WHITE PAPER

HOW SASE CAN IMPROVE SECURITY

With data and workloads spread among remote users and cloud services, a decentralized approach can help organizations manage threats.

CDW PEOPLE WHO GET IT

EXECUTIVE SUMMARY

The secure access service edge (SASE) approach to cybersecurity plays a crucial role in protecting today's distributed information systems. This evolving security strategy recognizes that organizations now have users working from home, on the road and in other remote locations. Those same users are no longer just accessing information stored in safeguarded corporate data centers but are likely using a variety of cloud-based services to help meet their business objectives. In this environment, it's no longer necessary or prudent to route all remote user traffic through a centralized data center.

SASE technology enables remote work and the use of cloud-based services by shifting the point of security policy enforcement away from the corporate network and applying it wherever users are located. End-user devices and other security tools understand and enforce the organization's security policies consistently, regardless of the device's physical location or network connectivity. This allows technology teams to sleep soundly, knowing that remote users are subject to the same security requirements as those who use devices on a corporate network.

SASE technology also simplifies branch-to-central and branch-to-branch network connectivity over highly sophisticated and comprehensive WAN technologies, along with enhanced cloud-delivered network security functions such as secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), Firewall as a Service and zero-trust network access (ZTNA) to support the dynamic secure access needs of digital transformation.

What Is Secure Access Service Edge?

SASE delivers users a secure network connection as a service. It combines many existing security technologies, such as identity and access management (IAM) platforms and cloud security tools with WAN technology to provide users with a secure network connection wherever they are located. Think of SASE as delivering a secure network connection as a cloud-based service without requiring a connection back to an organization's own data center.

The Landscape

The COVID-19 pandemic has permanently altered the ways organizations work, but only by accelerating workplace trends that were already gaining momentum in many industries. Chief among these: the growing adoption of cloud computing solutions and an increased reliance on remote work.

Over the past few years, organizations steadily moved applications out of their own corporate data centers to cloud-based solutions that offer increased flexibility, scalability and fault tolerance while reducing the total cost of ownership. Many technology leaders adopted a cloud-first philosophy that focuses on Software as a Service applications, such as Microsoft 365 and Salesforce. When they can't find an off-the-shelf SaaS solution to their business requirements, organizations now tend to adopt Infrastructure as a Service or Platform as a Service offerings from cloud vendors such as Amazon Web Services, Microsoft Azure or Google Cloud Platform.

This shift from centralized applications to the cloud helped drive the second important trend: an increase in the number of remote workers and the amount of time they spend working outside of the office. Employees now expect to be as productive as they are in the office when they are at home or on the road. They demand access to corporate data and use of the same applications they would have if sitting in the office.

As these trends continue, security teams face a new set of challenges supporting their users while maintaining an organization's security policies. After decades of building out security tools that protected a core data center, they now need to apply those same policies to protect a dispersed set of cloud services. Traditional models that apply a set of centralized security controls at a data center require that all remote user traffic be routed through that data center before reaching the internet. In a remote work, cloud-first world, that data center approach is difficult to enforce, unnecessarily increases the burden on the data center and results in both poor network performance and decreased user satisfaction.

The way organizations moved to the cloud has also complicated the deployment of sound security policies in those environments. Decisions around cloud computing were often made rapidly in response to the pandemic or by business units looking to address their needs without consulting IT teams. In these cases, security concerns often were not carefully vetted. Organizations also deployed Internet of Things (IoT) devices that reach back to cloud services in an effort to streamline their operations. Today, organizations are working to retrofit those rushed adoptions to align their existing security policies with the cloud's shared-responsibility model of cybersecurity.

The percentage of enterprises that are expected to have explicit strategies and timelines for SASE adoption by 2025[1]

Source: [1]Gartner, "2021 Strategic Roadmap for SASE Convergence," March 25, 2021

Threats

During the same time period that organizations rushed to adopt remote work and cloud solutions, the cybersecurity threat landscape also shifted dramatically. Organizations continue to be plagued by ransomware and phishing attacks, but those attacks are growing in sophistication and number. Advanced persistent threat actors now leverage technically advanced tools to penetrate even well-defended networks. This leaves organizations in a position where they must continue to protect the confidentiality, integrity and availability of their data despite a shifting threat environment.

Fortunately, many of the same cybersecurity tools used to protect organizations for many years still play an important role in this new environment. Organizations adopting a SASE strategy will find that this approach supplements those existing technologies with additional tools designed to combat modern threats.

Meet SASE

For many years, organizations approached cybersecurity with a containment mindset. They sought to build walls around enterprise data and then apply security controls to those isolated strongholds to protect them against external attack. This approach fails to meet the needs of modern organizations because the trends toward remote work and cloud services make building those virtual walls almost impossible. SASE approaches seek to flip the legacy model on its head. Instead of forcing endpoint communication through a central corporate location where security controls protect it, SASE acknowledges that clients and data services are distributed and seeks to put security between them and as close to the endpoints as possible, wherever they reside.

SASE and the Fight Against Ransomware

Ransomware attacks continue to cripple organizations across industry sectors. High-profile attacks against Colonial Pipeline and JBS Foods in 2021 made major headlines, but hundreds of other firms fall victim to these attacks every month. The attacks start when a cybercriminal gains an initial foothold on a network and manages to install malicious code that crawls the network and encrypts data, preventing its legitimate use. The attackers then demand payment of large sums in virtually untraceable cryptocurrency transactions before providing the victim with the means to decrypt the data and restore access.

SASE solutions play an important role in safeguarding networks against ransomware attacks by protecting data that flows over communication channels between an endpoint and resources that are connected to the internet. For example, a SASE solution can detect and block the download of a malicious payload to a client device while also preventing a client from connecting to known ransomware and bot command-and-control servers.

One of the most compelling selling points for SASE solutions is that organizations may adopt a SASE strategy while making use of their existing cybersecurity tools. SASE allows cybersecurity teams to apply controls to end-user devices making use of cloud services, simultaneously delivering a better experience for users and protecting the organization's data from compromise. Organizations adopting a SASE strategy may make more effective use of their firewalls, malware protection solutions and other tools while applying artificial intelligence and machine learning analytics to their cybersecurity programs.

SASE plays a particularly useful role when organizations pursue digital transformation efforts. Many of the IoT devices and other systems used in digital transformation lack standardized security controls. SASE applies consistent, centrally managed security policies to these assets across far-flung locations, disrupting potential attacks before they take root.

Enabling SASE

Effective SASE deployments build on a variety of tools and capabilities to create a layered approach to security. They bundle many different security services and capabilities and deliver them to endpoint devices through the cloud, protecting the organization's data and systems from a wide range of security threats. This requires that organizations build out a comprehensive set of security components and then supplement them with a strong network capability to deploy those services to remote users.

Security Components

Organizations adopting a SASE strategy should begin with an inventory of their existing cybersecurity controls. It is likely that they have already deployed many of the core technologies that make SASE possible and may leverage those components in their SASE programs with some reconfiguration or upgrades. While some organizations may need to acquire new solutions to fill the gaps in their current cybersecurity program, it's likely they can begin with the technologies they have and then add on new capabilities as their SASE program evolves.

Secure web gateway (web proxy): Many modern threats gain their initial foothold on endpoints by deceiving end users into visiting malicious websites and downloading content that compromises the security of their systems. Secure web gateway (SWG) technology seeks to mitigate these threats by inspecting end-user web activity and applying a consistent set of security policies to enforce safe browsing habits at the endpoint.

SWG solutions serve as web proxies, inserting themselves between end users and the web servers they wish to access. This intermediary approach allows the SWG to perform three core security tasks for all user web requests. First, each request is subjected to URL filtering that confirms that the request is not for a web page known to host malicious content or other content that violates the organization's filtering policies. Second, SWGs provide SSL/TLS inspection capabilities that allow them to peer inside otherwise encrypted content. Finally, these solutions provide malware detection with sandboxing capabilities that examine the actions and intent of executable software before it reaches end-user devices. SASE solutions build this SWG

capability directly into the bundle of services provided to users, automating the deployment of SWG functionality.

Cloud-delivered outbound firewall: While secure web gateways play a crucial role in protecting users from malicious network traffic, it's important to remember that not all network traffic uses the web. Cloud-delivered outbound firewalls provide a robust filtering service for other ports and protocols, protecting the organization with the ability to write context-specific rules for the types of network activity permitted from different endpoints. These rules may apply to the entire organization or may be dynamically modified based on contextual circumstances, such as a user's role in the organization or the application being used.

Traditional firewalls focus on the legacy model of building walls around protected networks and controlling inbound traffic. Outbound firewalls are better suited to SASE deployments because they focus on protecting traffic from dispersed endpoints and filtering their outbound traffic to the internet.

Intrusion prevention systems: Intrusion prevention systems provide another layer of network security, analyzing traffic to and from endpoints for signs of malicious activity that might escape the notice of a firewall or secure web gateway. IPS platforms combine signature detection techniques that look for known patterns of malicious activity with behavioral analysis technology that watches for activity deviating from normal baselines. Suspicious activity is automatically blocked before reaching endpoints. This approach stops distributed denial of service attacks, blocks command-and-control traffic associated with botnets and ransomware, and halts application attacks such as buffer overflows, SQL injection and cross-site scripting.

The percentage of IT professionals who consider application security to be of high importance when enabling remote access[2]

DNS security and control: The Domain Name System (DNS) serves as a crucial backbone of the internet, allowing systems to determine the correct IP addresses associated with each domain name. SASE solutions incorporate DNS security tools that leverage this centralized lookup server to enforce security policies. SASE endpoints receive DNS service through a trusted, secure DNS server as part of their cloud-delivered bundle of network services. That DNS service, in turn, provides filtering capabilities by redirecting requests for known malicious sites, protecting against both user error and the automated activity of malware. This capability provides an added layer of protection against phishing attacks, botnets, ransomware and other malicious software.

Cloud access security broker: Organizations use dozens, if not hundreds, of cloud services to meet different business needs. Each of these cloud services offers customizable security configurations that allow administrators to restrict user activity. Unfortunately, the proliferation of cloud services makes it extremely difficult for cybersecurity teams to stay on top of the many consoles and tools used to manage those security configurations.

Cloud access security brokers provide a unified platform that allows administrators to centrally configure policies for cloud service use. One common CASB solution is the proxy-based (inline) approach, which monitors and controls traffic between an endpoint and a SaaS system by proxying the HTTP/HTTPS connection. As the CASB monitors the session, it can both log events based on the observed traffic and prevent unauthorized actions.

In another approach, the CASB solution reaches into each of the cloud services used by the organization via its application programming interface (API) and configures the cloud service to enforce that policy.

Both approaches allow SASE administrators to enforce consistent security policies rapidly and effectively.

Data Loss Prevention: DLP platforms focus on protecting data (rather than systems) from compromise by monitoring outbound network traffic for potentially unauthorized exfiltration of sensitive information. They then step in and block transmissions that would violate security policies, preventing data from being irretrievably lost.

As with other cybersecurity technologies, network-based DLP solutions may be delivered as part of a bundle of cloud security services provided over an end user's network connection. Traffic that successfully passes through firewalls,

SASE and Zero Trust

Zero-trust network architecture (ZTNA) seeks to shift organizations from models where access decisions are made based on implied trust in a device or a network location to one where all trust decisions are based on the confirmed identity of a user and device. Zero-trust approaches require a robust set of security controls, beginning with a comprehensive IAM program that takes advantage of strong multifactor authentication technology and then uses network access control, mobile device management (MDM), network segmentation and other techniques to consistently enforce security policies based on the decisions made by the IAM platform.

SASE plays a crucial role in enforcing zero-trust policies by providing identity-based remote network access. It works with other security technologies to limit network access to authorized users and then restricts those users to carrying out activities that fit within their security profiles. SASE isn't a silver bullet that automatically achieves zero trust, but it plays a crucial role in enabling zero-trust approaches at the network edge.

Source: [2]checkpoint.com, "Secure Access Service Edge (SASE) Solutions are the Future: Survey Uncovers Organizations' Security Priorities for Hybrid Working," July 8, 2021

secure web gateways and IPS may be stopped in its tracks if it contains sensitive information being transmitted nonsecurely or to an unapproved destination.

Remote browser isolation: Some organizations go even further in their SASE approaches and seek to separate users' browsing activity from their hardware. Instead of launching browsers on local devices where they may be affected by malicious code, remote browser isolation technology provides web browsing to users as a service over the internet.

In an RBI deployment, users see a familiar web browsing interface and can navigate to any website that meets the organization's security policy. However, the user's computer doesn't run the browser and never interacts directly with the remote website. Instead, the user controls a web browser installed on the RBI platform. This approach provides a degree of separation, isolating the endpoint from any ill effects of browsing the web.

Network Components

The security components of a SASE deployment play a vital role in protecting users and devices from cybersecurity risks. However, these are effective only if they are delivered to endpoints as a bundled set of security services. The network components of a SASE deployment offer this delivery service.

VPN as a Service: SASE deployments provide users with a robust set of secure network services wherever they travel. This approach replaces traditional virtual private networks with a bundled service offering that uses VPN encryption to protect network traffic to and from endpoints while also adding on the other layers of SASE defense.

SASE Does Not Replace an Endpoint Security Solution

SASE solutions are focused on the security of network connections provided to endpoints wherever they are in the world. This technology ensures that the network connection is secure, whether the user is sitting in corporate headquarters, working from home, in a coffee shop or on an airplane. The endpoint automatically connects to the secure network and receives the complete bundle of SASE services to protect it from attack.

SASE does not, however, reach into the endpoint itself; thus, endpoints are still subject to a variety of threats ranging from malicious flash drives to physical theft. Cybersecurity professionals must ensure that they provide robust endpoint security that rounds out an endpoint's layered defensive posture. Endpoint detection and response platforms allow secure configuration and monitoring of endpoints to provide cybersecurity teams with the visibility and control they need. Effective SASE deployments combined with strong EDR can help organizations achieve their security objectives.

SD-WAN: Software-defined wide area networking rests at the heart of an organization's SASE deployment. The SD-WAN approach uses intelligent orchestration software to provide secure, reliable interoffice connectivity over internet circuits, rather than relying on expensive private circuits. SD-WAN allows organizations to avoid overtaxing their data centers with internet traffic by allowing remote offices to access the internet directly. SASE enables this approach by moving security to the service edge, allowing organizations to confidently move forward with direct internet access for remote offices.

Circuit aggregation and consolidation: SD-WAN and direct internet access allow organizations to dramatically reduce their connectivity costs by aggregating and consolidating communication circuits. Offices no longer require multiple circuits to connect to other locations and can instead rely on a single commodity internet connection (and perhaps an LTE/5G backup) to connect them to the SD-WAN environment.

Services

Organizations considering deployment of a SASE environment often rely on expert guidance to help them through the stages of their deployment. Bringing in outside advisers can help organizations design a SASE strategy that will avoid common pitfalls and serve them well for many years.

External advisers can help organizations with:

- General guidance on SASE strategies
- Planning and design of SASE security and networking components
- Deployment of SASE technology
- Adoption of SASE components by employees and business units
- Management of subscription services
- Management of cybersecurity operation centers and incident response
- Auditing and renegotiation of communication circuit contracts
- Analysis of cybersecurity risk exposures

Strategies for Effective SASE Deployment

As organizations consider the future of SASE deployments, they should also rethink both their security posture and their network connectivity model. Changing to a decentralized enforcement of centralized security policies marks a major paradigm shift, but it comes with the significant benefits of reduced network costs and improved security posture. With the right planning, SASE initiatives can deliver tremendous business value.

SASE deployments differ from other security projects organizations undertake. The cloud-based nature of SASE components requires organizations to make minimal capital expenditures because there isn't much hardware to purchase. This approach also dramatically reduces the risk of sizing and scaling the security components of a SASE deployment. Cloud-based SASE components can simply scale with the business, expanding and contracting to meet changing requirements. SD-WAN connectivity is perhaps the only area of a SASE deployment that requires careful sizing prior to selection.

The service-based nature of SASE solutions also provides organizations with a significant degree of flexibility over traditional tools. Organizations can avoid "big bang" upgrade and migration projects that cause service outages and instead opt for small, controlled pilot testing of new technology with isolated test groups. Once they're confident that the technology works properly, rolling it out to the entire organization is often as simple as flipping a switch. This approach improves the user experience and limits the negative impact of changes.

SASE solutions also fit nicely into efforts by organizations to automate their security operations. APIs offered by SASE component providers enable the direct integration of SASE tools with security orchestration, automation and response platforms. This allows both internet-based tools and on-premises security devices to play a role in the organization's automated responses to changing cybersecurity circumstances. By working cooperatively with other security tools, SASE components provide IT teams and security leaders with both enhanced visibility into their current security posture and rapid response capabilities when things go wrong.

The future of SASE deployments is bright. As these technologies mature, organizations should expect to see even greater benefits from their security ecosystems. SASE components will likely offer even tighter integrations with identity providers that help enable zero-trust initiatives. Security teams should also expect to see enhanced integrations with MDM and other security configuration tools, providing centralized and robust control of both devices and the network connections that serve them.

CDW: We Get Security

CDW is a full-lifecycle, full-stack IT solution provider with numerous service offerings for organizations looking to adopt a SASE model. Our team routinely works with organizations of all sizes and across industries who are designing, implementing and modernizing their SASE strategy. We often conduct SD-WAN and SASE advisory workshops that help technology leaders identify their secure networking needs.

With those needs in hand, our experienced staff of security and industry experts can help you find the right solutions and services to build a robust and secure endpoint computing environment and manage that environment effectively. CDW's subject matter experts assists customers with a variety of initiatives to meet their security requirements, accommodate their business needs and fit within the constraints of their budgets and teams.

CDW's security services include:

- Penetration testing
- Compliance assessments
- Framework assessments
- Professional services
- Consultation services

CDW AMPLIFIED™ Services

CDW Amplified™ Security services are composed of both information security and network security practices, offer an objective look at your current security posture and provide continuous defense against, detection of and response to growing threats.

DESIGN for the Future
All CDW Amplified Security services provide a comprehensive approach to prevent data breaches and proactively respond to cyberattacks.

ORCHESTRATE Progress
CDW Amplified Security engineers can assist with installation and deployment of advanced security techniques and ensure technologies are optimized for your needs.

MANAGE Operations
We can manage security solutions for you, helping you stay vigilant and maintain compliance while easing the burden on your IT staff.

Sponsors

Check Point SOFTWARE TECHNOLOGIES LTD.

cisco Partner

paloalto NETWORKS

To learn more about how SASE can improve your security posture, contact your CDW Account Team or call 800.800.4239

CDW PEOPLE WHO GET IT®