ESG BRIEF

Network Security Predictions for 2021

Date: January 2021 **Author:** John Grady, Senior Analyst

ABSTRACT: This brief looks at some of the key trends and events that will shape network security technologies, suppliers, and customers in 2021.

Overview

Considering the events of the last nine months, attempting to predict what 2021 has in store for us seems presumptuous to say the least. Thinking back to the 2020 RSA conference, who could have anticipated that come the holiday season we would be gearing up for a long winter of sequestration? Yet if the last year has taught us anything it is that while we cannot always predict the future, being prepared for the unexpected is critical. So while my predictions are based on the assumption that after the winter passes we will begin to slowly move back towards a semblance of normalcy, it may make for an interesting thought exercise for readers to also consider how the continuing spread, delays in vaccinations, or other factors could impact the predictions most applicable to them over the next twelve months.

With that caveat out of the way, here are seven network security predictions for 2021:

1. Remote work and zero trust access will remain top drivers for SASE through next year. When secure access services edge (SASE) was introduced, the branch office use case was prioritized, exemplified by the fact that the main focus was on converging security and networking. However, SASE really began to take off as organizations struggled to support and secure their remote workforce and began to look at alternative approaches to the traditional backhaul model supported by VPN gateways. I do not see that focus changing through 2021. Vendors will continue to plan for and promote the convergence of security and SD-WAN, and organizations that require a significant branch footprint will be receptive to this type of approach. Some "home SD-WAN" offerings may gain traction for organizations seeking to support executive, call center, and other specific use cases. However, the main driver for the majority of the market through 2021 will continue to be evolving remote access to provide a secure, consistent experience for employees, regardless of where they reside or which resources they are accessing.

2. A billion-dollar SASE acquisition occurs. While the focus in 2021 will be remote access, vendors must continue to plan beyond that horizon. The opportunities for acquisition are shrinking, but it seems likely that 2021 will see at least one significant acquisition of over $1 billion. Networking-focused vendors may look to a security pure-play to improve capabilities and appeal more to the security side of the organization. Conversely, a security vendor may follow in Palo Alto Network's footsteps and snatch up an SD-WAN provider to provide a complete, single vendor SASE architecture. Lastly, we may see a non- or limited-current participant buy-in to this dynamic market. To me, this is the most likely option to push over the $1 billion threshold. Whatever the combination, the limited number of tuck-in possibilities, high market valuations, and significant growth expectations all point to at least one, and possibly multiple, market altering acquisitions in 2021.

3. The appliance market evolves to remain relevant. For all the talk of SASE and cloud, the fact remains that a significant percentage of network security tools are still on-premises appliances. The transition to cloud is absolutely accelerating but will take time. To bridge the gap and provide customers with more flexible, resilient, and cost-optimized options, vendors will focus less on the hardware and layer additional subscriptions for things like throughput. This will allow vendors to consolidate appliance lineups for simplicity, providing customers with investment protection and added flexibility to expand capacity quickly without the need for additional hardware should the need arise.

4. Inspection without decryption gains traction. While privacy concerns are the top reason organizations do not decrypt and inspect all network traffic, the negative performance impact, complexity, and expense associated with decryption are also factors. While shifting decryption to the cloud (especially through a SASE-based approach) can help through centralized management and better performance via cloud-native architectures, privacy concerns will still result in a percentage of enterprise traffic remaining encrypted and unavailable for inspection. As an alternative, some vendors have begun to incorporate behavioral analytics to assess whether encrypted traffic is likely to be malicious. By examining the encryption keys being used, the TLS handshake itself, and a variety of other metadata about the traffic, attacks that would otherwise be able to bypass defenses can be detected. This is not likely to replace decryption, but as sophisticated attackers continue to compromise legitimate resources to bypass defenses, more organizations will be open to alternative approaches to reduce the attack surface and ensure attackers are not able to exploit the lack of visibility current decryption practices create.

5. Runtime application security continues to converge. With much of the network security market focused on SASE and zero trust, the emergence of web application and API protection (WAAP) has remained a bit more under the radar. However, within the application security space, this convergence is no less important. WAAP addresses three of the top pain points with regards to runtime application security today: traditional tools have often been appliance-centric and cumbersome to deploy; many organizations are prioritizing security over compliance with regards to protecting applications, which has not always been the case; and the interconnected nature of today's applications, coupled with multi-vector threats. With these challenges in mind, it only makes sense to aggregate highly effective, next-generation protections in a single cloud-based solution and provide complete visibility across all threat vectors. The acquisitions that have occurred in this space over the last two years set the stage for what I expect to be significant end-user interest in WAAP in 2021.

6. API protection gets its due attention as part of WAAP. Despite being a prominent part of the name, API protection has been a secondary consideration of WAAP and application security overall to date, with much of the focus on the WAF, DDoS protection, and bot mitigation components. With regards to API security, the capabilities in many WAAP solutions have been rudimentary, offering basic protections against bot traffic and standard OWASP Top 10 attacks targeting APIs, but only through the manual uploading of OAS/Swaggar files. This will change in 2021 as APIs continue to dominate application architectures and organizations begin to focus more on the security of these endpoints. More advanced API security features will be sought out by users as part of a holistic runtime application security platform. Automated inventorying, profiling, and more analytics-based protections for APIs will become critical components users seek in WAAP solutions over the coming year.

7. Automation, automation, automation. The acute shortage of cybersecurity skills continues to impact organizations of all sizes, while, at the same time, evolving towards a more modern zero trust approach to security is a priority for many. Yet while automation remains somewhat of a "buzzy" topic, its importance derives from a place of need. With the matrix of identities, workloads, locations, devices, and data continuing to grow more complicated, automation provides the only real avenue towards implementing zero trust strategies in today's dynamic

enterprise environment. There has been hesitancy among some organizations to fully embrace these capabilities—the potential for disruptions among the chief concerns. However, as the benefits are proven out and more organizations look to incorporate zero trust in 2021, automation will become a critical attribute of any solution supporting a zero trust strategy.

The Bigger Truth

While I'm sure that 2021 cannot come fast enough for all of us, it is worth looking back to consider how significant 2020 was for network security. SASE appears poised to remain a significant factor in the market for years to come, and finally re-platform what has historically been an appliance-focused market to the cloud. Well-established technologies such as VPN, secure web gateway, and firewall are being reviewed and reassessed in the context of SASE architectures, as organizations revisit approaches that have been in place for well over a decade. Zero trust also appears poised for a breakout thanks to further dissolution of the perimeter brought on by the increase in remote work and cloud adoption due to the pandemic. While we can certainly hope 2021 has much better things in store than 2020, we should not overlook the transformative year that it was.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188