



ESG BRIEF

Network Security Predictions for 2022

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

ABSTRACT: This brief looks at some the key trends and events that will shape network security technologies, suppliers, and customers in 2022.

Overview

Following an unprecedented 2020, there were hints of a return to normalcy in 2021. Specific to the cybersecurity industry, the pace of investment picked up notably with the massive Proofpoint acquisition by Thoma Bravo, as well as significant funding rounds based on unicorn valuations for multiple startups. Some hybrid industry events were held, hopefully paving the way for a successful, in-person RSA 2022.

Unfortunately, the threat landscape (which never really slowed down in the first place) remained as complex as ever. Supply chain attacks against providers of some of the most used software in the world impacted tens of thousands of businesses, and ransomware attacks on critical infrastructure pushed the federal government to issue an executive order and form the Joint Cyber Defense Collaborative to improve cybersecurity collaboration across the private and public sectors. Specific to network security, secure access service edge (SASE) and zero trust remained front and center, with many organizations beginning to implement the initiatives. So, with that as the backdrop, what is in store for the network security market in 2022? Here are five predictions on what will happen:

1. **VPN replacement begins in earnest.** This may seem more retrospective than predictive at first glance. Reading industry headlines, one would think that most companies have already disconnected their VPN appliances in favor of more modern secure remote access methods like zero trust network access (ZTNA). Yet many organizations were forced to double down on VPN investments when the pandemic forced workers out of the office, keeping the focus for ZTNA on specific use cases in most instances. In fact, ESG research has found that only 7% of organizations report using ZTNA for most of their remote access needs in order to move away from VPN. But more importantly, 62% say they're currently using ZTNA for specific use cases or applications and are actively expanding or planning to expand to move away from VPN.¹ There is no question that organizations have been looking more at longer term scalability when evaluating ZTNA solutions, even though initial rollouts remain targeted. However, 2022 will be the year in which VPN replacement reaches critical mass.
2. **Network security expands to the home.** With hybrid work likely to be the common model moving forward, organizations will continue to rethink their longer-term strategies for securing a distributed and diverse environment. While lip service was paid to the idea of "ten thousand branches of one" during the pandemic, much of the focus was on improving secure user access to the web and applications, as well as protecting the devices themselves. However, the range of connected home devices creates potential entry points that can serve as avenues of attack to corporate resources. Attempts have been made in the past to emphasize consumer network

¹ Source: ESG Complete Survey Results, [2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased](#), December 2021.

security (think the failed Norton Core experiment), but the market never truly materialized. The difference now is that organizations have a vested interest in helping their employees protect their personal networks and enterprise vendors see a growing business opportunity. As a result, 2022 will see an extension of SASE into the home network to ensure the isolation of corporate traffic from that of personal connected devices. Some vendors including Palo Alto Networks (Okyo Garde) and Fortinet (Linksys HomeWRK) are ahead of the curve in addressing this space but competitors are likely to quickly follow.

3. **Microsegmentation sees increased focus as a core component of zero trust.** Zero trust involves many different security disciplines. An organization starting a project today could begin with zero trust network access, some aspect of identity, or even response. Yet when narrowing the focus to the most basic tenet of removing implicit trust from the environment, the criticality of segmentation becomes clear. Segmentation and microsegmentation have been overlooked in the zero trust conversation at times due to perceptions that the initiative is complex and expensive. However, most do understand the importance of these practices and want to employ them. In fact, ESG research recently found that, while only 36% of organizations use microsegmentation today, 91% expect to 24 months from now.² Even if this represents an aspirational goal and not what the market will truly look like in 2 years, it points to increasing awareness of the criticality of these practices, and as a result, a massive opportunity for vendors to lean in and assist.
4. **Security services edge (SSE) fails to catch SASE.** It's not that the concept of converging separate security controls and replatforming them in the cloud fails to resonate as a standalone trend. ESG's position since the very beginning has been that this is a distinct initiative, and in fact was the basis of the [elastic cloud gateway](#) architecture concept introduced in August 2019. But the SASE horse is out of the barn and has become synonymous not just with network and security consolidation, but security convergence, cloud adoption, and zero trust. Security services edge will get some traction for a variety of reasons, not the least of which is analysts are rating vendors in the category. But I expect end users to push back on this acronym after grudgingly embracing "SASE" over the last 2 years. Ultimately, the SASE concept has been fleshed out enough that most understand it must be a phased journey and not an all-or-nothing, single vendor network and security approach.
5. **The long-anticipated coupling of network and security teams fails to materialize.** This is really the people part of prediction #4. One of the foundational assumptions underpinning the concept of SASE is the idea that network and security teams will begin to come together. Granted, I'm bearish on that prospect looking out across even the next few years. But even with that being the case, I do not expect to see a noticeable shift in this direction in 2022. These teams are still too different, often with conflicting charters and separate measures of success, and ultimately have to navigate too much transformative change within their own areas of expertise. Certainly, a focus on fostering better collaboration, information sharing, and proactive strategy planning between the network and security groups will yield dividends for any organization, but they will remain distinct entities for the foreseeable future.

The Bigger Truth


In many ways, 2022 will be a continuation of 2021. There have been some massive transitions over the last few years, and most users continue to work through them. In that regard, 2022 will be a year more of expansion and refinement than any sudden shifts. That said, it is important for vendors to understand where the priorities will be within the broader initiatives of SASE and zero trust, to maintain visibility and help end users navigate a crowded and noisy space.

² Source: ESG Complete Survey Results, [Network Security Trends in Hybrid Cloud Environments](#), December 2021.


All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



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