Where Technology Means More®

Your Checklist for Reducing Your Attack Surface

How to Strengthen Network Security

Digital transformation and the dramatic growth in connected devices and networks increase the enterprise attack surface. Now, every "thing" that is connected to your network to access or transfer data is a target. Securing such a distributed network ecosystem requires a security solution that can close gaps and help you stay ahead of cyberattacks. Essential components to a secure enterprise include:

Network Visibility and Detection. Software vulnerabilities and network blind spots are common security challenges that become even more difficult as enterprises implement digital transformation. Reducing these vulnerabilities and blind spots as your attack surface expands requires insight and control over all traffic, as well as the ability to monitor unauthorized devices or users requesting network access.

Centralized Policy Management. Today's enterprise networks are highly distributed, making it easy for cyberattacks to fly under the radar. Attacks often happen through unsanctioned employee-owned devices connected to enterprise networks or by way of employees accessing applications and data on unsecured Wi-Fi. Layered access and policy control capabilities help enterprises centrally manage and unify network access policies for all users, devices, and networks — including wired, wireless, and VPN connections. This ensures only authorized devices and users can connect, forcing verification of user and device identity to better safeguard networks.

Segmentation. The longer a cyberattack goes undetected, the more harm it can do. Once network entry has been gained, cyberattacks move laterally within trusted zones to avoid detection, spreading across the enterprise to compromise data and systems. Intent-based segmentation mitigates this risk by dividing the network into zones to prevent lateral movement. Once segmentation has been implemented based on data and process classifications, security teams can continuously review controls and monitor for unusual activity. Security controls and technology are perishable, so it's important to continually assess security policies.

4 Ways to Evaluate Network Security

There are four main areas when considering how to secure and protect an ever-expanding attack surface. Use this checklist to ensure you've addressed and reinforced network security to proactively mitigate attacks.

1. Visibility

- ❍ Can you see all devices including IoT and BYOD, users, and applications across all environments (on-premises, containers, private and public cloud)?
- ❍ Do you have best-in-class threat intelligence to identify attacks quickly and efficiently?

2. Segmentation

- ❍ Do you have a segmentation strategy that protects your network and data regardless of its location?
- ❍ How do you prevent unauthorized access to network resources?

3. Policies, Access Control and Compliance

- ❍ How do you manage external risks, inspect HTTP traffic, implement fine-grained policies, and ensure compliance?
- ❍ Do you have any imminent business mandates to reduce risk, achieve compliance, etc.?

4. Security Strategy

- ❍ Do you work with a vendor that takes a holistic view of your security needs?
- ❍ Is your vendor able to assess your current posture and provide solutions that help fill gaps to help reduce your attack surface?

About ePlus

ePlus leverages partnerships with leading technology providers like Gigamon and Fortinet and couples that with deep technical knowledge and experience to provide a comprehensive approach to improving network visibility, tailoring access control methods, and deploying organizationally appropriate network segmentation, with the goal of reducing your attack surface.

Contact ePlus at eplus-security@eplus.com or visit eplus.com/security to learn more.

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®