FUTURIOM
FUTURE OF CLOUD TECH

Cloud Market Trend Report

Cloud Secure Edge and SASE Trends

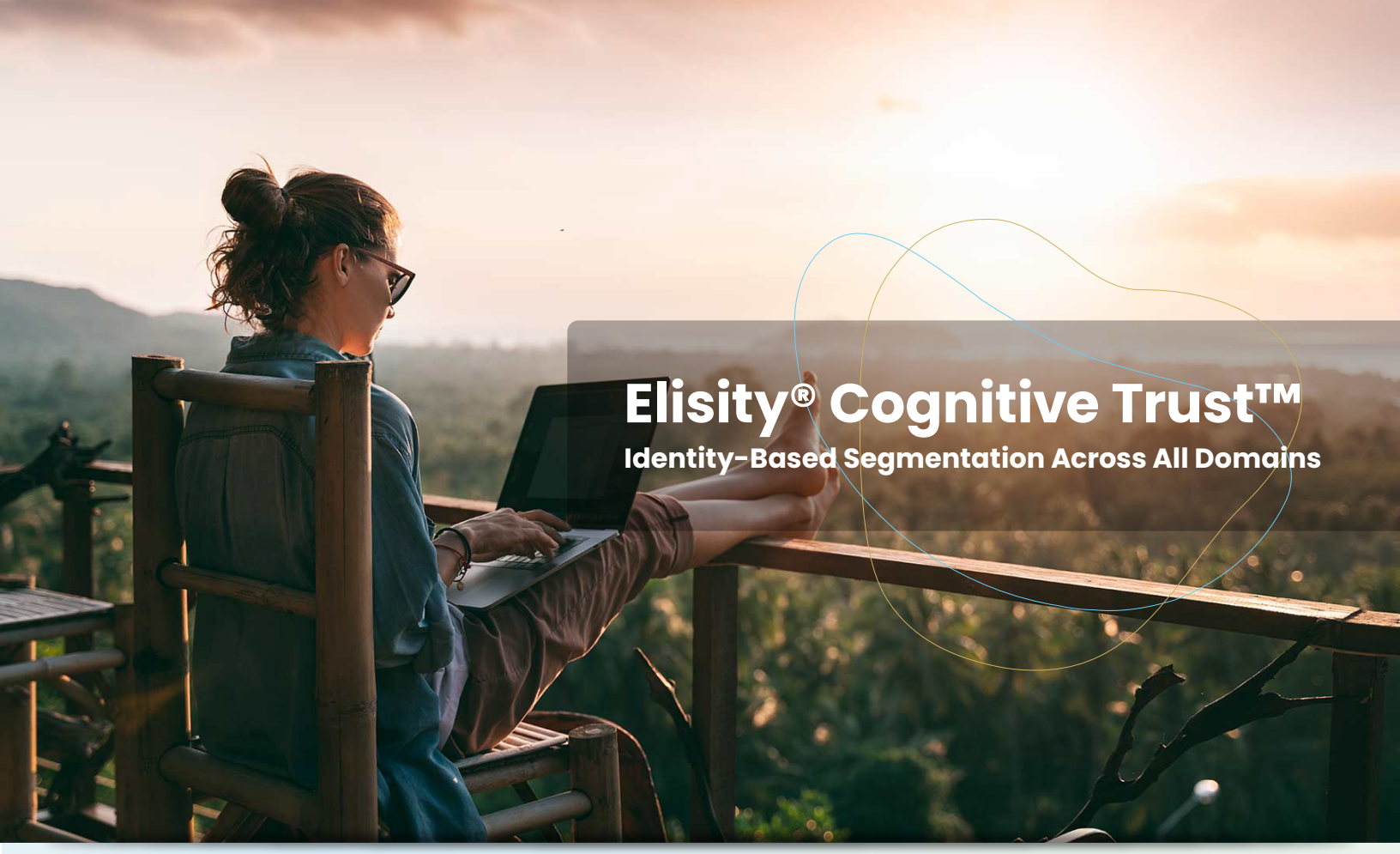
Demand for security integration, SD-WAN, and cloud services are likely to propel the secure access service edge (SASE) market upward for many years.

Sponsored by

www.futuriom.com

Cloud Secure Edge and SASE Market Highlights:

- **The SASE market is gaining momentum.** The secure access service edge (SASE) market represents an important convergence of networking, cloud, and applications security functions.
- **Integration and consolidation of security functions on the SASE platform will remain a strong trend.** End users we have surveyed and interviewed are asking for better integration of cloud and network security tools to adapt to end-user mobility, increased cloud applications access, and diverse security threats.
- **End users and technology vendors have aligned interests to drive SASE.** Core end-user needs, such as the integration of security tools and cloud networking elements, align with technology vendor efforts to consolidate and drive more value across integrated cybersecurity product portfolios.
- **SASE architectures address the need for more flexible security architectures in the cloud-based world.** Although different vendors are approaching this with a wide variety of architectures and solutions, nearly all of them are moving to flexible, services-based platforms that can be delivered to edge devices or delivered via the cloud, or both.
- **Strong M&A market expected to continue.** With many large acquisitions taking place in SASE areas such as cloud access service broker (CASB) and zero trust network access (ZTNA), expect this trend to continue as larger players roll up best-of-breed security functions into their SASE portfolios.
- **SASE is a huge addressable market.** With the opportunity to provide integration of many security functions, provide more secure cloud and remote access, and replace traditional virtual private networks (VPNs), the addressable market is tens of billions of dollars. SASE also has the potential to address and integrate dozens of other cybersecurity markets.
- **Companies mentioned in this report (partial list):** Akamai, Aryaka Networks, Cato Networks, Check Point Software, Cisco Systems, Citrix, Cloudflare, Elisity, Enea (Qosmos), Forcepoint, Fortinet, Juniper Networks, NetFoundry, Netskope, Nokia (Nuage Networks), Palo Alto Networks, Versa Networks, VMware, Zscaler.



Elisity® Cognitive Trust™

Identity-Based Segmentation Across All Domains

Elisity Cognitive Trust provides a unified access policy and control plane across all domains–campus, branch, remote, cloud, and everywhere–powered by identity-based user-to-app and workload-to-workload segmentation. Delivered as a cloud-based service, it is deployed as an overlay or underlay on whatever WAN and/or SD-WAN infrastructure an enterprise prefers to ubiquitously protect data, users, devices, and applications across all domains.

- Gain complete visibility to asset behavior
- Micro-segmentation of users, devices, and applications
- Limit the blast radius from ransomware attacks
- Secure the convergence of OT and IT networks
- Unify policy for remote and on-prem users
- Discover, secure and monitor userless devices

Request a free white glove proof of concept today!

Learn more at Elisity.com

Table of Contents

1. Introduction

Secure access service edge (SASE) is a concept initiated by the influential technology firm Gartner Inc. in 2019 as part of their “hype cycle.” And indeed, SASE is hitting the sweet spot of the hype cycle. Nearly every networking, security, and software-defined wide-area networking (SD-WAN) vendor has jumped on board the bandwagon.

What’s so appealing? The bottom line is that SASE was the right wave of technology for the right time. Although SASE does not apply to one specific cybersecurity or networking technology, it describes a basket of technologies that can be used to integrate solutions to attack multiple security challenges at once. That approach is appealing to organizations looking to build a unified security strategy.

The ubiquitous availability of mobile devices, high-speed connectivity, and cloud-based services has permanently altered how and where people work, and these advances have introduced numerous security concerns. The problem isn’t how to connect a fixed set of people, devices, and resources but rather how to dynamically connect an evolving mix of people, devices, and resources -- none of which necessarily lives in any permanent fixed physical location. These trends have complicated the provisioning of networking and security capabilities for some time. Attempts to shoehorn new business practices into old network and security architectures has led to inefficiencies in traffic routing, redundancies in equipment spending, and at times serious gaps in security protections.

Enterprise IT architectural decisions no longer revolve around computing and storage resources residing in fixed, on-premises datacenters. With the movement toward the cloud, traditional networking and security approaches need a rethinking, and this has led to a serious rethinking of the value and utility of deploying proprietary on-premises networking and security tools. These tools need to be more integrated with the cloud, using broad-based data resources of application programming interfaces (APIs) and data to drive telemetry and analytics.

The bottom line is that SASE underlines a larger trend toward consolidating technology tools and integrating them with cloud architectures. In speaking to a chief information security officer (CISO) at a major webscale company recently (he asked to remain anonymous), we learned that the major challenge today is integration of security, not the lack of functions available. In the CISO's words, he'd rather have a dozen B+ cybersecurity tools that are well integrated rather than a handful of A+ tools that aren't integrated.

"In the CISO's words, he'd rather have a dozen B+ cybersecurity tools that are well integrated rather than a handful of A+ tools that aren't integrated."

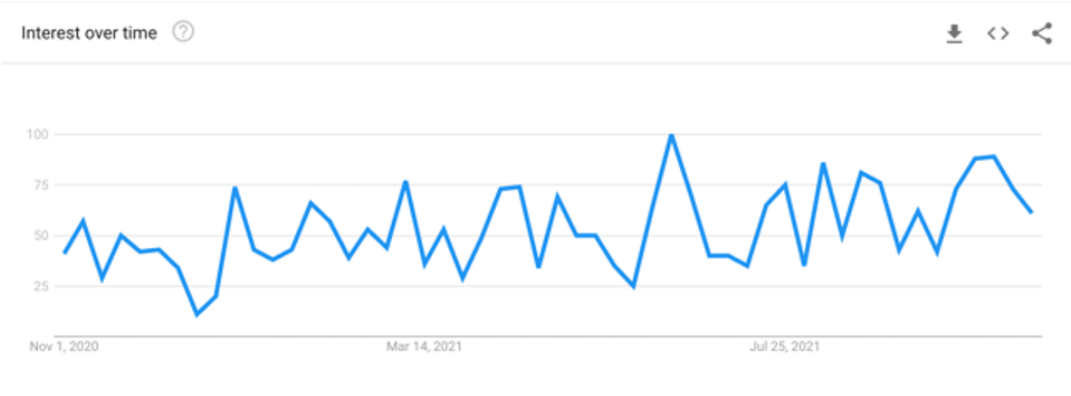
This integration is the trend behind SASE, which aims to roll up functions available on SD-WAN, CASB, ZTNA platforms, and FWaaS among many others. This report, based on months of research with end users and technology vendors, outlines the evolving definition of SASE, the market drivers, and where the SASE market is likely to go in the future.

2. Updating Our SASE and the Secure Edge Definition

Last year, we defined the SASE market as it started to gain traction. In the past year, the marketing folks have grabbed onto the theme and gone wild. In addition, this has already driven M&A activity among vendors as well as interest from end users.

SASE Is Trending

As you can see below, Google Trends shows a steady increase in SASE over time, as measured by search activity.



Source: Google Trends "SASE" search activity.

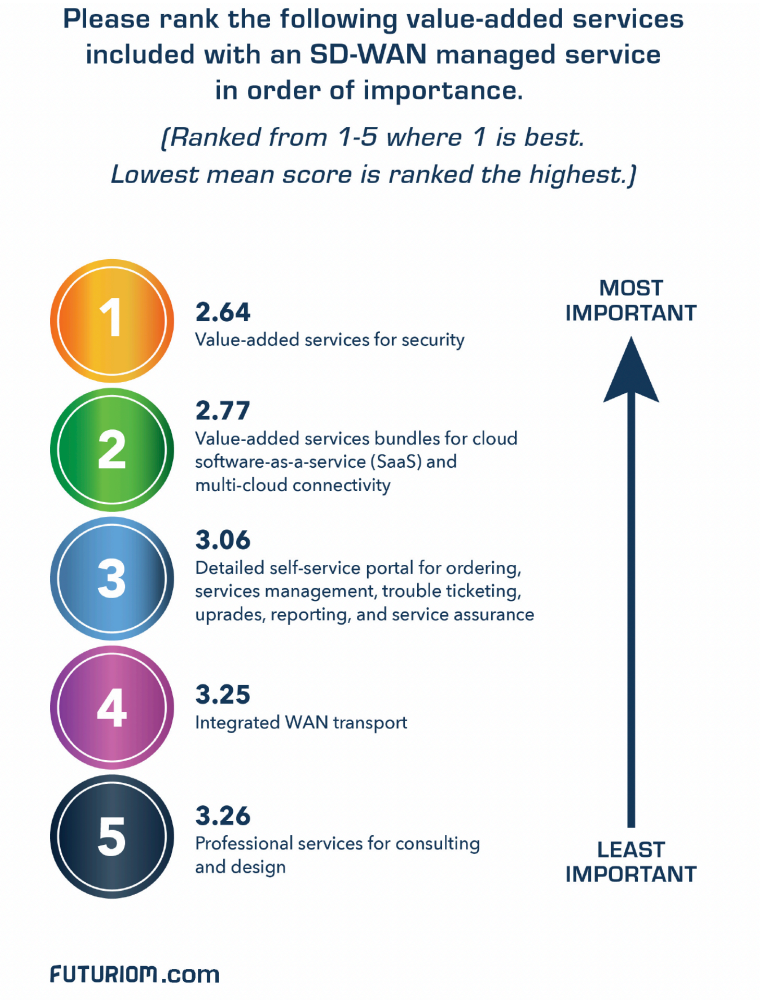
What's changed? The major themes driving the IT market include accelerated digital transformation and work from home (WFH). These trends accelerated during the pandemic. They show no signs of dissipating and they have taken deeper hold in corporate IT departments. Workers have become more mobile, applications have become more mobile, and network and security applications need to adapt.

The need for the convergence of networking and security, especially at the "edge" of the network, is well understood. Numerous technologies have appeared to facilitate the move, and the market has decided that SASE is part of that picture. For the purposes of this report we will refer to SASE as the general trend toward integration of cloud security (often traditional network security functionality migrated to the cloud) and networking functions at the network edge – which we are also calling "Secure Edge."

Extension of SD-WAN for Security

SASE started in the SD-WAN market, which enabled more efficient deployment and management of enterprise branch network connections using software-defined techniques. This is driven by end-user demand. Our 2021 Managed Services Survey of 120 enterprise end users indicated value-added security services were ranked as the highest priority for SD-WAN managed services.

Cybersecurity is still a dynamic problem that has its own area of expertise — with many niches and discrete functions —for the foreseeable future. But security does need to be better integrated into the network fabric, and that is where the Secure Edge comes in.



Secure Edge and SASE is not so much a new technology as a more strategic and rigorous integration of several existing technologies. Secure Edge and SASE also benefit from the established trend of delivering traditional network security functionality as cloud-native services.

Some of the key security functions and capabilities that are already associated with SASE and Secure Edge deployments include secure web gateways (SWGs), CASBs, firewall-as-a-service (FWaaS), and zero trust network access (ZTNA), which we will explain in more detail later. In addition, SASE vendors are increasingly integrating data loss prevention (DLP) and malware detection capabilities. All these technologies are merging under a common policy management and security umbrella that supports secure connectivity between endpoints and resources from any physical location.

At its core, SASE is a framework that attempts to further the goals of *zero trust*, which is a philosophy and an architectural goal, while SASE is a framework for implementing zero trust concepts. Zero trust goals include the following: that all connection requests should be considered potentially hostile, regardless of where they originate; that even approved access should be restricted, with connections being set up based on a policy of least-privilege access; and that those connections should be continuously monitored and authorization reassessed as appropriate.

Challenges Addressed by SASE and Secure Edge

One of the goals of SASE and the Secure Edge is to deliver security capabilities as cloud-based services. Industry consortium MEF has attempted to create standards around SD-WAN and has been an early champion of SASE and Secure Edge. The MEF defines a SASE service as "a service connecting users (machine or human) with their applications in the cloud while providing connectivity performance and security assurance determined by policies set by the subscriber." This is a tall order given that the goal is to enable any endpoint to connect to any resource.

Distributed networks have complicated security architectures. Should security devices be deployed at branch locations? Should all traffic be routed back to the datacenter for inspection (also called “backhauling”)?

What is the best way to reduce risk associated with remote users, or worse yet, contractors that might not even have an agent on their laptop (let alone one that is managed by the internal IT security team)?

Enterprises face similar questions when employees adopt cloud services. How can they provide enterprise-wide policy regarding authentication, authorization, access control, and security based on user and device identity, as well as current security posture? SASE architectures attempt to address these concerns by offering a more flexible platform for managing and delivering security applications. Although different vendors have different architectures, many of them are adopting more flexible platforms that can be delivered to edge devices or delivered via the cloud, or both.

3. Key Trends in the SASE Market

As the SASE market is driven by changing architectural needs of data centers, networking, and cloud, enterprises and organizations will need a new set of security tools to protect their cloud-based infrastructure. Backhauling all network traffic back to the datacenter for enforcement makes less sense now than ever. Indeed, with the dramatic rise in cloud consumption, many enterprises now have more users, devices, and data located outside of the traditional organizational perimeter than inside. Interestingly, decreasing the need for backhaul has been a driver of SD-WAN services, which optimize the routing of applications to cloud resources as efficiently as possible – which means the same platforms can be used to more effectively connect cloud-delivered security resources.

Secure Edge and SASE services can adapt to this architectural shift. Inspection engines can be placed at a nearby point of presence to push security enforcement decisions out to the edge of the cloud. Endpoints connect to local points of presence (PoPs) based on identity and context, and traffic is inspected and forwarded as appropriate through the Internet or provider backbone. The design connects fixed and mobile users, whether managed or unmanaged, with resources in traditional private datacenters or in the cloud. In addition, SASE services can connect to cloud security functions such as CASB.

The end result is that the SASE market is responding to the changing needs of the enterprise market, providing multi-layered drivers toward integration and consolidation of networking and security tools. Let's take a look at some of the strongest trends in the SASE market.

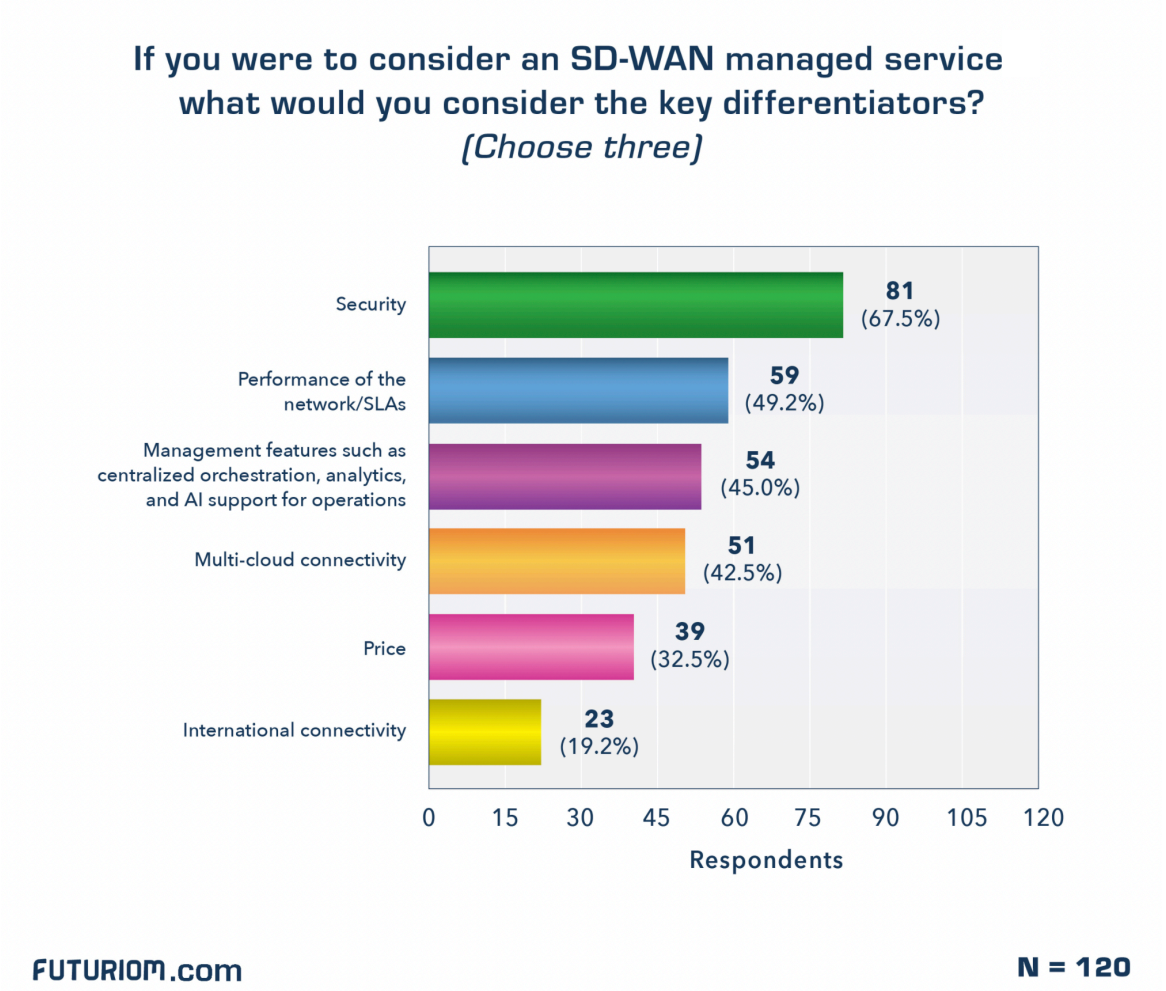
Established Technology Vendors Commit to SASE, Bundle Up

The SASE market is maturing quickly, and market activity and product development announcements were frequent in 2021. As discussed in the later sections of this report, many SD-WAN vendors are building out their SASE platforms, CASB functions are converging with SD-WAN, and cybersecurity vendors have realized the value in having a more deeply integrated portfolio. Below are some key examples.

- In February 2021, Akamai announced the creation of two new business units, Security Technology, and Edge Technology, to help it better align the company with security and edge technology solutions.

- In February 2021, Check Point launched Harmony, a unified suite of services for remote workers. Harmony combines ZTNA, SWG, DLP, next-generation firewall (NGFW), intrustion prevention system (IPS) and endpoint security. Harmony Connect Internet Access, and Harmony Connect Remote Access are positioned as SASE solutions. Other offerings in the suite include email, endpoint, mobile device, and browser security.

- In May 2021, Juniper introduced Security Director Cloud, its portal to SASE which manages on-premises, cloud-based security and cloud-delivered security – all within one User Interface (UI). Customers will be able to use Security Director Cloud to ensure security policies follow users, devices, and applications as they move locations, facilitating a seamless and secure shift to a SASE architecture, never breaking visibility or protective measures against threats. Security Director Cloud joins Juniper's Experience-First Networking portfolio, which includes AI-Driven SD-WAN and WAN Assurance which was announced earlier in the year solidifying Juniper's entry into the SASE market.



- In September 2021, Palo Alto Networks announced Prisma SASE, which brings together the Prisma Access and Prisma SD-WAN offerings. The new bundle combines ZTNA, SWG, CASB, FWaaS, and SD-WAN into a single solution. Palo Alto also announced the introduction of a new SD-WAN appliance with 5G WAN connectivity.

- In March 2021, Cisco announced that it was bundling all its SASE offerings with the option for customers to migrate to a simple unified subscription service. Cisco's security services are currently bundled under the Cisco Umbrella brand. Its ZTNA technology was acquired from Duo, and its SD-WAN hardware is supported both by Cisco and its Meraki business unit. Cisco also includes its ThousandEyes Internet and Cloud Intelligence agents as a component of its SASE solution.

- McAfee completed the divestiture of its enterprise business. The new entity, known as McAfee Enterprise, was acquired by Symphony Technology Group for $4 billion in cash. SASE will remain a primary focus for the new company.

Managed Security Service Providers Are Getting Serious About SASE

The communications service provider industry is once again under assault. Cloud services are stealing their thunder, once again threatening to relegate them to dumb pipes. Many service providers see managed services and SASE as an answer. They are stepping up their game in providing integrated security and network services.

The Futuriom 2021 SD-WAN Managed Services Survey, which surveyed 120 enterprise end users, showed that 67.5% of those surveyed said that security was the key differentiator in offerings.

Service providers are aware of this trend and have been adding to their portfolio of both SD-WAN and SASE managed services. Here are some examples:

- AT&T: In March 2021, AT&T Cybersecurity launched AT&T SASE Branch with Fortinet. In June 2021, AT&T also announced a partnership with Palo Alto to deliver a managed SASE service called AT&T SASE with Palo Alto Networks.

- Verizon: In June 2021, Verizon announced Advanced SASE, delivered as a single-provider managed solution that leverages Verizon Business's expertise in managed services. Initial technology partners include Versa Networks and Zscaler. Verizon Business promises to continue to expand its partners network to offer additional SASE services.

- Tata Communications has developed an extensive managed services security portfolio to enable its customers to secure their data, users, and infrastructure by leveraging an integrated secure access solution - Global Security Internet Gateway Service (GSIGS) 2.0. Based on SASE and ZTNA principles, GSIGS 2.0 is a secure gateway solution that offers fully managed secure network transformation for enterprises.

- IBM: In August 2021, IBM announced new SASE services. The IBM solution employs Zscaler's SASE products and services.

  IBM customers will also be able to leverage the company's managed security services, which include around-the-clock security monitoring, management, and continuous improvement of the SASE solution to evolving threats.

- Cloud NaaS vendors are also ramping up their own services. For example, Cato Networks offers SASE services on a subscription basis to enterprises across 190 countries worldwide (more on that below).

M&A Activity Continues Unabated

As we have described, SASE underlines a trend toward integration. Integration means that companies must expand and converge their cybersecurity portfolios. That means M&A.

Here's a look at just some of the M&A activity that has highlighted the SASE market over the past few months:

- Akamai: In September 2021, Akamai acquired Guardicore, an Israel-based micro-segmentation vendor for a reported $600 million.

- Aryaka: In May 2021, Aryaka closed on its acquisition of Secucloud GmbH, a security-as-a-service vendor based in Germany. Secucloud's platform supports cloud-based firewall-as-a-service and secure web gateway with additional threat protection capabilities.

- Comcast Business: In August 2021, Comcast acquired Masergy, whose Performance Edge technology allows users to leverage SASE and SD-WAN services over public broadband connections. Masergy's portfolio includes Managed SD-WAN, Unified Communications as a Service (UCaaS), Call Center as a Service (CCaaS), and Managed Security solutions.

- Forcepoint: In October 2021, Forcepoint acquired Bitglass, one of the few remaining independent CASB vendors. Bitglass was considered a leader in the CASB market and had built out a much more complete SASE portfolio that included SWG and ZTNA.

- Jamf: In May 2021, Jamf, a provider of enterprise management software for Apple devices, acquired Wandera, a provider of ZTNA for mobile devices. The deal was valued at $400 million. In addition to ZTNA, Wandera will extend Jamf's Apple Enterprise Management platform with mobile threat defense and data policy features.

- Lookout: In March 2021, Lookout, which is known primarily for its mobile security products, acquired CipherCloud for its SASE technologies. CipherCloud's SASE portfolio includes CASB, ZTNA, SGW, and DLP.

Investment in SASE Companies Remains Strong

SASE remains a fertile area of investment, with many independent startups scaling up.

- In July 2021, Netskope announced $300 million in additional investment funding. That brings the company's total funding since it was founded in 2013 to more than $1 billion.

- Cato Networks in October announced $200 million in Series F funding on a valuation of $2.5 billion – more than double its last "unicorn" valuation after raising $130 million less than a year ago. The round brings Cato's total funding to $532 million and attests to the momentum behind the vendor's approach to a SASE solution. Cato's Series F was led by Lightspeed Venture Partners with the participation of existing investors Greylock, Aspect Ventures/Acrew Capital, Coatue, Singtel Innov8, and Shlomo Kramer.

- Versa Networks, based in San Jose, Calif, is a private company in the SASE market that announced a Series D round of funding ($84 million) in June 2021. Versa has raised a total of almost $200 million since it was founded in 2012.

- Elisity, a startup led by Cisco, Meraki, and Viptela veterans, recently closed a $26 million Series A funding round co-led by Two Bear Capital and AllegisCyber Capital, with previous investor Atlantic Bridge also participating. Elisity takes an interesting approach to address the blind spots of SASE architectures by offering a virtual network overlay over existing infrastructures and unifying identity-driven policy and control planes for users, devices, and applications across campus, branch, cloud, and remote access.

DLP, MDR, and AIOps Also Grab Interest

Yes, the cybersecurity market is a soup of acronyms and buzzwords. But that's because of an expansion of the technology innovation that has created new ways to monitor, detect, and respond to risks. Tactical cybersecurity technologies such as artificial intelligence (AI) and outsourced capabilities such as managed detection and response (MDR) have been enabled by the cloud. These can be integrated into many platforms, including SASE.

- AIOps for identifying networking and security optimization opportunities is also drawing interest. For example, Palo Alto and VMware have been vocal about the benefits of AIOps integrated with SD-WAN, as have startups Masergy (recently acquired by Comcast Business), and Open Systems.

- DevSecOps, also often labeled as security as code, puts secure networking into the heart of the application development and delivery lifecycle. So, rather than start implementing SASE after the apps and networks are built, DevSecOps focused companies like startup NetFoundry enable development and xOps teams to embed Zero Trust networking into the actual application, and then enable AIOps type technology to manage the combined solution as code.

- DLP and MDR are currently seeing considerable interest from customers and vendors. For example, several prominent vendors are positioning their SASE solutions with an emphasis on their DLP heritage. This includes Symantec Data Centric SASE and Forcepoint Data First SASE.

SASE Differentiators

Zero trust is a philosophy and an architectural goal, while SASE is a framework for implementing zero trust concepts. Vendors will increasingly differentiate on breadth of offerings, even as customers approach SASE initially more tactically. That is, customers are currently addressing tactical pain points, such as remote work, but with an eye toward more strategically embracing SASE. Hybrid work requirements, which exploded during COVID, will become a permanent option for most knowledge workers. Simplified deployment and pricing options will remain important, which will provide additional opportunity for managed-service providers.

At its core, Secure Edge and SASE technologies can be built on a global SD-WAN foundation that leverages a suite of cloud-based security capabilities along with a minimal layer of customer premises equipment (CPE). Ideally, everything is orchestrated, performed, and processed within the cloud service and problems are solved first with software and only if necessary,with hardware.

There are dozens of characteristics associated with SASE, but the following attributes will be essential as differentiators:

Integration with the SD-WAN footprint. With its separation between the management plane, the control plane, and data plane, SD-WAN provides an ideal foundation for Secure Edge. SASE and Secure Edge service providers are striving to support a global SD-WAN service with worldwide PoPs, although some service intelligence will remain local and on premises.

Distributed policy enforcement and inspection. Security inspection and policy enforcement are enforced across a cloud-based Secure Edge provider's PoPs without the need to backhaul traffic.

Identity-focused approach. User identity is the key attribute for delivering security and network access, not an IP address. The MEF, for example, recommends the use of the following identity attributes: name of person, employee ID, MAC address of laptop, unique ID of IoT device.

Context aware. Access policy decisions should consider the context of the connection request. The context of a subscriber identity could include location, time of day, endpoint risk assessment, strength of authentication, and device characteristics, among other attributes.

Cloud-native security architecture. To ensure scalability and optimal cost advantage, the Secure Edge service should use a converged multi-tenant cloud-native software stack. The goal is to avoid a discrete chain of networking and security devices that perform multiple consecutive data inspections.

4. Expanded SASE Use Cases and Adoption

SASE solutions need to support a stack of security and networking services that can be delivered based on policy and use case. With SASE, the network perimeter is completely reconsidered. Instead of a traditional physical demarcation, such as a DMZ, the perimeter is a logical boundary that is mediated through a set of dynamic edge services. Ideally, these services will be built for and deployed natively in the cloud. But other types of integrations will be common, such as a security stack delivered through SD-WAN customer premises equipment devices.

SASE by definition needs to handle use cases at every edge: datacenter, branch, cloud, mobile, and unmanaged. Interoperability demonstrations will be important for all vendors, but as with all new security architectures, there is hope that organizations will be able to consolidate their security vendor list as they move to adopt unified SASE solutions.

SASE and Secure Edge will have to integrate many of the most common security approaches. On a high level, the key security use cases fall into four main categories:

- **Visibility:** Who is using cloud services in an organization (whether sanctioned or not), what the risk profile is of that user, and what data is being transmitted.
- **Data Protection:** DLP enforced for cloud assets.
- **Threat Protection:** This can include a diverse set of functionalities, such as malware, ransomware, and bot protection.

Use Cases Evolve

One can think of SASE and Secure Edge as a best-of-breed approach to networking and security that addresses many different access scenarios. As with any best-of-breed solution, the devil is in the integration details. As a first step, components need to share an understanding that the

identity of the entity requesting a connection is the critical determinant of access decisions, not IP addresses or physical location by themselves. From a foundation of access policies built on identity and security posture context, interoperability can find a footing.

Below are some of the new use cases and targeted applications of SASE products.

Hybrid workforce access: VPN augmentation or replacement to provide better scalability, management, and security for hybrid or remote work.

Compliance: This will be an important benefit to many early adopters who are driven by COVID 19-related changes to remote-work policies. Security policies can be tailored to geographies, specific industry regulations, and generalized privacy needs, such as data disclosure restrictions and anonymization.

Multitenancy for managed services: As a software- and cloud-based platform, SASE is naturally suited to multitenancy. The economics of multitenancy will remain extremely attractive. Cloud providers that can spread costs over multiple customers can have extremely competitive cost structures. The degree to which a SASE solution utilizes hardware will be one consideration when looking at bundled solutions. A chief appeal of SASE is also the low latency and scalability that is inherent in creating a stack of network security capabilities that can be invoked using a "single pass" architecture that runs multiple policy engines in parallel rather than as a series of discrete inspections.

Securing edge IoT applications. As is discussed throughout this report, SASE is an important component of enabling organizations to fully embrace network transformation. Increasingly, SASE engagements will be driven by adoption of 5G and IoT.

ZTNA/software-defined perimeter (SDP) adoption. This market is currently driven by VPN augmentation or replacement, which is a key target of SASE. ZTNA/SDP products and services reduce the attack surface of assets by limiting access to and visibility of resources. For example, ZTNA/SDP solutions provide application-level, instead of network-level, connections to applications and they can eliminate the need to expose applications to potential hackers with direct Internet connections using a Trust Broker.

CASB functionality. CASBs control access to cloud applications by managing security-policy enforcement requirements. They can manage single sign-on, authentication and authorization, device profiling, encryption, and audit and logging. CASBs can also support DLP and anti-malware capabilities. Specific use cases include uncovering shadow cloud-based IT and identifying account takeovers. As described in the section on M&A activity, the CASB functionality is being rapidly subsumed by SASE vendors and is likely to go away as a standalone market in the future.

SD-WAN and MPLS Replacement. The SD-WAN market has expanded into cloud security and SASE. The first high-value use case for SD-WAN was using software and cloud services to secure private IP and Internet circuits as an adequate replacement for more expensive Multiprotocol Label Switching (MPLS) services, which turned out to be a hit with enterprises, fueling its growth. The next step was adding value-added cybersecurity services. SD-WAN technology still has many benefits, including software-based management, applications prioritization, and improved security. The end users that Futuriom regularly speak to frequently cite SD-WAN's capabilities as an orchestration platform for a variety of networking services – including security. Typically, when SD-WAN users are selecting or installing SD-WAN platforms, they are doing the same for firewall- and cloud-based security services. If they have a platform that offers both SD-WAN and Secure Edge functionality, they are likely to consider the security solutions paired with the SD-WAN product, whether it's through direct integration or service-chaining with a cloud security service.

5. Key SASE Segments and Players to Watch

The Secure Edge and SASE markets remain crowded and extremely dynamic. As we have already discussed, vendors are approaching the market from numerous directions. In addition to SD-WAN vendors, we will discuss leading vendors in the CASB, FWaaS, SWG, and ZTNA/SDP markets, but keep in mind that the whole of network security could eventually be subsumed into SASE.

The CASB Market Evolves

Independent CASB vendors are increasingly becoming an endangered species as they are acquired by larger SASE players. M&A activity in the segment has been brisk. Lookout acquired CipherCloud and Forcepoint recently acquired Bitglass – both this year. McAfee acquired Skyhigh Networks in 2018. Forcepoint acquired Skyfence (through Imperva) in 2017. Proofpoint acquired FireLayers in 2017. Cisco acquired Cloudlock in 2016. And Symantec acquired Blue Coat Systems in 2016, which owned the assets of Elastica and Perspecsys. Microsoft acquired Adallom in 2015. Palo Alto Networks acquired CirroSecure in 2015.

Cisco, Forcepoint, McAfee Enterprise, Microsoft, Palo Alto Networks, Proofpoint, and Symantec are currently integrating acquired CASB technology into their larger security portfolios. The next couple of years are going to be painful for some of these vendors as they work to re-architect their broader portfolios to support native cloud deployment use cases. But most of the leading CASB vendors have already been acquired.

Netskope remains one of the few large independent CASB vendors. The company realizes it needs to continue to expand its capabilities and has positioned its security solution as next-generation SWG, which includes CASB, SWG, and DLP extended through a network of global PoPs.

FWaaS and SWG Segments

The consolidation of network security functionality is a well-established trend with NGFW and unified threat management (UTM), but the introduction of new threats has historically led organizations to keep adding new security products to their portfolios, making an overall reduction in the total number of security vendors they work with difficult even with the ongoing consolidation of legacy products.

As we have already seen, there is significant overlap between the leading firewall and SWG vendors, but the products have historically remained distinct. With its cloud-native architecture, SASE enables a suite of inspection engines to operate simultaneously in a single pass of

the data. As has been mentioned, scanning for malware and sensitive data will become more common in these solutions as will DNS security.

Leading firewall vendors include Barracuda Networks, Check Point Software Technologies, Cisco Systems, F5 Networks, Fortinet, Hewlett Packard Enterprise, Juniper Networks, McAfee Enterprise, Palo Alto Networks, Symantec, Tufin, Versa Networks, and Watchguard. Next-gen cloud service Cato Networks has its own FWaaS.

Leading SWG vendors include Barracuda, Check Point Software Technologies, Cisco, Citrix Systems, ContentKeeper, Forcepoint, iboss, McAfee Enterprise, Menlo Security, Sangfor, Symantec, Trend Micro, Versa Networks, VMware, and Zscaler. Menlo has become a key partner of VMware.

Traditional security appliance vendors have been very active in building out full SASE capabilities. Two hardware vendors with strong reputations, Fortinet and Palo Alto Networks, are leveraging those traditional strengths with managed security services providers (MSSPs). As mentioned, AT&T Cybersecurity launched AT&T SASE Branch with Fortinet. AT&T has also partnered with Palo Alto to deliver a managed SASE service: AT&T SASE with Palo Alto Networks.

Juniper Networks has recently made some impressive gains in a beefed-up security portfolio that now includes NGFW, advanced threat protection, encrypted traffic inference, session-based and secure vector routing, cloud workload protection, and a centralized cloud-based security management product, called Security Director Cloud. Juniper's acquisition in 2020 of 128 Technology for its Session Smart SD-WAN capabilities has many SASE applications.

Another vendor to keep an eye on is McAfee. In July 2021, McAfee completed the divestiture of its enterprise business. The new entity, known as McAfee Enterprise, was acquired by Symphony Technology Group for $4 billion in cash. SASE will remain a primary focus for the new company.

SD-WAN and Secure Edge Networking

SD-WAN is ground zero for SASE and Secure Edge development, as larger companies as well as startups buy, merge, or continue to build out their portfolio to position themselves for the convergence of SD-WAN and SASE. Large network equipment vendors that have built or bought their way into the market via SD-WAN include Cisco (Viptela), Nokia (Nuage Networks), and HPE (Silver Peak). Virtualization giants with SD-WAN offerings include VMware (VeloCloud) and Citrix, which also happen to be building secure virtualized environments – VMware with Workspace Security and Citrix with Workspace and Citrix Cloud.

VMware has made a concerted effort to integrate security with networking in its pursuit of end-to-end "intrinsic" security, as it calls it. Its NSX virtual networking provides microsegmentation for datacenter networking and it has now positioned VeloCloud as a full SASE offering. VMware partners with Menlo Security on the SWG side, and it recently launched what it calls an "inline CASB" as part of its SASE product.

Nokia's Nuage Networks Virtualized Network Services (VNS) has been a longtime presence in the SD-WAN market, enabling users to build virtualized services across a network spanning traditional branches, private data centers, and the leading public clouds, all from a single IT governance platform. On the security side, Nokia/Nuage has an integrated NGFW, but it has opted to go the partner route on more expansive security functions. Nuage interoperates with a wide range of security technology partners, including Zscaler.

The large firewall security vendors are starting to focus on the SD-WAN and SASE space as the traditional firewall market becomes less of a growth engine. It is notable that two leaders in the firewall market – Fortinet and Palo Alto Networks -- have made key moves to expand their SD-WAN offerings, with Fortinet building an SD-WAN product internally and Palo Alto buying Cloudgenix.

Cato Networks operates its own security network as a service (NaaS) providing a range of security services including SWG, FWaaS, VPN, and MDR from its own cloud-based network. Cato operates its own private global backbone through which it can also offer SD-WAN, remote

access, and native cloud connectivity. Versa Networks has a multitenant SD-WAN and security platform and has added new security products geared toward remote environments. It now has a full suite of security offerings, including CASB, SWG, threat detection, FWaaS, and ZTNA. NaaS provider Aryaka Networks offers its own security portfolio and recently targeted remote access security in its acquisition of Secucloud.

Going forward, as the SD-WAN market consolidates, the capability to deliver full-fledged SASE and Secure Edge functionality with SD-WAN capabilities is going to be a key differentiator.

ZTNA, SDP, and Identity Security

You may have noticed there is a theme here. In the interest of providing end users with better integration and full security functionality, the security markets are undergoing an enormous amount of consolidation, driven by the SASE movement. Just as markets such as SD-WAN and CASB have been a focus of consolidation, the ZTNA/SDP market is going to undergo considerable consolidation over the next several years. Moving toward a zero-trust orientation is one of the larger goals in enterprise security over the last decade. Futuriom believes that ZTNA/SDP is not only an important component of SASE deployments but also an important proof point to encourage the further adoption of a global zero-trust posture. Compared to other SASE security services, ZTNA is relatively new, but SDP was first coined by the Cloud Security Alliance (CSA) in 2013.

ZTNA/SDP vendors, as a class, were in the right place at the right time. Now that the party has come to them, we expect that they will move to expand their portfolios to include more Secure Edge functionality through acquisition, partnership, and product development. For example, one area to watch is the convergence of virtual networking and ZTNA with SWG. There are dozens of ZTNA/SDP vendors in the market, and many are offering functions as cloud-based services. These cloud-based versions are of the most interest to this Secure Edge discussion. Cloud-based ZTNA/SDP vendors include Akamai, Axis Security, Cato Networks, Cisco Systems (acquired Duo Security in 2018), Citrix, Cloudflare, Cognitas Technologies, Elisity, Google, InstaSafe, NetFoundry, Netskope, Okta, Fortinet, Palo Alto Networks, Perimeter 81, Proofpoint,

SAIFE, TransientX, (acquired by Deloitte in July 2021) Wandera, Versa Networks, VMware, Zero Networks, and Zscaler.

Many of these companies have unique approaches. For example, NetFoundry, one of the first ZTNA providers (back when it was mainly labeled as SDP), replaces IP addresses with X.509-based certificates to ensure each flow starts with a bi-directionally authenticated secure identity. This identity extends to apps which compile on NetFoundry SDKs, which means that apps (API, microservice, database query, IoT device, etc.) can leverage ZTNA across unmanaged devices, edges, cloud platforms, and networks without deploying an agent or relying on DNS or SAML integrations.

We've also noticed a new crop of startups focusing on identity-based security. The idea behind identity-based security is that managing policy-based access through networking hardware and devices is too cumbersome. It also may no longer be relevant in a cloud-based world. Identity-based security solutions and ZTNA can provide a more flexible way of securely providing access to applications. In addition to many of the providers mentioned above, some intriguing new startups in this space include Elisity, Infiot, and Prosimo. While all of these companies have slightly different approaches, the idea is to use software and identity-based trust systems to establish secure access, obviating the need for traditional VPNs or policy-based networking tied to individual networking platforms.

Elisity Cognitive Trust is an interesting pure-software solution that leverages the customer's existing hardware containers wherever available to create micro edges that work as adaptive policy enforcement points and SDP gateways. These PoPs inspect and control east-west traffic, thus enabling micro-segmentation. This approach allows for policy enforcement as close to the assets as possible, thus avoiding hair-pinning traffic to a data center, which would limit network performance and scalability.

And Some of the Other Elements…

If you haven't gotten the picture yet, SASE is likely to be a landing pad for many diverse security technologies. A couple of the other technologies we have mentioned include DLP and MDR. And of course there are other acronyms involved! Let's take a look at some of them.

DLP technologies have been used for years to protect sensitive information. These technologies have been deployed in the network and on endpoints. DLP features are commonly available in SWGs. It is therefore no surprise that DLP would quickly appear as an element of SASE solutions. Not surprisingly, vendors with strong DLP heritages, such as Forcepoint, McAfee Enterprise, and Symantec, have been vocal champions of this strategy, but so have many others.

MDR is a security service that delivers continuous threat detection and recommendations for how to respond to attacks. We are beginning to see MDR called out as a component of SASE solutions, most notably by Cato Networks and Open Systems. We expect this trend to continue.

Network analytics will be a key enabling technology for SASE. For example, Enea's Qosmos unit has an intelligent network traffic analytics product, the Qosmos ixEngine, that recognizes and classifies over 3,600 protocols. Qosmos ixEngine is designed for integration into third-party applications, and it can be used to help deliver SASE networking and security functions, ranging from SD-WAN to NGFW and CASB.

There are numerous additional security capabilities that can and should make their way into best-of-breed security solutions. These could include SSL interception; content isolation; advanced threat protection, including dynamic detonation; IPS as a service; DDoS/WAF as a service, DNS security, and cloud security posture management (CSPM). An additional segment that has the potential to move more aggressively into SASE and Secure Edge is content delivery Networks (CDNs). Vendors such as Akamai and Cloudflare have already built out extensive global infrastructure to deliver resources close to their customers. We expect CDN vendors to continue to add security services to their portfolios. Akamai has a long history of providing security services, including ZTNA solutions.

6. Conclusion: The Future of SASE Is Big and Complex

The broad and evolving SASE market leaves it particularly vulnerable to vendor hype and exaggeration. Many vendors may well have capabilities that fit into the category described as SASE, but that does not a complete Secure Edge and SASE solution make. What that means in practice is that it is up to customers to do their due diligence with respect to functionality, architecture, and particularly to interoperability.

The addressable market is also huge. With the VPN market alone estimated at $50 billion or so, it's safe to say that SASE will include many cybersecurity markets and niches. It's clear that the total addressable market (TAM) in the tens of billions of dollars. The winners will be able to roll up several markets in one and achieve stellar market growth.

Despite the hype, end users should be wary. Many of the benefits claimed for ZTNA/SDP were being made for Network Access Control (NAC) products in 2006. Every time we try to address the disappearing perimeter, we end up rethinking identity and context in ways to better deliver secure and fine-grained access control. SASE promises important benefits and integration across many of these approaches, but organizations should be strategic, with phased rollouts that can provide immediate value, contain costs, minimize disruptions, and provide tactical wins to maintain momentum for broader adoption.

A chief concern is complexity. Many of these Secure Edge solutions will be stitched together through vendor partnerships or M&A activity. All the classic considerations between best-of-breed vs. unified suite should be considered when evaluating these solutions. Third party interoperability testing is highly desirable.

The benefits of unified management that are possible with a pure-play Secure Edge or SASE vendor are attractive to be sure, but these vendors tend to be smaller, younger, and comparatively less well funded. Building out a global network of PoPs is not as expensive as it used to be, but it is far from a DIY project. Some SASE vendors are leveraging third-party IaaS as opposed to building out PoPs with colocation facilities.

And what about agents? Many use cases require an agent on the endpoint. The complexity of managing multiple security endpoint agents has been an industry concern for many years. Solutions built through partnership or acquisition will often require the deployment of multiple agents. Even then, platform support might be limited.

Deployment Considerations

Organizations need to be thoughtful in adopting SASE so as not to further complicate endpoint security management.

Questions to consider include the following:

- How much hardware at the on-premises edge makes sense going forward?
- Are the legacy network security vendors moving their portfolios in a direction that will allow them to fully exploit a Secure Edge or SASE architecture?
- Have existing network security investments embraced native cloud deployments?
- What does your networking and security refresh schedule look like over the next three years?

On the bright side, the market is helping make progress toward cybersecurity integration. Several product themes emerged in 2021. Most importantly, several leading vendors announced their first efforts at unifying their product portfolios into coherent SASE suites. We also began to see the much-anticipated support for 5G connectivity in SASE edge appliances. The appearance of MSSPs in the SASE space is also no surprise. Those managed services leverage SASE solutions discussed in this report.

Build, Buy, or Buddy?

As noted earlier, SASE is not brand-new technology; rather, it is the integration of several existing technologies. The combination is required to enable customers to connect and secure endpoints regardless of the edge use case. Many vendors are augmenting their portfolios with a combination of acquisitions, partnerships, and internal development.

Large networking incumbents are keenly aware that the window of opportunity is closing and they have made strategic moves to snap up many security and SD-WAN companies. Partnership and OEM relationships are also common both for technology vendors and service providers.

Established vendors will use SASE as a cybersecurity roll-up strategy to chase some of the faster-growing companies that have more recently come to market. As seen in the chart below, the growth of security companies with cloud-based architectures, such as Zscaler, Okta, and Cloudflare, have been growing at a faster rate than traditional networking and security vendors. This is why SASE has grabbed the attention of established networking and NGFW vendors such as Cisco, Check Point, Palo Alto Networks, Fortinet, and Juniper, many of which have quickly pivoted to a broad-based SASE strategy, with mixed results. Their success will bear out in the numbers, so growth will be interesting to track. One notable point from the data below, drawn from company reports on security revenue in the 1H of 2021, is that Cisco's efforts to bundle its security portfolio and many acquisitions has not resulted in growth, while vendors such as Fortinet, Palo Alto, and Juniper Networks have been growing nicely.

	Date of report	Revenues	% Change
Zscaler	July 31, 2021	$197.1 million	57%
Okta	July 31, 2021	$316 million	57%
Cloudflare	June 30, 2021	$152.4 million	53%
Fortinet	June 30, 2021	$801.1 million	30%
Palo Alto Networks	July 31, 2021	$1.2 billion	28%
Juniper Networks	June 30, 2021	$171.7 million (security solutions only)	11%
Check Point Software Technologies	June 30, 2021	$526 million	4%
Cisco	July 31, 2021	$823 million (security solutions only)	1%

What Does the Market Look Like in Three Years?

We are likely in the very early days for SASE adoption. A survey of 450 IT and security professionals done by Check Point Software found that although 94% of respondents were familiar with the term SASE, only 9% had begun implementation, with another 21% in planning stages.

The next several years are, therefore, going to be very much focused on organizations creating SASE strategies, which will first require the bringing together of networking and security teams to better map requirements. This effort will be further complicated as organizations more seriously consider the use of SASE to protect and connect IoT devices.

Concurrently, the SASE market will evolve and consolidate rapidly over the next three years. Over the same period, the core definition of SASE will continue to expand as new threats require new tactics. As we have discussed, DLP and MDR are currently seeing considerable interest. Network security has been a story of constant innovation against new threats and consolidation of new functionality into existing appliances.

The adoption of SASE will help to accelerate the shift of cybersecurity functionality to the cloud. This will happen over the next several years. In addition to all of the features and functions already discussed, additional services will include IPS/IDS, cloud application discovery, UEBA/ Fraud, DNS protection, obfuscation/privacy, WAF/WAAP, remote browser isolation, WIFI protection, and Network encryption/decryption. The future of network security is in the cloud.

Bottom Line

Organizations should view SASE and Secure Edge as their friend -- a trend that is pushing a wider basket of integrated cloud-based cybersecurity technologies to them in a more consumable form. But end users and market participants must also be patient in waiting for these technologies and integrations to mature and provide sensible architectures. At the same time, a gold rush is at hand, as the larger vendors scramble to acquire the “picks and shovels” they need to deliver broad-based SASE services. We’re going to see a huge amount of consolidation, integration, and M&A in the SASE market over the next few years.

7. Leadership Profile

Elisity

https://www.elisity.com/

San Jose, Calif.-based Elisity is led by veterans of Cisco, Qualys, and Viptela. It has raised a total of more than $33 million in funding. Elisity Cognitive Trust provides a unified access policy and control plane across all domains–campus, branch, remote, cloud, and everywhere–powered by identity-based user-to-app and workload-to-workload segmentation. Delivered as a cloud-based service, it is deployed as an overlay or underlay on whatever WAN and/or SD-WAN infrastructure an enterprise prefers to ubiquitously protect data, users, devices, and applications across all domains.