Where Technology Means More®

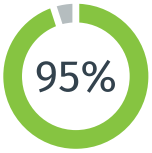
Four Proven Ways to Mitigate Risk and Reduce Your Attack Surface in the Age of Digital Transformation

Corporate America is embracing digital transformation and investing heavily in technologies like cloud, virtualization, hybridized environments, edge computing, and mobility. While these new technologies have accelerated business processes and efficiency, they have also created a larger attack surface of connected things sharing data via networks. Read this paper to discover four critical steps to reduce your attack surface with comprehensive network and access security to fully mitigate this risk.

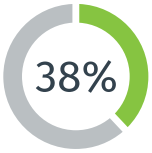
Today's infrastructures are interconnected and dispersed with a wide range of devices tethering to the internet through wired and wireless networks to access applications and data. It's now estimated that investments in digital transformation will reach nearly $2 trillion in 2022.[1] As digital transformation accelerates, new technologies like the Internet of Things (IoT) and cloud have created network vulnerabilities — weak points in which cyber criminals can breach data via legitimate devices that have authorized network access, making these breaches difficult to identify and mitigate. With the number of IoT devices expected to reach 50 billion by 2020, the attack surface posed by these devices continues to expand.[2]

This rapidly growing attack surface includes a vulnerable network environment for cyber thieves looking to exploit protocols, interfaces, hardware, and software. Sophisticated hackers are using artificial intelligence (AI)-driven programs to scan networks and find weak points. Supply chain attacks involving trusted third-party suppliers are also on the rise. And now, with IoT and mobility, connected devices are cyber security targets. Once an attack surface is compromised, hackers have access to the environment, where they can extract or compromise data.

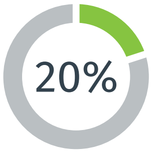
Digital Transformation Under Attack



of employees reportedly use at least one mobile device for work[2]



of companies say detecting and reacting to security incidents in the cloud is a top security challenge[2]



of all attacks will target IoT devices by 2020[7]

Nearly 80% of organizations are introducing digital innovations faster than their ability to secure them against cyber attacks.[7]

The Widening Perimeter

Today's attack surface now includes networks and anything that connects to them. Every endpoint is a lock to be opened, and every network is a doorway to the environment. An industrial control unit left unchecked can be leveraged by cyber criminals to gain access to mission-critical systems and accounts. Data breaches have increased 75% since 2016[3] — even though spending on risk mitigation is on the rise. Consider the fact that cyber security spending is expected to reach $250 billion by 2023.[4] The problem isn't the lack of investment in cyber security solutions, but the gaps in protection that exist. A firewall that blocks outside intruders doesn't mitigate inside attacks. Take for example VoIP phones. These are network endpoints, many configured with open-source code that makes them vulnerable to hacking. It's a real-world problem with real-world consequences. In fact, it was recently discovered that some Avaya enterprise VoIP phones were vulnerable to hackers who could gain access to the DHCP server and gain full control of the devices to spoof and change messaging, exfiltrate audio calls, and spy on conversations.[5] It was also reported that hackers stole customer data from a casino via an aquarium running a temperature-controlled heater connected via Wi-Fi to the internet.[6]

4 Ways to Mitigate Rising Attack Surface Threats

Reducing the attack surface requires a new type of cyber security protection — one that assumes zero trust, forcing verification of every person and device trying to access networked resources. It must also automate response with insight and intelligence into who and what is connected to networks — and where the vulnerability exists. It requires a unified and holistic view of threat detection and mitigation. Here are four ways to reduce the attack surface by identifying blind spots and eliminating unsecured points of entry:

1. Improve Network Visibility

With digital transformation comes digitization of almost everything with connectivity via networks. Such is the case with hyperconverged systems. The network requirements of these systems moving data between data centers and the cloud creates network traffic that can be vulnerable to hackers. Enterprises need comprehensive network traffic visibility, including the ability to identify devices connected via on-premises, virtual, and cloud environments. There are millions of traffic flows, thousands of events and hundreds of changes occurring within an infrastructure daily, so visibility needs to be pervasive, intelligent, and dynamic. This is evidenced by the fact that 36% of IT managers cannot provision mirror/SPAN ports fast enough and 38% have monitoring/security tools that can't keep pace.[8] A new approach to visibility is a top priority for many IT professionals, 75% of whom say they could benefit from a visibility platform.[8]

What's needed today is intelligent network insight that helps companies safeguard network traffic across physical nodes, virtual nodes, TAPs, and traffic aggregators. Once visibility is achieved, detection and protection can ensue — and analysis tools can be used to identify patterns of vulnerability. Companies that have gained deep network visibility via the use of platform-based security tools have been able to achieve a 75% increase in the visibility of network data.[9] This includes network traffic visibility across physical and virtual environments such as private and public clouds, with analytics to identify blind spots before they can turn into costly, disruptive breaches. The key is to layer in security and network tools to speed detection and response, identifying network threats based on patterns of suspicious activity.

2. Strengthen Network Access and Policy Controls

An organization's ability to regulate who and what can view or access their networks is essential to reduce the attack surface — yet trusted, authorized users (and systems) are routinely and automatically granted access. Consider the threats posed when a trusted partner, provider, or user with legitimate network access either deliberately or unknowingly allows unauthorized access. Target and Equifax are two high-profile examples of these types of attacks, and these incidents aren't isolated. As many as 56% of companies reported a breach caused by a vendor in 2018.[10] Employees are also a weak point, as in the case of users accessing company data and applications via the cloud or public Wi-Fi. Robust access and policy controls are essential for secure network access. The complexity of this task is enormous, as employees and third parties are accessing networks and data across multiple devices, locations, and roles.

Strong network access control and policy management must be enforced to ensure that only the right people are granted access to networks and applications from authorized devices. The most effective tools for achieving this are the ones that unify network access policies across the distributed enterprise to provide consistent, secure access regardless of how or where connectivity occurs, via wired, wireless, or VPN connection. For example, an effective network access control solution that restricts device access to networks to include only necessary network access would be essential to safeguarding endpoint security, as would the ability to automate the onboarding of endpoints, users, and guests.

3. Segment Networks and Devices

Traditional networks are configured on flat topology with built-in trust that makes it possible for cyber criminals to exploit the system by becoming part of the trusted zone and running in stealth mode. This allows cyber attacks to move laterally through the network undetected, spreading quickly to do maximum damage. As these threats move deeper into the network, they become harder to contain.

Segmentation helps manage the devices and applications that have legitimate access to networks. It protects network data by limiting an attacker's lateral movements across the corporate network to stop breaches in their tracks. Advances to this, such as intent-based segmentation, stop lateral attacks by segmenting network and infrastructure assets regardless of their location — across distributed networks and geographic boundaries. This approach delivers granular access control and continuously monitors trust levels and adapts security policies accordingly. It isolates critical IT assets to speed threat detection and response by dynamically adjusting policies governing a network segment, significantly limiting the scope of a potential network breach.

4. Close Protection Gaps

Many companies deploy multiple point security solutions to safeguard devices, networks, and data. This patchwork approach to cyber security leaves gaps in protection and is error-prone and highly manual. Disparate tools that aren't connected and don't share information isolate cyber security insight within silos. Many of these point solutions only address a single element of the attack surface — without communicating with each other.

As organizations attempt to roll out disparate security solutions, the level of complexity increases and can often result in gaps across the attack surface. An integrated security solution provides broad visibility across an array of devices, tight integration of a common operating system, and threat intelligence and automated trust assessment that results in real time threat detection. It eliminates blind spots by binding security protection, breach prevention, and automated response via APIs to ensure capabilities work seamlessly when deployed together in a given environment.

Conclusion

The challenge of preventing cyber attacks in an age of always-on, always-connected devices requires a robust security solution that shines a light on network compromise, safeguards the full perimeter, and prevents breaches from spreading. Organizations today must have a comprehensive security policy based on best practices and deployed with an outcome-based approach to help companies identify vulnerability and protect connected things wherever they are — on premises or in the cloud. Comprehensive network security should be integrated, automated, and unified across the enterprise. It must reduce the attack surface by delivering deep network visibility and access control, so enterprises can embrace digital transformation with security.

Learn more at eplus.com/security

[1] IDC, "Worldwide Spending on Digital Transformation Will Be Nearly $2 Trillion in 2022 as Organizations Commit to DX, According to a New IDC Spending Guide," Nov. 2019.
[2] ePlus, "Reduce Your Attack Surface," 2019.
[3] Information Age, "Data Breach Reports See 75% Increase in Last Two Years," Sept. 2018.
[4] Market Watch, "Cyber Security Market 2019 Leading Growth Drivers, Emerging Audience, Global Segments, Sales, Profits, and Regional Study," April 2019.
[5] CSO, "Popular Avaya Enterprise VoIP Phones Are Vulnerable to Hacking," Aug. 2019.
[6] The Hacker News, "Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer," April 2018.
[7] Fortinet, "Fortinet Security Fabric Powers Digital Transformation," Oct. 2019.
[8] Gigamon "Pervasive Visibility Platform," Dec. 2017.
[9] Gigamon "The Evidence Is Conclusive, Gigamon Visibility Fabric is the Choice for Managing and Securing Your Network Traffic" web page, accessed Oct. 2019.
[10] CSO, "What is a Supply Chain Attack? Why You Should Be Wary of Third-Party Providers," Jan. 2019.

CONTACT US TODAY

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

CORPORATE HEADQUARTERS:

13595 Dulles Technology Drive
Herndon, VA 20171-3413
Nasdaq NGS: PLUS

In Partnership with

Gigamon® FORTINET®