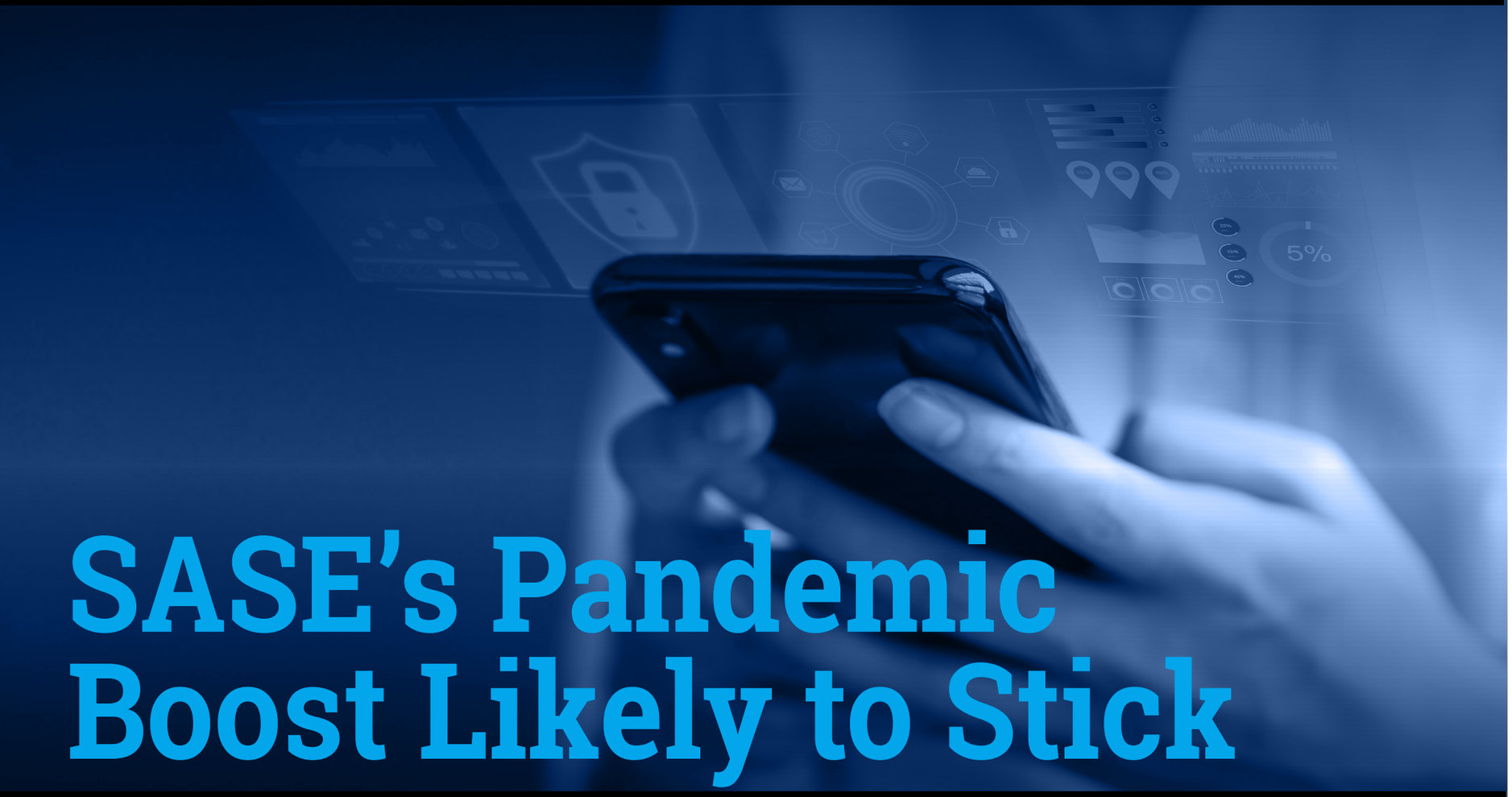
NETWORKComputing

APRIL 2021



SASE's Pandemic Boost Likely to Stick

Many changes invoked to keep businesses running during the pandemic are likely to fade away once there is a return to normal. That is not the case with Secure Access Service Edge (SASE). Its great strength of offering a framework that combines networking and security functions into a single, cloud-native environment drew great attention and was proven out during the pandemic.

informa tech

INSIDE:

Next

Is it Prime Time for SASE?

The workforce disruption brought on by COVID-19 changed network traffic patterns and introduced new security challenges. Many enterprises started to consider SASE because it helps address both issues.

By Salvatore Salamone, Managing Editor, Network Computing

Politicians from Winston Churchill to Rahm Emanuel have often uttered something along the lines of "never let a good crisis go to waste." The point is to seize the opportunity during a calamity to do something you could not do before. That seems to be the case with proponents of Secure Access Service Edge (SASE).

SASE is an enterprise networking technology category introduced by Gartner in 2019. It converges the functions of network and security point solutions into a unified, global cloud-native service. It allows an architectural transformation of enterprise networking and security. That, in turn, lets IT provide an agile and adaptable service to its users.

Until the pandemic, its adoption was limited. A 2021 industry survey of 750 IT leaders, including CIOs, CTOs, IT, and network directors, found that less than 12% of enterprises fully embrace the framework last year. Part of the problem is confusion about what SASE is. One-third of the 750 professionals surveyed cannot even confidently define SASE.

That said, its adoption exploded thanks to the networking and security challenges of the pandemic. One leading provider of SASE services reported 200% growth.

Why the interest?

SASE is a framework that brings together networking and security services into a unified solution. It is designed to provide strong security from edge-to-edge, delivered as a service to the data center, remote offices, roaming users, and more.

As originally framed by Gartner, SASE brings together two elements: one related to connectivity, and one related to security.

A SASE service might offer features to help people and sites connect and do so efficiently from the connectivity side. Specifically, an offering might include a

Previous Next

software-defined WAN (SD-WAN), content delivery network, WAN optimization, and more features, all delivered in the form of a network-as-a-service offering.

From the security side of an offering, a SASE service might offer network security features such as a cloud access security broker (CASB), web application and API protection as a service (WAAPaaS), domain name system (DNS) services, cloud secure web gateway (SWG) elements, and support for zero-touch network access (ZTNA) and virtual private networking (VPN).

How is this different from other offerings? SD-WANs are widely used for enterprise connectivity. They offer cost savings, performance, and safety by giving users easily manageable links to branch offices and other remote groups for data, voice, or video communication. Unfortunately, without the assistance of third-party applications, SD-WANs often lack important security attributes, such as VPN protection and web gateways.

Strong security became even more critical during the COVID-19 pandemic. Most employees had to work from home. Yet, they needed the same robust security afforded in the office. As a result, many enterprises began turning to SASE because services offer SD-WAN capabilities with tightly integrated security tools.

SASE revamps network security in somewhat the same way that software-defined networking (SDN) is impacting network infrastructures. Both take advantage of virtualization networking, powerful low-cost cloud resources, and a new generation of network services. SASE adoption is also being fueled by the arrival of increasingly complex security challenges (e.g., the ever-evolving cyber threat landscape) and the overall increased use of managed services.

SASE's COVID boost

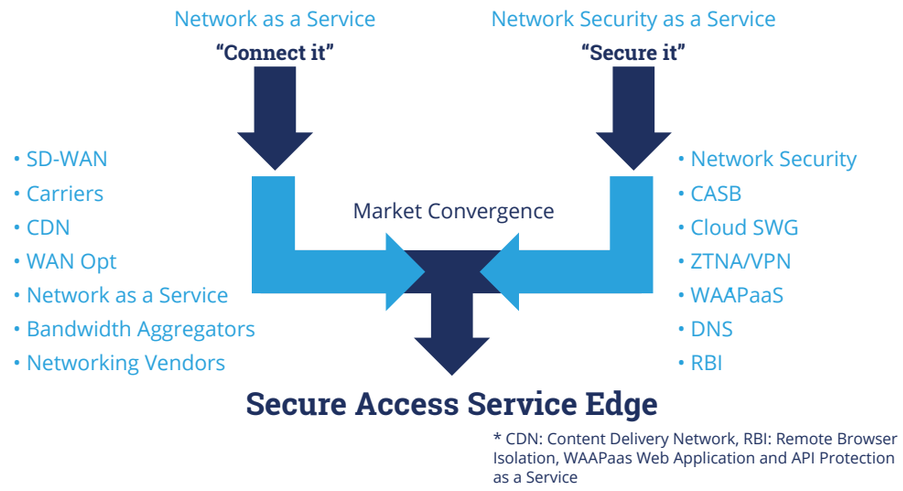
SASE got a boost due to the impact of COVID-19 on enterprise operations. It is now more important than ever for distributed teams to access the network resources they need securely. Traditionally, enterprises used firewalls and enterprise VPNs to secure network traffic through an encrypted tunnel. These measures are rapidly becoming obsolete in a world where data is now increasingly distributed and perimeter-less.

In other words, now that enterprises simply don't use the old hub-and-spoke topology that routed remote users' network traffic through a single data center, neither should their modern security frameworks.

Transitioning from these traditional network security models, network administrators shifted to cloud-centric security strategies that let people securely work from anywhere. Such agility is essential in today's enterprise networks, where traffic often traverses multiple cloud networks.

Bottom line: SASE is designed for today's s perimeter-less environments. It eliminates the need to force traffic through a central site and makes it easier for remote groups to securely work over distributed networks.

What is SASE?



Reference: 2019 Gartner

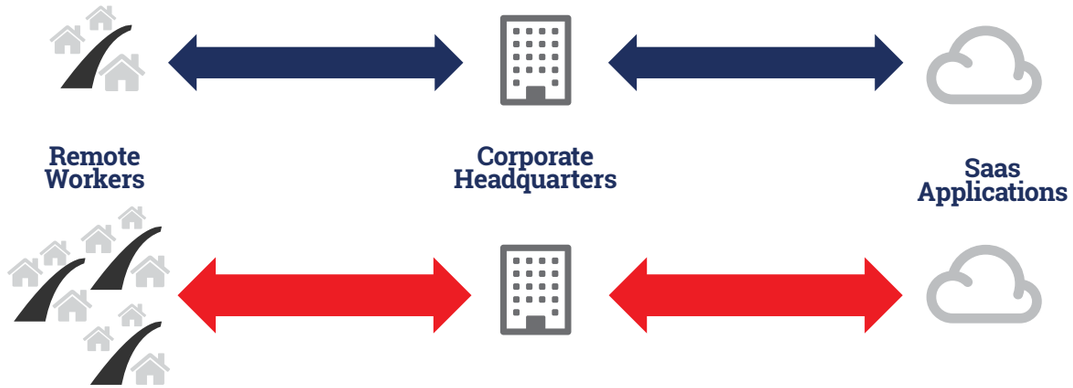
Additionally, SASE got such great interest during the pandemic because network traffic patterns were radically changed. Until recently, most businesses required that employees work out of a corporate office. As such, security architects could deploy network security tools within the confines of the corporate network. Examples of these tools include firewalls, intrusion prevention systems (IPS), SWGs, and ZTNA. Deploying network security tools directly on the corporate network brought security services in line with the natural flow of network data between end-users and the applications and data they were accessing. This is true regardless of whether the data and services resided on-premises or the public cloud.

Looking at the branch office and remote users, however, there is a different traffic flow. Users are increasingly accessing applications and data in public clouds. In these situations, branch and remote user traffic must first be backhauled to the corporate network, and then out to the internet where the cloud services reside. The reason for the backhaul is because the data flows must first be examined and okayed by the various network security tools. Backhauling remote traffic obviously creates sub-optimal paths from a network perspective that can add latency.

A centralized network security deployment architecture makes complete sense if a business largely manages its data and applications within private data centers. But as IT departments migrate applications and data to public clouds, forcing users to send data to the corporate headquarters for network security no longer provides optimal traffic flows. Combine this with the fact that the number of remote employees is expected to continue to rise, and it is clear why SASE is becoming popular.

Because a great deal of business traffic is now being directed out the internet to public clouds, branch office, and WFH user traffic flows must be rearchitected to access public cloud resources directly while also accessing network security services. This is the purpose of SASE as network security tools are migrated from private data center deployments into the public cloud. All users, regardless of physical location, have the same access and network flow efficiency. It also means that both corporate internet edge and branch office WAN traffic will decrease as remote user traffic no longer has to be backhauled to the corporate network. A positive side benefit of such a reduction in traffic is that it often translates into the downsizing of corporate Internet broadband and private WAN throughput capacity.

Pandemic-Related Network Traffic Change



Reference: Network Computing

Make way for a new framework

SASE addresses the varied problems with traditional cybersecurity methods used in the cloud. Many of those problems go back to the idea that network security architectures must be placed at the center of connectivity in the data center. SD-WAN showed that there was a viable alternative approach for network connectivity. It offered the flexibility to distribute the intelligence and processing away from the data

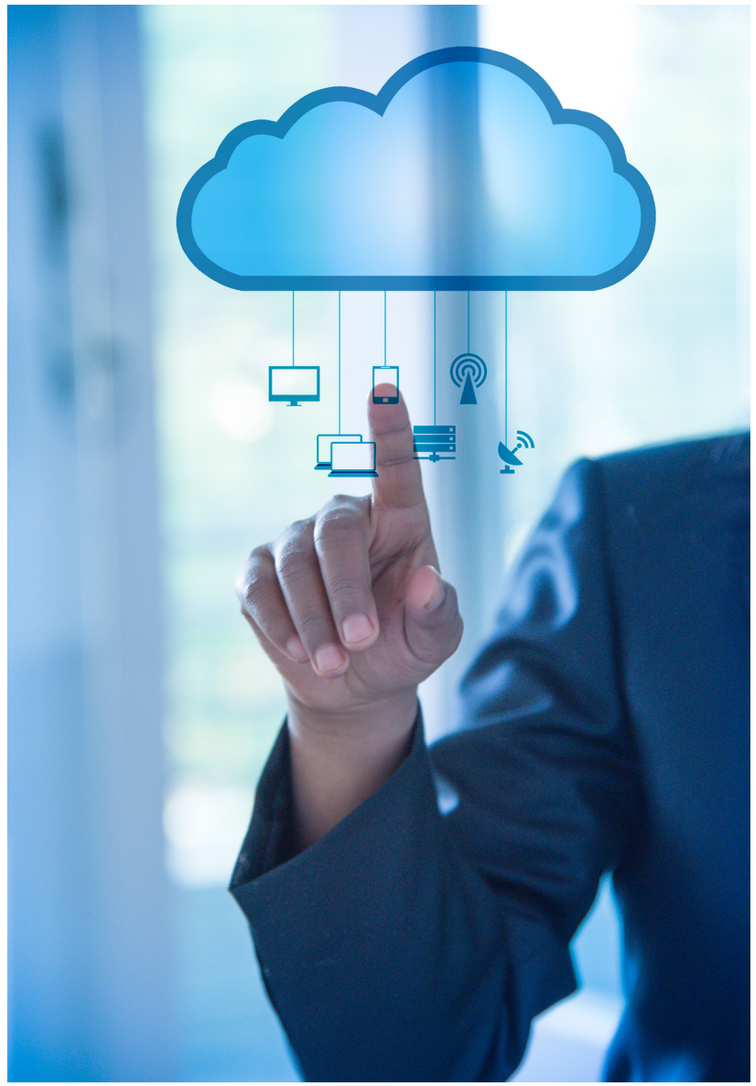
center. As such, SD-WAN is an essential pillar of a SASE framework.

Another reason for the great interest in SASE is its ability to be delivered as a managed cloud service. Most enterprises are already moving in that direction for other purposes. SASE aligns with that school of thinking.

Some of the top reasons for using any managed service are to shift from a CapEx model to OpEx and offload recurring management chores from in-house staff to that of the provider. SASE delivers in these areas in several ways.

For example, the traditional way to connect remote offices via public services was to use what is frequently called a box-heavy approach. Each office would have its own branch router, next-generation firewall, and perhaps an appliance for bandwidth optimization, traffic prioritization, and more. SASE allows a transition to a "thin branch" where a managed cloud service replaces those boxes. The features and capabilities that were available on-site in such offices are now carried out and delivered by the provider. There still needs to be customer premises equipment, but the equipment is much simpler to install and is fully managed by the provider.

Many providers offer cloud-delivered and managed SD-WAN services as the foundation of such SASE offerings. They deliver security as a value-added service on top of SD-WAN.



Looking ahead

SASE will become an important consideration as enterprises implement their next-generation branch networks. Industry analysts expect enterprises to adopt SASE over a 5- to 10-year period. Many enterprise organizations will start with SD-WAN and phasing in SASE over time. The reason: Familiarity with SD-WAN technology and its wide availability from many providers. That brings up an important point to remember. SASE is relatively new. As noted above, a third of IT managers in one survey said they could not define SASE.

Organizations likely to adopt SASE faster than others are those that are embracing a cloud-first or cloud-native philosophy. Such organizations may find SASE is a good complement to their way of thinking. Businesses that may delay the adoption of SASE have common traits. Typically, they have many legacy applications (i.e., applications that are not cloud-native), large data centers, and most of their network traffic is still within the enterprise perimeter.

Another factor to consider is the way SASE services will be delivered. There are two aspects to this. One involves the integrated security features, the other relates to performance.

Remember, while SASE services are relatively new, SASE itself is not a new technology. It is the integration of several existing technologies. There are very few pure-SASE

providers. Many offering SASE services today are network service providers or cloud providers that are partnering with cloud security vendors to offer an integrated service. But the challenge they face is that the various security pieces of SASE have to be tightly interoperable with the underlying SD-WAN architecture.

So, it is worth the time to explore the many options they offer. For example, the shift to work from home caused by the pandemic has made it much harder for companies to backup files and data. Certainly, the shift to cloud application services helps in that the provider maintains the data on their systems. But there is still a great need for data protection on the many corporate devices workers are using in their homes. If this is the case, a company may need to look for integrated data loss prevention or a backup and recovery as additional security services a SASE provider offers to satisfy company requirements.

From a performance standpoint, latency is the most important factor. Users need low latency access to applications and data regardless of location. A SASE provider can deliver the required low latency if they have a global network with local points of presence that align with a company's user base.

Conclusion

SASE offerings are attracting attention because they address today's enterprise pain points. SASE does not require organizations to fundamentally change the way they approach IT. It lets organizations evaluate where their resources reside and gives them the security and networking capabilities to support today's distributed, work-from-home model. SASE also is a perfect match and a path forward for organizations that are moving to cloud-native architectures.

Short-term, the pandemic has forced many organizations to alter their daily operations, including the need to support many remote workers. SASE greatly improves cybersecurity for today's home workers and, in the future, will provide the same connectivity and security for geographically dispersed branch offices, as well. As a result, SASE will likely become more crucial for successful business operations once things return to normal.

Organizations likely to adopt SASE faster than others are those that are embracing a **cloud-first** or **cloud-native philosophy**.

Salvatore Salamone is the managing editor of Network Computing. He has worked as a writer and editor covering business, technology, and science. He has written three business technology books and served as an editor at IT industry publications including Network World, Byte, Bio-IT World, Data Communications, LAN Times, and InternetWeek.

The New Normal Requires a New Enterprise Security Framework

Managing network architecture while moving to SASE requires pragmatic, secure access solutions for existing hybrid infrastructures that are future-compatible.

By David Canellos, President and CEO, Ericom Software

When COVID-19 forced office closures, enterprises either fast-tracked digital transformation initiatives or expanded IT resources to mobilize remote workers. Enabling hundreds, even thousands, of remote workers stretched traditional enterprise network security stacks to their limits, straining infrastructure and exposing network vulnerabilities – inside and out.

Many organizations have begun to accelerate the movement of their IT resources and workloads to the cloud. This has generated momentum for the adoption of Secure Access Service Edge (SASE)—Gartner's network security framework based on an identity-driven, cloud-native, globally distributed platform that securely connects users to applications wherever they reside (WAN, cloud, mobile, and IoT).

While the future of network security is certainly SASE, much of the current state of enterprise networking is earthbound. Managing network architecture while organizations transition to SASE requires pragmatic, secure access solutions for existing hybrid infrastructures that are future-compatible.

Network security in transition

Secure access requirements for enterprises have taken on a new paradigm. Some applications are on-premises, while others are in the cloud, and some users are on-site, while others are remote. Network security requires a new model that considers all scenarios and positions organizations for the move to SASE, including:

- Out-to-In: Remote workers need access to private apps or resources that reside within the enterprise local area network (LAN).

Previous Next

- Out-to-Out: Remote workers need access to corporate apps that are located on the public cloud or internet.
- In-to-Out: On-site workers who are connected to the enterprise LAN require access to corporate apps on the public cloud or internet.
- In-to-In: On-site workers who are connected to the enterprise LAN require access to corporate apps located on the enterprise LAN.

Let's look at each of these scenarios to understand the issues and identify potential solutions.

Out-to-In

When remote workers need access to private apps or resources on the LAN, organizations need to administer least-privilege zero trust access for authenticated users. This approach eliminates the implicit trust typically granted by most current security architectures once a user is connected inside the corporate network.

In this scenario, Zero Trust Network Access (ZTNA) capabilities can be used to secure all remote interactions with network apps, data, and resources, enhancing VPNs and NGFWs and enabling micro-segmented access to network resources and applications. Technologies such as multi-factor authentication (MFA), identity-based seg-

mentation, and software-defined perimeter (SDP) further secure and strengthen granular, per-user policy access.

Out-to-Out

Remote workers need access to corporate SaaS apps in the public cloud as well as general internet and web-based resources, but it is inefficient to route this traffic through corporate security stacks in the datacenter. Organizations must secure this "direct-to-net" traffic with new approaches.

With cloud-delivered remote browser isolation (RBI) services, which air-gap all web interactions away from endpoints in secured cloud containers, and MFA and cloud access security broker (CASB) capabilities, organizations can control access to the web and without inefficiently routing traffic through corporate data centers.

In-to-Out

Every user working in the office accesses the public internet via the corporate LAN — email and cloud apps are among the most important use cases. While internet access is essential for productivity, it is the top threat vector for executing cyberattacks since the majority are initiated via phishing emails or malicious sites.

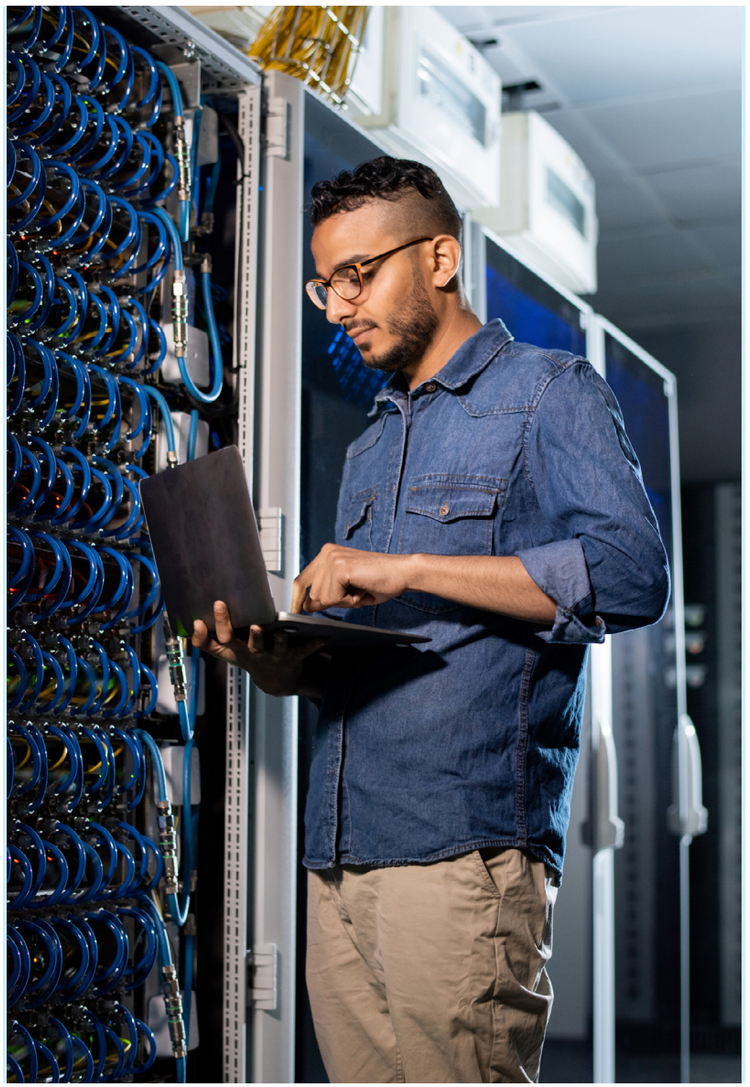
RBI-as-a-service is a next-generation web security tool that safeguards enterprise networks by proactively preventing web and email-based malware and ransomware attacks. It ensures users can use their devices to safely access any site or web app that is necessary without compromising their devices or networks.

In-to-In

On-site workers who are connected to the enterprise LAN and need access to local corporate network apps should be treated the same as anyone who gains access from outside the network perimeter, as in the Out-to-In scenario.

Surprisingly, that is often not the case. In this scenario, internal traffic must be subject to least-privilege access controls. For example, applications authorized users are not permitted access to would be invisible to them (e.g.,

When remote workers need **access to private apps** or resources on the LAN, organizations need to administer **least-privilege zero trust access** for authenticated users.



cloaked from their network visibility). Additionally, in this environment, any unauthorized users who somehow breach the network would be left completely in the dark.

If possible, creating granular, per-user authorization policies will limit access to the most secure level possible. AI/ML tools should be investigated to help in the "heavy-lifting" of creating these types of policies. Identity-based micro-segmentation solutions can be used to enforce least-privilege access policies I described, as well as cloak applications from cybercriminals.

Moving toward SASE

Organizations are starting to transition toward the SASE security framework. During this time when remote work has been the focus, the Out-to-In and Out-to-Out access paths are getting the most attention. This new enterprise security framework includes the other scenarios and encourages a comprehensive approach to network security using user and resource location to ensure that all access options are secured.

David Canellos is President and CEO at Ericom Software.

Networks Must Change to Support Mainstreaming of Working from Home

More than half of all enterprises expect their work-from-home populations to remain elevated after the pandemic ends. This permanent shift means that IT organizations need to adjust network architecture and network operations.

By Shamus McGillicuddy, VP of Research, Network Management, EMA

Working from home is not new. This writer has been using a home office since 2006. However, before the COVID-19 pandemic, remote work had been more of a perk than a way of doing business. Now millions upon millions of people are working from home, and many of them are never going back to an office. This new reality means that enterprise networks must evolve.

Enterprise Management Associates (EMA) recently published the research report "Enterprise WAN Transformation: SD-WAN, SASE, and the Pandemic," based on a survey of 303 IT professionals. This research found that, prior to the pandemic, the average enterprise had about 14% of its employees working from home on a regular basis. Now 64% of employees are working from home. More than half of these enterprises expect their work-from-home populations to remain elevated after the pandemic ends. This permanent shift means that IT organizations need to adjust network architecture and network operations.

Evolving networks with SD-WAN and SASE

Software-defined WAN (SD-WAN) and Secure Access Service Edge (SASE) will be essential technologies for supporting an architectural shift toward a work-from-home network. One of the foundational elements of SD-WAN is the creation of an overlay for secure site-to-site connectivity across any network. Theoretically, SD-WAN can be extended to home offices, and enterprises in our research recognize this opportunity. Eighty-four percent of enterprises told us that SD-WAN could support business continuity during the pandemic, and the primary opportunity with SD-WAN is the enablement of secure connectivity for home offices via an extension of the SD-WAN overlay.

Many research participants also told us that they expect to apply the WAN remediation capabilities of SD-WAN

Previous Next

solutions to home offices. For instance, some vendors offer forward error correction on their appliances, which could improve the home office user experience. In the future, some vendors might introduce software clients with such capabilities.

SASE is an emerging technology that will also support a new network architecture. The concept of SASE is still emerging, with few vendors offering a complete solution, but right now, it's best described as a cloud-delivered integration of SD-WAN, secure remote access, and network security. In our new research, 82% of IT professionals believe SASE can support business continuity during the pandemic. The primary opportunity is secure remote access, such as a cloud-delivered alternative to traditional remote VPN solutions.

EMA has observed many SD-WAN vendors evolving their solutions during the pandemic. Some have extended their overlays by discounting appliances or introducing new software clients. Others have accelerated their pivot toward SASE by integrating a secure remote access solution with SD-WAN.

Evolving network operations

On the operations side of things, EMA found that IT organizations are prioritizing two key points of visibility for supporting the home office user experience. First, 67% of IT organizations will focus on application health and performance. This focus makes sense because many IT organizations are already equipped to monitor their applications, particularly those hosted within their own data centers. Cloud applications, especially SaaS applications, may require new tools and processes. For instance, with the growing importance of conferencing applications like Zoom, IT organizations may acquire new tools for directly monitoring such a SaaS service.

The other **priority for monitoring** home office user experience is the availability and performance of local internet service providers (ISPs).

The other priority for monitoring home office user experience is the availability and performance of local internet service providers (ISPs). ISP performance has been inconsistent during the pandemic, with remote workers contending with members of their households and their neighbors for bandwidth. In addition to remote work, remote learning, telemedicine, online gaming, and streaming services are all experiencing all-time highs, which has strained ISP networks. Moving forward, IT organizations need visibility into these networks to protect the home office user experience.

ISP visibility will require new enterprise-grade monitoring tools to scale support of home workers. A troubleshooting process that relies on an end-user running a speed test on their local ISP won't scale. For instance, an IT organization might have hundreds of users simultaneously affected by the same ISP problem. Rather than collect the results of individual speed tests, IT administrators would benefit from an end-to-end view of ISP performance, where they can proactively identify trouble before end-user productivity is undermined. A tool that passively monitors internet traffic could help here, or an active monitoring tool that generates test traffic from agents on client devices could offer a more centralized and systematic alternative to the tests performed by an individual speed test application.

EMA believes that enterprise networks will evolve significantly post-pandemic, not just in the home office. Data center networks and certainly campus and branch office networks, too. We will research this topic extensively in 2021, so stay tuned.

Shamus McGillicuddy is a VP of Research, Network Management, at Enterprise Management Associates (EMA).

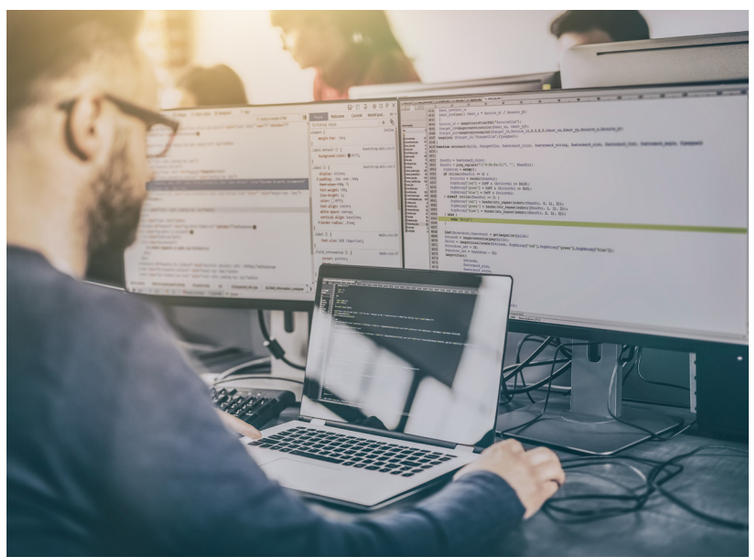
Breaking Down SASE

Deeply integrating security with networking functions provides higher-order protections for applications and data regardless of the paths that workflows or transactions take.

By John Maddison, EVP, Fortinet

SASE, or Secure Access Service Edge, is one of the hottest topics in both networking and security at the moment. And for good reason. Businesses, and the workers and networks that support them, have been thoroughly disrupted. Organizations, and especially their IT departments, have been wrestling with digital innovation for the past several years. With largely the same budget and staff they had at the start of this disruption, these teams have had to plan, design, implement and manage the rapid expansion of the traditional network to include multi-cloud environments, SaaS applications, the massive adoption of IoT, and next-gen branch offices that need rapid and reliable access to all of these applications and services.

And in just the last few months, the entire networking model has been inverted. Huge numbers of traditional workers now having to access business applications and networked resources from home. And this isn't just a temporary change. One recent survey reports that nearly a third of organizations are planning on having more than half of their employees continue working remotely full-time even after the pandemic subsides.



Defining SASE

As a result of all of this disruption, the arrival of SASE couldn't have been better timed. The basic concept is that SASE ensures secure access to distributed resources to a widely distributed and highly mobile workforce. And like SD-WAN, it also ensures reliable connectivity and performance across the public internet while keeping data, applications, transactions, and workflows secure.

However, while the high-level view of SASE is indeed promising, there is still some confusion about what a SASE solution is, the technologies it encompasses, and how it should be implemented. For example, is SASE just a cloud solution, or should it be integrated with physical, on-premises devices? Regardless of how organizations decide to address the implementation of a SASE solution, however, the most important thing to remember is that the definition isn't really all that important. What organizations really

need to focus on is designing and implementing a secure access strategy that can grow and adapt along with their business requirements.

SASE must start with a strong foundation

So, where do you start in selecting and deploying a SASE solution? Here are three critical concepts that should drive your SASE strategy.

Unify Security and Networking. First, you will need to bring security and networking together into a single, unified strategy. Far too often, network expansion driven by digital innovation results in siloed environments. For example, individual cloud environments — even when deployed as part of a multi-cloud strategy — are often secured using different security tools that do not interoperate. Branch offices often end up with their own security solutions that do not line up with those deployed in the cloud or on the LAN. And remote workers can weaken the chain by further fragmenting security.

Such environments — characterized by vendor sprawl, mismatched security solutions, and inconsistent policy enforcement — severely limit visibility and constrain control. While SASE is designed to help secure dynamic connectivity issues, the challenge is that SASE tends to be limited to cloud deployments, potentially contributing to a fragmented security strategy. But in the real world, where the LAN edge is just as important as the WAN and cloud edge, what's needed is a more comprehensive approach.

A security-driven networking strategy can overcome this limitation. Consistent solutions deployed in every branch, cloud, remote worker, or traditional network environment — including those chosen as part of a SASE solution — ensure broad visibility and control. And by deeply integrating security with networking functions, security can do more than span the entire network, providing higher-order protections for content, applications, and data regardless of the paths that workflows or transactions need to take. It can also adapt as that network infrastructure adapts to changing circumstances and requirements.

> Security technologies deployed in different cloud environments, for example, need to be able to gather and **share threat intelligence** between each other.

Integrated Products. The second-most important element of a SASE strategy is choosing security solutions designed to work together. Security technologies deployed in different cloud environments, for example, need to be able to gather and share threat intelligence between each other. But they also need to do this with similar security solutions deployed in branch offices and physical data centers, as well as on remote worker networks and devices. This enables the aggregation of data, so security teams can more effectively identify and respond to even the most sophisticated, evasion-enabled threats, as well as apply a single, consistent response that leverages resources from across the network.

Flexible Consumption Models. Finally, solutions need to support a variety of consumption models depending on where you're integrating your security stack — whether in hardware, virtual environments, or as cloud-hosted solutions. Security tools need to be chosen not just for their efficacy at addressing threats but also because they can be deployed across the maximum number of environments in the widest variety of form factors. This also includes interoperating with other third-party solutions — whether security or networking technologies — using APIs and common standards. This ensures a single view across the network, combined with centralized management and consistent orchestration of policies and configurations so that the entire enterprise is uniformly protected.

SASE is all about flexible, anytime, anywhere security

To be truly effective, SASE cannot be a "one size fits all" proposition. By integrating cloud-based SASE technologies with such things as physical access points and WAN and LAN controllers, organizations can implement a much more universal SASE strategy. By combing virtual solutions with physical systems, organizations can more effectively establish and enforce consistent policies, such as zero-trust networking that provides consistent protections and access controls to critical resources across the entire network, not just a piece of it. This ensures that any user, anywhere, on any device, can securely access the resources they need to do their job, and at the same time, do not have access to systems or resources not needed to do their job.

Once all the hype surrounding SASE — or really, any new networking solution or strategy — goes away, these three fundamentals remain in place. With the right foundation in place, you won't have to go out and buy a bunch of products to have a "SASE" solution. Instead, if you start building your network with the above three principals in mind, your network can be easily expanded to include SASE — or any other new development — while remaining resilient, secure, and manageable from end to end. That approach stands the test of time and allows organizations to stay ahead of the latest hype.

John Maddison is EVP Products & Solutions at Fortinet.

Ready for Whatever's Next

Try it Now

800+ Happy SASE Customers

Steve Waibel
Director of IT • Brake Masters

Tobias RÖlz
Marketing & Digital Service • Komax

Fabrice De Biasio
Director of IT • ASL Airlines

CATO NETWORKS