FUTURIOM
THE FUTURE OF TECH

Cloud Market Trend Report - 2020

Cloud Secure Edge and SASE Trends 2020

Sponsored by

aryaka

www.futuriom.com

aryaka

The Cloud-First WAN Company

#1 End-to-End SD-WAN Provider for the Cloud-First Enterprise

We Help With

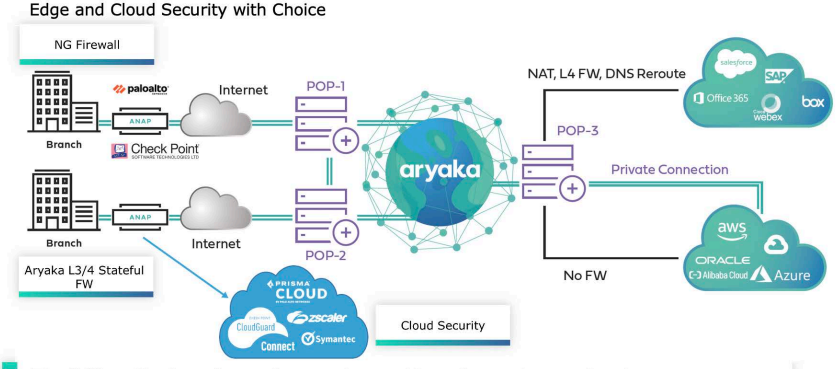
- Digital Transformation
- MPLS Migration
- Multi-Cloud Connectivity
- Paving the Road to SASE
- Application Acceleration
- Operational Simplicity and Flexibility

Why Aryaka?

- Multi-Cloud Networking made Fast and Easy
- Direct Connectivity to leading IaaS, PaaS & SaaS Providers
- Global High-Performance WAN & Multi-Cloud Fabric
- Choice of WAN Connectivity: Private Core, Internet, MPLS
- Flexible Cloud and Edge Security with Tier 1 Partners: Zscaler, Palo Alto Networks, Check Point
- The Only Managed SD-WAN Provider in the Gartner Voice of the Customer for the WAN Edge

Aryaka SmartSecure Overview

Edge and Cloud Security with Choice



Flexibility: Choice of security vendor and location, edge or cloud
DIY or Managed Security-as-a-Service

The Cloud-First WAN for dummies

Gartner Peer Insights 'Voice of the Customer' WAN Edge Infrastructure, April, 2020

1. Introduction

Networking and Security have converged. Not necessarily because they want to but because they must. This is not a new idea or a first attempt, but work habits and technology adoption have made it an imperative and have finally put it within reach. The ubiquitous availability of mobile devices, high-speed connectivity, and cloud-based services has permanently altered how and where people work, as well as made a new universe of unmanned devices economically viable.

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 infrastructure is no longer about managing devices with fixed IP addresses so that they can communicate with compute and storage resources that reside in fixed, on-premises datacenters. This has led to a serious rethinking of the value and utility of deploying proprietary on-premises networking and security devices and connecting locations primarily through dedicated Multiprotocol Label Switching (MPLS) links.

2. Defining SASE and the Secure Edge

The need for the convergence of networking and security, especially at the "edge" of the network, is well understood. Numerous technologies have appeared that facilitate the move. The term Secure Access Service Edge (SASE) is attributed in media reports to Gartner Inc. to describe and help identify this convergence of networking and security, particularly as has been spurred by the integration of Software-defined wide-area networking (SD-WAN) and security functionality. There are no specific standards for SASE, although industry group MEF is working to define some of these standards. *For the purposes of this report, we will refer to SASE as the general trend toward integration of cloud security and networking functions at the network edge – which we are also calling "Secure Edge."*

SASE and Secure Edge is an outgrowth of SD-WAN, which has now reached billions of dollars, according to our research (as predicted by our first report four years ago). This has been driven by the broad adoption of SD-WAN, which offers a software-defined architecture for deploying and managing networking and security resources and functions.

Security functionality is now being added across the board as SD-WAN morphs into Secure Edge and SASE. According to Futuriom's June 2020 SD-WAN Growth Report, the top four benefits of SD-WAN adoption are improved security, better management/agility, bandwidth optimization/ cost savings, and faster cloud application performance. One of the trends identified in this year's report is the increased integration of security features, which are now must-have stakes in the SD-WAN portfolio.

SD-WAN is a technology that has delivered on its promise. That is not to say, however, that SD-WAN solves every problem. 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 are not so much a new technology as it is a more strategic and rigorous integration of several existing technologies.

Some of the key security functions and capabilities that are already associated with SASE and Secure Edge deployments include Secure Web Gateways (SWGs), Cloud Access Security Brokers (CASBs), Cloud based firewalls (FWaaS), and Zero Trust Network Access (ZTNA) -- also known as Software Defined Perimeter (SDP) services. All of these technologies are merging under a common policy management and security umbrella that supports secure connectivity between endpoints and resources from any physical location.

What do we need to solve with the Secure Edge?

A key element of the Secure Edge is that the security capabilities can be delivered primarily 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 as it requires connecting any endpoint 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 sec teams)? 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 identity and current security posture?

Meeting these needs requires a converged networking/security/policy framework that can be used by both service providers and enterprises. This framework would describe Secure Edge services, which would be used to connect and secure digital assets regardless of their location. This requires a rethinking of both networking and network security because enterprises have spent the last three decades positioning the datacenter as the hub of network security architectures and have networked traffic flows accordingly.

Today's typical user is outside the corporate datacenter and needs resources that reside on a cloud service. The private datacenter is no longer the physical and logical core of enterprise networks. And 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.

As more mission-critical applications migrate to the cloud, the need to address security and QoS issues, such as latency, will only increase. These requirements can be at cross purposes given the time and compute resources needed to decrypt and inspect all encrypted traffic to and from the Cloud. The need for finer grain access controls that take into account the security posture of the endpoint requesting access to resources can also increase latency.

Networking and Security Convergence

This need for highly secure, low latency, access to digital assets regardless of location requires a tight integration of networking and security capabilities. Secure Edge and SASE can deliver on this promise by integrating cloud-based security services with a global fabric of points of presence that leverage SD-WAN.

Rather than forcing traffic back to the datacenter for inspection, Secure Edge and SASE services can place inspection engines at nearby point of presence. 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.

The global rollout of 5G wireless networks over this decade will further revolutionize the delivery and cost of ubiquitous bandwidth and will enable a new generation of Internet of Things (IoT) devices and use cases. This in turn will further accelerate the rapid adoption of edge computing devices as additional computing power is pushed out to enable these distributed systems.

3. Key Components of Secure Edge and SASE

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 within cloud services and problems are solved first with software, and not hardware.

There are dozens of characteristics associated with SASE, but the following attributes are essential:

1. **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 generally striving to support a global SD-WAN service with worldwide PoPs, although some service intelligence will remain local and on-premises.

2. **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.

3. **Identity-focused.** User identity is the key attribute for delivering security and network access, not an IP address. 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.

4. **Context aware**. Access policy decisions should take into account 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.

5. **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.

Secure Edge and SASE Services

Traffic inspection requirements may vary but a suite of cloud-based security services making up a Secure Edge solution would typically include CASB, Secure Web Gateway (SWG), Firewall, and Zero Trust Network Access (ZTNA).

Firewalls and SWGs are foundational network security devices, and cloud-based versions of both products will play similar roles in Secure Edge architectures. Firewalls, of course, block traffic and segment networks and SWGs provide URL filtering for both security and corporate policy enforcement.

CASB has seen amazing growth over the last couple years. CASB are designed specifically to protect data assets residing in Cloud services, be they IaaS, PaaS, or SaaS. CASBs are not anchored to existing enterprise networking or security architectures. As such they provide visibility and reach that is typically beyond existing security products.

CASB services provide four broad capabilities. Most importantly, CASB provide visibility into which cloud services are being accessed by which end users. This requires an endpoint (or browser-based) agent. Secondly, CASB provide a way to enforce access control to cloud services. Unauthorized activity can be blocked based on data-centric security and other corporate policy. These features often build on traditional Data Loss Prevention (DLP) functionality. Thirdly, CASB provide ongoing endpoint assessment and user behavior analytics to support real-time access controls. And finally, CASB support control and reporting features to assist in meeting data residency and regulatory compliance mandates.

ZTNA is another relatively new security category. These products and services build on the security doctrine that all connection requests are inherently suspect, regardless of whether they come from inside or outside the traditional network perimeter. Zero Trust is an idea that has been gaining strong traction over the last decade. Zero Trust concepts were incorporated into the Cloud Security Alliance's Software Defined Perimeter (SDP) specification that was released on 2014. SDP is a leading approach to delivering ZTNA. SDP is designed to support 5 layers of security (1) authentication and validation of devices, (2) authentication and authorization of users, (3) creation of two-way encrypted communications, (4) support for dynamic provisioning of connections, and (5) a layer of obscuration of all resources.

ZTNA/SDP solutions deliver application-level access to resources based on identity and with a least privilege model. The idea is to move away from trust built chiefly on IP address and physical location. ZTNA/SDP is often deployed as an augmentation or even replacement for VPN deployments, for secure remote access. These technologies can be used to deliver identity-driven network access control, as well as network micro segmentation to end users.

The CSA-defined SDP architecture includes initiating (e.g. laptops) and accepting (e.g., servers) hosts, an SDP controller, and SDP gateways. The hosts communicate with the controller through the control plane for authentication and authorization. The gateway provides the secure connection between hosts. Some ZTNA vendors, such as Google BeyondCorp, take a clientless approach. This is attractive for interacting with unmanaged devices but typically limits access to applications that employ HTTP/HTTPS.

Paths Toward Better Edge Security

The component security pieces of Secure Edge have to be interoperable with the underlying SD-WAN architecture. Futuriom follows the SD-WAN market closely and tracks its leading vendors. As we watch alliances form in the SASE and Secure Edge area, it's important to consider the broader strategies of each player to better predict future investments and partnerships. For example, SD-WAN has attracted vendors with very different core businesses, and very different investment strategies.

Large networking incumbents are keenly aware of this shift and have made strategic moves to position, snapping up many security and SD-WAN companies.

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. Most vendors will initially approach the SASE market through technology alliances and will assuage any potential customer concerns with interoperability demonstrations, and certification programs. Consolidation is already occurring with significant M&A activity underway.

4. Use Cases and Adoption

Because SASE and Secure Edge is an integration of existing technologies, we can examine the most popular use cases and think about how they will be implemented into a SASE architecture.

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 traditional network perimeter becomes less a physical demarcation but rather 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.

The economics of multitenancy will remain extremely attractive, however. Cloud providers that can spread costs over multiple customers can have very attractive 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.

As with many technology investments, customers need to balance the potential cost, integration, and management advantages that can come with single vendor solutions against the ability to leverage existing investments and ensure best of breed features when deploying multi-vendor solutions.

Typical Scenarios

The MEF released a whitepaper in July 2020 called the MEF SASE Services Framework, and it does a good job of providing an overview of typical security and network services and edge devices needed to connect and protect various endpoints and resources. A typical scenario has a subscriber endpoint initiating a connection through a subscriber edge device that connects out through an SD-WAN to a service provider (or datacenter) edge device. Traffic then passes through a SASE security cloud before being allowed to reach the service provider (or datacenter) endpoint.

SASE by definition needs to handle use cases at every edge: datacenter, branch, cloud, mobile, and unmanaged. This will require partnerships for many providers. MEF is taking the most visible early role in attempting to provide guidance and set expectations in the market.

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 SASE.

Use Cases and Adoption of the Secure Edge

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, all of these components need to share an understanding that identity of the entity requesting a connection is the critical determinant of access decisions, not IP addresses or physical location. From a foundation of access policies built on identity and security posture context, interoperability can find a footing.

SASE and Secure Edge will have to integrate many of the most common security use cases. Most of the key security use cases fall into four main categories:

- **Visibility**: Who is using cloud services in in organization (whether sanctioned or not), what the risk profile is of that user, and what data is being transmitted.
- **Data Protection:** Data Loss Prevention (DLP) can be developed and enforced for cloud assets.
- **Threat Protection:** This can include a diverse set of functionalities such as malware and ransomware protection.
- **Compliance:** This might be the most important benefit to many early adopters. Policies can be tailored to geographies, specific industry regulations, and generalized privacy needs such as data disclosure restrictions and anonymization.

Let's drill down and see how each of these are being applied and where they might go in the future.

VPN augmentation or replacement is currently the primary driver of ZTNA/SDP adoption. 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 through the use of a Trust Broker.

SWGs and firewalls are the most mature of the technologies that make up the core of SASE and Secure Edge solutions. The rationale for deploying them as native cloud services is by now familiar, network security capabilities need to be more naturally in the path between end users and resources without the need for backhauling and without introducing additional latency. Secure Edge solutions also need to treat access control as a dynamic process that continues throughout the lifetime of each connection. By analyzing user behavior, and remaining in the data path, security solutions can continually evaluate risk and adjust access permissions on the fly.

SD-WAN 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 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.

Futuriom expects the SD-WAN tools and software market to accelerate to a growth rate of 34% CAGR to reach $2.0 billion in 2020, $2.85 billion in 2021 and $4.6 billion by 2023. SD-WAN is experiencing explosive growth because it provides benefits over existing solutions. For example, SD-WAN can deliver significant cost benefits compared to traditional MPLS connectivity. On the other hand, SD-WAN can significantly reduce the latency issues that come with the use of public Internet connectivity. SD-WAN adoption will therefore be an important driver in the speed of SASE uptake.

5. Key Players and Areas to Watch

The number of vendors in the Secure Edge and SASE areas is large and growing. We have already discussed the leading SD-WAN vendors. Security vendors in the space likewise come into the market from a diverse set of paths. 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 be subsumed into SASE.

CASB

CASB started to appear on the market early last decade. This is one of the key areas to watch for convergence in the SASE and Secure Edge markets, because CASBs are essentially cloud-based security networks that have some of the characteristics of SD-WAN in addition to those of Content Delivery Networks (CDNs). CASB solves a lot of problems by creating a protected, proxy-based network for cloud services, and the area is experiencing rapid growth and adoption.

The CASB market has been consolidating and is fertile ground for M&A, with a fair number of acquisitions of CASB vendors in the last several years, mostly by more established security vendors. CASB vendors include Bitglass, CipherCloud, Cisco, Forcepoint, McAfee, Microsoft, Netskope, Palo Alto Networks, Proofpoint, and Symantec.

Independent CASB vendors are currently adding additional security functionality. Netskope, for example, has positioned its security solution as next-generation SWG, which includes CASB, SWG, and DLP extended through a network of global PoPs. Bitglass, for example, also offers an SWG as well as a host of zero-day threat protections.

Cisco, Forcepoint, McAfee, 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-architecture solutions to support native cloud deployment use cases. Additional security vendors will embrace SASE and additional CASB acquisitions are likely. Indeed, the remaining independent CASB vendors will be prime targets for acquisition over the next several years.

Bitglass (2013), CipherCloud (2010), and Netskope (2012) remain as independent CASB vendors. Cisco acquired Cloudlock in 2016. Forcepoint acquired Skyfence (through Imperva) in 2017. McAfee acquired Skyhigh Networks in 2018. Microsoft acquired Adallom in 2015. Palo Alto Networks acquired CirroSecure in 2015. Proofpoint acquired FireLayers in 2017. And Symantec acquired Blue Coat Systems in 2016, which owned the assets of Elastica and Perspecsys.

FWaaS and SWG

The consolidation of network security functionality is a well-established trend with next-generation firewalls (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. In addition to FWaaS and SWG, DNS security, and data loss prevention (DLP) will increasingly become components of standard SASE security suites.

Most firewall vendors now offer cloud-based versions of their products. Some products are simply virtualized versions of their on-premise appliances and customers should fully evaluate their current and future needs when looking to adopt FWaaS and SWG within broader SASE deployments.

Firewall vendors include Barracuda Networks, Checkpoint Software Technologies, Cisco Systems, F5 Networks, Fortinet, Hewlett Packard Enterprise, McAfee, Palo Alto Networks, Symantec, Tufin, Versa Networks, and Watchguard.

SWG vendors include Barracuda, Check Point Software Technologies, Cisco, Citrix Systems, ContentKeeper, Forcepoint, iboss, McAfee, Menlo Security, Sangfor, Symantec, Trend Micro, Versa Networks, VMware, and Zscaler.

Over several decades, Check Point has developed one of the broadest security portfolios. The company has been aggressive in positioning its services to address the SASE market. It continues to add functionality, most recently with the September 2020 acquisition of ZTNA start up Odo Security.

Versa is an intriguing independent SD-WAN company that has also developed its own security suite available both in the cloud and on-premises. Versa runs on VOS, a multi-tenant OS with full routing capabilities. The company says its approach dramatically decreases latency, significantly improves performance, and mitigates security vulnerabilities introduced when running multiple software stacks, service chains, or appliances. Versa services include SWG, NGFWaaS, NGFW, WAF / WAAP, RBI (beta), VDI, Sanitized DNS, Network Sandbox (beta), Network Obfuscation (via McAfee), Edge Compute Protection, CASB (beta), Legacy VPN, ZTNA-as-a-Service (Versa Secure Access), ZTNA stand-alone, routing, SD-WAN, and analytics.

Cisco has understood the need for network and security convergence as along as anyone. The company's SASE portfolio includes Cisco SD-WAN, Cisco Umbrella, which includes firewall, SWG, and CASB; and its Identity and Access solutions, which includes ZTNA technology acquired from Duo.

Fortinet also fields a broad set of Secure Edge and SASE capabilities, but the company has traditionally delivered functionally with its hardware appliances. In July 2020, Fortinet acquired ZTNA startup OPAQ to further bolster its ability to deliver cloud-based security services.

In July 2020, McAfee announced that it had certified interoperability with six leading SD-WAN vendors: Citrix, Fortinet, Viptela (Cisco), Silver Peak, VeloCloud (VMware), and Versa Networks. Silver Peak, Fortinet, and Versa Networks are also members of McAfee's Security Innovation Alliance (SIA) program.

Palo Alto Networks made a big bet on SASE with the March 2020 purchase of SD-WAN vendor CloudGenix for $420 million. Palo Alto will integrate the CloudGenix technology into its Prisma Access SASE bundle.

Zscaler is particularly well positioned to become an important player in the SASE market. The company's cloud security platform is accessible from 150 POPs worldwide. Zscaler's customers can connect via their existing SD-WAN to Zscaler's datacenter PoPs and access Zscaler's security services.

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 especially in networking, integrating its NSX virtual networking solution from the datacenter with VeloCloud for SD-WAN with various security offerings that can be bundled together. Large security vendors have also entered the space. 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.

Emerging venture-funded vendors with SD-WAN and security offerings have also evolved to expand their security focus. These include network as-a-service (NaaS) vendors Aryaka Networks, which offers a full security portfolio on its network including virtual firewall support

from both Palo Alto Networks and Check Point, as well as management of both physical and virtual firewalls. Another security-focused NaaS supplier is Cato Networks, which takes the thin client approach to SD-WAN coupled with a powerful suite of cloud security offerings. Secure Edge, SAAS, and SD-WAN vendor Versa Networks offers a multi-tenant SD-WAN platform with its own suite of security services (see above under FWaaS and SWG for more details). Versa also recently launched a cloud-managed remote security service called Versa Secure Access, part of its Versa SASE offering.

Finally, there are numerous pure play SD-WAN vendors in the market that will need to make Secure Edge plays. Others SD-WAN players to watch include Bigleaf Networks and FatPipe Networks. Going forward, as the SD-WAN market consolidates, the capability to deliver full-fledged Secure Edge functionality with SD-WAN capabilities is going to be a key differentiator.

ZTNA/SDP

Similarly, 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. The term 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 as Secure Edge momentum pushes the market toward them, accelerated in part by the need for Work from Home (WFH) solutions in response to the COVID pandemic. 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.

One interesting ZTNA pioneer, NetFoundry, recently told us how cloud-native ZTNA is being increasing integrated into multi-dimensional Secure Edge RFPs. NetFoundry offers a zero trust, high performance network platform replacing the need for VPNs – enabling customers to create a zero-trust overlay networks in minutes. The solution connects apps, edge devices/locations to any cloud with micro segmentation and cloud-native orchestration.

There are dozens of ZTNA/SDP vendors in the market and many are offered 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, Google, InstaSafe, NetFoundry, Netskope, Okta, OPAQ (acquired by Fortinet in 2020), Palo Alto Networks, Perimeter 81, Proofpoint (acquired Meta Networks in 2019), SAIFE, TransientX, Wandera, Versa Networks, VMware, Zero Networks, and Zscaler.

Some of the Rest …

While we are focused on the primary components of the Secure Edge in this report, 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. Watch for CDN vendors to continue to add security services to their portfolios. Akamai has a long history of providing security services, including ZTNA solutions.

Conclusion: Benefits, Risks, and Things to Watch For

The comprehensiveness of the evolving Secure Edge 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. Caveat emptor! 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. Third party testing is highly desirable.

It always pays to understand where we are in the “hype cycle” when evaluating a new technology, architecture, or concept. 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, but organizations should be strategic with phased rollouts that can provide immediate value, minimize disruptions, and 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 of the classic considerations between best of breed vs. unified suite should be considered when evaluating the solution.

There will be additional considerations and concerns. Keep in mind that single tenant, virtualized appliances are not the future of networking or security. Questions to consider include the following:

- Should those investments form the foundation of a broader Secure Edge solution or should security evaluations be the catalyst to retire those products or services and move to a more holistic solution?
- Have existing network security investments embraced native cloud deployments?
- How much hardware at the on-premise 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?

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's far from a DIY project. 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. Organizations need to be thoughtful in adopting SASE so as not to further complicate endpoint security management. More generally, there is currently a lack of industry agreement on SASE service attributes and this is likely to lead to market fragmentation, which may act as an inhibitor to market adoption.

What market evolution needs to occur for Secure Edge/SASE to be successful?

Secure Edge and SASE is attracting attention because it addresses pain points in today's enterprise. Proponents are not advocating that organizations fundamentally change the way they approach IT but rather that organizations take a hard look at where their resources currently reside and make networking and security investments based on where current trends have already taken them. SASE is designed to mediate the handoff at any edge, but clearly some edges are becoming more important than others.

With that in mind, organizations need to understand where broader technology trends (e.g., cloud, 5G) are leading them and approach SASE with this future in mind. Organizations may determine that some assets will gracefully age out of their current architectures. To successfully develop a SASE strategy, organizations need reasonable visibility into end user behavior and resource use. If that visibility is lacking, a good start would be in developing it through the deployment of CASB, and other tools. For organizations considering SASE deployments, CASB investments will be relatively low risk in the sense that the CASB value proposition requires

broad technology partnership and interoperability and therefore these vendors are not likely to become a dead end with respect to broader SASE integration.

Organizations should also start migrating to cloud-based network security services wherever possible, if they have not already done so. These are safer investments because of their lower switching cost if a security vendor fails to deliver on a proper SASE integration roadmap. Consolidating around a smaller group of strategic security vendors is also recommended. Vendor fatigue in managing and integrating disparate security products and services is widespread.

Regardless of where organizations start in a SASE journey, they should view third-party interoperability testing as critically important. Organizations considering SASE should make such testing a requirement in product and service evaluations. SD-WAN evaluations are an important opportunity to review WAN and security interoperability. Organizations should recognize the value of vendors that combine SD-WAN and security capabilities. That said, all SD-WAN vendors should be aggressive in building out security ecosystems with demonstrated interoperability and eventually unified management. Comprehensive SASE offerings are emerging, but most vendors are still working to bring the component pieces together. All vendors in the space need a roadmap that explains how they will provide all core SASE capabilities and deliver them globally.

What does the market look like in 3 years?

The SASE market will evolve and consolidate rapidly over the next 3 years. Over the same time period, the core definition of SASE will continue to expand as new threats require new tactics.

As we discuss in the SD-WAN Growth Report (June 2020), one of the biggest trends in SD-WAN today is integration with major cloud providers to build interconnection and virtual networking functionality at specific points of presence. Many of the SD-WAN players are taking advantage of these PoPs and virtual connection points to enable customers to instantly build far-reaching virtual WANs that connect directly with cloud services. This will help accelerate the positioning of many SD-WAN vendors as foundational SASE providers and when taken together provide a roadmap for how SD-WAN will be used to connect to multiple cloud platforms. With the use of API gateways and PoP interfaces, there will be opportunity to provide connectivity across multiple clouds.

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 much of the functionality being delivered through native cloud applications. We agree with the MEF that a full suite of security functionality will become SASE services. This will happen over the next several years. In addition to those already discussed, these services will include IPS/IDS, Cloud app discovery, UEBA/Fraud, DNS protection, Sensitive data discovery, 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 an emerging market that needs to be watched carefully over the next several years. It would be unwise over this time period to purchase any component pieces of the Secure Edge without having a clear roadmap toward a potential, broader SASE and Secure Edge deployment. Organizations should only consider vendors with a demonstrated history of success in product and service integration, techno logy partnership and interoperability, or successful M&A.

Company Leadership Profile: Aryaka Networks

Aryaka, based in San Mateo, Calif., calls itself the "Cloud-First WAN company," targeting agility, simplicity, and a great experience in delivering WAN-as-a-service. The company's optimized global network and technology stack deliver a managed Cloud-First WAN service and application performance. Aryaka's SmartServices offer connectivity, application acceleration, security, cloud networking, and insights leveraging global orchestration and provisioning. Aryaka SmartSecure offers best-of breed security as-a-service, paving the road to SASE with deployment options that are tailored to address any enterprise's particular needs due to enterprise architecture or regulatory requirements.

Cloud Market Trend Report - 2020

FUTURIOM

THE FUTURE OF TECH