SOLUTION BRIEF

The Network Is Changing. How Does Cybersecurity Keep Pace?

Executive Summary

Organizations have been steadily implementing digital innovation for years. But the pace of implementation has recently accelerated. Although individual efforts may differ, they have one thing in common: Technology, even when implemented correctly, exposes new vulnerabilities to the outside world. And if not properly secured, the overall impact increases an organization's vulnerability to a successful cyberattack.

Unfortunately, a cyberattack will likely come sooner rather than later due to today's robust threat landscape. Hackers and cybercriminals are very opportunistic. They see the disruption and vulnerabilities caused by innovations as easy targets, including expanding network environments, the growth in remote workers and mobile devices, the rapid adoption of business applications, and systems in constant flux. These are many of the reasons behind the dramatic increase in ransomware attacks.

Addressing these issues requires a change in how we approach cybersecurity. Rather than taking a problem-by-problem, solution-by-solution approach that will only complicate addressing the different threats and concerns, a structured cybersecurity platform approach like the Fortinet Security Fabric is the optimal choice.

The Evolution of Networks

Traditionally, networks and security have evolved incrementally, with security being centralized and deployed in the data center to protect fixed networks and predictable traffic. This made sense at the time because all the applications were also in the data center, and remote sites were connected via a VPN or a service such as multiprotocol label switching (MPLS). But times have changed.

SD-WAN and SASE have transformed wide area networking (WAN), leveraging an abundance of low-cost broadband options. Applications are located both on-premises and off across multiple private and public clouds and are consumable "as-a-Service." Users and devices can be located anywhere and everywhere and need secure access to applications—regardless of where they or the applications are.

At the same time, threat actors have upped their game with a threat landscape constantly increasing in volume and sophistication. Centralized and fragmented security, typically consisting of multiple siloed point products from various vendors cobbled together as a network overlay, is no longer an appropriate option. The complexity of managing various consoles, fragmented visibility, and the inability to establish meaningful automation hinder threat response. And the scale of the growing attack surface leaves organizations unnecessarily exposed to attacks.

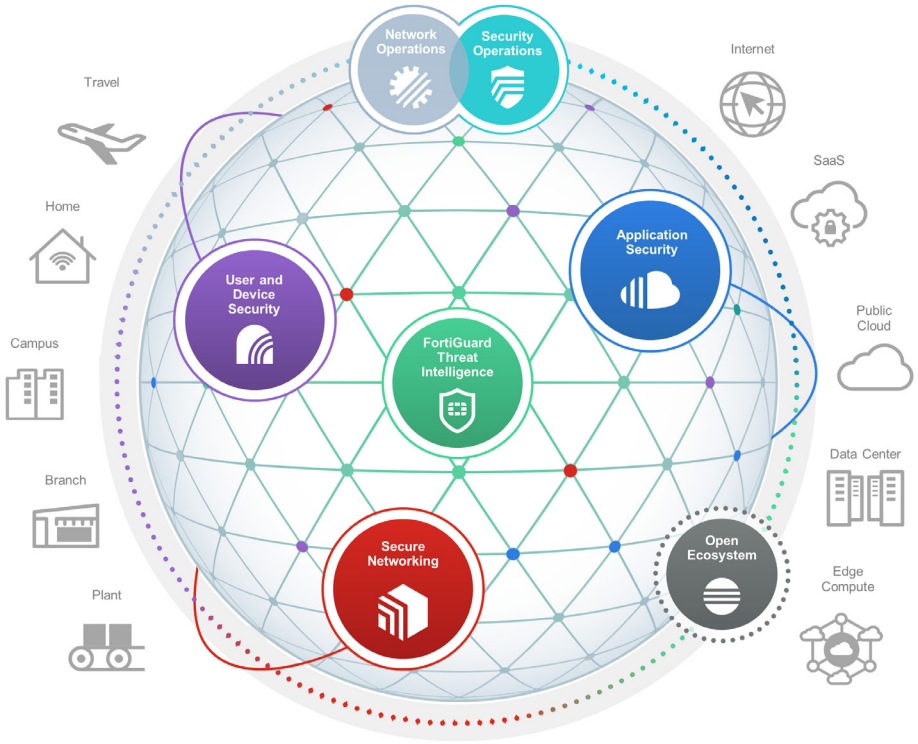

Figure 1: Fortinet Security Fabric

Consolidation, Convergence, and Platform

To address these issues, the Fortinet Security Fabric consolidates technologies to reduce complexity in a typical organization's network. Two of the key principles of consolidation are convergence and the adoption of an integrated cybersecurity platform. The question is how these can reduce complexity and improve an organization's vulnerability profile.

By converging networking and security, they can work together as a unified system, whether deployed in the data center or at the branch office across WAN and LAN. This allows security to automatically adapt as the network infrastructure it is protecting shifts to meet dynamically changing business requirements. And management of the solution is also simplified with only one console for both networking and security.

The next step in consolidation is the adoption of a unified cybersecurity platform. It's not uncommon to find organizations with 40 or more individual security and networking vendors to manage. The principle behind a cybersecurity platform approach is vendor rationalization. The objective is to identify strategic vendors that can provide multiple technologies designed to work together. Such a grouping of technologies creates a "mini-platform" of robust, highly interoperable solutions that can dramatically reduce the number of discrete vendors that need to be managed. The caveat, however, is that each mini-platform must integrate with the other mini-platforms to ensure end-to-end visibility, automation, threat detection, and response.

The Fortinet Security Fabric combines all necessary networking and security technologies represented by these mini-platforms to enhance interoperability, simplify management, and optimize policy orchestration and enforcement. The benefit of this approach is that it enables collaboration between different technologies, improving overall protection levels through automatic threat sharing to improve threat detection and intrinsic coordination to enhance response. It also reduces operational complexity and its burden on the IT team. And with the judicial application of artificial intelligence (AI), the Security Fabric improves the overall efficacy of the organization's cybersecurity investments.

Still, the best solutions in the industry can quickly become obsolete if they cannot keep pace with the threat landscape. The Fortinet Security Fabric is supported by FortiGuard Labs, Fortinet's internal threat intelligence arm. By combining multiple streams of threat intelligence, threat research and real-time threat data gathered from Fortinet customers worldwide, and AI-powered services designed to enhance responsiveness, the different security technologies and services that make up the Fortinet Security Fabric are continuously and automatically updated—without any user intervention.

And because of our commitment to innovation, the solutions found in Fortinet's expansive networking and security portfolio are available in multiple form factors, ensuring that the right technology for each attack vector is deployed where it is needed. With the deep integration between these solutions, the Fortinet Security Fabric can provide a level of efficiency and automation that is impossible for point products.

Pillars of Security

The Fortinet Security Fabric enables organizations to secure digital innovations being deployed to meet evolving business objectives. To help, the different technologies of the Security Fabric are grouped into pillars: Secure Networking, User and Device Security, Application Security, and Network and Security Operations.

Such segmentation allows the organization to "land and expand," first by focusing on an organization's most pressing requirements and then expanding those solutions as needed, but at its own pace. The integrated nature of the Security Fabric ensures that as the pillars of security expand, the overall protection of the Security Fabric expands as well to maintain consistent protection without ever creating unexpected security gaps.

The Security Fabric also alleviates pressure from overworked and often understaffed IT and operations teams via its single-pane-of-glass approach to network and security operations. Incident detection and response are also improved through the synergy of threat detection technologies such as EDR, XDR, and sandboxing, and traditional SOC tools such as security information and event management (SIEM) and security orchestration, automation, and response (SOAR).

Regardless of how many technologies are part of the Security Fabric, it will never have every technology an organization may want or need. That's why, to ensure integration into existing and changing environments, the Security Fabric also features an open ecosystem with a series of APIs and interfaces so it can integrate with non-Fortinet technologies. And today, it includes integrations with over 500 Fabric-Ready partners. This open ecosystem ensures that the Security Fabric can meet the critical challenge of continuous technology evolution.

Key benefits of the Fortinet Security Fabric:

- Consolidating technologies reduces the number of vendors, reducing complexity and improving threat detection and response capabilities.
- Converged security and networking enable security to be quickly deployed where it's needed.
- Every solution is supported by a single source of threat intelligence from FortiGuard Labs.
- Broad form factors ensure protection across all edges.
- Interoperability between networking and security enables the fabric to adapt as the network and threats evolve.

Cybersecurity Platforms Are the Future, Today

The intensity and sophistication of today's threat landscape are outstripping the traditional approach to cybersecurity, which includes an unmanageable collection of siloed products from various vendors. Today's network and its security infrastructure can no longer operate as separate entities layered on each other. The future is a cybersecurity platform incorporating the convergence of networking and security and the consolidation of critical technologies to reduce complexity and improve protection.

With the Fortinet Security Fabric, that future is now.

FORTINET

May 30, 2023 12:58 PM
2163625-0-0-EN