INDUSTRY INSIGHTS

Unified SASE: The Third Era of Network Security

Today's three largest cybersecurity markets are endpoint security, network security, and identity. While there are other large cybersecurity markets, including email security, web security, cloud security, SIEM, and SOC, these three account for over 50% of the cybersecurity market and are a big part of any organization's budget.

Today's cybersecurity solutions are sophisticated and powerful. However, many of them still operate as individual point solutions. But this is beginning to change. Many vendors have started integrating their point solutions into a platform that increases interoperability, simplifies management, and can span today's hybrid networks.

But this isn't where cybersecurity started. Like any market or technology, network security has undergone several cycles of evolution since its inception, especially as critical new functions and features are developed to support today's complex networks and to combat increasingly determined threat actors. Network security has now begun its third era of growth—but where did it all begin?

The First Era of Network Security: The Stateful Firewall

Trust everything and connect everything as fast as possible. That original objective of networking remains true today. However, malicious actors quickly made it their job to exploit largely open connections between networks and devices. So, back in the mid-1990s, the stateful firewall was invented to control access to private networks.

These initial stateful firewalls could block traffic based on IP addresses, ports, and protocols. This allowed IT teams to create trusted and nontrusted networks and sometimes a demilitarized zone between both. This was a significant improvement from simply connecting everything.

Many firewall vendors began to add secure remote access via virtual private networks (VPNs). This allowed remote users and branch offices to work as though they were on the network. However, this now required them to add an agent to extend secure connectivity to remote endpoints. As users increasingly connected to the internet, a proxy was put in between the user and the internet. This proxy would act as an intermediary between users and the internet. Caching devices were incorporated to improve internet performance when bandwidth was at a premium.

It should be noted that while the network firewall has evolved, traditional stateful firewalls have not disappeared entirely and are unlikely to do so. Use cases such as internal segmentation, for example, remain essential to protecting networks against the lateral movement of threats.

The Second Era of Network Security: NGFWs and UTM Devices

Application ports, such as HTTP and HTTPS, began to be well-known, and threats started to target applications. The original Layer 7 filtering that redirected application traffic to these ports was no longer an adequate defense as it was not granular enough. As threat actors began to target application traffic, a lot of compromised traffic began to pass through the firewall without inspection. As a result, it became critical for security tools to inspect traffic content to assess whether application traffic was malicious. In other words, threat protection was becoming a critical job for the firewall. Because of this, stateful firewalls evolved into unified threat management (UTM) devices, later known as next-generation firewalls (NGFWs).

These NGFWs were placed at the network edge, usually at the data center perimeter, for traffic accessing external applications and the internet. They could identify applications and mitigate most threats in flight, making them critical for in-path communications. Deeper content inspection and understanding of a URL's application content provided more visibility and granularity to mitigate threats.

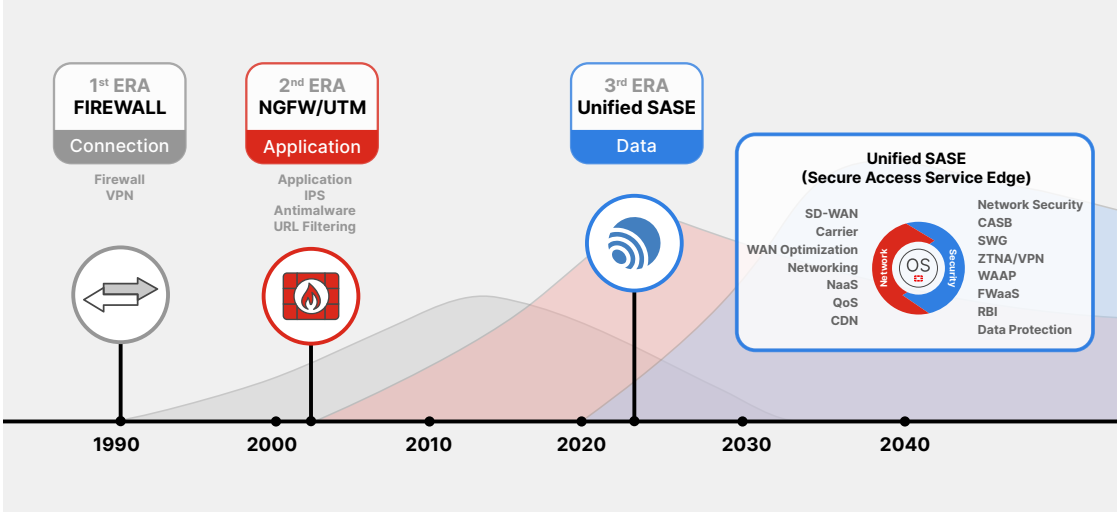
However, these additional layers of inspection, including SSL and deep packet inspection, required more security-specific processing power than the off-the-shelf processors powering most NGFW appliances. Fortinet developed the industry's first security processing unit to address this challenge, a purpose-built ASIC designed to increase performance by offloading critical security functions.

At the same time, intrusion prevention systems (IPS) became a security tool used by InfoSec teams to protect endpoints from attack, with different IPS signatures for different types of applications. Because IPS and NGFW devices were usually deployed on the same edge, it became apparent that inspection and enforcement worked just as well—and sometimes better—as part of the NGFW.

As internet attacks increased, additional security was added to the traditional proxy, which became known as the secure web gateway (SWG). This included URL filtering, antivirus, data leakage protection, and SSL inspection.

The Third Era of Network Security: Unified SASE

As we move into the third era of network security, the traditional perimeter has been completely reimagined. To secure today's highly distributed environment, a new, more expansive type of platform is required—one that can work across the hybrid workforce, distributed edge, and multi-cloud environments. It must also expand the convergence of networking and security across all edges by supporting multiple form factors—physical and virtual appliances, multi-cloud platforms, and "as-a-Service." We call this Unified SASE (secure access service edge).



This new approach allows protections to move beyond simply defending against external threats to consistently securing data wherever it might be. To do this, Unified SASE components must be deeply integrated, and the solution must be AI-based to detect, correlate, and respond to threats wherever they target the network in near real time.

Unified SASE goes beyond traditional SASE solutions by converging end-user connectivity with critical networking by incorporating a software-defined wide area network (SD-WAN). SD-WAN quickly became a crucial technology for replacing simple routers at branches and campuses with faster, smarter, and more cost-efficient connections to the rest of the network. Adding SD-WAN to Unified SASE ensures end-to-end visibility and control.

Unfortunately, early SD-WAN solutions did not take security seriously. They needed a separate firewall appliance and security solutions that had to operate as a separate overlay, which diminished the value of SD-WAN's flexibility. Fortinet solved this problem by building enterprise-class secure SD-WAN directly into the firewall.

As SaaS applications became more popular, a cloud access security broker (CASB) based on API access was also included. When this was added to SWG, the solution became known as security service edge (SSE) and became cloud-based. It plays a critical role in the Unified SASE solution.

So does zero-trust network access (ZTNA), which provides application-specific access. It is used with SSE to replace or complement remote access via VPN.

As we move to Unified SASE, endpoint and network security must be intrinsically connected. VPN, SASE, and ZTNA ensure that endpoint devices function as an extension of the extended network. However, a digital experience monitoring (DEM) element also needs to be present to measure end-to-end experience. Of course, it should include an endpoint protection platform, endpoint detection and response functionality, and agentless options.

The critical elements of Unified SASE include:

Core Elements		Expanded Elements	
1	Security service edge	7	Digital experience monitoring
2	Inline SaaS controls	8	Network sandboxing
3	Branch/campus appliance	9	DNS protection
4	Secure remote access (ZTNA)	10	Remote browser isolation (RBI)
5	Firewall-as-a-Service	11	Web application and API protection
6	Unified agent	12	API access to SaaS (CASB)
		13	Private backbone transport/telco
		14	Content delivery networks
		15	Cloud on-ramp

Unfortunately, most vendors are not taking an integrated approach to SASE. Instead, they build their platforms by acquiring companies and bolting their technologies together. While this may look attractive on the surface, it's not a platform underneath, which means things don't really work together the way they need to, making end-to-end visibility and control difficult to achieve. Indeed, not all platforms are equal.

A true Unified SASE platform should use a single OS, a unified client, a single analytics engine, and a single policy engine that can run on physical and virtual appliances, in the cloud (including all major cloud-provider platforms), and as-a-Service. It should also be powered by integrated threat intelligence and AI.

Setting the Stage for the Next Era

This third era of network security expands security to every edge by integrating protections designed for clouds, connections, networks, and endpoint devices into a unified security strategy. The integrated, platform-based approach of Unified SASE enables organizations to build and evolve their networks as they need, allowing them to respond to business demands without compromising security, performance, or user experience. Its innate adaptability also provides a path for meeting the next era of challenges.

May 3, 2024 4:15 PM

2682119-0-0-EN