MARKET PERSPECTIVE

Network Edge Security as a Service: A Functional Road Map to SASE Migration

Christopher Rodriguez Philip Bues Frank Dickson Jay Bretzmann

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Reimagining a Secure Global Edge Framework

The accelerated digital transformation (DX) era, spurred by the pandemic, led to the search for an all-inclusive security framework for mobile and remote workers. The spotlight has landed on the secure access service edge (SASE) concept. The cyber community, realizing that this will fundamentally alter how these edge solutions are delivered, began to develop and deploy their own versions. To bring us closer to a unified global security protocol for SASE, network edge security as a service (NESaaS) is being introduced.

Key Takeaways

- SASE spans many different functional areas, some of which are now remote because of the pandemic, which can be factional and temporary in nature. It's a huge lift, technically and culturally, for previously siloed teams to join ranks. Breaking SASE into chunks fosters a pragmatic approach to DX.
- Incremental complexity should be avoided at all costs. Establishing a "daisy chain" of trust with a small number of NESaaS partners provides the agility to react with changing global business conditions.
- Cloud security during and after the pandemic necessitates continually raising the bar. As organizations' cloud consumption grows, a top priority for CISOs is finding the right mix of cloud-first or cloud-native enterprise security controls within a subscription-based platform.

Recommended Actions

- The true value of SASE is an enabler for threat hunting, XDR, DLP, and other "big picture" security practices. As opposed to a solution that simply consolidates multiple security tools to "check a box," IDC recommends that buyers seek out solutions with a deeper purpose such as improved threat detection.
- A comparison of network technologies and strategies, such as the IDC functional market of "network security" delivered as public cloud services, should be used to ascertain the underlying infrastructure that is needed. There is no one solution that fits all.
- To combat the rapidly expanding attack surface, initiating zero trust concepts is a given, whichever strategy is chosen. Make no mistake, technologies such as SD-WAN, endpoint, and network detection and response are vital in preventing existential threats to your organization, customers, and the supply chain.

Source: IDC, 2021

September 2021, IDC #US48208421

NEW MARKET DEVELOPMENTS AND DYNAMICS

Introduction

What Is SASE?

What's all this talk about secure access service edge (SASE)? What is it, and more importantly, how can it help your organization? In its most distilled form, the original definition of SASE is the integration of networking and network security as a single unified, cloud-delivered service. Core security capabilities include firewall, intrusion prevention, secure web gateway, cloud access security broker (CASB), data loss prevention (DLP), and VPN or zero trust network access (ZTNA) alternatives. Optional security capabilities include sandboxing, remote browser isolation, and web application firewall (WAF). SASE was first coined in 2019 and experienced a massive hype cycle in 2020, leading to customer confusion, massively inflated expectations, and suboptimal approaches. For IT buyers, key foundational questions must be answered before further SASE migration plans are solidified.

So where does SASE fall on CISOs' priority list for digital resiliency? Before organizations take the plunge, they first need to ask: Why SASE? What's the goal? Is it evolutionary, a natural extension of the on-premises security stack to the cloud, or transformative? IDC would argue it should be the latter. As a simple consolidation play, SASE has the potential to maintain or exacerbate many of the same security challenges inherent in legacy approaches. However, a transformative SASE approach will ultimately enable better security outcomes and business value.

Depending on where your organization is in its digital transformation journey, a SASE migration will require a different strategy and goals. "Cloud first" may take advantage of all that cloud has to offer and efficiently transition some on-premises rules and policies to the SASE solution, establishing an agile, secure, and cost-effective solution. If you are cloud native, the goal becomes a seamless elevation of your current security architecture to one in which SD-WAN enables your network as a service and completes the transformation of your security perimeter.

Currently, the single greatest hurdle the market is facing is a high degree of hype and confusion. In its current state, SASE must be explained over and over again and customer expectations must be managed. Contributing to the confusion, IDC notes that there is no single provider that features a comprehensive integrated SASE solution with best-of-breed capabilities in every security category at this time.

This document will offer insight into the SASE concept — spanning definitions, examples, benefits, and challenges — as well as a pragmatic approach to SASE adoption called network edge security as a service (NESaaS).

Industry Dynamics

As of this publication, the industry lacks consensus on a consistent SASE definition. It is commonly referred to as secure access service edge, but similar concepts such as elastic cloud gateway and zero trust edge also exist. Whatever the name, SASE, in one form or another, has taken off partly because of the proliferation of the "work from anywhere" (WFA) hybrid work economy with its corresponding rise in cybersecurity threats and breaches.

As the definition of SASE evolves, it is helpful to keep sight of the original goal: securing remote and mobile worker access and saving on costs. These two objectives became some of the top concerns during the COVID-19 pandemic. While the world continues to make gradual progress toward a return

to normalcy, IDC surveys show that there was never an expectation to return to the same levels of onsite work as pre-pandemic levels. Working from home (WFH) has been generally well received, offering flexibility to workers and productivity benefits to employers. For a post-pandemic future, the WFA option holds the potential to improve productivity, particularly for workers that spend significant time on the road already. Hybrid models that allow organizations to adapt systems and policies to a more distributed workforce while keeping workers satisfied are a likely outcome for many organizations as well. Therefore, organizations need consistent, distributed, and holistic security visibility and implementation across all environments including SaaS, hybrid cloud, and multicloud, irrespective of device type.

SASE, at its core, is about convergence but should be viewed through a microscope — not a telescope. The original definition of SASE is expansive, attempting to combine every network security technology possible. Convergence may be driven by the benefits of consolidation at some level, but should really be driven by the inimitable advantages of smart integrations. Specifically, what combinations of security technologies deliver the optimal security outcomes? Concentrating on integration via smaller buckets of transformational cloud security services — that focus on core use cases, organizational structure, and/or key control points — ensures that when we scratch the surface, we are left with a solution that can be delivered and implemented safely and securely.

Two Sides of the Same SASE Coin

The SASE concept has placed tremendous pressure on vendors to combine networking and network security into a single as-a-service offering. In theory, this consolidation will offer their buyers benefits such as a reduced number of network appliances and endpoint agents, one vendor to work with (a single throat to choke), the possibility for deeper discounting, and greater security visibility. In practice, SASE challenges have emerged such as customer confusion, different buying centers, and a lack of cogent solution offerings. The rush to consolidate security results in bundling instead of integration and is likely to result in a checkbox solution wherein some of the technologies may not be best of breed. This approach is not ideal and may introduce security gaps while ramping up. On the other hand, while an integrated solution may be compiled from suboptimal components, visibility across all of an enterprise's data, IT platforms, and tools would likely improve, offering opportunities for more efficient threat detection and mitigation. An integrated solution exceeds the capabilities of the parts summed individually.

For buyers, SASE is often marketed as a magic panacea for addressing all security use cases. While the cloud will clearly play a larger role in network security in the future, realistically, it will take multiple smaller steps to take precedence. Pressure on buyers to switch over to a pure cloud-based security model prematurely has the potential to leave behind many organizations and use cases. IDC research shows that the reality for many today is a hybrid cloud architecture. In the ideal state, these organizations would be able to integrate with existing on-premises systems but also have the available resources for a full cloud migration. Today's solutions fall short of that goal.

For any project to be successful, there needs to be a shared, attainable vision between provider and customer. Unfortunately, when a solution is a mix of distinct solutions in a single stack flexibility, interoperability, scaling, and visibility issues are inevitable. While many vendors are on their way to assembling a full SASE solution, some have fewer of the puzzle pieces and others are attempting to identify their role in this framework. Whether SASE is a conceptual framework, platform, or service, IDC believes there is no single provider today that features a truly comprehensive, integrated solution

with best-of-breed functionality across every security category captured within SASE (see the Vendor Examples section).

Market Strategies

As of 2021, most SASE offerings are incomplete, and as is the nature of security investments, combinations of technologies from two or more providers are often promoted (see the Partnerships and Alliances section). Vendors have approached SASE by integrating existing security offerings, developing cloud services, or partnering for missing aspects of SASE.

Vendor Examples

- **Palo Alto Networks (Prisma Access/Prisma SD-WAN):** Palo Alto Networks' core SASE offering includes the integrated Prisma Access and Prisma SD-WAN products. Prisma Access is descended from the company's GlobalProtect VPN technology. Palo Alto Networks then acquired CloudGenix's cloud-delivered SD-WAN technology, which has since been rebranded to Prisma SD-WAN, making its SASE more powerful on the networking capabilities. Prisma SD-WAN is optimized for the cloud and thus complements SASE.
- **McAfee (MVISION):** MVISION Unified Cloud Edge (UCE) is a comprehensive data protection solution that encompasses networks, devices, and the cloud. MVISION UCE is a cloud-native solution that seamlessly converges core security technologies such as data loss prevention, cloud access security broker, and next-gen secure web gateway (SWG) to help accelerate SASE adoption. The most recent announcement includes McAfee Private Access, which completes the security aspects of a SASE portfolio, leaving only the need for networking partnerships to address SD-WAN.
- **Fortinet (FortiGate):** Fortinet is among the earliest security companies to integrate networking and security, offering SD-WAN as a value-adding feature of its FortiGate firewalls since 2017. Fortinet's OPAQ acquisition in 2020 provided the cloud delivery model that is considered a requisite of SASE. More recently, the company introduced its zero trust network access as a natively available FortiGate capability in the FortiOS 7.0 release. This solution enables a WFA model via the enforcement of explicit application access per user across all SD-WAN edges.
- **Cloudflare (Cloudflare One):** Cloudflare One operates on Cloudflare's global edge network of interconnected datacenters spanning more than 200 cities in over 100 countries globally, including 25 in mainland China. This cloud security architecture addresses the edge aspect that is most challenging for most security vendors in most SASE solutions. Cloudflare first launched its ZTNA solution (Cloudflare Access) in 2018 and launched Cloudflare One in 2020 to integrate ZTNA with secure web gateway (Cloudflare Gateway), browser isolation, WANaaS (Magic WAN), virtual network services (Magic Transit), and network-level firewall (Magic Firewall).
- **Akamai:** Akamai offerings include Enterprise Application Access, a secure web gateway (Enterprise Threat Protector), multifactor authentication (Akamai MFA), mobile threat defense (SPS Secure Mobile), and its WAF service (app and API protector [AAP]). These and other Akamai security solutions are built on the global Akamai Intelligent Edge Platform deployed in 4,300 networks and 130 countries. Akamai is helping customers transition to SASE via its Programmable Edge, which enables integration of existing enterprise security products and future investments in a unified architecture.
- **Broadcom:** Broadcom has a number of existing security technologies in its toolbox that it integrates under its SASE framework including a secure web gateway (Web Protection Suite), CASB (CloudSOC, with Mirror Gateway for unmanaged devices), ZTNA (Secure Access Cloud), DLP with single controls for on premises and cloud, UEBA (Information Centric Analytics), and browser isolation. The company has recently revamped its web and cloud

security portfolio to be more flexible, with options for on-premises or cloud, including unified policy controls, deployment options and licensing. This will address a significant aspect of SASE but will feature partnerships for networking aspects.

- **Cisco:** The Cisco SASE framework uses technology from Cisco's acquisitions of OpenDNS, as well as Cloudlock, Viptela, and Meraki. For Cisco, Umbrella offers a single security service that combines secure web gateway, CASB, firewall, intrusion prevention system (IPS), DLP, and DNS functionality. The solution is complemented by Cisco SD-WAN, powered by Viptela and Meraki, and sold as an integrated offering that provides the building blocks for SASE.
- **CATO:** Cato SASE Cloud runs on a private global backbone of 65+ points of presence (POPs) connected via multiple SLA-backed network providers. The POP software continuously monitors the providers for latency, packet loss, and jitter to determine, in real-time, the best route for every packet. This has been positioned for smaller enterprises and businesses.

Partnerships and Alliances

- **AT&T** has partnerships with Palo Alto Networks and Fortinet. Fortinet was its first managed SASE service. AT&T uses Fortinet's SASE stack, including SD-WAN and security capabilities, which is fully managed by AT&T Cybersecurity. The services are integrated with the AT&T Alien Labs Threat Intelligence platform. In 2021, AT&T also announced a partnership with Palo Alto Networks to offer the Prisma Access solution as an AT&T Cybersecurity fully managed service.
- **Verizon** Advanced SASE merges SD-WAN capabilities with comprehensive network security services. The company has targeted partners with extensive brand recognition, uniting Versa Networks' SD-WAN and Zscaler's cloud-based ZTNA, SWG, and CASB capabilities.
- **Lumen** is partnering with leading SD-WAN and security technology providers to deploy SASE solutions on the Lumen Platform infrastructure in flexible self-managed, comanaged, or fully managed as-a-service models. With this strategy, Lumen is evolving and combining its SD-WAN solutions with vendor SASE capabilities deployed across cloud, vendor, and Lumen-distributed points of presence to provide ultra-low latency and secure performance. For example, Lumen announced a partnership with VMware in February 2021. Lumen supports SASE services with automated threat detection and response through its Rapid Threat Defense capability powered by Black Lotus Labs, the Lumen threat intel practice, and will complement SASE solutions with its DDoS mitigation service and web application security portfolio.

Scenarios/Use Cases

The Road (or Un-Road) Warrior

Organizations with many remote employees could be well served by SASE or ZTNA solutions. These types of users are currently served by a conglomeration of frustrating VPN solutions and disparate CASB, web security, and identity tools — and potentially client software required for each of these. Organizations realize the challenges of this legacy approach and have increased diligence to prioritize client software for only essential functions. Most likely, this leads to convergence as well, as fewer endpoint agents hogging memory and requiring updates is generally considered "better." More importantly, as a cloud service, SASE presents a low-friction means to support remote workers without requiring backhauling traffic back to a centralized security inspection point.

The Distributed Enterprise

Organizations with workers at many branch offices, sites, or locations, benefit from the cost savings and performance of integrated SD-WAN. In fact, SD-WAN was born in response to the rigidity and high costs of multiprotocol label switching (MPLS). However, depending on the needs and sophistication of the security team, varying degrees of SD-WAN can exist from lightweight to "I can sleep well tonight." To make the most of this solution, businesses should focus on a Mazlow's hierarchy of needs. First and foremost, remote sites require connections that are robust, stable, and performant. When connections fail, or are disrupted, businesses lose productivity and potentially sales — and nobody can afford a work stoppage because of IT.

Note, however, the need for performance as a very close second place. Many organizations continue to rely on critical applications and systems that are not designed for remote access or web protocols. Latency, even small amounts, can cause applications to break. Thus, while SASE specifically requires a cloud delivery model, there remains a need for integration with on-premises tools to support devices that cannot install an agent or that are otherwise cloud challenged. While SASE is a potential option for supporting branch workers, it is likely an extension rather than a replacement in the branch office segment because of the continuing need to support specialized applications, devices, or connections via on-premises tools.

Finally, security is an essential layer, and even that is layered. For example, if encryption is broken, businesses would be best served by not communicating sensitive data across the public internet at all. However, a business might be able to operate, at least temporarily or in limited fashion, without other security layers such as sandboxing and or browser isolation.

The Zero Trust Adopter

Zero trust is a framework for ensuring security practices such as least privileged access, segmentation, and continuous monitoring. As a guiding principle, zero trust treats all content as potentially malicious — whether or not it's from a trusted source — and treats all users as potential insider threats, regardless of authentication. One way in which zero trust principles have been translated to a tangible technology set is ZTNA. ZTNA is viewed as a replacement for VPN, although such a change will not happen overnight, especially for large enterprises.

While SASE incorporates ZTNA technology as a means of enabling worker productivity securely, the core principles of zero trust are not an inherent aspect of the current market approaches to SASE. SASE is a framework of security technologies, and zero trust is a framework of modern security practices and principles. Similar to the migration to SASE, there will be appropriate use cases for ZTNA and appropriate use cases for VPN. The SASE definition does incorporate ZTNA as an optional technological component in the security stack, though the SASE solutions available today primarily emphasize integration of existing security technologies as a cloud-delivered service. Table 1 provides a comparison of emerging security frameworks.

TABLE 1

Comparison of Modern Security Frameworks

Framework	Description	Inclusive of
SASE	Integrated solution combining networking and security across all worker use cases for performance and convenience purposes	▪ Network security (firewall, IPS, ZTNA, SWG, CASB, RBI, WAF, and sandboxing) ▪ Networking (SD-WAN primarily)
ZTNA	A modern approach to secure access that emphasizes least privileged access, continuous monitoring, and cloud scalability and flexibility	▪ Considered comparable or competitive with VPN ▪ UEBA/continuous monitoring optional ▪ Possible future additions of/integrations with adjacent control points such as endpoint security
NESaaS	An actionable solution that focuses on specific security use cases and emphasizes integration for security efficacy improvements	▪ Network security (firewall, IPS, ZTNA, SWG, CASB, RBI, WAF, and sandboxing)

Source: IDC, 2021

One key difference between SASE and ZTNA is a growing trend for ZTNA vendors to utilize the end device health as a context for determining risk and controlling access. For example, in 2020 CrowdStrike announced a partnership strategy that would allow customers to integrate endpoint visibility and telemetry with identity insight and data security from Okta, Netskope, and Proofpoint. Another example is Trend Micro that offers valuable identity insight and device health via its Vision One XDR solution, offering threat detection as well as security posture assessment that ZTNA solutions can utilize to assess and reduce risk.

The Square Peg and Round Hole

SASE is optimized for the cloud. It is synonymous with SaaS. However, legacy IT systems, applications, and onsite OT/IoT requirements might require security to retain an onsite footprint. This is the reality for many organizations that either are embarking on their cloud journey, are working in heavily regulated industries or in the government where some sensitive data must be kept on premises, or are otherwise concerned about the potential impact of loss of connectivity due to cloud-related issues. These are complex issues that could be exacerbated when factoring in the new federal compliance standards recently released by the Biden Administration Executive Order.

The rush to deliver a SASE solution to market introduces potential for corner cutting or lack of transparency. As a result, uncertainty about the true origin of the underlying technology and depth of integration is likely to persist and delay migrations among certain industries.

SASE Market Outlook: Network Security (SaaS) And SD-WAN

In IDC parlance, functional software markets are the focal point of IDC's analysis for which it analyzes revenue by vendor, geography, deployment type, and in some instances, additional segmentations such as operating environment, license type, enterprise size, industry, and use cases. Competitive markets are combinations or carve-outs of tracked functional markets. SASE is inherently a competitive market, as it incorporates multiple technologies across networking and security. IDC tracks network security and networking markets as separate functional markets.

To properly assess the SASE market, it requires a clear understanding of its components. For that, we need to dissect (break down) the SASE definition and compare it with a known set of mature, comparable, and tested technologies, such as security as a service (SECaaS) in this case, many of which serve as foundational elements for our NESaaS premise.

Security as a Service Versus SASE

SASE is a cloud-delivered solution that moves the security technology stack from on-premises firewalls and security gateways to the points closest to where end users connect, while also integrating networking capabilities.

In practice, SASE has largely been an extension of existing security solutions into cloud POPs, with access provided to end users via endpoint client. SD-WAN has been added in some solutions but is often delivered via partnerships. For more information about the SD-WAN market, see *Worldwide SD-WAN Infrastructure Market Forecast, 2021-2025* (IDC #US47272921, July 2021).

SECaaS is a type of delivery model for various network security solutions. Many of the technologies included in *Worldwide Security as a Service Forecast, 2021-2025* (IDC #US47956921, June 2021) are included in the SASE definition or are considered an optional component of a SASE architecture. More importantly, these categories address the same security use cases. Therefore, a comparison of SASE versus the "network security" SECaaS category, as shown in Table 2, is very reasonable.

TABLE 2

Comparison of SASE and Security as a Service

Security Technology	SASE	Security as a service
Firewall/UTM	Required	Included
Intrusion prevention system	Required	Included
VPN/ZTNA	Required	Included
Secure web gateway	Required	Included
CASB	Required	Included
DLP	Required	Included
Sandboxing	Optional	Included
Remote browser isolation	Optional	Included
Web application firewall	Optional	Included
SD-WAN	Required	Not Included
DDoS mitigation	Not included	Included

Source: IDC, 2021

Deployment

The original definition of SASE is strictly limited to cloud-delivered security services. IDC covers network security as a SaaS form factor – all SASE is SECaaS, but not all SECaaS is SASE. Many SASE proponents will argue that SASE is different than SECaaS because of the level of integration. The point is valid, though subjective and vulnerable to manipulation. First, few complete pure-play SASE solutions exist in the market today. Second, the availability of a complete, integrated SASE solution does not preclude the option to insert a specialized security solution into the service chain either. Clearly, this approach would defeat the purpose and undermine some of the value proposition of SASE as a "one-stop shop," but it's a real possibility.

ADVICE FOR THE TECHNOLOGY SUPPLIER

Break SASE into Chunks: Removing Networking from the Network Security Equation

SASE is a big concept with many moving parts and hurdles. IT buyers require a road map for adoption that addresses key use cases, fits with existing infrastructure and practices, and accounts for organizational realities. The IDC concept of NESaaS meets these requirements by highlighting logical areas for integration. Furthermore, NESaaS emphasizes integration along the lines of security practices and objectives, more so than the underlying access technologies. The result is a holistic security framework that fosters a pragmatic approach to digital transformation, supports hybrid environments, and emphasizes superior security outcomes.

Under NESaaS, SASE first breaks out networking and network security. Networking and security are fundamentally different practice areas, with distinct decision makers, requirements, priorities, and budgets. While a truly integrated SASE offering (a solution with one converged code base, and one SKU) may meet the needs of small and medium-sized businesses (SMBs) with limited resources, NESaaS embraces the distinctions between these different organizations.

To be clear, security solutions such as firewalls may continue to offer value-adding capabilities such as SD-WAN. Similarly, networking companies are increasingly offering security functionality in their products such as stateful firewall or VPN. In these cases, IT buyers will ultimately decide which they prefer: a premium SD-WAN with added security or a purpose-built security solution with SD-WAN features. In the most practical sense, IT organizations will use whichever technology best meets their needs for connectivity, including reliability, performance, latency, and cost considerations. Security is expected to support these networking technologies, and buyers will search for the security solution that provides security without introducing bottlenecks, complexity, or further challenges.

The NESaaS approach also alleviates pressure from vendors, most of which are challenged to deliver both SD-WAN and security as an integrated solution. A few companies already offer both SD-WAN and network security products, making bundling a natural first step toward SASE. However, deeper integration has been a more challenging proposition. Technology partnerships also offer networking and security companies paths to deliver an integration story. Multiple managed security services providers (SPs) have announced partnerships with best-of-breed security and networking vendors, offering to perform the integration on behalf of customers as well as layering on monitoring, detection, and response services to customers for additional value. Refer back to the Partnerships and Alliances section and the Vendor Examples section for specific examples.

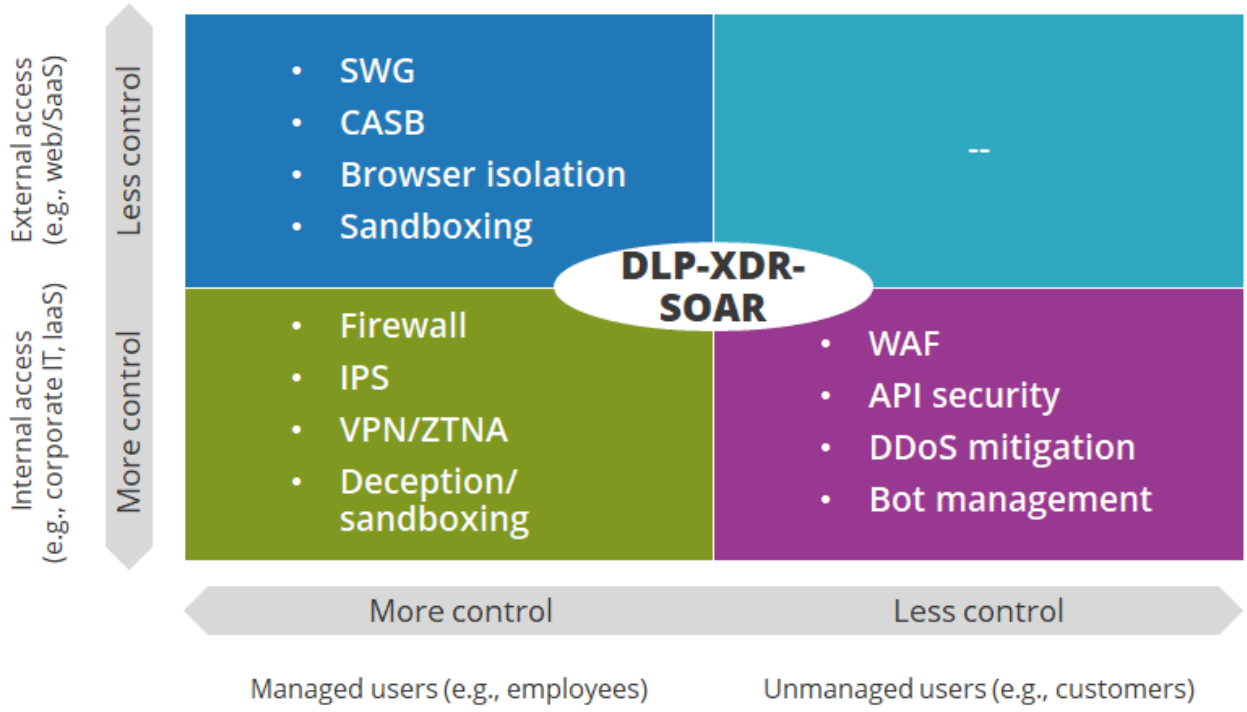
Network Edge Security as a Service Provides a Road Map for Security Transformation

Next, NESaaS further breaks down the SASE question along the lines of security use cases. In theory, SASE would be all things to all buyers. In reality, SASE implies a controlled user/device (typically a worker, contractor, or another known entity) accessing internal applications. This "ingress" use case requires a common set of protections such as firewall, VPN (or ZTNA), and IPS. Because the device is managed, likely with client software installed, the idea to add various "egress" protections such as web security or CASB is an obvious next choice. Note that the core definition of SASE includes WAF as optional. Some vendors offer basic WAF solutions as part of the SASE story. Otherwise, IDC finds that SASE has largely overlooked the uncontrolled aspect of ingress (i.e., unknown users accessing internal

applications and resources). Figure 2 diagrams these use cases in the context of managed versus unmanaged users and internal (corporate owned) versus external (third-party owned) resource access.

FIGURE 2

SASE Alignment to Key Security Use Cases



Source: IDC, 2021

By comparison, instead of attempting to force integration, NESaaS breaks down SASE to the fundamental security control point categories of "ingress" and "egress." Trusted edge access (ingress) includes security technologies designed to support worker access to corporate IT systems and resources, such as ZTNA, firewall, intrusion prevention, and VPN. Secure internet access (egress) provides security functions such as SWG, CASB, sandboxing, and browser isolation that supports users as they access various web, cloud, and internet resources. In both cases, the security stacks are optimized, applying only the security technologies necessary to enable productivity (see Figure 3).

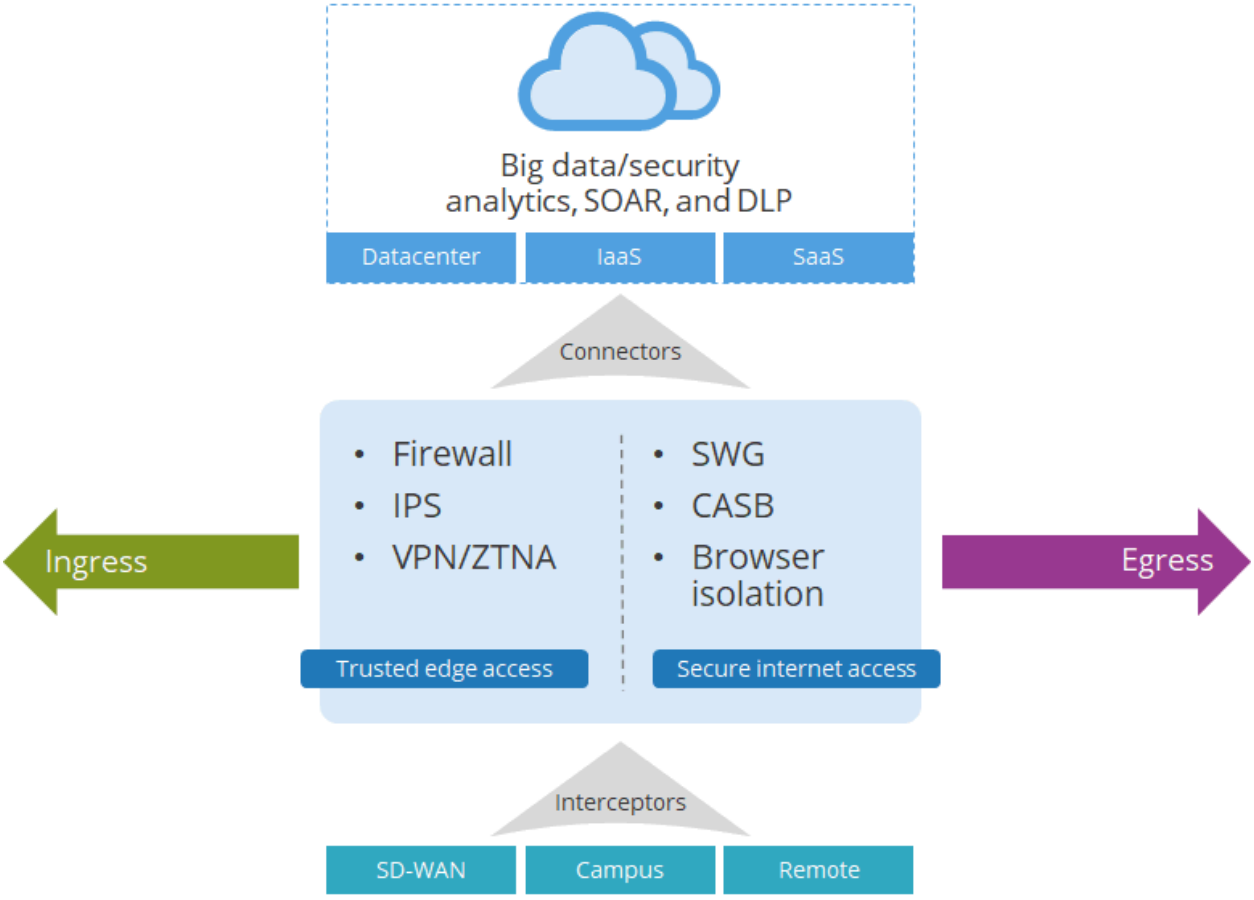
The core components of a NESaaS architecture are presented in Figure 3 but generally align to two key paths. Whether accessing from an SD-WAN gateway, on-premises appliance, or "branch of one" client, the traffic is intercepted and steered to the security provider's cloud where relevant security inspections and policy enforcement occur. At this control point:

- Ingress connections are subject to ZTNA controls, firewall policies, and intrusion prevention.
- Egress connections are protected by web security and cloud security controls such as SWG and CASB but also potentially browser isolation or sandboxing, depending on the risk level.

Note that these are not strict checkbox requirements, but opportunities for purposeful bundling and integration by security vendors. For example, a next-generation firewall (NGFW) offers application visibility and control that can address the security requirements of a worker accessing the web or SaaS services. The broader point is that at the end of the day, the security stack for these two use cases will look different. Buyers should take inventory of what functions they expect from a security solution and seek out vendors that can accommodate and meet these expectations. For some buyers, this approach offers flexibility or a lower price point when compared with a full SASE deployment. For others, a truly comprehensive security solution will be preferable.

FIGURE 3

Network Edge Security-as-a-Service Architecture



Source: IDC, 2021

While these various tracks may involve different gateways, controllers, forward proxies, or reverse proxies, these are best abstracted away for buyers, as security functions "just have to work." The security provider is then responsible for connecting users to the requested resources, whether or not that is owned by the buyer, including on-premises datacenters, IaaS environments, and SaaS. As previously noted, this security layer offers tremendous visibility and telemetry that can feed into

security data lakes and analytics tools such as XDR, DLP, and SOAR for more efficient and effective threat detection and mitigation.

While the concept of SASE is primarily in service of consolidation, IDC notes that the most strategic value of SASE is as an enabler for threat hunting, XDR, DLP, and other "big picture" security practices. As opposed to a solution that simply consolidates multiple security tools to "check a box," IDC recommends that buyers seek out solutions that have a deeper purpose such as improved threat detection, likely using big data/security analytics (e.g., XDR and/or SOAR). The real measure of a security tool is in its ability to reduce risk, and the movement to a modernized cloud-native solution offers the opportunity for security vendors and buyers alike to "get it right this time."

Since NESaaS provides near-total visibility of all endpoints, entry points, and users, the system has the potential to provide massive amounts of contextual data for advanced security analytics tools. However, these are treated as separate/standalone functions to ensure the separation of duties, have a more manageable daisy chain concept of NESaaS, and limit the potential for vendor lock-in scenario.

As previously noted, the concept of "ingress" may also refer to the use case of web, application, and content delivery wherein a digital business must expose web applications, APIs, and other content to the largely uncontrolled users and devices accessing via the web. These systems often require specialized capabilities such as WAF, API security, bot management, and DDoS mitigation. By comparison, NESaaS purposefully addresses the needs of the managed/known user. For the unmanaged user, IDC addresses these requirements separately under the concept of pervasive application edge defense (PAED) (see *Pervasive Application Edge Defense: An Application-Based Framework for Trust,* IDC #US46810219, September 2020).

The Next Generation of Security Requires Digital Transformation

IDC covers a range of network security solutions offered as SaaS, referred to as SECaaS. However, not all SECaaS solutions are primed for the digital transformation era. In particular, SASE, zero trust, NESaaS, and other modern security frameworks inherently necessitate solutions that are themselves built on modern architectures. This includes the need for solutions built on cloud-native technologies such as containerization and serverless functions for elastic scalability, with microservices designs and API integrations for the expansion of new features and functionality to meet the needs of the modern, digital workforce. In addition, while NESaaS vendors technically need not own their cloud infrastructure, ownership of POPs and datacenters and peering arrangements provides performance benefits that can appear subtle on paper but provide a notably superior user experience.

Develop or Buy SD-WAN Capabilities

SD-WAN ensures high-quality, stable, performant connections. This is the first step in working remotely — a Maslow's hierarchy of needs, ensuring that businesses have connections that are reliable and performant. SD-WAN satisfies the most basic, essential need for security — availability. In fact, in-house SD-WAN can be offered as a value add. It would require the IT department to learn about the technology and players and to procure and deploy the equipment in-house. Once the knowledge is gained, it pays for itself many times over. However, many SMB organizations find that a managed SD-WAN service is more realistic and efficient.

But buyer beware: Acquired SD-WAN solutions should be treated as a paid functionality, or risk negative customer perceptions such as a "small business" solution. Ostensibly, SD-WAN is not a giveaway type of technology and, in most cases, represents a separate SKU or is otherwise built into

the final SASE pricing. Buyers should remain cognizant of the fact and perform cost-benefit analysis to determine whether a standalone solution is more appropriate for their needs.

IDC'S POINT OF VIEW

SASE Is Futuristic

SASE is designed for a cloud-first world that most buyers are only just now able to imagine, as IDC has observed in its *Future Enterprise Resiliency and Spending Survey* (FERS), Wave 4, published in April 2021, across the United States, Asia/Pacific and Europe, the Middle East, and Africa. It found that 37% of organizations were accelerating a move to cloud-native applications and agile development and 46% of all respondents agreed that better integrating data sources and analytics tools to improve business insight was the top priority. These sentiments captured their digital infrastructure resiliency efforts over the next two years. As more resources and recognition of security are realized, it gives IT the leeway to plan and strategize such efforts.

The original definition of SASE is strict and foregoes the possibility of on-premises security architecture. This requirement is a challenge for many organizations as on premises is key for many in backup and recovery services. Also, particularly for government, having reduced/limited control over deployments is not a reality. Any SMB or enterprise businesses in highly regulated industries should also proceed with caution and avoid multitenancy, which can lead to performance and security issues.

This upcoming digitally transformed world will require very resilient, powerful, and performant cloud services. Most network security buyers, though, have traditionally been very wary to shift security entirely to the cloud at this point (for example, manufacturing companies that cannot afford a minute of downtime). The massive hype surrounding SASE is driving interest in migrating to the next generation of network security, but failed deployments and disappointing outcomes may ultimately result in greater skepticism and hesitancy in future digital transformation efforts. In the short term, IT organizations will require road maps and milestones for success that they can utilize to keep true to the originally stated goals of transformation, to measure and assess outcomes, and to communicate successes (or failures) as needed.

Convergence Benefits Face Reality Checks

Convergence *is* a good idea for security efficacy, business value, and other benefits that have yet to be imagined. The combination of SD-WAN and network security services such as firewall, CASB, and ZTNA can deliver benefits such as reduced endpoint agents, the security value of comprehensive visibility, more data to feed into XDR, more consistent policies and DLP, and the list goes on. With so many technologies to choose from and the likelihood of a piece-meal approach, a converged solution will not meet all needs. The following list of practical considerations weigh heavy on the prospects of a rapid SASE migration:

- Networking teams may be choosy about their SD-WAN functionality.
- Compromise may not be possible or could be completely dissatisfactory for one or both teams.
- Integration overhead gets real, real fast.
- The true vision for SASE, with true convergence leading to network security and networking sharing the same code base, violates a tenet of security of "separation of powers" — too many eggs in one basket. SASE may never be a good option for some organizations.

SASE Is A Huge "Cultural" Lift for Everyone

SASE spans many different functional areas, some of which are now remote because of the pandemic, which can be factional and temporary in nature such as development, architecture/engineering, network, operations, and security. It's a huge lift both technically and culturally for previously siloed teams to join ranks.

These teams are now working together in stair-step fashion. They are challenged to deliver SASE quickly and efficiently as few are able to deliver a good SASE. Many are still experiencing growing pains and assembling the right parts needed at this time. Other challenges include keeping vendors and partners up to date with consistent messaging, product management, and supply chain transparency. Technically speaking, by connecting previously disparate systems, organizations can gain a view of their environment that is both complete and summarized with drilldown, detailed, and/or role-specific views such as operations, threat hunting, and compliance. But cultural challenges will be harder to solve long term.

Network Edge Security as a Service Aligns to Key Control Points

NESaaS is the glue that unites the four key security control points: applications, identities, endpoints, and data. It is worth noting again that SASE was introduced in 2019. At this same time, IDC proposed the future of cybersecurity unifying these four central control points as network- and perimeter-centric security measures were becoming more permeable. The key differentiation is that while SASE is network and security as a single as-a-service offering, NESaaS offers a modular ecosystem of SaaS-based security.

Endpoints are the next most obvious point of integration for NESaaS. Network access control (NAC) first attempted to control local network access based on device hygiene, health, and user identity in 2004. NESaaS provides the opportunity to leverage endpoint status and telemetry as a key decision point for network or application access. At a minimum, convergence with endpoint security tools holds potential for further consolidation (reduced number of endpoint agents).

Applications can be viewed in the context of NESaaS ingress and/or content delivery. While NESaaS provides controls closer to the user, applications may require a distinct security stack, most likely aligning to the pervasive application edge defense framework envisioned by IDC.

LEARN MORE

Related Research

- *Worldwide Cybersecurity AIRO and Tier 2 SOC Analytics Market Shares, 2020: The Seeds That Become Cloud-Native XDR* (IDC #US47081421, July 2021)
- *Worldwide Security as a Service Forecast, 2021-2025* (IDC #US47956921, June 2021)
- *Worldwide Cloud Workload Security Forecast, 2021-2025: Expanding Requirements and the March to Cloud Fuel the Market* (IDC #US47837321, June 2021)
- *IDC's Worldwide Cybersecurity Software and Appliance Taxonomy, 2021* (IDC #US47212220, January 2021)
- *Worldwide Content Inspection Forecast, 2020-2024: Traditional Threat Vectors Surge During Crisis* (IDC #US46832319, October 2020)

- *Pervasive Application Edge Defense: An Application-Based Framework for Trust* (IDC #US46810219, September 2020)
- *Worldwide Network Security Forecast, 2020-2024: A "New Normal" Forces Faster Digital Transformation* (IDC #US46640120, July 2020)

Synopsis

This IDC Market Perspective discusses network edge security as a service (NESaaS) being the functional road map to SASE migration.

"NESaaS is the glue that unites the key security control points: applications, identities, endpoints, and data," said Christopher Rodriguez, research director, Network Security Products and Strategies program at IDC. "The key differentiation is that while SASE is network and security as a single as-a-service offering, NESaaS offers a modular ecosystem of SaaS security."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com