FORTINET

Struggling To Securely Keep Up With Digital Acceleration

Table of Contents

Modern Networks Require a Security Re-think

In today's digital economy, businesses must move fast, rapidly adapting to changes. Increasingly, this means adopting the latest technologies to maintain optimal user experience across a hybrid network and mobile workforce. However, ubiquitous connectivity, application migration to the cloud, and investments in next-generation technologies to enable digital acceleration have resulted in a rapid expansion of network edges, and as a result, potential attack surfaces.

And as digital acceleration continues, users and devices will become even more widely dispersed while the perimeter becomes increasingly fragmented. Applications and data are already no longer contained within the corporate data center but reside across distributed multi-cloud and hybrid data center networks. And the continued adoption of work-from-anywhere strategies, expansion of hybrid networks, and accelerating IoT deployments will only add to the challenge.

The resulting complexity organizations are undergoing has created a perfect storm for cybersecurity. To survive, they must address the significant complexity and risks accompanying their rapidly expanding—and highly dynamic—attack surface. But for far too many organizations, their approach to security has not kept up with development elsewhere across their network. And unfortunately, legacy security systems are simply unable to keep up with today's business mandate to maintain high performance and optimal user experience while simplifying operational management.

Cyber incidents are the top concern for companies worldwide in 2022. The threats of ransomware and similar cyberattacks, data breaches, and major IT outages worry organizations more than business and supply chain disruption, natural disasters, or the COVID-19 pandemic.[1]

Out With the Old but Where's the New?

Unfortunately, this is not a new problem. According to a Ponemon Institute report,[2] organizations have deployed an average of 45 security solutions across their organizations, while many of those tools—and the security teams managing them—operate in silos. These disconnected solutions only add to the complexity of securing today's networks, requiring IT teams to integrate best-of-breed point solutions using disparate management systems and multiple policy and administration requirements using workarounds that need constant adjusting.

And as a result, according to a recent Fortinet survey,[3] 82% of IT teams with 10 or more security vendors in place will spend nearly a third of their time addressing issues related to vendor complexity. And that doesn't even begin to address the need to deeply integrate security with the underlying network infrastructure—an effort that would enable policies to seamlessly adapt to dynamic networks and follow applications and workflows end to end.

Another major challenge resulting from siloed security solutions is the sheer volume of work involved in following up on security alerts and incidents that cannot be automated. Because it is difficult to automate security processes using disparate, isolated solutions, IT teams rely on humans to assess the more strategic implications of alerts and incidents. Unfortunately, those teams are operating against a global cybersecurity talent shortage, meaning these efforts are often under-resourced. But even with adequate staffing, today's attacks occur at speeds that exceed human intervention, making AIOps essential for identifying and responding to threats targeting today's dispersed networks. But such solutions are impossible to deploy when networking and security solutions are not designed to interoperate.

Sensing the opportunity at hand, cyber criminals are taking an increasingly sophisticated and holistic approach. For example, according to the Google Transparency Report,[4] the volume of encrypted traffic on the web continues to rise, now hovering at 95%. This has made detecting new attack vectors even more challenging as most legacy security solutions struggle to inspect encrypted traffic—especially streaming video—without impacting user experience. Bad actors know this and intentionally hide their malicious activities in encrypted streams so they can remain undetected. Adding fuel to the fire, most networks still operate as a flat, open environment without any security inspection past the perimeter. So, once hackers manage to breach the network perimeter, they can easily spread laterally, seeking valuable resources, sowing ransomware and other malware, and disrupting business.

At the same time, the first generation of AI-enabled attacks has begun to emerge, enabling sophisticated threats to automatically detect and exploit vulnerabilities and identify and evade security countermeasures without needing instructions from a command-and-control server. And in addition to trying to counter such sophistication, organizations also have to deal with the growing volume of attacks resulting from new malicious (and highly profitable) criminal services being sold on the dark web. Ransomware-as-a-Service, for example, is now available to bad actors who do not otherwise possess the skills needed to identify and target vulnerable enterprises.

According to the World Economic Forum's Center for Cybersecurity,[5] there has been a 300% increase in reported cybercrime since the beginning of the COVID-19 pandemic, with more than 60% of ransomware attacks targeting industries with critical infrastructure, led by healthcare, utilities, and manufacturing. And much of that is being fueled by Cybercrime-as-a-Service offerings.

Taking the Structured Platform Approach to Cybersecurity

Addressing these challenges requires rethinking cybersecurity strategies. The most critical issue is ensuring that security solutions and countermeasures are equal to the task. Legacy security solutions and strategies were never designed to address the challenges posed by today's complex and highly distributed networks.

Instead, today's security solutions must operate as a single, integrated solution, regardless of where they are deployed. They must also support the convergence of networking and security to ensure that critical protections automatically scale and adapt as the underlying network adjusts to meet shifting user and application demands and dynamic business requirements. This requires a fully integrated and automated strategy that can not only span the entire network but follow users, workflows, and applications end to end. To do this, it must consolidate a variety of security technologies on a single, integrated platform that can be deployed universally in any environment—physical or virtual, local or remote, on-premises, in private or public clouds, and at branch and home offices. These components of a structured platform approach are essential for maintaining visibility, ensuring consistent policy enforcement, and automating threat responses.

[1] "Allianz Risk Barometer," Allianz, January 2022.

[2] "Security Response Planning on the Rise, But Containing Attacks Remains an Issue," IBM, June 30, 2020.

[3] Joel Boyd, "The Impact of Complexity on Organizations Over Time—and How SMBs Can Prevent It, Fortinet, October 18, 2021.

[4] "HTTPS encryption on the web," Google, January 2020.

[5] Jeremy Kaye, et al., "Protecting critical infrastructure from a cyber pandemic," World Economic Forum, October 20, 2021.

www.fortinet.com

February 17, 2022 12:13 PM

1413093-0-0-EN