POINT OF VIEW

Security Needs To Start With a Fabric

Executive Summary

As organizations accelerate their digital innovation initiatives, it is essential that their security infrastructure is able to keep up with the new network edges being put in place along with the increasingly complex and fast-evolving threat landscape.

Securing the Expanding Network Edge

The explosion of network edges—data center, LAN, LTE/5G, OT, CASB, SASE, and WAN—continue to expand and splinter the perimeter. And new attack vectors, such as home networks, off-net devices, and digital supply chains, require organizations to engage in cyber war on multiple fronts simultaneously. While some of these new environments that need protection are being added to address urgent business requirements, others enjoy a level of trust they do not deserve and therefore fly under the radar.

In all cases, given the rate of innovation, there is rarely enough time to make them part of a cohesive or comprehensive security strategy. In fact, nearly 80% of organizations are introducing innovations faster than their ability to secure them against cyberattacks.[1] And when security is deployed ad hoc to try and keep up, the resulting vendor and solution sprawl creates complexities that further limit visibility and restrict control.

This creates far more than just a management or logistical challenge.

Cyber criminals are spending time and energy looking for new ways to circumvent security controls, infiltrate networks, and achieve their objectives. To do this, their attacks are gaining in sophistication. New attacks target different network edges simultaneously to obscure their attack methods and identify the most easily exploited link in the security chain. Some are even leveraging cloud compute resources to deliver polymorphic attack sequences at rapid scale and with full automation. Few distributed networks that rely on traditionally isolated point products are able to see, let alone counter, these sorts of threats.

Traditional Security Solutions and Strategies Do Not Work

The clear challenge is that the disconnected and isolated security tools put in place to secure rapidly expanding and multiplying network edges don't work together. This disconnection creates security and performance gaps that make it impossible to see and respond effectively to sophisticated and distributed attack sequences. And even if a security team happens to stumble across an attack in progress, and can marshal enough resources to fight it off, there is no way to preserve that intelligence to fend off the next attack.

The reason this is happening is because much of the digital innovation being put in place is being deployed piecemeal, which means there is no unifying security strategy or framework to hold things together. Instead, most organizations have accumulated a wide variety of isolated security tools designed to monitor a specific function or protect one segment of the network in isolation. This leaves overburdened security teams with the responsibility of correlating, identifying, and manually responding to the full attack sequence. But relying on humans to look for and respond to attacks that can often be measured in microseconds is a recipe for disaster. It's part of the reason why, during the last six months of 2020, there was a sevenfold increase in ransomware attacks.[2]

Solutions and hybrid deployment sprawl across hardware, software, and "X-as-a-Service" models have made maintaining networkwide visibility and consistent policy enforcement next to impossible, let alone maintaining and monitoring the various security and networking solutions in place. This has been made even less effective as cyber criminals develop more sophisticated attack strategies designed to exploit these limitations, along with new, innovative Cybercrime-as-a-Service strategies that compound the effectiveness and volume of attacks.

Start With a Fabric—Five Fundamentals for Effective Security Design

Instead, organizations simply fall further behind in delivering the expected high-performance and secure user-to-application connection that is needed. And when they can, the approach usually can't scale. The choices are to either slow down business or introduce more complexity—and risk—to the network.

The approach to network security needs to evolve. Here are five fundamental principles and practices that every organization needs to consider if they hope to get in front of and stay ahead of their current security challenges:

- To establish and maintain control over every edge, a unified security fabric is needed. It must be able to span the distributed and evolving network to detect threats, correlate data, and seamlessly enforce policy. This isn't about selecting a single vendor. It's about choosing the right vendors. This means that priority needs to be given to those vendors that leverage application programming interfaces (APIs) and common standards to support interoperability—especially those that allow policy decisions to be made outside of their solution.
- Deployed security solutions also need to have access to common datasets across all network edges, endpoints, and clouds, enriched with real-time global and community threat intelligence shared from every area of the organization. Network, endpoint, and clouds alike are common intelligence framework enables holistic analyses of the security and performance state, identifies emerging threats, and enables unified response across the organization.
- An integrated security framework needs to support and enable advanced data analysis, combined with the ability to automatically create new protections across the full attack cycle when those analytics detect previously unknown threats. This system should also be able to function autonomously within simpler environments. And, it should be linked to extended detection and response (XDR), security information and event management (SIEM), and security orchestration, automation, and response (SOAR) solutions for increasingly advanced network operations center (NOC) and security operations center (SOC) environments.
- This security fabric also needs to be able to rapidly launch a coordinated threat response across the entire ecosystem the moment a threat is detected. This breaks the attack sequence before its objectives can be realized. Leveraging machine learning (ML) and artificial intelligence (AI) tied to dynamically generated playbooks makes this possible without introducing slowdowns or human error.

- Because change is the only constant in today's digital world, a security fabric needs to be dynamic, meaning that it must be designed to scale up and out as the network it is securing evolves and adapts. This requires deep integration between security and the network components and functions so organizations can continually innovate and expand networking and operations ecosystems without a lag in protections.

A Fabric-based Security Strategy Starts With Convergence, but Relies on Integration

At the end of the day, security is only as good as its ability to provide broad visibility and real-time granular controls across today's increasingly complex and ever-evolving network. Reducing complexity is the first step in achieving that. Only then can advanced analytics, threat correlation, dynamic adaptability, and integrated threat response be possible. And those functions, combined with broad deployability, deep integration between security tools and between security and the network, and dynamic automation augmented by AI, are the hallmarks of any security system capable of defending today's dynamic networks and connected ecosystems.

[1] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Ponemon Institute and Accenture, 2019.

[2] "2H 2020 Global Threat Landscape Report," FortiGuard Labs, February 2021.

March 6, 2021 4:23 AM

D:\Fortinet\2021 Rebranded templates\POV\March\Accelerate Fabric and OS7\pov-FA-network-security-needs-to-start-with-a-fabric-362021\pov-FA-network-security-needs-to-start-with-a-fabric-362021

919921-0-0-EN