ensure critical threat and response information is always available as it happens.

CRITICALSTART

© 2020 CRITICALSTART. All rights reserved.

# Qualities you might look for in an MDR Partner

| Requirement | Ability to Provide? | |
|---|---|---|
| Contractual refunds based on missed-SLA's | Yes | No |
| Access to the comments, rules, audit logs, and people working on alerts | Yes | No |
| 50% or greater employee owned business | Yes | No |
| Actively contributes zero day research in excess of 20+ zero days/year | Yes | No |
| Service provides metrics for effectiveness | Yes | No |
| Ability to collaborate/talk to analysts, investigate endpoints, and isolate, if required, from mobile device | Yes | No |
| SOAR vs SIEM based approach | Yes | No |
| 24/7 capabilities | Yes | No |
| US-based SOC | Yes | No |
| SOC retention rate of 100% over 3+ years | Yes | No |
| Investigate every alert looking for known good events against a database of known good behaviour / Auto-resolves known good behaviour | Yes | No |
| Can leverage multiple endpoint solutions / Service is not tied to one technology manufacturer | Yes | No |
| A trusted-behaviour-orientated method of handling false positives (not a resource-, input-, or priority-orientated method) | Yes | No |
| Ability to review activity for investigated alerts that are not forwarded  to client | Yes | No |
| Provider has positive cash flow | Yes | No |
| Less than 1.5% voluntary turnover on executive leadership over 3+ years | Yes | No |
| Cyber security is the primary business focus, not a tangential business unit | Yes | No |

CRITICALSTART

© 2020 CRITICALSTART. All rights reserved.

# Is it Really MDR?

As you're evaluating solutions, it's important to determine if what you're evaluating is a Managed Security Service Provider (MSSP) or true MDR. An MSSP takes incident and event data and monitors it 24 x 7. But an MSSP can be overly broad and does not dive deeply into the underlying causes of alerts. MDRs use their own SOC, security processes and infrastructure to really absorb alert information and uncover the hidden reasons behind them. Effective MDRs also have a much deeper and more sophisticated response plan in place to identify both vulnerabilities and threats, and then they take a dynamic response to resolving those issues.

# Endpoint or SIEM?

Exactly what information should be fed into an MDR process is an interesting question. Many providers simply ingest data from Endpoint Detection and Response tools. These tools primarily search for advanced threats on endpoints, with activities such as registry monitoring, searching for modifications to file structures and validating signatures. The behavioral analysis ability of these tools also provides a capability for forensics during incident response.

But to be truly effective, MDR must process a wider depth and breadth of information. Data from Security Incident and Event Management (SIEM) tools is also essential, as it can identify, monitor, record and analyze security events in real-time. It provides a comprehensive and centralized view of the entire security scenario of an IT infrastructure. It can provide correlation to offer context on data and to create relationships based on predefined rules, architecture or alerts. It's also adaptable to different vendors, sources of information and data formats. While many companies neglect SIEM, or relegate it to log collection and compliance needs, any MDR approach must be comprehensive enough to make use of all the robust capabilities that SIEM has to offer.

CRITICALSTART

© 2020 CRITICALSTART. All rights reserved.

# Treat Every Alert as Critical

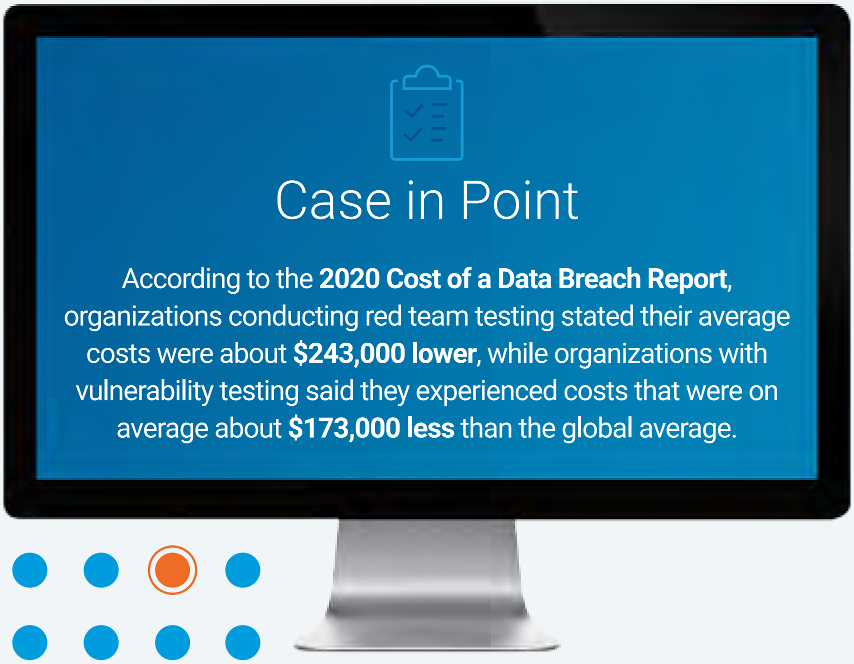
The most essential component of any successful MDR provider is that every alert collected must be treated equally. With thousands of alerts pouring in from EDR and SIEM tools, many vendors will actually disable detection logic to prevent alerts that they feel do not require attention. Others may rank alerts by categories such as critical, high, medium, low or informational, and only focus on the alerts that appear critical, (or maybe high if they have the time.)

The problem is that attackers are increasingly being detected through a SIEM platform appearing through medium, low and even informational alerts. A top-down approach to dealing with alerts is simply not sufficient in today's threat environment.

> A far more effective strategy is to use a trust-oriented approach to handling alerts at scale. An MDR vendor should work with their client to build a Trusted Behavior Registry (TBR) to determine which alerts indicate normal behavior and can be trusted. Resources can then focus on the alerts outside of this registry,  regardless of how threatening they may appear at first.

# Going the Extra Mile

An MDR provider should also be fluent in all vulnerability detection, threat identification and active mitigation strategies. These include intrusion detection systems (IDS) and intrusion prevention systems (IPS), threat hunting and SOC services. They must be able to analyze an environment and make recommendations on the right tools for the job. And these recommendations must not be limited to what the vendor is comfortable with, but instead focus on the needs of the client. This includes supporting implementation, optimization and monitoring to ensure that all tools work together in concert to deliver maximized efficiency and protection.



## Case in Point

According to the **2020 Cost of a Data Breach Report**, organizations conducting red team testing stated their average costs were about **$243,000 lower**, while organizations with vulnerability testing said they experienced costs that were on average about **$173,000 less** than the global average.

CRITICALSTART

© 2020 CRITICALSTART. All rights reserved.

# How to Measure Success

When working with an MDR provider, if they have the right team, tools, methodology and process to protect your organization, then **over 99 percent of security alerts should be resolved effectively**.

We've also found that many companies accept dwell times, or the time from when an incident is first detected to the final resolution, of 100 days or more. With the right MDR in place, we've found that **dwell time should be 22 minutes on average**.

## How CRITICAL**START** Achieves These Types of Results

The CRITICAL**START** approach to MDR achieves results by following all of the highly-successful strategies outlined in this paper, and through an industry-first combination of the following:

**Resolution of every alert**

A zero-trust policy toward alerts, by building a **trusted, known-good registry**

**100 percent transparency** for client teams, including the industry's first MOBILE**SOC** where you can remotely resolve and remediate endpoints, and collaborate with SOC analysts with full audit trails

Integration with industry-leading security tools including:

Microsoft Defender Advanced Threat Protection

SentinelOne

DEVO

CROWDSTRIKE

splunk>

CORTEX BY PALO ALTO NETWORKS

vmware Carbon Black

BlackBerry

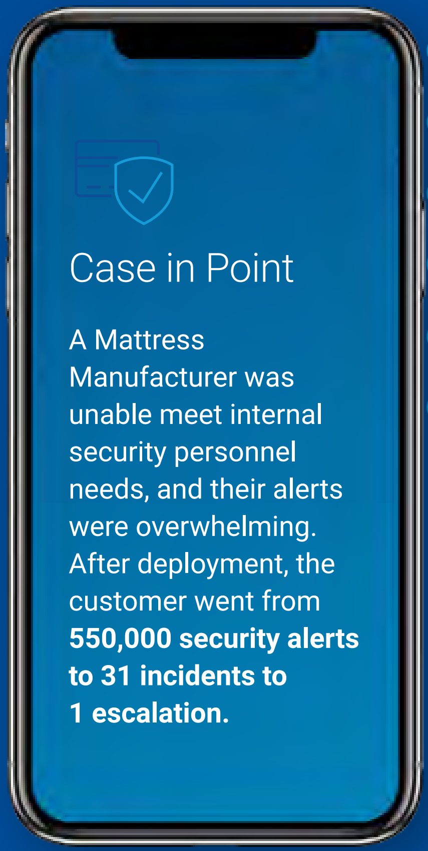
CRITICAL**START**

© 2020 CRITICAL**START**. All rights reserved.

# CRITICALSTART Delivers:

We support a **State Information Technology Provider** with **30,000 Endpoints through MDR** that provides a single correlated view and active response services to threats.

We enable an **International Energy Infrastructure Provider** to present a strong united cybersecurity front with the least amount of user and business obstructions through deep API Integration of their tools, **24x7x365 monitoring, and robust analytics.**



## Case in Point

A Mattress Manufacturer was unable meet internal security personnel needs, and their alerts were overwhelming. After deployment, the customer went from **550,000 security alerts to 31 incidents to 1 escalation.**

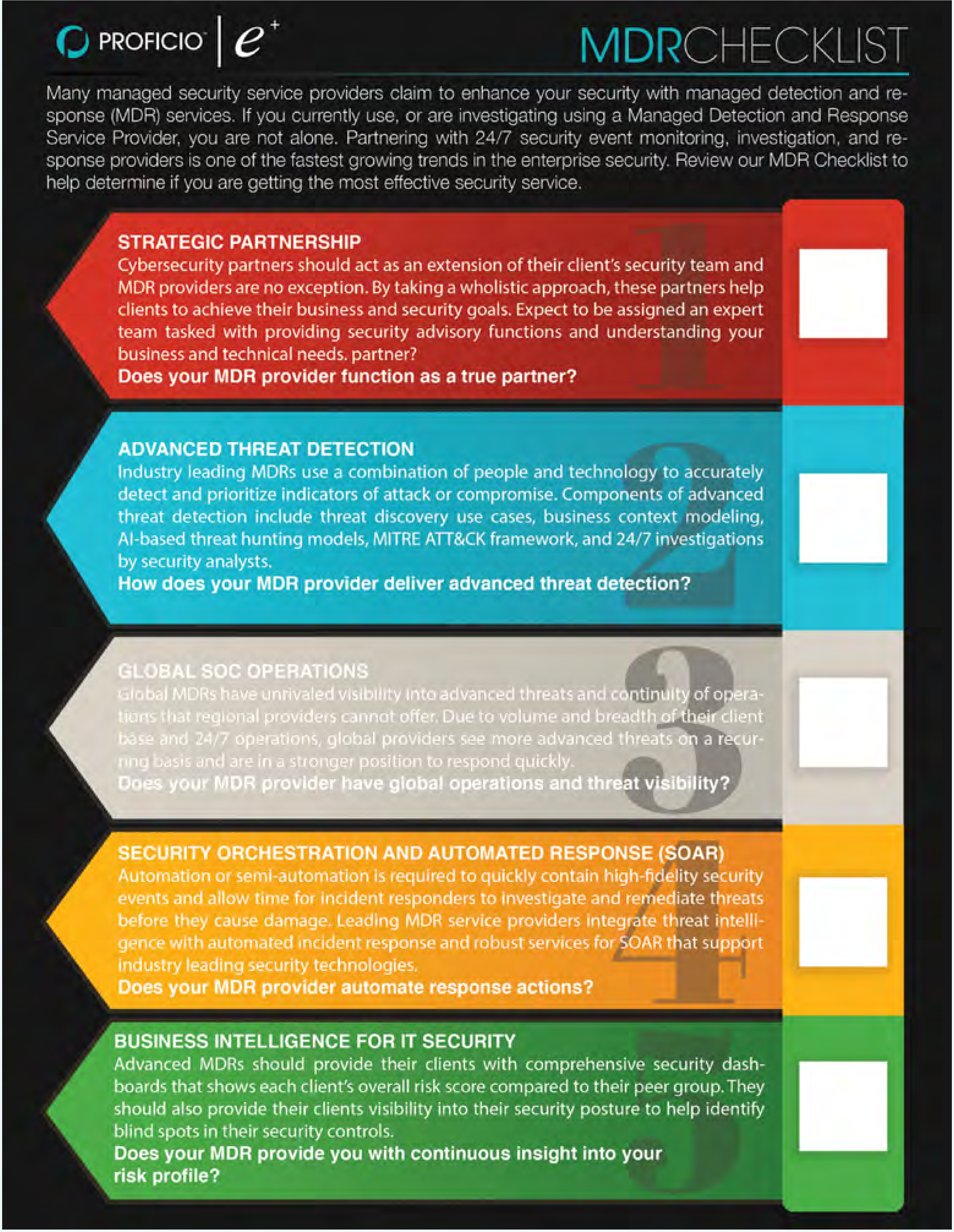
## Ready to Learn More?

This overview is meant as a primer to guide your MDR decisions, but it's only the first step. Contact a CRITICALSTART representative so we can learn about your unique security situation and how we can customize our MDR platform to help you resolve every alert and shut down any vulnerabilities your business may be facing.

**To see how we can help, contact us at criticalstart.com/contact**

CRITICALSTART

© 2020 CRITICALSTART. All rights reserved.



PROFICIO | e+

# MDRCHECKLIST

Many managed security service providers claim to enhance your security with managed detection and response (MDR) services. If you currently use, or are investigating using a Managed Detection and Response Service Provider, you are not alone. Partnering with 24/7 security event monitoring, investigation, and response providers is one of the fastest growing trends in the enterprise security. Review our MDR Checklist to help determine if you are getting the most effective security service.

## 1 STRATEGIC PARTNERSHIP

Cybersecurity partners should act as an extension of their client's security team and MDR providers are no exception. By taking a wholistic approach, these partners help clients to achieve their business and security goals. Expect to be assigned an expert team tasked with providing security advisory functions and understanding your business and technical needs. partner?

**Does your MDR provider function as a true partner?** □

## 2 ADVANCED THREAT DETECTION

Industry leading MDRs use a combination of people and technology to accurately detect and prioritize indicators of attack or compromise. Components of advanced threat detection include threat discovery use cases, business context modeling, AI-based threat hunting models, MITRE ATT&CK framework, and 24/7 investigations by security analysts.

**How does your MDR provider deliver advanced threat detection?** □

## 3 GLOBAL SOC OPERATIONS

Global MDRs have unrivaled visibility into advanced threats and continuity of operations that regional providers cannot offer. Due to volume and breadth of their client base and 24/7 operations, global providers see more advanced threats on a recurring basis and are in a stronger position to respond quickly.

**Does your MDR provider have global operations and threat visibility?** □

## 4 SECURITY ORCHESTRATION AND AUTOMATED RESPONSE (SOAR)

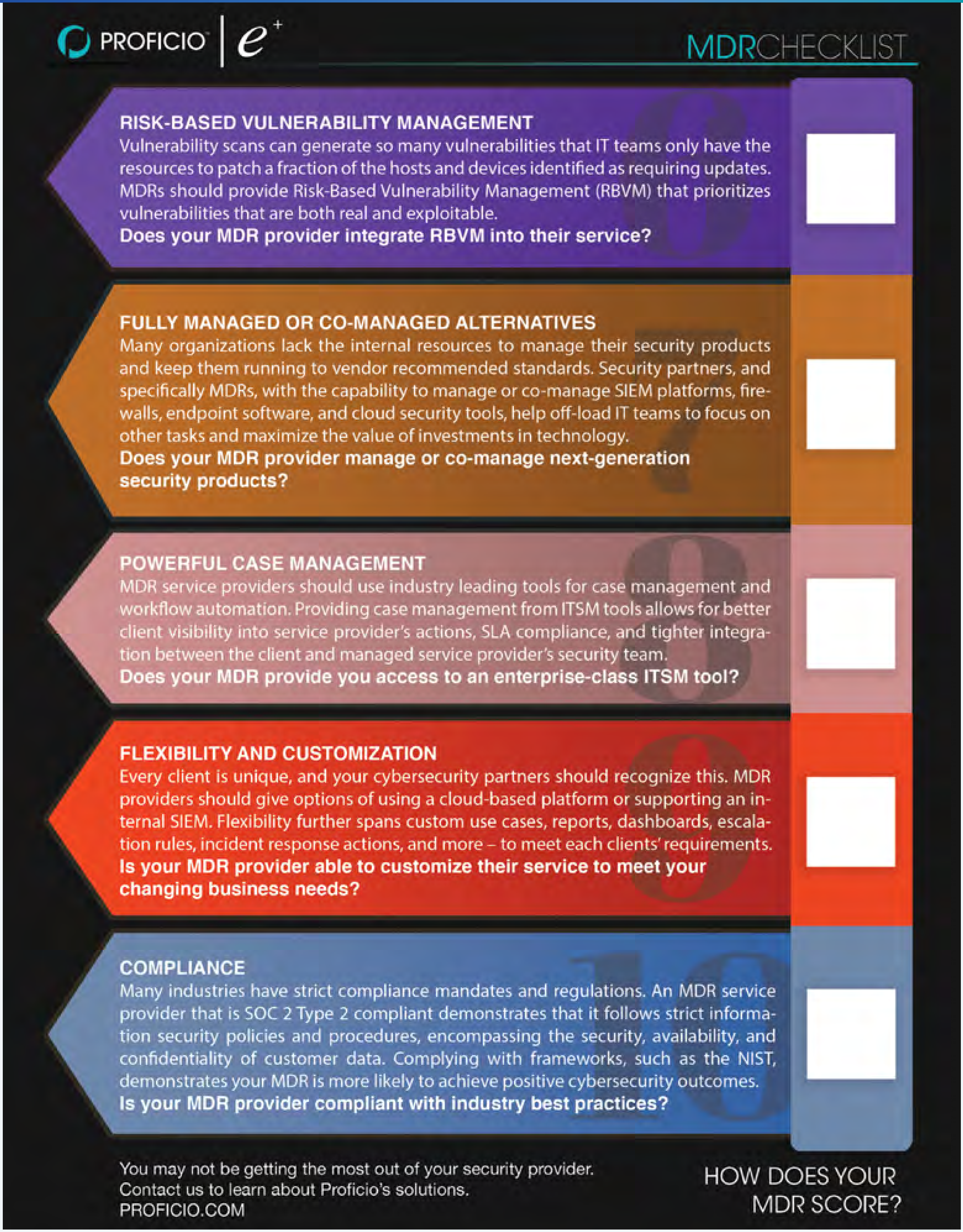
Automation or semi-automation is required to quickly contain high-fidelity security events and allow time for incident responders to investigate and remediate threats before they cause damage. Leading MDR service providers integrate threat intelligence with automated incident response and robust services for SOAR that support industry leading security technologies.

**Does your MDR provider automate response actions?** □

## 5 BUSINESS INTELLIGENCE FOR IT SECURITY

Advanced MDRs should provide their clients with comprehensive security dashboards that shows each client's overall risk score compared to their peer group. They should also provide their clients visibility into their security posture to help identify blind spots in their security controls.

**Does your MDR provide you with continuous insight into your risk profile?** □



PROFICIO | e+

# MDRCHECKLIST

## 6 RISK-BASED VULNERABILITY MANAGEMENT

Vulnerability scans can generate so many vulnerabilities that IT teams only have the resources to patch a fraction of the hosts and devices identified as requiring updates. MDRs should provide Risk-Based Vulnerability Management (RBVM) that prioritizes vulnerabilities that are both real and exploitable.

**Does your MDR provider integrate RBVM into their service?** □

## 7 FULLY MANAGED OR CO-MANAGED ALTERNATIVES

Many organizations lack the internal resources to manage their security products and keep them running to vendor recommended standards. Security partners, and specifically MDRs, with the capability to manage or co-manage SIEM platforms, firewalls, endpoint software, and cloud security tools, help off-load IT teams to focus on other tasks and maximize the value of investments in technology.

**Does your MDR provider manage or co-manage next-generation security products?** □

## 8 POWERFUL CASE MANAGEMENT

MDR service providers should use industry leading tools for case management and workflow automation. Providing case management from ITSM tools allows for better client visibility into service provider's actions, SLA compliance, and tighter integration between the client and managed service provider's security team.

**Does your MDR provide you access to an enterprise-class ITSM tool?** □

## 9 FLEXIBILITY AND CUSTOMIZATION

Every client is unique, and your cybersecurity partners should recognize this. MDR providers should give options of using a cloud-based platform or supporting an internal SIEM. Flexibility further spans custom use cases, reports, dashboards, escalation rules, incident response actions, and more – to meet each clients' requirements.

**Is your MDR provider able to customize their service to meet your changing business needs?** □

## 10 COMPLIANCE

Many industries have strict compliance mandates and regulations. An MDR service provider that is SOC 2 Type 2 compliant demonstrates that it follows strict information security policies and procedures, encompassing the security, availability, and confidentiality of customer data. Complying with frameworks, such as the NIST, demonstrates your MDR is more likely to achieve positive cybersecurity outcomes.

**Is your MDR provider compliant with industry best practices?** □

You may not be getting the most out of your security provider.
Contact us to learn about Proficio's solutions.
PROFICIO.COM

HOW DOES YOUR
MDR SCORE?

# Secure Teleworker Solutions

Now more than ever organizations are leveraging workforces that are operating from remote locations – including employee homes. This introduces many new points of entry for cyber attacks, including additional wireless networks connecting into the corporate hub – not to mention an exponential increase in devices – from laptops to tablets and mobile phones. Add to this a substantial increase in cloud usage – to accommodate regular data traffic as well as disaster recovery and back-up – and you've created a swirling vortex of additional weak points that can be exploited. For this reason, it has become critically important to ensure your security program accounts for not only endpoints, but all of these additional entry-points to your network, as well as the data paths connecting them.

There are many tools available to enable you to create a secure remote environment for your teleworkers. We have included a helpful set of information resources in this section that can help you navigate some of the available options – and start enhancing the protocols you have in place to accommodate a largely remote workforce.

CISCO

Secure Remote Workers Whitepaper

Read now

FORTINET

Designing a Secure Telework Program

Read now

Gigamon®

When Networks Meet the New Tomorrow

Read now

JUNIPER NETWORKS

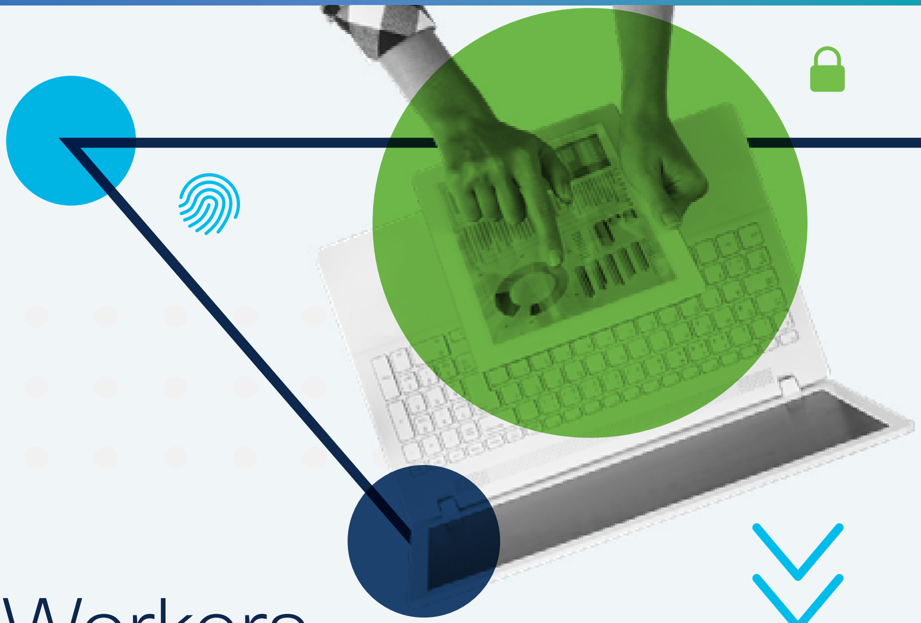
Enterprise at Home Infographic

Read now

Contact ePlus for any questions about these technologies, or to discuss your security program.

**eplus.com/security**
**eplus-security@eplus.com**

cisco Secure



# Secure Remote Workers

Cisco wants to help your employees work remotely and securely. Right now, the abrupt shift towards massively supporting remote workers creates a series of security challenges – keeping your business running in a very different environment or at a greater scale than ever before. This is putting a sudden strain on both your security and IT teams who are being tasked with quickly providing support for an unprecedented number of offsite workers and their devices – without compromising security.

Taking into account this new reality, you need a simple and easy way to secure remote workers at the speed and the scale of your business. The Cisco Secure Remote Worker solution unifies user and device protection at scale, making it easy to verify, enable secure access and defend remote workers at anytime from anywhere. This integrated solution helps accelerate your business success with security that works together, delivering the power of three: Cisco Duo, AnyConnect and Umbrella.

## Duo

verifies the identity of all users before granting access to corporate applications.

Learn more

## AnyConnect

enables secure access to the enterprise network for any user, from any device, at any time, in any location.

Learn more

## Umbrella

provides the first line of defense against threats on the internet wherever users go.

Learn more

Get started with the integrated Cisco Secure Remote Worker that is part of Cisco SecureX platform built for the security needs of today and tomorrow.

© 2020 Cisco and/or its affiliates. All rights reserved.

cisco Secure

# Cisco Secure Remote Worker Offer Sign Up & Program Details

## Duo

**Current Duo Customers**

Allow customers to add unlimited additional users during offer period

**New Customer**

30-day evaluation with unlimited users, after which the customer will need to purchase 10% of the current user population for 1 year and allow customer to add unlimited users during the offer period only

signup.duo.com

## AnyConnect/Next Generation Firewall

**Current AnyConnect Customers**

Allow customers to install additional users beyond their purchased limit during offer period

**Current ASA/Firepower Customers Without AnyConnect**

90-day evaluation of AnyConnect

**New to AnyConnect**

Significant discount program for ASAv30

90-day evaluation of AnyConnect

**More Information**

www.cisco.com/go/anyconnect

## Umbrella

**Current Umbrella Customers**

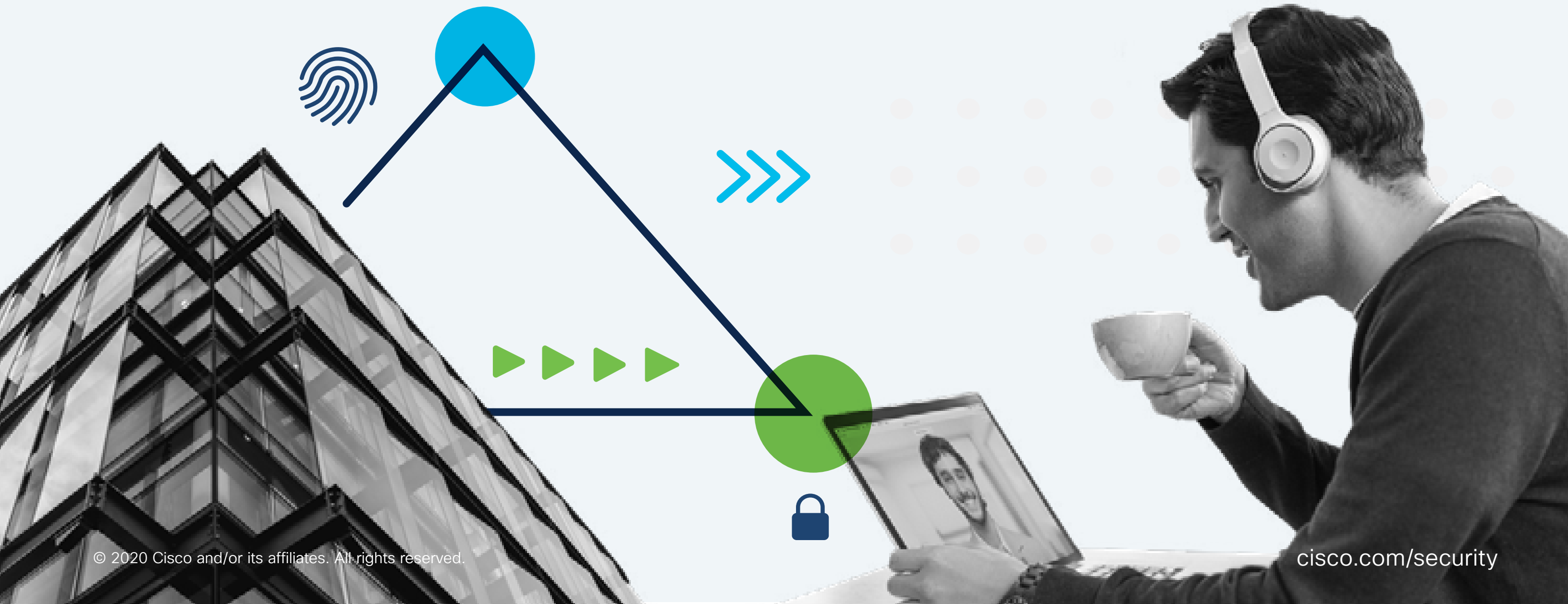
Ability to exceed purchase user count during offer period

**New Customer**

90-day evaluation of Umbrella DNS Advanced or SIG

signup.umbrella.com

Ask your Cisco sales representative for more information



© 2020 Cisco and/or its affiliates. All rights reserved.

cisco.com/security

FORTINET®

# Identifying Security Requirements for Supporting a Remote Workforce at Scale

## Designing a Secure Telework Program

# Table of Contents

FURTINET

## Executive Overview

Organizations should support telework as a component of their business continuity plan, which requires the ability to rapidly transition to a partly or wholly remote workforce. Doing so creates new networking and security challenges for an organization since the company network is being used in a very different way from on-site employees.

Securing a remote workforce requires identifying and deploying security solutions that meet the needs of the employees and the headquarters network. The majority of employees only need secure access to the corporate network and cloud-based applications, which requires VPN access and multi-factor authentication (MFA). Network administrators and executives may have additional network requirements, such as persistent connectivity and a secure telephony solution. The organization's headquarters network must also be capable of supporting and securing the network connections coming from the vast majority of an organization's workforce, requiring robust user authentication and advanced perimeter security.

## Introduction

The ability to support remote workers can help improve an organization’s business continuity plan. It allows the organization to adapt when unforeseen circumstances, such as natural disasters or a pandemic, make it impossible for employees to work on-site.

Under these circumstances, an organization may be forced to rapidly transition to a mostly or wholly remote workforce. When designing or implementing a telework solution, it is important to consider not only networking requirements but also the additional security concerns created by remote work.

## Meeting Basic Telework Requirements

Employees may have different requirements of their remote work environment. However, all teleworkers have a set of basic requirements to ensure that they have a secure, authenticated connection to the enterprise network. These include access to a virtual private network (VPN) and a strong authentication solution to protect accounts from compromise.

### Virtual Private Networking

When teleworking, an employee will be processing sensitive company data on their home network. Protecting this data against compromise requires the ability to ensure that a teleworker's connection to the company network is secure.

Teleworkers must have access to a VPN that provides direct and encrypted connectivity between their machine and the corporate network. This not only protects the confidentiality and integrity of sensitive company data in transit but also ensures that all traffic between the employee and the public internet is monitored and protected by the organization's existing cybersecurity infrastructure.

### Multi-factor Authentication

With employees working from home, there is an increased probability that stolen login credentials, combined with access to an unattended machine, could enable unauthorized access to a user's account. In these situations, many of the features used to detect anomalous access patterns, such as the location and time of the authentication attempt, may not be applicable as employees' work patterns shift due to working from a home office.

Securing access to the corporate network, resources, and data requires a more robust authentication solution than traditional usernames and passwords. All teleworkers should be issued a secure authentication token. Options for MFA tokens include physical devices such as a key fob or software-based solutions such as a mobile application, which can be used to verify a user's identify before they are able to initiate a VPN connection to the corporate network or access other sensitive company resources.

**PCI DSS guidance for remote work requires that employees accessing cardholder data authenticate via a VPN and use multi-factor authentication.[1]**

## Supporting Remote Power Users

While many teleworkers can get by with a VPN connection and an MFA token, others have additional requirements. Power users, including network administrators and executives, require a more advanced remote office to perform their core job duties. These users may need persistent connectivity to the enterprise network and a secure telephony solution.

### Persistent Connectivity

Some users, such as network administrators and security personnel, require more flexible and persistent access to the corporate network. These employees may have multiple devices that must be connected to the company network or require long-lived connectivity not limited by automatic session timeouts.

The requirements of power users working from a home office can be satisfied by the deployment of a wireless access point, which can provide a reliable VPN tunnel to the corporate network. In order to ensure a secure connection, this wireless access point should be combined with a desktop-based next-generation firewall (NGFW) to provide traffic inspection, access management, and advanced threat protection.

## Secure Telephony

When working remotely, it is essential that staff members—especially executives—have access to a secure telephony solution in order to protect sensitive communications and company data. Otherwise, a company risks exposure of sensitive data due to eavesdropping on cellular networks or using malicious mobile applications.

An effective way to provide secure telephony to off-site workers is to leverage Voice-over-IP (VoIP) communications. If a user already has access to a secure, persistent, and reliable internet connection, then routing their voice traffic over this connection requires minimal additional overhead. This also enables the organization to monitor voice traffic and scan it at the network perimeter for potentially malicious content intended to exploit vulnerable VoIP software.

Telephony solutions for teleworkers should provide them with all of the features of their on-site business phones. This minimizes the probability that workers will use personal devices for business communications. Important options include the ability to make and receive calls, access voicemail, check call history, and access the organization’s telephone directory.

**72% of a CEO’s workday is spent in meetings, making secure telecommunications essential for their remote offices.**[2]

## Headend Security and Stability

Security solutions for a remote workforce are not limited to the client side. An increased number of teleworkers introduce new security threats and network requirements at the organization's headquarters as well.

When designing a telework program to ensure business continuity, it is essential to ensure that the headquarters network is capable of authenticating users and devices attempting to access it remotely and managing and securing a much larger number of inbound VPN connections.

### Authenticating Users and Devices

A zero-trust security model is very important when an organization is supporting a mostly or wholly remote workforce. Employees may attempt to connect to the company network using unknown or personal devices, and systems connected to untrusted networks have a greater probability of being compromised by cyber-threat actors.

Securing the organization's network and the sensitive data and resources that it contains requires the ability to authenticate users and devices attempting to connect to it. This can be accomplished by using a centralized authentication server with connectivity to the organization's active directory, Lightweight Directory Access Protocol (LDAP), and Remote Authentication Dial-In User Service (RADIUS).

This server should be capable of scaling to meet the needs of a larger remote workforce without hampering user productivity. Support for single sign-on (SSO), certificate management, and guest management also ensures user authentication without creating a significant burden for remote employees.

### Securing the Network Perimeter

One difference between an on-site and remote workforce is the number of VPN connections that an organization must be capable of managing. On-site employees are connected directly to the corporate LAN, but teleworkers must send all of their traffic over a VPN connection. An organization's NGFW must be capable of terminating all VPN connections and performing inspection of a large number of encrypted network connections. Since encrypted traffic inspection is computationally expensive, it is vital that an organization's NGFW can scale to meet demand. Doing so requires NGFWs with dedicated advanced security processors. These minimize latency and maximize throughput, preventing network bottlenecks that can significantly degrade employee productivity.

NGFWs at the headend must also perform Layer 7 inspection of all traffic. This is important in any enterprise context, but with a remote workforce, an organization can expect a higher concentration of malicious content on inbound connections from remote workers. This is because employee machines connected to personal networks have a higher probability of being infected with malware, which may attempt to move laterally through them to the corporate network. A Layer 7 NGFW can identify the application that an inbound packet is trying to reach and block packets from applications with known vulnerabilities. Headend NGFWs should also be integrated with sandboxing capabilities to safely analyze suspicious content that cannot be associated with any known threat.

**Inspection of transport layer security (TLS)/secure sockets layer (SSL) decreases firewall throughput by 60% on average.[3]**

## Conclusion

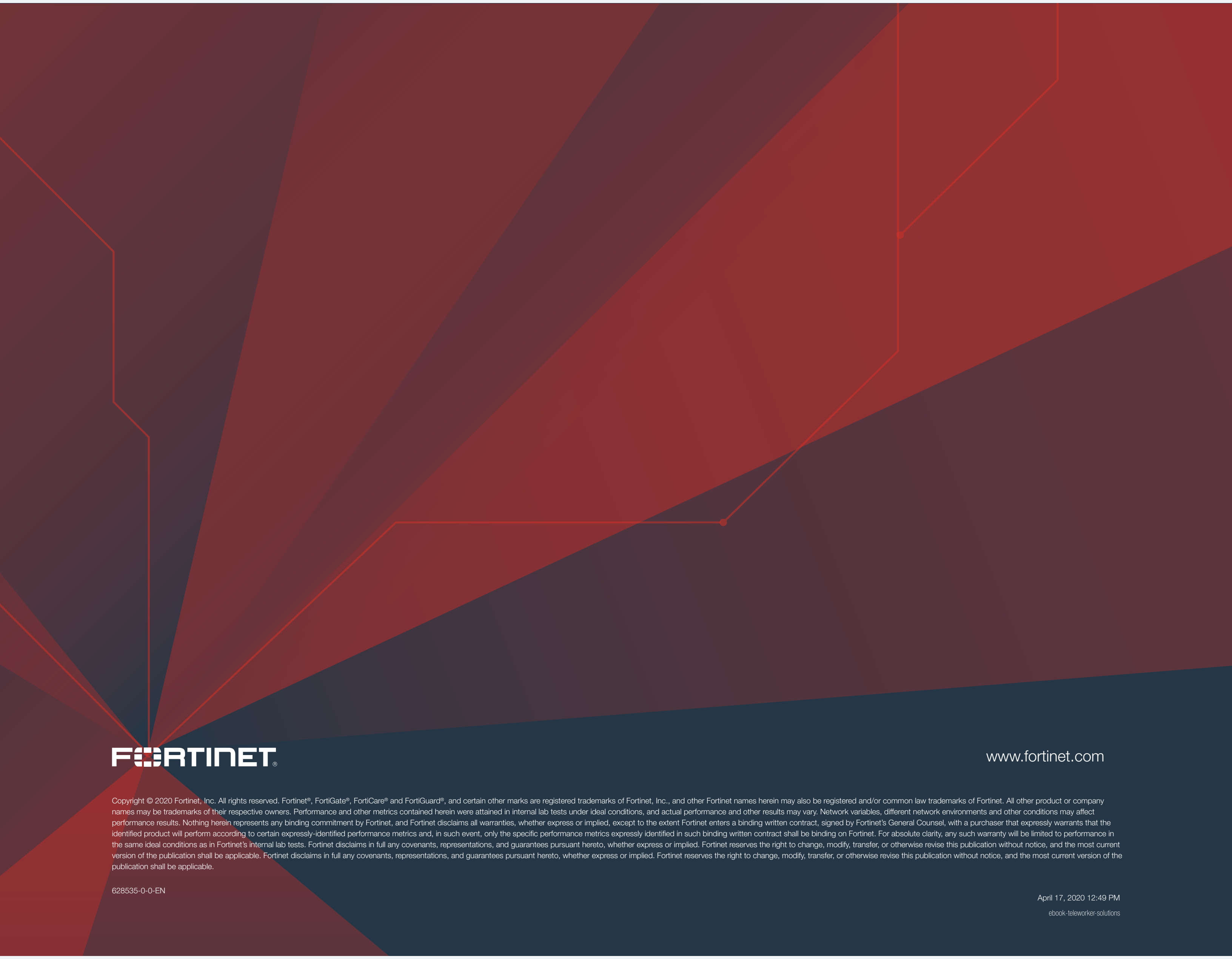
When transitioning quickly and massively to teleworking, it is essential that an organization not only be able to sustain operations but also to ensure the security of teleworkers and the sensitive data that they process.

Doing so requires an organization to deploy security solutions both at teleworkers' remote work locations and on the main corporate network. When doing so, it is essential to select solutions capable of addressing the unique infrastructure requirements and security concerns associated with a remote workforce. During a disaster situation, when an immediate response is required, selecting a solution that can be deployed quickly and easily ensures minimal impact to business operations.

[1] Emma Sutcliffe, "How the PCI DSS Can Help Remote Workers," PCI Security Standards Council, March 26, 2020.

[2] Michael E. Porter and Nitin Nohria, "How CEOs Manage Time," Harvard Business Review, July 2018.

[3] "NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports," NSS Labs, July 24, 2018.



www.fortinet.com

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

628535-0-0-EN

April 17, 2020 12:49 PM
ebook-teleworker-solutions

# When Networks Meet The New Tomorrow

**A Work-from-Home Model, Borderless Security and Shrinking Budgets. Here's How to Cope.**

Gigamon®

# Introduction

The world just changed. Within a short period of time, unforeseen global events have led to vast changes in our working and everyday lives.

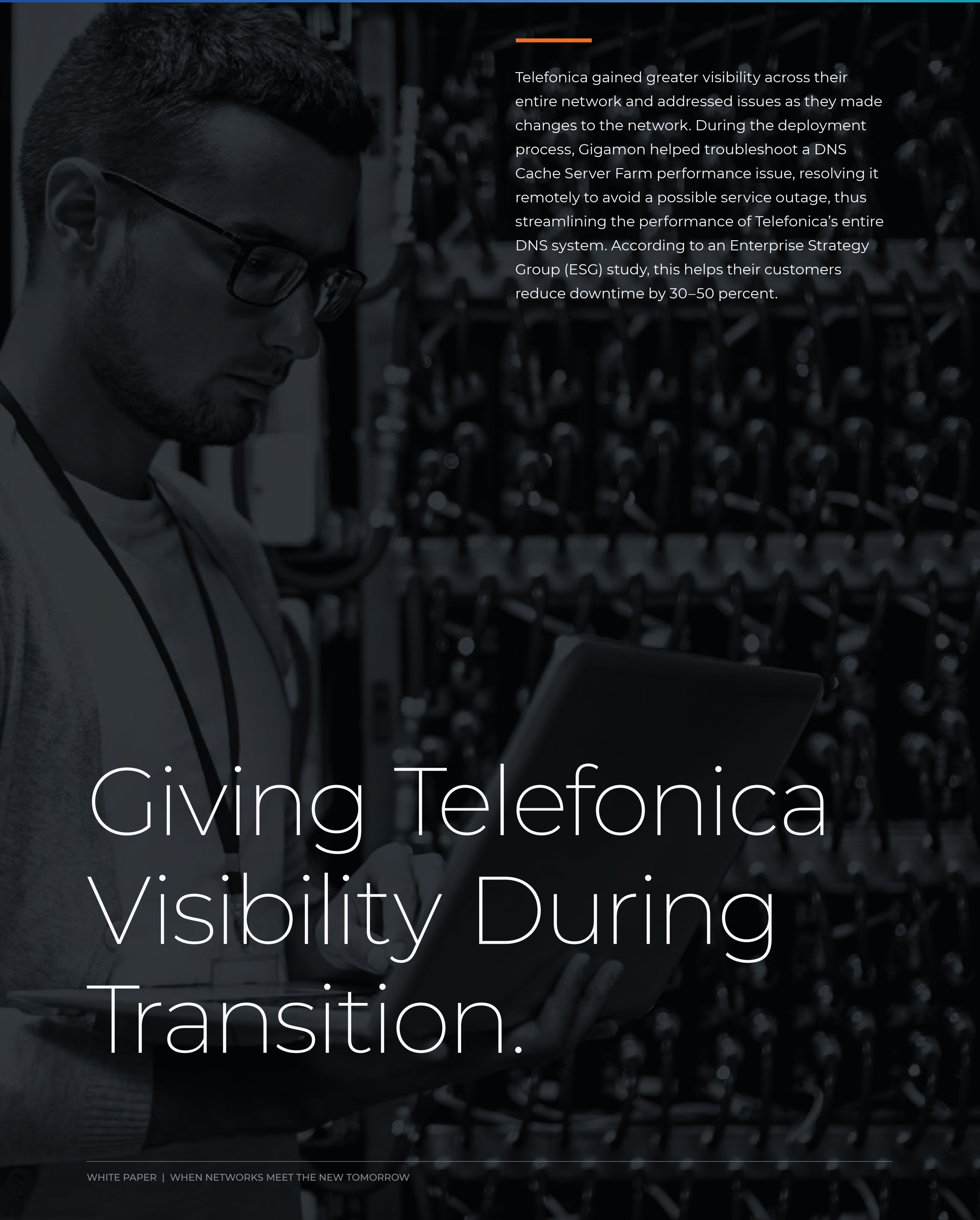
In the context of network operations and information security, this means supporting a newly distributed workforce and digital processes with a shrinking budget. Most organizations' networking infrastructure and tools were designed to support a predominantly office-based workforce. Overnight, IT has had to retool to support a remote workforce that is two to three times larger than was ever planned. On top of that, security needs to be maintained as network traffic has turned from the inside, out. Rapid network and tool modifications are raising new security, resilience and performance concerns. Similarly, the applications we depend on, whether custom, packaged or web-based, are all being pushed to previously untested limits.

# Overview

This paper looks at IT priorities that organizations will need to address now and in the new tomorrow:

- **TODAY**
  The imperative is to ensure security and continuity of operations in this new inside out environment while redeploying network resources to maintain the highest level of customer and internal user experience
- **THE NEW TOMORROW**
  Faced with uncertainty at all levels from capital markets, supply chains, government policy and consumer sentiment, organizations need the agility to respond quickly and cost-efficiently to new and unforeseen challenges and opportunities

We would like to share our thoughts on how organizations can best navigate these unchartered waters based on what we are seeing across our customer base of leading organizations in every industry.



# Giving Telefonica Visibility During Transition.

Telefonica gained greater visibility across their entire network and addressed issues as they made changes to the network. During the deployment process, Gigamon helped troubleshoot a DNS Cache Server Farm performance issue, resolving it remotely to avoid a possible service outage, thus streamlining the performance of Telefonica's entire DNS system. According to an Enterprise Strategy Group (ESG) study, this helps their customers reduce downtime by 30–50 percent.

# Today

IT is being asked to deploy additional capacity and services faster than ever before, but also to balance this new capacity with three critical requirements:

## A New Work-from-Home Model

Certain aspects of infrastructure and applications are facing scaling challenges, perhaps at unprecedented levels. The sudden and rapid shift to working from home (WFH) has left IT teams with little time to scale their remote access infrastructure for employees. As they scramble to bring remote working capacity online quickly, by repurposing older or existing infrastructure, issues such as failures and bottlenecks can arise in the new network segments and infrastructure. Detecting these issues in a timely manner is critical. But with already stretched resources, these issues becomes a truly significant challenge.

In addition to supporting internal users, IT is faced with an upsurge in usage of external apps. Customers are now engaging with companies mostly through mobile applications or online.

Our clients in the financial services, healthcare, entertainment and retail industries are seeing a significant increase in the number of users and frequency of use for their consumer apps. As new application containers, microservices and virtual machines are being stood up rapidly to meet sudden growth in user demand, IT and infrastructure teams risk being left behind by fast-working DevOps and applications teams. This mismatch in alignment can have serious consequences. While application capacity may ramp up, infrastructure capacity may lag and network bandwidth issues, reduced user experience, and application and data access or usage may not be monitored adequately for threats.

## Borderless Security, Beyond the Network

Any additional network user activity in new network segments can become a source for threats, such as data leakage or ransomware. Bad actors are quickly exploiting the prevailing paranoia and uncertainty in an effort to compromise users' systems. These threats use droppers, which are then used to download additional malware on user's systems to compromise credentials, ultimately leading to ransomware attacks, and potential data exfiltration. (See examples here[1] and here[2].)

Compounding the inside out challenge is that remote workers use their home network and/or personal devices for work. And it's not certain that every worker is following recommended security protocols. Even the mandated use of VPNs may not solve the problem, especially if endpoints have not been recently patched. As an example, vulnerabilities are being found and reported in various VPN and firewall manufacturers, which allow Mirai botnet–type variants to take control[3]. In an effort to ramp up capacity, enterprises need to make sure that if they are using older gear, these are fit for purpose and can be patched and secured.

## Working with Reduced Budgets

As many sectors of the economy start to slow down, organizations are already planning for a potential recession. Travel, entertainment and service industries are all being severely impacted. The trickle effect of this on the broader economy is something that organizations are planning for in the form of budgets cuts, hiring freezes and spending constraints. IT and applications teams are particularly feeling the impact as they are being asked to scale up without scaling their resources — the need to do more with less has never been more pressing.

[1] https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#37bf4a0a75fd

[2] https://www.businessinsider.com/hackers-are-using-fake-coronavirus-maps-to-give-people-malware-2020-3

[2] https://krebsonsecurity.com/2020/03/zxyel-flaw-powers-new-mirai-iot-botnet-strain/

# The New Tomorrow

## Stay Focused While Assessing Your Options

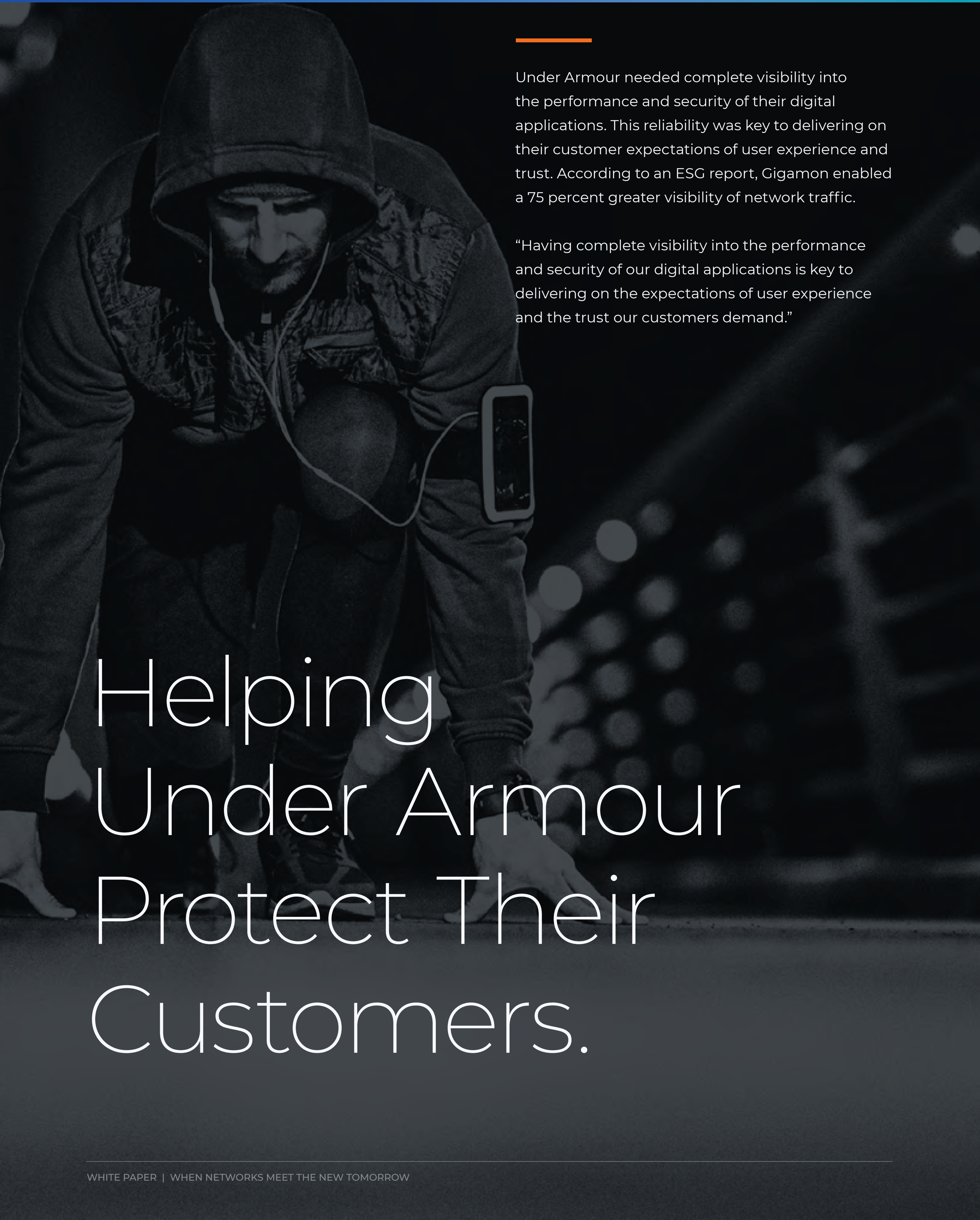
As the economy absorbs the shock of recent weeks, many organizations are already planning for a potential recession. Global supply chains were initially disrupted in Asia and these effects are now compounded and amplified by the dramatic changes in the European and U.S. economies. These changes deeply impact travel, hospitality, retail, entertainment and service industries. And, for those not directly affected by forced closures, the trickle effect of closures on the broader economy is causing almost all IT organizations to review spending priorities and budgets.

As business and IT organizations assess their priorities, they are faced with uncertainty: How long will the crisis last? What additional network bandwidth, applications and services will need to be added? How should they cope with both the challenges and in some cases, the opportunities of this crisis? Will work-from-home become a permanent model for their organizations?

One approach to addressing many of these challenges is to leverage network information-in-motion for application, user and device discovery, troubleshooting, application performance, user experience monitoring, and security.

Network data is the single source of truth about the performance and security of your network. If this data is reliable and up to date, teams will not have to keep changing log levels on servers, reminding application developers to instrument applications or adding new applications for monitoring.

To ensure that this data is reliable enough to be classified as a single source of truth, it is imperative that it includes information-in-motion from physical, cloud and virtual environments, systems of record, log files and other data sources. A best practice is to use a wire once model, where all information-in-motion becomes immediately available to security and performance-monitoring tools as new network segments are brought online. Getting access to network data should be done quickly, with minimal intervention and little to no reliance on applications, DevOps and other teams.



# Helping Under Armour Protect Their Customers.

Under Armour needed complete visibility into the performance and security of their digital applications. This reliability was key to delivering on their customer expectations of user experience and trust. According to an ESG report, Gigamon enabled a 75 percent greater visibility of network traffic.

“Having complete visibility into the performance and security of our digital applications is key to delivering on the expectations of user experience and the trust our customers demand.”

# Stay Focused While Assessing Your Options

While the outcome of today's crisis remains unknown, here are our recommendations for how you can prepare your organization to succeed.

**APPLICATION USER EXPERIENCE.**
More than ever, it is apparent that digital applications are critical to organizations, and the need to ensure that they delivering the best possible customer and user experience has never been more important.

To achieve this, it is important to use tools that not only monitor and visualize application usage and user experience, but also are able to take action based on the performance and behavior of these applications.

For example, surges in video conferencing traffic due to the intensive use of applications like Cisco WebEx, GoToMeeting, Skype and Zoom can very quickly overwhelm out-of-band security tools such as intrusion detection. IT teams must be able to quickly visualize which applications are causing these traffic surges, decide whether to analyze this traffic and at what depth, and then filter out safe or low-risk traffic to preserve bandwidth for other applications.

**BORDERLESS NETWORK SECURITY.**
Against a backdrop of ever more frequent and sophisticated cyber-attacks, the COVID-19 pandemic has unleashed a new wave of bad actors seeking to take advantage of stretched InfoSec teams and users seeking information about the virus both at a global and local level. As such, having the right security tools and rich network data has never been more important.

Examples of the types of tools that can provide both short- and long-term assistance include:

+ **THREAT DETECTION AND RESPONSE**
  With attack surfaces and vulnerabilities increasing as a result of the shift to WFH, on rapidly expanded VPN architectures, it is imperative that organizations have powerful tools to detect and respond to these new threats. For example, pointing tools at ingress/egress links and behind VPN concentrators provides a targeted approach to mitigating potential risks.

+ **CENTRALIZED TRAFFIC DECRYPTION**
  While many tools can decrypt encrypted traffic, deploying a centralized solution to decrypt and inspect encrypted traffic is often the most efficient solution for many organizations. Centralizing TLS decryption capabilities allows traffic to be decrypted and inspected once before being re-encrypted and shared across multiple tools. The ability to look into encrypted traffic to and from applications can be important to realizing whether application and data access is legitimate or illegitimate. As application capacity is dynamically increased, applications are being quickly rearchitected and new applications are being spun up.

+ **USE METADATA TO DRIVE SIEM EFFICIENCY**
  Where organizations are using solutions like Splunk or other SIEMs for active security monitoring, feeding both system and application metadata to these can be a powerful way to help ensure compliance while bringing new applications and capacity online. Organizations should strive to ensure that only precise and relevant metadata is sent to these tools in order to maximize the context being provided to them while minimizing the amount of data being sent to them. This is particularly important with SIEM tools where the billing model is based on the volume of data processed or stored.

- **ZERO TRUST**
  Many organizations were already in the learning, planning or implementation stages of a Zero Trust initiative. This crisis may prove to be the tipping point in accelerating these initiatives. The basic tenets of Zero Trust are to eliminate implicit trust associated with locality of access and to move an organization's defensive perimeter from the edge of the network to assets using the network, i.e., users, devices, data and applications.

In a world where a workforce, as a result of the COVID-19 crisis or planned changes in the business model, is shifting towards a "work anywhere, work anytime" model, moving towards a Zero Trust architecture simply makes sense. Visibility into all information-in-motion on the network is critical to supporting a comprehensive Zero Trust solution.

As is often said, Zero Trust is a journey that requires significant thought to ensure successful execution. Many organizations have been delayed in planning or starting this journey. But with the reimagining being forced upon us by the COVID-19 pandemic, the need to streamline and unify the security infrastructure has never been as urgent as it is now.

## COST SAVINGS BY TOOL INVESTMENT OPTIMIZATION.

Most organizations have made significant investments in the network and security tools they use to manage and safeguard their networks and applications. As traffic shifts from LAN to WAN, it is critical that the data flow to these tools doesn't cause tool overload, visibility blind spots or other issues from the increased traffic.

In order to maximize the efficiency – and ROI – of an organization's tools, it is essential that network traffic from physical, virtual and cloud environments is optimized before it is delivered to your tools. Failure to do this can result in tools overload, teams having to manually intervene in otherwise automated processes and network availability, reliability and security issues.

The U.S. Department of Health and Human Services (HHS) upgraded their network to 10GBps, but many of their security tools had 1Gbps network interfaces. With Gigamon, the older tools were able to operate on traffic from the faster network. According to an ESG study, Gigamon provides the ability to right-size hardware and tooling for a savings of 40–50 percent.

# Finding Speed and Savings for the U.S. Department of Health and Human Services.

# Final Thoughts

The series of current global events has changed our reality overnight. NetOps and InfoSec teams have to manage a massive disruption as users work from home and prepare for an uncertain future. In this situation, visibility and infrastructure agility have become key success factors in an organization's ability to respond to these challenges.

# About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all information-in-motion, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation.

Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations, including over 80 of the Fortune 100.

**For the full story on how Gigamon can help you, please visit www.gigamon.com.**

We invite you to join our online community and, specifically, our Working from Home Collaboration Group, where you can share your concerns, thoughts and ideas with your industry peers and with Gigamon experts.

©2017-2020 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Gigamon®

**Worldwide Headquarters**
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

# Bring Your Network To Your Employees With **Enterprise at Home**

Mist A Juniper Company

**The Enterprise at Home solution leverages Mist Wi-Fi, Mist Edge, and Juniper Connected Security to extend the AI-driven enterprise to remote workforces. Using zero-touch provisioning, Juniper security hardware and Mist Wi-Fi access points can be deployed remotely without a technician visit.**

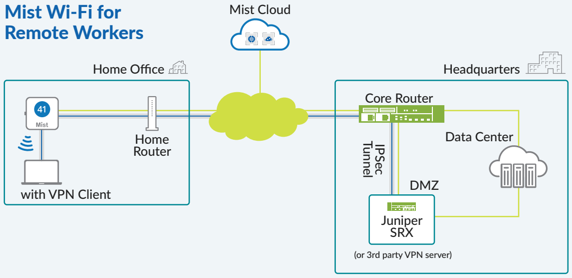
**The shift to a remote workforce has made business continuity more important. Keeping users connected, productive and secure without losing the agility and reliability needed to scale to support evolving demands.**

Up to 75 million U.S. employees could work remotely.*

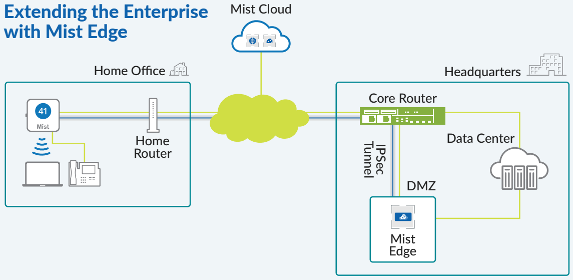
According to a recent Gartner CFO survey, nearly a quarter of respondents said they will move at least 20% of their on-site employees to permanent remote positions.**

62% of employed Americans currently say they have worked from home during the crisis, a number that has doubled since mid-March.***

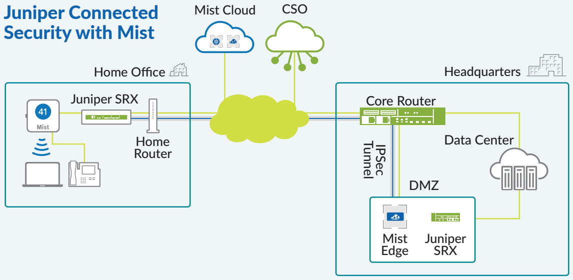
## Mist Wi-Fi for Remote Workers



## Extending the Enterprise with Mist Edge



## Juniper Connected Security with Mist



Gain AI-driven insights into remote user experiences

Eliminate overlay VPN technologies

Monitor Wi-Fi to secure corporate traffic

Increase security and segment business traffic

Keep threats in check with advanced security services

Cultivate a dynamic, flexible, adaptable network

**Learn more about Enterprise at Home. Get started at:**
**https://www.mist.com/enterprise-at-home/**

*Global Workforce Analytics, 2020 **Gartner Press Release (Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently, April 3, 2020) ***Gallup, 2020

JUNIPER NETWORKS | Mist A Juniper Company

**Corporate and Sales Headquarters**
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

**APAC and EMEA Headquarters**
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Mist Systems, Inc. | mist.com | sales@mist.com | @mistsystems | +1 408-326-0346 | 1601 S. De Anza Blvd. #248, Cupertino, CA 95014
Copyright © 2020 Juniper Networks. All Rights reserved. Mist, Mist Systems and the Mist logo are trademarks of Juniper Networks, Inc. in the United States and other countries.
This product is protected by U.S. and international copyright and intellectual property laws.

eplus.com/security

eplus-security@eplus.com

Where Technology Means More®

©2020 ePlus inc. All rights reserved. ePlus, the ePlus logo, and all referenced product names are trademarks or registered trademarks of ePlus inc. All other company names, product images and products mentioned herein are trademarks or registered trademarks of their respective companies, and used with permission.