CHECKLIST

How To Simplify Security With Cybersecurity Mesh Architecture

As networks become more complex and distributed, detecting and responding to threats has become increasingly difficult. Addressing this through a "best of breed" or "point product" approach[1] has led to security sprawl that complicates management, fragments visibility, and limits the ability of organizations to respond effectively to threats. Case in point, today's enterprises have deployed an average of 45 security solutions across their networks, making any sort of centralized management nearly impossible. And worse, detecting and responding to a cyber incident requires coordination across all these tools, leading to complex workarounds that must be constantly managed and reconfigured every time a device is upgraded.

Legacy standalone "best-of-breed" approaches to cybersecurity have become an outdated crutch for many organizations. Instead, what organizations need to pursue is a "best-of-breed AND integrated" approach, known as a "cybersecurity mesh architecture" (CSMA), to speed and automate response to threats while reducing complexity.

Organizations driving digital acceleration must leverage a broad, integrated, and automated cybersecurity platform as the core foundation of a true CSMA. This ensures that they build robust, scalable, and manageable secured deployments.

The four necessary capabilities of a cybersecurity mesh platform:

Fortinet helps CIOs reduce network security complexity and the costs of continuously adding on more isolated products to cover new threats or risk exposures.

☑ Broad.

Choose a platform that provides the flexibility to implement distributed security controls across all network, device, cloud, and application edges for broad visibility and protection across the entire digital attack surface to better manage risk.

☑ Integrated.

Integrated. An integrated platform eliminates silos and offers a unified solution that reduces management complexity while sharing threat intelligence across the entire deployment.

☑ Automated.

Choose a platform that enables collaboration between deployed solutions and provides automated self-healing networks, augmented with artificial intelligence (AI)-driven security, for fast and efficient detection, operations, and response.

☑ Open Ecosystem.

A true cybersecurity mesh platform breaks down technology and vendor silos. Choose a platform that enables and supports a broad, open ecosystem of technology partners.

Conclusion

For over a decade, Fortinet has adhered to the doctrine that a broad, integrated, and automated cybersecurity mesh platform, provided by the Fortinet Security Fabric, is essential for reducing complexity and increasing overall security effectiveness across expanding networks. Fortinet's portfolio of more than 50 security and networking technologies—the largest in the industry—is designed from the ground up to interoperate by sharing threat intelligence, correlating data, and automatically responding to threats as a single, coordinated system. Additionally, Fortinet consolidates cybersecurity technologies while also converging security and networking (security-driven networking) through industry-first innovations such as Secure SD-WAN.

Fortinet also believes that a true cybersecurity mesh platform should further break down technology and vendor silos by enabling and supporting a broad open ecosystem of technology partners. To this end, over 450 third-party Fabric-Ready Partners currently interoperate as part of the Fortinet Security Fabric, and Fortinet is committed to continually expanding its partnerships.

[1] "Cost of a Data Breach Report," IBM, 2021.

www.fortinet.com

December 31, 2021 9:24 AM