A SASE MARKET SNAPSHOT:

The Convergence of Conventional Technologies with Cloud and Zero Trust Lean into SASE

RESEARCH REPORT

CYBER THEORY

A CyberTheory Research Report: A SASE Market Snapshot:

The Convergence of Conventional Technologies with Cloud and Zero Trust Lean into SASE

Published: 10 November 2020 – CT0746631

Advisory Analysts: Steve King, CISM, CISSP, Kiren Chaudry

Participating Contributors and Reviewers:

Chuck Brooks, Adjunct Faculty Professor in the Applied Intelligence Program at Georgetown University and in the Graduate Cybersecurity Program, teaching graduate level courses in Risk Management, Homeland Security Technologies, Emerging Technologies and an SME for the Homeland Defense and Security Information Analysis Center (HDIAC)

Don Cox, CISM, Global Executive CIO & CISO | Digital Transformation & Security Strategy Planning, Leadership, and former Vice President, Chief Information Security Officer (CISO) for MEDNAX, Health Solutions

A CyberTheory Research Report: A SASE Market Snapshot:

The Convergence of Conventional Technologies with Cloud and Zero Trust Lean into SASE

Published: 10 November 2020 – CT0746631

Advisory Analysts: Steve King, CISM, CISSP, Kiren Chaudry

Participating Contributors and Reviewers:

Chuck Brooks, Adjunct Faculty Professor in the Applied Intelligence Program at Georgetown University and in the Graduate Cybersecurity Program, teaching graduate level courses in Risk Management, Homeland Security Technologies, Emerging Technologies and an SME for the Homeland Defense and Security Information Analysis Center (HDIAC)

Don Cox, CISM, Global Executive CIO & CISO | Digital Transformation & Security Strategy Planning, Leadership, and former Vice President, Chief Information Security Officer (CISO) for MEDNAX, Health Solutions

Introduction

Post COVID-19 WFH and the adoption of newer technology, combined with the ubiquitous availability of mobile devices, pre-G5 high-speed connectivity and multiple cloud-based services, have resulted in a permanent alteration of how and where people work.

Secure access service edge (SASE) has entered upon this stage and is immediately being touted as the end-all solution by a host of vendors who are clamoring to become leaders in the space. A recent report by Dell'Oro Group noted that SASE is expected to grow at a CAGR of 116% from last year to 2024, or more than 20% per year!

SASE blends SD-WAN, cloud, firewalls, secure web gateways, and security functions like zero trust to help remote workers safely access their connectivity services regardless of where they may be located.

This new reality has complicated the provisioning of networking and security capabilities and has challenged the need to inject new business processes into old network and security architectures. The result has been major inefficiencies in traffic routing, redundancies in equipment spending, and serious gaps in security protections.

In addition, enterprises are faced with IT infrastructure that is great at managing devices with fixed IP addresses for communication with compute and storage resources that reside in fixed, on-premises datacenters, but is essentially useless for managing the convergence of software defined networks supporting multi-cloud environments.

As a consequence, the industry has finally begun rethinking the value and utility of deploying proprietary on-premises networking and security devices through dedicated Multi-protocol Label Switching (MPLS) links.

Secure Edge and SASE

The need for a next generation of converged networking and security is now accepted and well understood. The term Secure Access Service Edge (SASE) was coined by Gartner in 2019 to describe and identify this convergence of networking and security, and adoption has increased due to the network integration of Software-defined wide-area networking (SD-WAN) and improved security functionality.

The markets have no established specific standards for SASE, so in the interim, we will refer to SASE as the general trend toward integration of cloud security and networking functions at the network edge – which will also be known as the "Secure Edge." SASE and Secure Edge is an outgrowth of SD-WAN, which has now reached billions of dollars, according to our research.

The primary benefits of SD-WAN adoption have been improved security and 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 table-stakes in the SD-WAN portfolio.

SD-WAN is a solid technology that has delivered and out-performed its expectations. Cybersecurity, however, is still a dynamic problem space that continually morphs, obscuring unprotected domains and functions. And since security needs better integration into the network fabric, the Secure Edge arises to address that requirement.

SASE Components

While the Secure Edge and SASE are not new technologies, they represent a strategic and rigorous integration of several existing technologies. Some of the existing security functions and capabilities that are now part of many SASE and Secure Edge deployments encompass 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 have merged under a common policy management and security umbrella that supports secure connectivity between endpoints and resources from any physical location.

A key differentiator of Secure Edge is that the security capabilities can be delivered primarily as cloud-based services. Distributed networks have complicated security architectures. As such, they pose serious challenges for enterprises now that remote workers and contractors that

might not even have an agent on their laptop (let alone one that is managed by the internal IT sec teams), have expanded the threat landscape dramatically.

Addressing that challenge requires a converged networking/security/policy framework that can be used by both service providers and enterprises. That framework must describe Secure Edge services, which would be used to connect and secure digital assets regardless of their physical location. This requires a rethinking of both networking and network security because enterprises have for the last 30 years, developed their implementation architecture around the notion that the datacenter was the hub of network security architectures. Even before the pandemic, a typical user has been outside the corporate datacenter and relied upon cloud-based resources.

Network Traffic and SD-WAN

The private datacenter is no longer the physical core of enterprise networks and there has been a sizable increase in cloud consumption. These two factors have thus combined to create an environment where the backhauling of all network traffic back to the datacenter for enforcement no longer makes sense. The decreased need for backhauling has been one primary driver of SD-WAN services, which natively and efficiently optimize the routing of applications to cloud resources. This ability also translates to the same platforms being used to connect cloud-delivered security resources.

The more that mission-critical applications migrate to the cloud, the need to address latency-centric security issues will continue to increase. These requirements may find themselves 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 more granular access controls that manage the security posture of the endpoint requesting access to resources will also expand latency.

The fact that Secure Edge and SASE can deliver highly secure, low latency access to digital assets regardless of location, is based on the tight integration of networking and security capabilities. Rather than forcing traffic back to the datacenter for inspection, Secure Edge and SASE services can place inspection engines at nearby points of presence (PoPs), connecting endpoints and inspecting traffic based on identity and context. This design connects fixed and mobile users, whether managed or unmanaged, with resources in traditional private datacenters or in the cloud.

5G Impact

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, along with an exponential increase in the slope of threat vectors.

We will see a rapid adoption of edge computing devices as additional computing power is pushed out to enable these newly distributed systems. Secure Edge and SASE technologies will be built on a global SD-WAN foundation that leverages a suite of cloud-based security capabilities, like those found in superior public cloud architectures and infrastructures like the Google Cloud Platform provides, enabled by a minimal layer of customer premises equipment (CPE).

Essential Characteristics

Among the dozens of characteristics associated with SASE, the following 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 the ideal foundation for Secure Edge. SASE and Secure Edge service providers support a global SD-WAN service with worldwide PoPs, while service intelligence remains largely on-premises.

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

3. Identity-focused. The IP address has been replaced by the user identity, and is used as the key attribute for delivering security and network access. The dominant identity attributes will be name, employee ID, MAC address of laptop, and or the unique ID of an IoT device.

4. Context aware. Access policy decisions must take into account the context of the connection request. The context of a subscriber identity might include the physical location, time of day, endpoint risk assessment, strength of authentication, and device characteristics.

5. Cloud-native security architecture. To ensure scalability and optimized cost benefit, the Secure Edge service should use a converged, multi-tenant cloud-native software stack. The objective is to avoid a discrete chain of networking and security devices, and far greater security protection. 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 block traffic and segment networks and SWGs provide URL filtering for both security and corporate policy enforcement.

CASB's Role

CASB has become increasingly popular across broad global markets, and while designed specifically to protect data assets residing in cloud services, they are not anchored to existing enterprise networking or security architectures, which enables them to provide visibility and reach that is typically beyond the reach of existing security products.

CASB services provide visibility into which cloud services are being accessed by which end users which usually requires an endpoint (or browser-based) agent. CASB also provides access blocking based on data-centric and policy, which are features found in most modern DLP solutions and their ongoing endpoint assessment and user behavior analytics, controls and reporting features assist with satisfying data residency and regulatory compliance mandates.

The ZTNA Doctrine

The ZTNA doctrine assumes that all connection requests are inherently suspect, regardless of whether they come from inside or outside the traditional network perimeter. Zero Trust concepts go back to 2014 where they were incorporated into the Cloud Security Alliance's (CSA) Software Defined Perimeter (SDP) specification.

Software Defined Perimeter leads the way toward ZTNA, as it is designed to support authentication and validation of devices and users, the creation of two-way encrypted communications, dynamic connection provisioning and a layer of obscuration of all resources.

ZTNA/SDP solutions deliver application-level access to resources based on identity and a least privilege access model.

The goal is to eliminate trust built on IP address and physical location. ZTNA/SDP is generally deployed as an augmentation or even replacement for VPN-enabled secure remote access. These technologies can be used to deliver identity driven network access control, and network micro segmentation to end users. The CSA-defined SDP architecture includes initiating and accepting remote points of presence, hosts, an SDP controller, and SDP gateways. The hosts communicate with the controller through the control plane for authentication and authorization while the gateway provides the secure connection between hosts.

SD-WAN and Secure Edge

SD-WAN is an innovation that has become a replacement for existing MPLS-based networks, by delivering improved corporate network performance, agility and security. SD-WAN represents a relatively new approach to networking evolving from initial experiments with software-defined networks back in the late 90s-early 2000s when MPLS was born.

Back then, security and networking architects were beginning to focus on WAN traffic optimization, which led to SD-WAN as a concept. Building on that history, and faced with the new borderless network reality where identity is the new perimeter, SD-WAN has the unique

potential to start transforming connectivity for enterprises by connecting home, branch, and multi-cloud environments in 2021.

Obviously, the robust security of SD-WAN is not only critical for keeping the customers' traffic and data safe but is also a key enabler for the rapid adoption of the technology. In context, the component security pieces of the Secure Edge have to be interoperable with the underlying SD-WAN architecture. CyberTheory follows the SD-WAN market closely and as we observe alliances form in the SASE and Secure Edge area, it's important to consider the broader strategies of each player.

As an example, SD-WAN has attracted vendors with very different core businesses, and very different investment strategies. Large networking incumbents are precisely aware of this shift and have made strategic moves to positioning, acquiring or partnering with emerging and mature SD-WAN companies.

A SASE Framework

MEF is a global industry forum for network and cloud providers. They released a whitepaper in July 2020 called the MEF SASE Services Framework, which provides 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.

Because SASE by definition, needs to handle use cases at every edge: datacenter, branch, cloud, mobile, and unmanaged, and because it is a composite of varying technologies required to deploy, it is necessary for providers to partner with specialized vendors in the space.

MEF, as part of their mission is taking an early role in attempting to provide guidance and set expectations in the market. Their mission is to develop a global federation of network, cloud and technology providers in establishing dynamic, assured, and certified services that empower enterprise digital transformation. MEF interoperability analysis suggests a best-of-breed approach to networking and security that addresses many different access scenarios.

Fundamentally, all components need to share an understanding that identity of the entity requesting a connection is the critical determinant of access decisions, versus IP addresses or physical location, and that a foundation of access policies built on identity and security posture context will enable secure interoperability.

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

1) Visibility: The ability to see actors who are using cloud services in in organization (whether sanctioned or not), identify the risk profile of that user, and discover the exact data is being transmitted.
2) Data Protection: Data Loss Prevention (DLP) functionality that can be developed and enforced for cloud assets.
3) Threat Protection: Straight-forward malware and ransomware protection.
4) Compliance: As the most important benefit for many early adopters, native compliance assures that policies are tailored to geographies, specific industry regulations, and generalized privacy needs such as data disclosure restrictions and anonymization.

VPN Replacement Driver

VPN replacement is currently the primary driver of ZTNA/SDP adoption. ZTNA/SDP products and services reduce the attack surface 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 and the rationale for deploying them as native cloud services places network security capabilities 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.

Typically, when buyers 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 SDWAN 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.

SD-WAN and CASB Market Growth

Futuriom expects the SD-WAN tools and software market to accelerate to a growth rate of 34% CAGR to reach $2.85 billion in 2021 and $4.6 billion by 2023.

The reason why SD-WAN is experiencing explosive growth owes to its ability to provide significant benefits over existing solutions, which means SD-WAN adoption will be an

important gating driver in the speed of the SASE uptake. The number of vendors in the Secure Edge and SASE areas is already large and on a non-linear growth curve.

CASB entered the market early in the last decade and because the solution is composed essentially of various cloud-based security networks that have some of the characteristics of SD-WAN, their adoption has influenced the uptake in the SD-WAN space.

Leading CASB and SASE Vendor Markets

CASB vendors include Microsoft, Cisco, Palo Alto Networks, Bitglass, McAfee, Forcepoint, CipherCloud, Netskope, Proofpoint, and Symantec. Independent CASB vendors are currently adding additional security functionality and 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 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 near term future is going to be challenging for some of these vendors as they work to re-architect solutions to support native cloud deployment use cases.

New and existing security vendors will embrace SASE and along the way, additional CASB acquisitions will continue and the independent CASB vendors like Bitglass (2013), CipherCloud (2010), and Netskope (2012) are likely to remain as such.

Microsoft acquired Adallom in 2015. Palo Alto Networks acquired CirroSecure in 2015. Cisco acquired Cloudlock in 2016. Symantec acquired Blue Coat Systems in 2016, which owned the assets of Elastica and Perspecsys. Forcepoint acquired Skyfence in 2017. Proofpoint acquired FireLayers in 2017. McAfee acquired Skyhigh Networks in 2018.

The consolidation of network security functionality has been rapidly advancing with the maturity of next gen firewalls (NGFW), and unified threat management solutions (UTM), but the advancement of new threats has kept pace and has caused security defense vendors to continue adding new security functionality to their portfolios. The result has been an overall reduction in the total number of security vendors they work with more challenging even with the ongoing consolidation of legacy products.

Through its cloud-native architecture, pure SASE solutions will have enabled a full suite of inspection and detection capability to match the most advanced threat vectors and will be able to operate simultaneously in a single pass of the data. Supplemented with FWaaS and SWG, DNS security, and data loss prevention (DLP) capabilities, modern SASE security suites will engage with some fierce competitive positioning battles among the current market leaders in firewall and SWG solutions.

While most firewall vendors now offer cloud-based versions of their products, some are simply virtualized versions of their on-premises appliances and buyers should fully evaluate their current and future requirements when assessing FWaaS and SWG solutions within more broadly defined SASE deployments.

Firewall and SWG vendors include all of the usual suspects from Barracuda Networks to CheckPoint, F5 Networks, Cisco and Fortinet, HP Enterprise, Citrix, Forcepoint to McAfee, and a cash-rich Palo Alto Networks, Menlo Security, with strong niche players like Tufin, Zscaler, Symantec, Trend Micro, Versa Networks, and VMware in the market as well.

Check Point has intentionally developed one of the broadest, yet more focused security portfolios, and has been aggressively positioning its services to address the SASE market. The recent acquisition of Odo Security's unique clientless, cloud-delivered secure remote access adds a layer of ZTNA functionality. Unlike traditional secure remote access solutions, this technology enables users to connect through a unified portal to a wide range of applications, remote desktops, database servers, cloud and corporate servers, without the need for client or software installation.

It also enables security administrators to easily deploy the solution in less than five minutes from the cloud. This enables enhanced visibility including full audit trail of user activity, and a ZTNA to define access policy allowing the right people in the right context, with the least privileged access to applications and significantly reducing the attack surface at the same time.

Versa Networks 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 objective is to dramatically decrease latency, significantly improve performance, and mitigate security vulnerabilities introduced when running multiple software stacks, service chains, or appliances.

Significantly, 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. A fully rounded service offering in the space.

Cisco's approach to market dominance through an invigorated 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, and through the mid-summer acquisition of ZTNA startup OPAQ, it has further increased its ability to deliver cloud-based security services.

McAfee announced mid-summer 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 additionally members of McAfee's Security Innovation Alliance (SIA) program.

At the beginning of the pandemic in March, Palo Alto Networks spent $420 million on its acquisition of SD-WAN vendor CloudGenix and is integrating it into its Prisma Access SASE suite.

Partly because Zscaler's cloud security platform is accessible from 150 POPs worldwide, they are positioned to become a significant leader in the SASE market. Zscaler's customers can connect via their existing SD-WAN to Zscaler's datacenter PoPs and gain access to Zscaler's security services.

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 and recently launched a cloud-managed remote security service called Versa Secure Access, now part of its Versa SASE offering.

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 Vendors

Moving toward a zero-trust orientation has been one of the larger goals in enterprise security over the last decade and that rolling tide will pull the consolidating ZTNA/SDP market along with it.

ZTNA/SDP is an important component of SASE deployments and serves also as a defined proof point that will encourage the further adoption of a global zero trust posture.

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-19 pandemic.

There are many ZTNA/SDP vendors in the market today and it is fair to say that most are offered as cloud-based services. These cloud-based versions are the definition of true Secure Edge solutions.

Cisco's acquisition of Duo and its access management solution has solidified its zero trust approach. Combined with Cisco's micro-segmentation technology, SD-Access policy and network access solution, Cisco is staking out an early leadership position in the zero trust security market.

Illumio is attempting to arch beyond zero trust to fill a number of additional security needs, and its automation and management features are appealing to the smaller SMB market.

Illumio's workload and endpoint security platforms fit nicely into the zero trust space, and with its microsegmentation and whitelisting abilities, it can even prevent the spread of ransomware. With capabilities that span vulnerability management, microsegmentation, network visibility and encryption, Illumio has put together a strong ZTNA security offering with solid automation and management features.

Palo Alto Networks combines strong security across gateways, firewalls, intrusion prevention systems and endpoints. By acquiring Twistlock, RedLock, PureSec and CloudGenix, Palo Alto has been able to extend its security offerings into the cloud, containers, and SD-WAN, and is expanding on its strategy to achieve a future leadership position in the ZTNA space through acquisition and integrated solutions

Akamai is leveraging its dominant position in edge delivery of both data and content into an impressive platform, with zero trust at the center. With solid identity and application access, single sign-on with multi-factor authentication, and threat and DDoS protection, Akamai is able to protect a wide swath of applications while accelerating performance and emerging as a potential leader in the ZTNA CDN space.

Okta has long been a leader in access management, authentication and single sign-on and their zero trust security strategy builds on the concept of identity and access as the new perimeter, taking a never-trust, always-verify approach to everyone operating within a network. The company's Zero Trust Reference Architecture combines and analyzes risk signals across devices, identities, networks, geographies, and resources, and forces all users without exception to provide appropriate methods of authentication based on a risk posture and at each step of the way to access applications, servers, APIs, and machines.

Unisys Stealth is a surprising and yet formidable zero trust vendor that leverages their work in high-security government agencies to create a ZTNA security platform that, according to Forrester is "one of the few real applications of actual machine learning that we've seen in production in any security analytics or automation system." The Stealth software suite offers visibility, microsegmentation, identity, cloud and mobile support, and services.

Symantec, now part of Broadcom, has assembled a comprehensive portfolio of zero trust offerings that include Secure Access Cloud, Cloud Workload Protection, Web Application Firewall, CASB, Control Compliance Suite and the Symantec Protection Engine.

Symantec positions Secure Access Cloud as a replacement for VPNs. It uses SDP to blanket and protect data center resources, isolating them from end users and the internet and thus eliminating the network as an attack surface. Symantec automates it through its Integrated Cyber Defense Platform, which makes the vendor a good choice for buyers who want a one-stop shop.

AppGate SDP is another software-defined perimeter product aimed at replacing legacy VPN systems. The solution is uniformly praised by consumers owing to innovation, dynamic adaption, extremely granular access control and its native support for multi-cloud environments. For buyers looking to isolate specific environments, Appgate DP gets rave reviews.

Other vendors who are assembling components of a formidable ZTNA/SDP zero trust solution include Proofpoint, Check Point, Forcepoint, Forescout, Fortinet, Guardicore, BlackBerry, MobileIron, Netskope, Zscaler, Pulse Secure, Perimeter 81, NetFoundry, Citrix, Cato Networks, Cloudflare, Wandera, and BlackRidge.

Key Takeaways.

Lots of vendors provide capabilities that in one way or another fit into the SASE category but very few have a complete SASE solution today. The market segment is open to hype and exaggeration. Buyers should avoid the hype and fantastic messaging and instead concentrate on functionality, architecture, and interoperability.

In a classic textbook example, many of the features and functions claimed for ZTNA/SDP in 2020 were being made for Network Access Control (NAC) products 15 years ago.

Many vendors are drawn to addressing the new vacant perimeter, and in that process they come up with new and differing features around identity and context that characterize the delivery of secure and fine grained access control. Not all of these stories are true. Solution complexity is a growing concern in the space as many vendors will point to loosely defined partnerships as a way to claim a stake in the ZTNA, SD-WAN, and/or SASE segments.

Some of these will have legitimate claims based on completed integrations or tight coupling with acquirer's product suites, but a larger population of others will not be quite as unified as their marketing efforts might imply.

Building out a global network of PoPs is not as difficult or costly as it once was, but it is definitely not a summer garage-band project either. One doesn't just solve overnight, the complexity of managing multiple security endpoint agents, nor do any of these solutions intend to further complicate endpoint security management. Because we lack an industry agreement and/or standards on SASE service attributes, market fragmentation is sure to result and can act as an inhibitor to general market adoption.

SASE and secure edge proponents recognize that buyers need to carefully examine networking and security investments in the context of all of their edge computing options. Some may find that certain assets can be allowed to sunset from their current locations without further security or access considerations. Without visibility into end user behavior and resource consumption, it becomes more difficult to move immediately toward a pure SASE deployment.

For those users, CASB investments represent a relatively safe technology partnership and reliable interoperability without forestalling a more broad-based SASE integration at a point in time in the future. We believe that organizations who begin migrating to cloud-based network security services and consolidating around an intentionally small group of strategic security vendors will be better protected and prepared to pivot should one or more vendors fail to live up to their promise.

Given that the edge will soon host trillions of transactions, it presents a unique challenge around the issue of authentication and continuous re-authentication. Moving from a world in which we are used to identifying, challenging, and extending authorization for the duration, it will be critical for vendors to demonstrate that their authentication processes are continuous in nature. Between edge computing and the pervasiveness of IoT and OT devices on the network, authentication and continuous re-authentication needs to live on the edge or very close to it so as to resolve anomalies in near real-time especially under 5G traffic speeds.

Every vendor in the space will need to provide a roadmap that explains how they will deploy all core SASE capabilities and deliver them globally, regardless of their ability to provision interconnection and virtual networking functionality at specific points of presence.

The benefit to users is that while many of the SD-WAN players are taking advantage of these PoPs and virtual connection points, it enables the creation of extensive virtual WANs connecting directly with cloud services. This capability will properly position SD-WAN vendors as foundational SASE providers deploying through API gateways and PoP interfaces, expansive connectivity across multiple cloud platforms.

We also agree with the MEF that a full suite of security functionality will become the standard for SASE services and will include IPS/IDS, cloud app discovery, UEBA/Fraud, DNS protection, sensitive data discovery, obfuscation/privacy, WAF/WAAP, remote browser isolation, Wi-Fi protection, and Network encryption/decryption.

Since the foreseeable future of network security will be a complete relocation to some version of the cloud, buyers should evaluate SASE and Secure Edge in the context of emerging market conditions and establish a thorough roadmap prior to purchasing any component pieces of the Secure Edge in the hope that a little will go a long way toward the ultimate goal.

Any vendors considered should be able to produce a demonstrated history of success in product and service integration, technology partnership and interoperability, or success in executing M&A activity that forms the basis for their SASE and SD-WAN solution.

If selected vendors are unable to produce viable evidence, we recommend a wait and see approach that monitors growth and consolidation in the space and suspends immediate realization until proof develops around a single vendor or segment solution.

CYBER THEORY

We are a full-service cybersecurity marketing advisory firm. We constantly collect and analyze the latest customer data segmented by security practitioner, industry, and region. Our extensive knowledge model allows us personalized targeting of each and every cybersecurity buyer persona.With strategic insights from global education services, media providers, intelligence analysts, journalists, and executive leaders, we're always adapting to the latest industry trends. Our network of relationships encompass all aspects of cybersecurity as well as the related fields of fraud, audit, compliance, and risk management.

(212) 518-1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018 • www.cybertheory.io