SASE BUYING GUIDE

The ultimate SASE buying guide

Key considerations for today's buying teams

WINDSTREAM ENTERPRISE

Table of contents

SECTION 1

Introduction

Introduction

Today's businesses are dealing with more data than ever, and it is located and moved between more and more endpoints as the 'edge' of the corporate network continues to expand outward. Companies are also leaning more on public cloud strategies, which place data outside of their corporate networks and can often require egress between public and private cloud environments. Securing that data and the networks it travels on has always been important, but is now becoming absolutely mission critical.

Of course, not all companies are on the forefront of next-generation data security. Oftentimes, they have constructed rigid security architectures over the years, consisting of disjointed point solutions from various vendors. These piece-mealed approaches cannot adapt to emerging technical requirements and the evolving threat landscape. The result is lower business agility and increased risk made worse by lack of resources and scarce cybersecurity skills in part due to staffing and personnel shortages.

With the idea of convergence at the forefront, forward-thinking companies are leveraging a new approach to network and data security called Secure Access Service Edge (SASE)—an emerging "as a Service" framework.

SASE is more than a single product for security:

It is a layered, interwoven fabric of network and security technologies that work together to protect an organization's data and systems from unwanted access, and when delivered via a managed services provider, delivers the additional value of a finely tuned, converged system with complete visibility and co-management control through a single management portal.

Introduction: A brief history of SASE

Analyst firm Gartner® was the first to coin and implement the term SASE in 2019[1], defining it as the convergence of two separate technology markets, namely the WAN edge (SD-WAN) and network security.

To support the growing need for security all the way to the network edge, SASE represented a global, cloud-delivered service that could provide secure and optimized access to any user, at any location and to any application.

According to that same Gartner glossary[1], the security component of SASE included multiple services, such as:

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Zero Trust Network Access (ZTNA)
- Firewall as a Service (FWaaS)

These components are all delivered as a cloud service. Optimized versions of SASE combine all of these into a single solution from a single vendor, with one management portal providing complete visibility into all network security-related activity.

Security Service Edge (SSE)[2] includes the same security components as SASE and can be combined with an existing SD-WAN to give organizations a secure network path between public and private applications for all locations and end users.

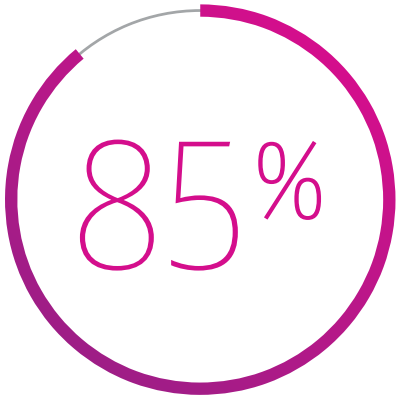
Introduction: Network and security convergence is the future

Enterprises are now faced with a decision on how to approach the "converged future" of their IT infrastructure. Some organizations will go for the full SASE convergence from the outset, while others will slowly migrate through multiple steps, starting with SSE and then integrating the network component either when they're ready or business conditions, such as expiring contracts or poor network performance spark a move.

For most enterprises, keeping this full transformation route open by using a single vendor SASE is a strategic decision. The closer these technologies are integrated, the better the visibility, security posture, operational simplicity, cost savings and business agility. SASE capabilities enable organizations to deliver protected networking and security services as the threat landscape continues to evolve.

For this reason, Gartner estimates that by 2025, at least 80% of enterprises will have explicit strategies and timelines for SASE adoption, up from 20% in 2021.[4]

The market for SASE will grow at a CAGR of 36%, reaching almost $15 billion by 2025.[5]



By 2026, 85% of organizations seeking to procure SSE-related security services will purchase a consolidated SSE solution, rather than stand-alone cloud access security broker, secure web gateway and ZTNA offerings.[3]

The time is now to move to a comprehensive, single-vendor SASE approach, or at the very least, begin the process of migrating disparate point security solutions and outdated network technologies such as MPLS to a more agile, converged SASE solution.

This detailed guide will outline the individual components that can be combined into a cloud-based SASE solution and explore the purchasing process when acquiring a SASE implementation for your company. With cross-functional team buying becoming more prevalent, we will also look at which roles should be involved in the purchasing process, when they should be engaged and what role-specific concerns they should address during their customer journey.

Introduction: SASE what-ifs?

- **What if** you could see security risks and synchronize security policies across every user and device on your network?
- **What if** you could eliminate the CAPEX and complexity of dozens of disparate devices that are out of sync and failing to secure your network?
- **What if** you need to support constant changes in branch locations, bandwidth and access methods?
- **What if** you could mitigate the data security risks associated with a remote workforce and cloud applications?
- **What if** you could see and make changes to your application prioritization in real time—or better yet—automate them?
- **What if** you need to do all of this with tight budgets, timelines and limited IT staff?

With SASE, you can.

SECTION 2

SASE defined for today

SASE defined for today

Software-defined Wide Area Network (SD-WAN)

SD-WAN stands for Software-defined Wide Area Network. SD-WAN technology is designed to help organizations reduce the cost and complexity of managing their WANs, while also improving application performance, resiliency and security.

SD-WAN achieves this by separating the network control plane from the data plane and centralizing the control of the WAN using software. This allows network administrators to set priorities for every application that are then automatically used to manage network traffic flow dynamically, based on the application, user and network conditions.

SD-WAN also allows organizations to leverage multiple types of network connections, including broadband internet, MPLS and LTE, to optimize resiliency and ensure that critical applications are always prioritized.

SD-WAN delivers reliability and performance by optimizing your network for cloud-based applications and services. When built upon a solid foundation of SD-WAN, SASE offers enhanced security and less network complexity to support workforce mobility.

When implemented as part the enterprise's security posture, SD-WAN can provide:

1. **Cost savings:** SD-WAN helps organizations reduce their WAN costs by using multiple network connections, including broadband internet, to provide connectivity between locations. This reduces the reliance on expensive MPLS connections, resulting in significant cost savings.
2. **Improved application performance:** SD-WAN optimizes application performance by dynamically steering traffic over the most efficient path based on the application and network conditions. This helps to ensure that critical applications always receive the necessary bandwidth and low latency, resulting in a better user experience.
3. **Enhanced network security:** SD-WAN improves network security by encrypting traffic and providing secure connectivity over the internet. SD-WAN can also provide granular access control and segmentation, enabling organizations to isolate traffic and protect against threats.
4. **Simplified network management:** SD-WAN provides centralized management and visibility of network traffic, making it easier for network administrators to manage and troubleshoot the network. This results in greater operational efficiency and reduced downtime.
5. **Increased agility:** SD-WAN lets organizations quickly and easily add or remove locations and applications from the network, without the need for significant manual configuration changes. This increases agility and enables organizations to respond more quickly to changing business needs.

SASE defined for today

Firewall as a Service (FWaaS)

Firewall as a Service is a type of network security service that provides firewall functionality in the cloud. It enables organizations to implement network security policies and controls without the need for on-premises hardware or software.

FWaaS works by routing network traffic through a cloud-based security platform. This platform can be hosted by a third-party service provider or by the organization itself. The firewall policies and rules are defined and managed through a centralized management console, which provides visibility into network traffic and security events.

This next-generation cloud firewall capability can be integrated into a SASE platform to provide a wide range of network security benefits:

1. **Scalable:** FWaaS helps organizations add or modify security policies without the need for additional hardware or software.
2. **Cost-effective:** FWaaS is often less expensive than traditional firewall solutions, as it eliminates the need for on-premises hardware and reduces the need for dedicated IT resources.
3. **Easy to manage:** FWaaS offers a centralized management console that simplifies the management and configuration of firewall policies and rules. This reduces the need for dedicated IT staff to manage and maintain firewall hardware.
4. **Highly secure:** FWaaS provides a high level of security, as traffic is routed through a cloud-based security platform that is designed to detect and prevent security threats.
5. **Flexible:** FWaaS enables organizations to choose the level of service that best fits their needs, whether it is a fully managed service or a self-managed service.

SASE defined for today

Secure Web Gateway (SWG)

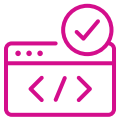
Secure Web Gateways (SWGs) are network security solutions designed to protect users and devices from web-based threats. SWGs are typically deployed at the network perimeter or in the cloud, and they inspect all web traffic to and from the organization. This component offers enhanced visibility and protection against web-based threats by enforcing security policies that safeguard users from harmful websites and applications.

SWGs are an important component of modern network security architectures, as they help organizations protect users against phishing and other web-borne threats and enforce security policies to ensure compliance with industry regulations and internal security requirements.

When implemented as part of a converged SASE solution, SWGs offer:

1. **URL filtering:** SWGs can block access to websites that are known to be malicious or unsafe, or that violate an organization's acceptable use policy.
2. **Malware detection:** SWGs can scan web traffic for malware and other threats, and block access to websites that are known to host malware or distribute malicious content.
3. **Content filtering:** SWGs can be configured to block access to inappropriate or non-business-related content, such as social media, streaming video and other non-work-related sites.
4. **SSL inspection:** SWGs can inspect encrypted web traffic to detect and prevent threats that may be hidden within SSL/TLS-encrypted sessions.

SASE defined for today



Remote Browser Interface (RBI)

Remote Browser Isolation is an advanced cybersecurity interface that protects organizations by isolating browsing activity from end-user devices and corporate networks. RBI serves as a powerful ally to SWGs, extending protection by seamlessly handling new or uncategorized websites. RBI acts as a buffer zone, executing potentially harmful content in a secure, remote environment—away from the organization's main infrastructure.

RBI is particularly crucial for contemporary business models, where hybrid and remote work arrangements expand the attack surface and elevate the risk of web-based attacks.

When integrated within a SASE framework, RBI provides:

1. **Enhanced security measures:** By preventing direct interaction with untrusted web content, RBI shields critical IT assets from malware, phishing attacks and other advanced threats, including zero-day exploits.
2. **Isolation of threats:** RBI creates a virtual gap between users and potential cyberthreats, ensuring that any malicious content is detained and neutralized within a disposable virtual environment.
3. **Compatibility and user experience:** RBI supports a variety of browsers and devices, affirming a frictionless user experience while maintaining strict security controls. Users benefit from secure and unrestricted web access without sacrificing performance or safety.
4. **Protection for distributed workforces:** As remote work becomes increasingly prevalent, RBI safeguards remote employees' online activities, maintaining robust security regardless of their location.

SASE defined for today

Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) is a security model that facilitates secure access to applications and resources based on the identity of the user, device and context of the request, rather than relying solely on network or location-based controls. ZTNA provides remote workers with scalable and secure connectivity to applications, data and services based on clearly defined access control policies, to ensure rigorous threat protection via a high-performing network and optimized user experience.

ZTNA assumes that all access attempts, even those originating from inside the network, are potentially malicious and untrusted. ZTNA is critical for companies with remote workers or data that lives at the edge.

As such, this security protocol provides a layered approach that includes:

1. **Authentication and authorization:** ZTNA requires users and devices to be authenticated and authorized before granting access to resources. This helps ensure that only approved users and devices are accessing applications and data.
2. **Micro-segmentation:** ZTNA uses micro-segmentation to isolate workloads and resources to limit the potential impact of a security breach. This helps prevent lateral movement and limits the scope of a security incident.
3. **Least privilege access:** ZTNA enforces the principle of least privilege, which ensures that users and devices only have access to the resources and data that they need to perform their job functions.
4. **Continuous monitoring:** ZTNA continuously monitors user and device behavior to detect and respond to anomalies and security incidents in real-time.

As a security component of SASE, ZTNA enables organizations to provide secure access to resources and data from any device, anywhere, without relying on traditional network-based security controls that can be easily bypassed by attackers.

By 2027, the majority of CIOs will prioritize secure work from anywhere (remote, branch or campus), elevating it from a secondary security concern to a primary business priority.[6]

SASE defined for today

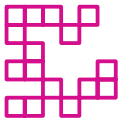
Cloud Access Security Broker (CASB)

Cloud Access Security Broker (CASB) is a security component that enables organizations to extend their security policies and controls to cloud-based applications and services. CASB provides visibility into cloud application usage, enforce security policies and detect and respond to cloud-based threats.

As component of a SASE solution, CASB provides protection for network extensibility to cloud-based applications, along with:

1. **Discovery and visibility:** CASB discovers and classifies cloud applications and services that are being used within the organization and provides visibility into how they are being used.
2. **User and Entity Behavior Analytics (UEBA):** CASB uses UEBA to monitor user and entity behavior within cloud applications and detect and respond to suspicious activities or potential threats.
3. **Data protection:** CASB provides Data Loss Prevention (DLP) and other data protection capabilities to ensure that sensitive data is not exposed or leaked in cloud environments.
4. **Access control:** CASB offers granular access controls to cloud applications and services and enforces authentication and authorization policies to ensure that only authorized users and devices are accessing cloud resources.
5. **Compliance and governance:** CASB delivers compliance and governance capabilities to help organizations meet regulatory requirements and enforce security policies in cloud environments.

SASE defined for today



Data Loss Prevention (DLP)

Data Loss Prevention is a critical line of defense in the protection of an organization's sensitive data. DLP integrates seamlessly with SASE architecture. This integration is pivotal in securing data at all stages—whether at rest, in use or in transit across the network. It is a comprehensive approach to guard against data breaches, maintain regulatory compliance and protect against internal vulnerabilities, ensuring that your data's integrity remains intact.

When integrated into a converged SASE solution, DLP provides:

1. **Data classification:** DLP automatically categorizes data to ensure that only the appropriate users have access to sensitive information.
2. **Policy enforcement:** DLP implements custom policies that control and monitor the transfer of critical data across the enterprise.
3. **Incident management and reporting:** DLP offers customized dashboards for real-time insights, trend identification and threat mitigation.
4. **Advanced inspection techniques:** DLP utilizes sophisticated methods to scrutinize information content within objects like files, applications or data streams.
5. **Regulatory compliance support:** DLP ensures adherence to various compliance standards, such as PCI-DSS for payment card information and HIPAA for healthcare records.

SASE defined for today

Threat Prevention

Threat Prevention goes beyond traditional anti-virus software, utilizing an array of cutting-edge technologies to thwart both known and emerging malware threats. Designed for deployment in diverse environments, Threat Prevention ensures comprehensive protection by performing deep packet inspection and leveraging its multi-layered, tightly integrated anti-malware engines.

By incorporating Artificial Intelligence (AI), Machine Learning (ML), Behavioral Detection, Exploit Mitigation and a cloud-based architecture, Threat Prevention delivers an agile and adaptive security posture that is critical for the protection of enterprise networks. This purpose-built AI-based reputation system autonomously scores information from 250+ threat intelligence feeds.

When integrated within a SASE framework, Threat Prevention provides:

1. **Intrusion Prevention System (IPS):** Real-time protection against advanced threats and attacks utilizing known and unknown exploits applies to all traffic, Internet, WAN and Cloud preventing data theft and ransomware.
2. **Next-Gen Anti-Malware (NGAM):** Provides malware detection for zero-day attacks in real-time as files are transmitted across the Internet, WAN and Cloud.
3. **DNS security:** Prevents malicious activity attempts hiding within the protocol's traffic by blocking DNS requests to malicious destinations before a connection is made.
4. **Threat intelligence:** AI-based system autonomously aggregates reputation scores from 250+ threat intelligence feeds. An updated and aggregated blacklist is automatically published to all PoPs ensuring up-to-date protection with near zero false positives.
5. **Real-time AI/ML:** Phishing & malware protection detects attack techniques like Domain Squatting and Domain Generation Algorithms (DGAs).
6. **Anti-phishing:** Blocks known phishing sites based on reputation. Inline AI/ML identifies sites not yet blacklisted.

SASE defined for today

Endpoint Protection Platform (EPP)

EPP is a security solution that safeguards individual devices (endpoints) from malware and security threats, providing an additional layer of protection for your enterprise network.

Organizations should adopt a robust, multi-layered security strategy that combines both network and endpoint protection. This is essential because not all threats can be stopped at any single point.

This is where EPP (Endpoint Protection Platform) comes in. Deployed directly on laptops and smart devices, EPP safeguards individual endpoints and, by extension, your entire enterprise. It complements existing network security measures. EPP uses a wide range of technologies to ensure continuous endpoint protection, preventing the execution of malicious files.

When integrated within a SASE framework, Endpoint Protection Platform (EPP) provides:

1. **Endpoint malware defense:** Protects individual devices from file-based threats (viruses, trojans, etc.) utilizing a combination of detection techniques like signature matching and behavioral analysis.
2. **Exploit mitigation:** Blocks attempts to leverage software vulnerabilities for malicious purposes, preventing zero-day attacks and reducing the attack surface on endpoints.
3. **Application control:** Allows administrators to define and enforce rules for which applications are permitted on endpoints, preventing unauthorized software and mitigating associated risks.
4. **Device-level firewall:** Provides an additional layer of protection at the endpoint by filtering incoming and outgoing network traffic based on specified security rules.
5. **Data encryption:** Secures sensitive data stored on endpoints by rendering it unreadable without the proper decryption keys, safeguarding information in the event of device loss or theft.

SASE defined for today

Managed Extended Detection & Response (MXDR)

Managed Extended Detection and Response is a security service for enterprises seeking to enhance their cybersecurity posture with advanced threat identification and remediation capabilities. Gain the assurance of continuous monitoring and comprehensive protection with this Security-as-a-Service solution that allows businesses to extend their security operations.

When integrated within a SASE framework, MXDR provides:

1. **Continuous 24/7 monitoring:** MXDR provides vigilant oversight of the IT environment, detecting and alerting on any signs of malicious activity around-the-clock.
2. **Expert threat hunting:** MXDR proactively searches for potential threats before they escalate into breaches, utilizing the latest in cyberthreat intelligence.
3. **Immediate threat response:** MXDR ensures swift action to isolate and neutralize threats, minimizing impact and safeguarding assets.
4. **Forensic analysis and investigation:** MXDR offers detailed examination of security incidents to uncover the root cause and implement preventative measures.
5. **Compliance assurance:** MXDR strongly adheres to regulatory requirements, assisting businesses in meeting compliance and audit standards with ease.

SASE defined for today

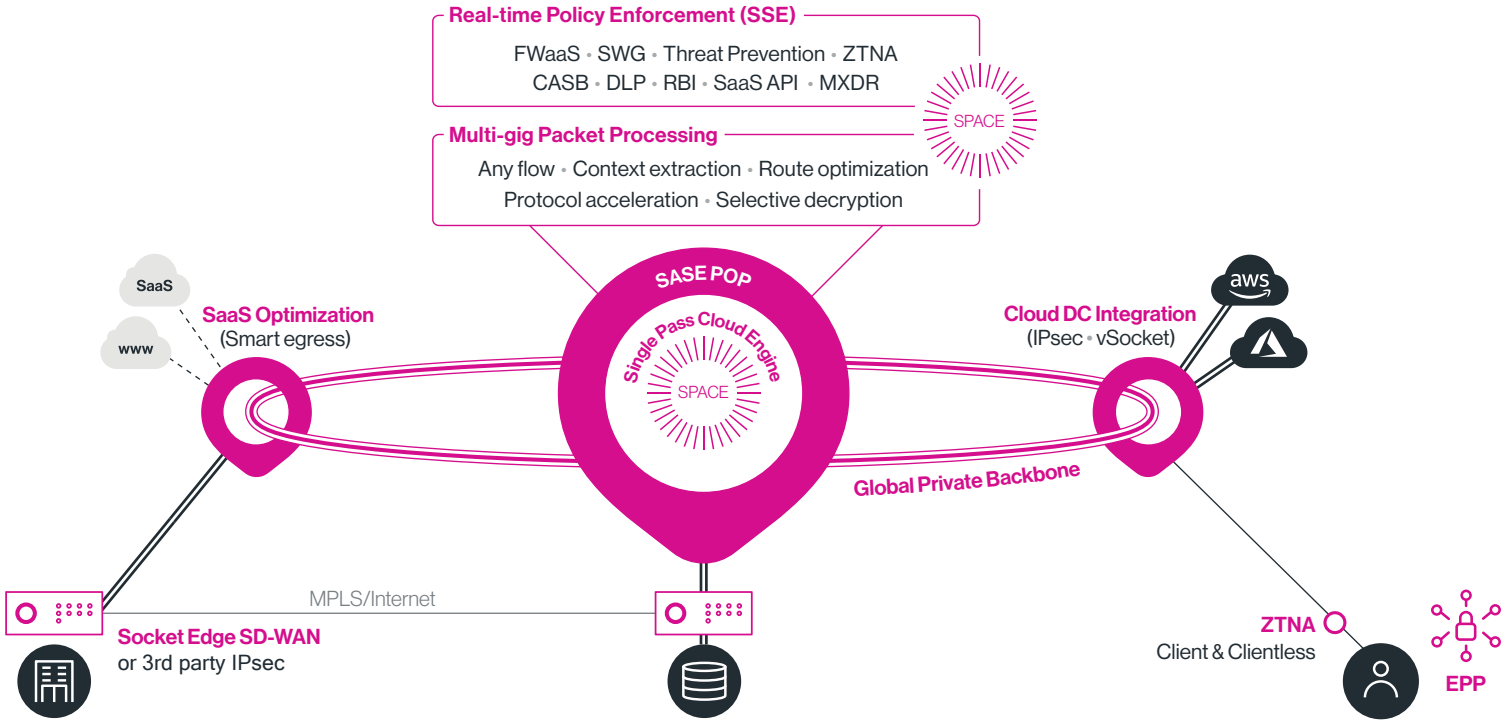
Security as a Service API (SaaS API)

A Security as a Service API facilitates secure and controlled connectivity between organizations and third-party applications. SaaS APIs are critical in managing the interactions with external apps and services that are increasingly integral to business operations. These APIs provide out-of-band visibility, meaning they monitor and manage data exchanges without interfering with the data path, ensuring that the integrity and performance of communications are maintained.

When integrated within a SASE framework, SaaS APIs provide:

1. **Out-of-band management:** SaaS APIs provide a separate control channel that gives IT teams the ability to monitor and manage third-party app interactions without affecting the data flow.
2. **Enhanced security:** By establishing secure API connections, organizations can protect their data and systems from unauthorized access and potential breaches when interacting with third-party services.
3. **Compliance assurance:** SaaS APIs help enforce compliance with industry standards and regulatory requirements by controlling how data is accessed and transferred to external applications.
4. **Streamlined operations:** These APIs allow for the seamless integration of third-party services into business workflows, promoting efficiency and productivity without compromising security.
5. **Real-time visibility and control:** SaaS APIs give IT administrators real-time insights into the data exchange with third-party apps, enabling immediate response to any unusual activity or potential threat.

SASE defined for today



SECTION 3

Market trends that lead to a buying decision

Market trends that lead to a buying decision

Enterprise-grade security needed by all

Summary

Highly rigorous levels of cybersecurity protocols have traditionally been employed only by those companies that had the most to lose—large enterprise banks, healthcare organizations and government agencies that housed petabytes of sensitive data and PII (Personal Identifiable Information).

But according to a report by Verizon[7]

28%

of data breaches occurred in small businesses, while

41%

occurred in mid-sized businesses.

This indicates that mid-sized companies are being targeted more frequently by cybercriminals, making it critical for them to implement robust cybersecurity measures to protect their sensitive information and prevent financial loss.

Buying points to consider

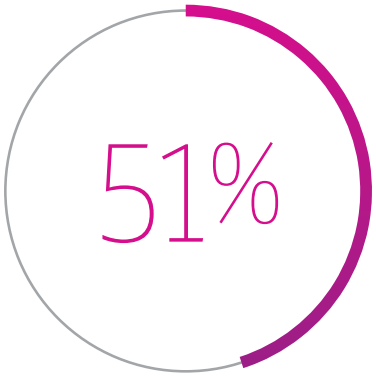
- If your organization has a small IT staff that is already at their capacity and cannot implement and manage a new network and cybersecurity services, consider a managed services provider for SASE.
- If your IT department is more of a service organization and is more adept at moves, adds, changes, hardware management, etc. than enterprise-grade cybersecurity, a converged and synchronized solution may be wiser than trying to make disparate technologies work together.
- Is your organization distributed? If you have multiple office locations and remote workers, you have created network edges that you need to protect.

Market trends that lead to a buying decision

Cloud adoption on the rise

Summary

Organizations of all sizes are moving their data and applications to the cloud, either wholly or through a migration and use of a hybrid cloud strategy.



According to Gartner,[8] **by 2025, 51% of IT spending** on application software, infrastructure software, business process services and system infrastructure markets will shift from traditional solutions to cloud.

Data on the move means it is vulnerable to security threats, requiring protection while on the move and at rest.

Buying points to consider

- Perform an audit of the SaaS or cloud-based applications you are currently using, and which level of data sensitivity is being used by each. There should be security measures in place across the network where data transverses and where it enters and exits your private cloud and edge.
- Consider which apps you have in your own data center (private cloud) versus which apps you have placed in the public cloud (AWS, Azure, Google Cloud, etc.). Do you have a hybrid cloud strategy, or is this just where you have ended up by way of adopting these applications?
- Do you currently employ CASBs to monitor and protect their data as it moves to and from your cloud-based applications? What secure web gateways are in place already to protect web traffic?

Market trends that lead to a buying decision

Workplace flexibility is the new norm

Summary

As more employees access corporate networks and data from their personal devices and home networks, the risk of cyberattacks increases.

According to a recent survey by Gallup[9], the average U.S. worker spends

3.8 days per month working from home.

While many companies have pushed the use of best practices for cybersecurity, such as strong passwords, encrypting data, updating software, avoiding phishing emails and using a VPN, enterprise-grade cybersecurity requires a more robust, enterprise-wide solution set like SASE.

Buying points to consider

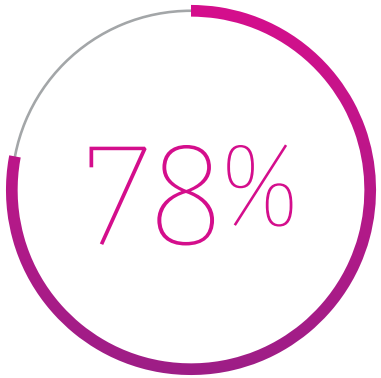
- Calculate the number of remote and mobile workers in your organization and understand their intention for staying remote. Does the company have a long-term security strategy for those employees?
- Legacy VPNs used by edge employees have become inadequate for preventing modern cyberthreats—they often have limited access controls, have trouble scaling and were not designed to handle traffic to and from cloud-based applications. As a result, many organizations are moving away from legacy VPNs and adopting newer, more advanced technologies, such as Perimeter (SDP) solutions, ZTNA solutions and cloud-based security as provided by SASE.
- ZTNA is required when organizations need to provide secure and granular access controls to users and devices, particularly in remote or cloud-based scenarios and when compliance and regulatory requirements need to be met. By implementing ZTNA, organizations can reduce their attack surface, minimize the risk of data breaches and improve their overall security posture.

Market trends that lead to a buying decision

Increase in cyberattacks at the edge

Summary

Cybersecurity Ventures[10] predicts a new ransomware attack will occur every 2 seconds as perpetrators progressively refine their malware payloads. A cyberattack happens every 39 seconds according to the University of Maryland[11]. Phishing and ransomware tend to be the most lucrative for hackers, and no company is completely safe. In fact, the larger the enterprise, the more money is at stake. Some of the largest cybercrimes of 2022 involved companies, such as Twitter, Uber, Nvidia, Rockstar Games and Medibank.



of organizations expect to be impacted by a successful cyberattack within a year.[12]

Buying points to consider

- The COVID-19 pandemic accelerated the shift towards remote work, which has led to an increase in the use of online communication and collaboration tools. This has also created new opportunities for cyber criminals to target individuals and organizations with new and sophisticated attack vectors. Examine what you are doing differently from a cybersecurity standpoint year after year to combat threat frequency.
- Consider your depth of protection: Corporate cyberattacks, particularly phishing, are getting more sophisticated, and are spreading beyond emails to text messages and other forms of personal communication.
- Consider your width of protection: With more users and data existing at the edge, the landscape of protection is increasing with more remote employees accessing the corporate network from not only their laptops, but their own personal devices (known as a Bring Your Own Device [BYOD] approach).

Market trends that lead to a buying decision

Legacy networks are built around physical corporate locations

Summary

Legacy network infrastructure is designed to connect devices within a physical building or campus, with data centers and other critical IT resources located on-premises. The move to the cloud forces a re-architecture of networking and security to support users access to all applications—anytime, anywhere.

Buying points to consider

- Many organizations are modernizing their networks by leveraging SD-WAN and network virtualization technologies, converged with security features to protect the network edge and cloud app access—which creates a unified SASE solution.
- Your network should not be bound by the physical location of data centers, or even office locations. Future strategy planning should focus on distributed network access, with centralized network management and security control, ideally from a single management platform.

Market trends that lead to a buying decision

Backhauled internet traffic slows secure cloud access

Summary

As the volume of internet and cloud-bound traffic increases, it does not make sense to send all traffic through data center firewalls. This is because firewalls are designed to inspect traffic and block malicious traffic from entering the network. However, if all traffic is sent through the data center firewall, it can create a bottleneck that can slow down network performance and cause delays.

Buying points to consider

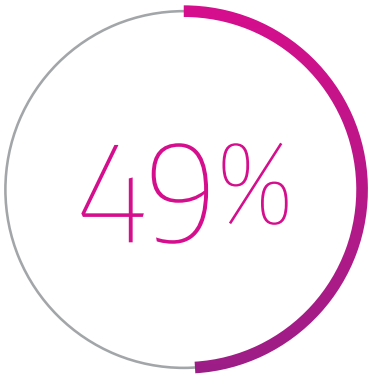
- Adopting a distributed FWaaS architecture allows inspection of traffic closer to the source. This is achieved through the use of cloud-based firewalls that are activated at the network edge. This approach allows organizations to inspect traffic as it enters the network, without the need to send all traffic through the data center firewall.
- Research a ZTNA security model that assumes all traffic is potentially malicious and requires authentication and authorization before access is granted. Threats can be identified and blocked in real time, regardless of the source or destination of the traffic.
- CASB, another component of a converged SASE solution, can help organizations gain more control over cloud-based applications and services, without the need to backhaul all internet traffic. This can help reduce latency and improve network performance, while also improving security by enabling organizations to monitor and control access to cloud-based resources.

Market trends that lead to a buying decision

Disjointed solutions require complex management

Summary

A collection of point solutions for security, piece-mealed and forced to work together, increases the manual workload in the IT department. Often, these solutions are built over time and are subject to the contract expiration dates with individual vendors, meaning that it never actually makes sense to rip and replace everything to employ a new, converged security solution.



Forrester reports that 49% of enterprise businesses say their number one challenge in adopting SD-WAN are the security concerns on how to design, deploy and manage dispersed set of Firewalls, IDS/IPS and other security services to protect all internet traffic.[13]

Buying points to consider

- You need a converged security solution, such as SASE—one that can be coupled with network connectivity and managed in a single portal. The question to consider is how to implement a single system strategically so you save money by leveraging existing investments while mitigating excessive workload on the IT or network administration team.
- SASE can support a migration to a complete converged system, leveraging the investments made in existing contracts and integrating or replacing them as contracts expire. This is made easier if you are working with a single managed services provider who can oversee the process and help you strategically make the transition.
- Examine all existing contracts for security and network services. Often these contracts can be expensive to terminate early, so develop a strategic plan with your SASE provider to migrate to a converged solution.
- Consider adding SSE to your existing SD-WAN to minimize network disruption and honor existing network contracts. SSE delivers all the security features of SASE and when your SD-WAN contract expires it is easy to move to an integrated single vendor SASE solution.

15% in 2023 60% by 2026

By 2026, 60% of new SD-WAN purchases will be part of a single-vendor SASE offering, up from 15% in 2023.[14]

SECTION 4

Enterprise impacts of SASE adoption: Benefits of SASE

Enterprise impacts of SASE adoption: Benefits of SASE

SASE enables organizations to move away from inflexible and disjointed IT architecture—one where disparate security point solutions are forced to operate over outdated and expensive networking technology, such as MPLS or even T1s. SASE instead provides a converged platform delivered as a cloud service, which operates on a flexible SD-WAN network architecture.

Using a managed service provider as a trusted advisor, enterprises can reduce cost and complexity with simple management through a single pane of glass management portal, leverage expertise that can identify and mitigate evolving security threats and create a single point of contact for any and all issue resolution or platform optimization.

Using SASE, enterprises can address new and emerging security trends, such as cloud migration, hybrid cloud environments which pass data between public and private clouds and risks involved with an increasingly mobile workforce that needs protection at the network edge.

In this chapter, we will examine the benefits of enterprises implementing or migrating to a SASE solution, alongside the potential impact it can create.

Enterprise impacts of SASE adoption: Benefits of SASE

Complete visibility and transparency

Traditional web-based security applications are built on legacy architecture, making them blind to non-web traffic and non-human traffic from network devices, IoT and applications, and have limited support for securing access to internal applications. Furthermore, they neglect the performance aspects of the access and rely predominantly on the unpredictable public internet to serve as the application access transport.

SASE offers total traffic visibility and control for the entire enterprise. SASE is able to "see" all traffic across all ports, protocols, sources and destinations, and applies the full range of its access control, threat prevention and data protection capabilities to that traffic.

Built on a private backbone, application access is fully optimized through a predictable and reliable transport that works equally well for application in physical data centers, cloud data centers and the public cloud.

Secure sensitive data

SASE enables full visibility and control of sensitive data, using features like CASB, DLP, SWG, IPS and ZTNA to examine any and all traffic that tries to enter the private network via the edge. The platform can enforce granular policies on data access from corporate and BYOD (bring your own devices), restricts access according to device posture and required level of access and controls data sharing across applications. Enterprises can reduce the risk of sensitive data loss and reputation impact and better comply with regulatory requirements.

Instant deployment of security capabilities

All security elements of the platform are converged into a unified SASE solution from a single vendor and can be deployed with a "flip of a switch" without complex integration, capacity planning and multiple management consoles. All security policies and analytics are managed through a single management portal, known as a single "pane of glass" approach, and are guaranteed to work at the geographies, capacities and resiliency defined by current deployment without requiring further planning.

Enterprise impacts of SASE adoption: Benefits of SASE

Future-proof and zero maintenance security

Forward thinking enterprises should consider a SASE solution for the same reasons that Software as a Service is valuable to them: SASE is self-maintaining, self-evolving and self-healing. Delivered as a cloud service, you can ensure that you are always using the latest version of any application. Working with a single managed provider also removes the grunt work associated with the upkeep of on-premises infrastructure and uses a team of security experts to maintain optimal security posture against emerging threats.

Optimizes global application access

SASE leverages the service provider's private backbone, so to reap the optimal benefits of the solution it is essential to leverage a globally diverse network. For example, Windstream Enterprise partners with Cato Networks to deliver their SASE solution, and Cato has a geographically distributed, SLA-backed network of 80+ Points of Presence (POPs) worldwide, interconnected by multiple tier-1 carriers and Internet exchanges peered with multiple service providers.

Each POP runs the full set of SASE capabilities to ensure minimal latency for connected users and locations. In addition, the backbone provides routing optimization, self-healing capabilities, WAN and Cloud optimization for maximum end-to-end throughput, and full encryption. Unlike typical SSE, this approach has SSE running applications traffic across the backbone ("the middle mile") instead of dropping it to the Internet, to ensure optimized user experience.

Enterprise impacts of SASE adoption: Benefits of SASE

Flexibility and ease of use

SASE can help your IT team simplify their vendor and contract mix while providing the delivery flexibility to meet the unique security needs of each individual enterprise. SASE can be delivered in a simplified, subscription-based approach by location for both its network and security elements, and for ZTNA it is based on the number of end users.

The right managed services provider will offer flexible deployment options, combing the desired security features as requested. The single pane of glass portal enables administrators to easily modify security policies that are immediately updated across all locations and for all end users.

Migrate to single-vendor simplicity

As stated earlier, it is possible to make a migration to single-vendor SASE as your other security point solutions reach their contract expiration dates. Working with a single managed services provider comes with many benefits, including:

- Reduction in the number of overall vendors in your mix, which includes points of contact, for support, trouble resolution and invoicing
- Synchronizing security policies for all locations and end users
- Reduces the need for specialized skills on the IT team and allows members to focus more on revenue-generating strategic innovation rather than tactical tasks
- Single portal for complete visibility and co-management control for all locations and end users

Unified and scalable architecture

Modern cloud-based services are built to scale along with your organization—this can mean expanding or contracting as needed in order to provide the right-sized approach and reduce overprovisioning and overpaying. Managed services providers for SASE should offer an elastic architecture, with a modern DevOps approach that is built on micro-services: small units of loosely coupled code that can be updated individually without taking the entire platform offline for maintenance and upgrades.

SECTION 5

Top use cases for SASE

Top use cases for SASE

On a macro scale, enterprises are all experiencing shifts in the work landscape that include a movement to cloud IT, widespread adoption of a hybrid/remote work strategy and changing WAN requirements due to evolving traffic patterns, such as increased use of web-based AI tools.

SASE broadly addresses these challenges by providing a cloud-based approach that enterprises can easily consume as-a-service, delivering consistency across networking and network security policies at any time and location for workloads.

This chapter will also dive into more specific use cases for SASE, including forward-thinking IT strategies that might cause an enterprise to begin their migration.

1

MPLS migration to SD-WAN

Since its development in the 1990s, MPLS provided a faster network connection option than public internet routing. This advantage was particularly beneficial for large businesses that needed to boost traffic speed across geographically dispersed infrastructures. Much has changed since then, with companies leaning on SD-WAN for secure networking to multi-cloud environments as opposed to the hub and spoke approach offered by MPLS.

By connecting its gateway network with a global private backbone, SASE enables organizations to swiftly shift from expensive and capacity-limited MPLS networks to a more cost-effective alternative that harnesses high-capacity internet connections. This alternative provides or better performance and reliability to MPLS, but at a more affordable price point. Unlike the deployment of MPLS, which can take several weeks or months, SASE installation at each location typically takes just a few days or even hours when deployed over existing internet connections. Once integrated, SASE boosts operational capacity, enhances resilience, optimizes performance and maximizes throughput for both on-premises and cloud-based applications.

Top use cases for SASE

2

Optimized global connectivity to support growth and expansion

Enterprises that are either opening or acquiring new locations nationwide can suffer from high-latency and network inconsistency across their dispersed locations as they inherit legacy networking technology.

SASE can deliver a better user experience for both on-premises and cloud applications by leveraging the MSP's global network of gateways connected by a private backbone of SLA-backed network providers and built-in WAN and cloud optimization. This convergence of network security and global network connectivity provides a secure, low-latency experience that connecting over the public internet or MPLS cannot provide.

3

Secure branch internet access

SASE can improve security at branch offices and the remote network edge, supporting companies that are growing both in the number of physical branch offices and remote and hybrid employees at home. Branch office and remote home WAN security is greatly improved and simplified with SASE.

By connecting to the SASE gateway, all traffic is safeguarded, including both Internet-bound and WAN traffic, with enterprise-grade cloud-based security services. The hassle of backhauling Internet traffic to a datacenter or managing different security appliances and solutions for each branch is eliminated. SASE ensures the synchronization of all security policies and updates, which are implemented in the cloud and immediately applied to all locations and users.

Top use cases for SASE

4

Cloud acceleration and control

With more applications moving to the cloud—Gartner predicts more than half of IT spending will shift to cloud by 2025[8]—management, inspection and control of the traffic going to and from applications in the public cloud is paramount. Supporting cloud traffic acceleration is bolstered by SASE, which directs traffic from all network edges over its global private backbone to the closest gateway to the cloud data centers.

Major cloud providers have the same data center footprint as SASE gateways, ensuring minimal latency between the SASE framework and these providers. Optimizing cloud application access is as simple as adding a single application-level rule to specify where cloud application traffic should egress the SASE cloud.

5

Remote access security and optimization

Enterprise grade security features are no longer limited to just large office locations—even mobile and remote users can access the same levels of security as those working in an office. No longer are mobile users treated as second-class citizens of the network and security infrastructure.

Rather than authenticating users to the entire network, SASE uses ZTNA to limit users to the resources they're allowed to see. Using simple mobile clients, the SASE security stack protects them against threats everywhere and enforces application access control. ZTNA achieves this by treating all network traffic as a threat, thoroughly inspecting and validating anything that crosses the network edge.

Top use cases for SASE

6

VPN replacement for work-from-home employees

We touched earlier on the IT trend and challenge of supporting the increasing number of remote employees. Traditionally, these employees have not had the same level of security on their network connections to the corporate network.

With SASE, all employees working at home have the same scalable cloud-native infrastructure, management and security policies on their site-to-site and cloud connections. Using self-service provisioning of client software, the SASE platform provides a global private backbone that optimizes home traffic of thousands of users to all applications and continuously inspects traffic for threats and access control. The result is that all home users get the same fast, secure network and application experience—and the same productivity—they had at the office.

7

Simplified management

Enterprises commonly utilize a large number of SaaS applications and software, often resulting in thousands of individual logins and management platforms. While it is not possible to eliminate these numerous apps, SASE aims to consolidate them by offering a single management console that provides insight and transparency into all security and networking apps. This approach enables access to richer data context, eliminates the need to switch between different consoles to gather important information and streamlines troubleshooting of network and security issues.

As a result, SASE provides enhanced visibility into network and security issues, simplified optimization and troubleshooting and ensures consistent policies across WAN, mobile and home deployments. Additionally, certain solutions offer real-time analytics, which provide valuable insight into network issues like packet loss, jitter and latency, thereby aiding IT in configuring the network for the best possible user experience.

Top use cases for SASE

8

Consistent security policy enforcement

For enterprises that store data at the edge or employ a hybrid cloud strategy where data is transferred between public and private clouds, SASE can help secure that data by connecting all edges on a single security platform. All traffic between edge and cloud is inspected, and the software can implement your predetermined corporate policies for threat and data protection to any and all traffic across the network.

9

Reduction of total attack surface

An attack surface refers to the total number of points of vulnerability in a system or network that an attacker can exploit to gain unauthorized access or cause damage. It encompasses all the entry points, hardware devices, software applications, network protocols and user accounts that are connected to or part of the system. The larger the attack surface, the greater the potential for vulnerabilities and the easier it is for attackers to find a weakness to exploit.

SASE implements ZTNA, ensuring users only have access to authorized applications. All traffic is continuously monitored for anomalies, threats, attacks and sensitive data loss. By minimizing the attack surface, organizations can better protect their network assets and reduce the risk of data breaches, downtime and other security incidents.

Top use cases for SASE

10

Improved security posture

To ensure a robust security posture, organizations must regularly assess their security policies and identify potential gaps or weaknesses that may expose them to cyberthreats. This can be done through regular security audits and risk assessments, as well as ongoing monitoring and analysis of network activity. Companies are focused on the product or service they provide so this assessment is not always feasible by internal IT teams. Implementing SASE through a managed services provider ensures that you can remain focused on your business and remove the burden of manually mitigating emerging threats while remaining confident that your cloud, network and edge are protected.

11

Lower operational overhead

With skills gaps and recruiting issues continuing to affect the labor market, especially in the IT space, it is becoming even more critical for enterprises to properly allocate personnel resources in order to lower operational overhead. A managed SASE provider can fully manage, monitor and maintain security software and devices, so IT does not need to constantly update, patch and scale appliances. The use of SaaS-based security applications can help create cost efficiencies, eliminating updates, patching and scaling associated with on-premises software.

Top use cases for SASE

Why MPLS will not cut it anymore

Traditional MPLS hub-and-spoke networks and their associated security architecture were built for a set purpose, an ideal way for organizations to run multiple business-critical applications from data centers.

In today's environment, the "data center-centric" approach is showing its limitations.

Geography
With VPN connections into the data center, these networks are not equipped to serve a remote workforce that's more geographically distributed.

Security
Traditional network security models were designed to accommodate employee devices and systems that were located within a physical perimeter, assumptions that no longer hold true.

Traffic
These networks also are not built to deal with the increased volume of traffic that traverses public, private, hybrid and multi-cloud environments en route to its destination.

Flow
Constantly routing traffic to and from data centers through a centralized security stack and ultimately out to the Internet creates network congestion.

Speed
All these factors and the resulting congestion combine to hinder application performance which affects end users' experiences and productivity. Many MPLS networks were deployed using T1s which is insufficient bandwidth for the many apps modern networks must support.

Resiliency
Many MPLS networks are single threaded as it was cost prohibitive to add a second connection, resulting in outages. Most organizations desire 100% uptime for mission-critical apps.

Forward thinking enterprises are turning to SD-WAN for flexibility to utilize a combination of public and private networks, reduce costs by utilizing more affordable broadband and wireless connections and provide greater security than MPLS networks, with advanced security features, such as encryption, firewalls and intrusion detection and prevention systems as part of a converged SASE solution.

SECTION 6

Security considerations and trends: Why now?

Security considerations and trends: Why now?

Year after year, cyberthreats are becoming more sophisticated, with the level of advancement of each kind of threat continuing to evolve. The exception here is generative AI, whose increased use has been proliferated by consumer-accessible tools, such as ChatGPT and DALL-E. This means that bad actors have another means to penetrate a company network, but AI can also be used for good by training AI models to detect and deter cyberattacks across a company's network environment.

This constant evolution requires company stakeholders to not only be educated on the latest security trends, but also have access to cybersecurity and breach mitigation technologies that can adapt as fast or faster to new security challenges.

This chapter will examine the top cybersecurity considerations as outlined by research firm Gartner,[15] as well as how a SASE approach from a managed services provider can help solve those challenges.

1

AI used for both cybersecurity and hacking

While AI can be a powerful tool for cybersecurity, it can also be used for malicious purposes to hack into systems, using some of the following approaches:

- **Password guessing:** AI can be used to create intelligent password guessing algorithms that can quickly and accurately guess passwords, especially weak passwords. These algorithms can be trained using data obtained from previous data breaches or through social engineering techniques.
- **Social engineering:** AI can be used to generate convincing phishing emails or messages by analyzing social media data and creating messages that appear to be from trusted sources.
- **Malware development:** AI can be used to create intelligent malware that can evade traditional security measures by analyzing security systems and adapting its behavior accordingly.
- **Vulnerability exploitation:** AI can be used to scan systems and identify vulnerabilities that can be exploited to gain unauthorized access.
- **Automated attacks:** AI can be used to automate attacks by identifying vulnerable targets and launching attacks without human intervention.

Security considerations and trends: Why now?

Solving the challenge with SASE

AI is also being implemented into security components within a SASE solution, such as ZTNA, CASB and FWaaS to further enhance threat detection and mitigation across the corporate network and the edge.

- **Threat detection:** AI can detect threats by analyzing large amounts of data and identifying patterns that indicate an attack. Machine learning algorithms can also be trained to recognize patterns of malicious behavior and alert security personnel.
- **Fraud detection:** AI can be used to detect fraud by analyzing patterns in financial data and identifying suspicious transactions.
- **User authentication:** AI can be used for user authentication by analyzing user behavior and identifying anomalies that may indicate unauthorized access.
- **Malware detection:** AI can detect malware by analyzing code and behavior patterns and flag any anomalies.
- **Vulnerability management:** AI can help identify and prioritize vulnerabilities in a network or system by analyzing data and identifying potential weaknesses.
- **Incident response:** AI can be used to automate incident response by analyzing data and taking action to mitigate the impact of a security incident.

2

AI used for cybersecurity and application protection

Every application used by the business is potentially vulnerable to hacking, identity theft and zero-day attacks—and when they reside in the public cloud they have even more threat exposure. Even though apps are developed with security in mind, a secure architecture and strong verification of data inputs, additional measures should be taken at the company network level to protect the traffic to and from those applications.

Solving the challenge with SASE

Within a SASE framework, CASB and SWGs combine to protect cloud applications, by monitoring data uploads and downloads, enforcing access controls and detecting and blocking malicious activity. They also help prevent data loss by applying policies that prevent sensitive data from being accessed or shared outside the organization. Additionally, CASB can help organizations comply with regulatory requirements by providing audit logs and reports that track cloud activity.

Security considerations and trends: Why now?

3

Mobile and edge security

This refers to increased usage of mobile phones for business, but also includes any device that accesses the company network outside of a physical location, such as a laptop, tablet, wearable, etc. These devices make up the "edge"—the mobile extension of the network that has no boundaries just proves to be ever more challenging to protect in the same manners as on-premises devices. As edges expand, the number of attacks is expected to increase, and opportunistic malicious actors will continue to exploit vulnerabilities in e-commerce, banking services and online booking to their advantage whenever possible.

Solving the challenge with SASE

SASE protects devices at the edge through a combination of network security and application security measures. For network security, SASE can provide secure connectivity to the corporate network through a secure private connection. These services can encrypt mobile device traffic and prevent unauthorized access to corporate resources. For application security, SASE can inspect mobile device traffic for malicious content and protect against phishing attacks, malware and other types of cyberthreats. SASE can also enforce policies that restrict access to certain applications or data based on user identity, device type and location.

4

Protection in the Internet of Things (IoT)

IoT does not just apply to home appliances—it encompasses any kind of device connected to the network at the edge. This could include tablets, company-issued laptops or devices in machinery and vehicles. As an example, more cars are being manufactured with elements that connect to the Internet—safety airbags, climate control and other essential functions included.

Solving the challenge with SASE

SASE can protect IoT devices through network segmentation, which can isolate devices and restrict access to unauthorized users or devices. SASE can also enforce policies that control access to IoT devices and data based on user identity, device type and location. Additionally, SASE can provide secure connectivity for IoT devices through a secure private connection which can encrypt traffic and prevent unauthorized access. Furthermore, SASE can inspect traffic from IoT devices for malicious content and protect against malware, phishing and other types of cyberattacks.

Security considerations and trends: Why now?

5

Rise in remote employees

The rise of remote work has resulted in a loss of control for companies over their employees' adherence to safe data practices. This has created an opportunity for cybercriminals, phishers and social engineers to exploit the situation, employing sophisticated attack methods to compromise company networks.

Solving the challenge with SASE

To safeguard this sector, the primary measures for protection are secure authentication management and authorized access to company data. SASE can authenticate users, devices and applications before granting access to sensitive data. SASE can enforce access control policies that restrict access to company resources based on user identity, device type and location. These policies can also be customized to grant different levels of access to different users based on their role within the organization. Additionally, SASE can provide secure connectivity for remote users and IoT devices through a secure private connection.

6

Cyber insurance

Cyber insurance provides financial protection to organizations in the event of a cyber incident, including data breaches, network attacks, cyber extortion and other types of cybercrime that can result in financial loss or damage to an organization's reputation. Cyber insurance policies typically cover costs related to the investigation, recovery and notification of affected parties in the event of a data breach. They can also cover losses resulting from business interruption, theft of intellectual property and liability for damages to third parties.

Cyber insurance in tandem with SASE

SASE can complement cyber insurance policies by offering a robust security infrastructure that can prevent and detect cyberthreats before they cause damage. By leveraging cloud-based security services, SASE can provide continuous monitoring and real-time threat detection that can mitigate the risk of a cyberattack.

SASE can also provide a detailed audit trail of user activity, which can assist in the event of a cyber insurance claim. This information can help insurers determine the cause and scope of a cyber incident, allowing for more efficient claim processing. Furthermore, SASE can enforce security policies that are in line with cyber insurance requirements, such as data encryption, secure authentication and access control.

Security considerations and trends: Why now?

7

ZTNA—the fastest growing form of network security

Gartner believes that ZTNA is the fastest-growing form of network security, which will grow by 31% in 2023 and completely replace VPNs by 2025[16]. Unlike VPNs, which provide access to the entire network, ZTNA verifies the user's identity and device before granting access to specific applications or services. This approach minimizes the attack surface and reduces the risk of lateral movement within the network. ZTNA can also provide granular access control, allowing organizations to enforce policies that restrict access based on user identity, device type and location.

ZTNA is a critical component of SASE

ZTNA can be implemented through a SASE platform, establishing a more secure and flexible access model that can accommodate the needs of mobile workforces and remote users. This approach can enhance security posture while reducing the complexity and cost associated with VPNs.

8

Attack detection is now absolutely necessary

With data breaches of cloud-based applications and network gateways to the cloud resulting in millions of dollars in losses, spending on CASBs and detection services is predicted to increase to nearly $7 billion in the coming years, according to Gartner[17].

Solving the challenge with SASE

CASBs, as part of a converged SASE platform, monitor user activity in real-time to detect anomalous behavior or suspicious activity that may indicate a cyberattack. CASB can also enforce security policies that restrict access to sensitive data and applications based on user identity, device type and location.

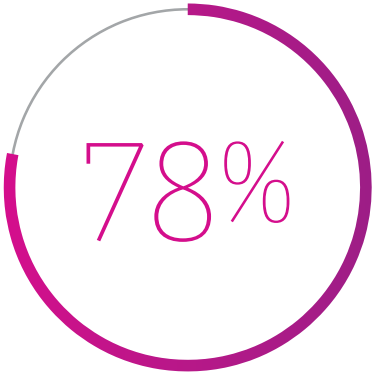
Additionally, CASB can detect and prevent data exfiltration by monitoring and controlling the flow of data between cloud services and users. CASB can also provide threat intelligence that can detect and prevent known malware and phishing attacks.

Security considerations and trends: Why now?

9

Outsourcing cybersecurity

Outsourcing cybersecurity has become an increasingly popular trend in recent years as companies seek to enhance their security posture while also reducing costs. One trend that has emerged is the use of managed service providers (MSPs) who offer a range of cybersecurity services including threat intelligence, incident response and security assessments. Another trend is the use of cloud-based security solutions which offer the advantage of scalability and flexibility.



of organizations expect to be impacted by a cyberattack within a year.[18]

Why use an MSP?

When it comes to outsourcing a SASE solution, forward thinking enterprise IT leaders want a partner, not a vendor. MSPs can provide ongoing monitoring and management of the SASE solution to ensure it remains up-to-date and effective in protecting against emerging threats. MSPs can work closely with clients to identify the most critical applications and data, and then design a SASE solution that provides the appropriate level of security and performance. The SASE provider should act as an extension of your IT team, working closely to address the unique security needs that may be unique to your industry.

Extend the promise of SASE with MDR

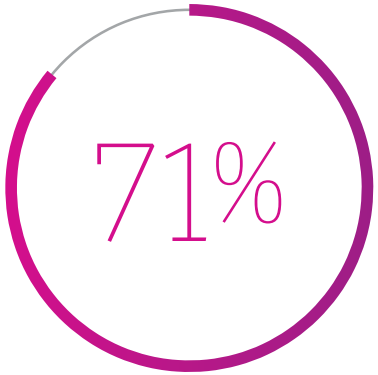
Many companies do not have the manpower or skills to hire cybersecurity staff. MDR uses AI to detect and automated responses to make customers aware of incidents.

SECTION 7

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

When it comes to large-scale IT purchases impacting the entire organization, rarely does the decision lie just with the IT department. Enterprise technology decisions and buying processes are driven by a team purchasing process involving many stakeholders from departments across the company, each weighing in at critical stages. However, not all companies have a pre-defined process for large procurements and purchases.



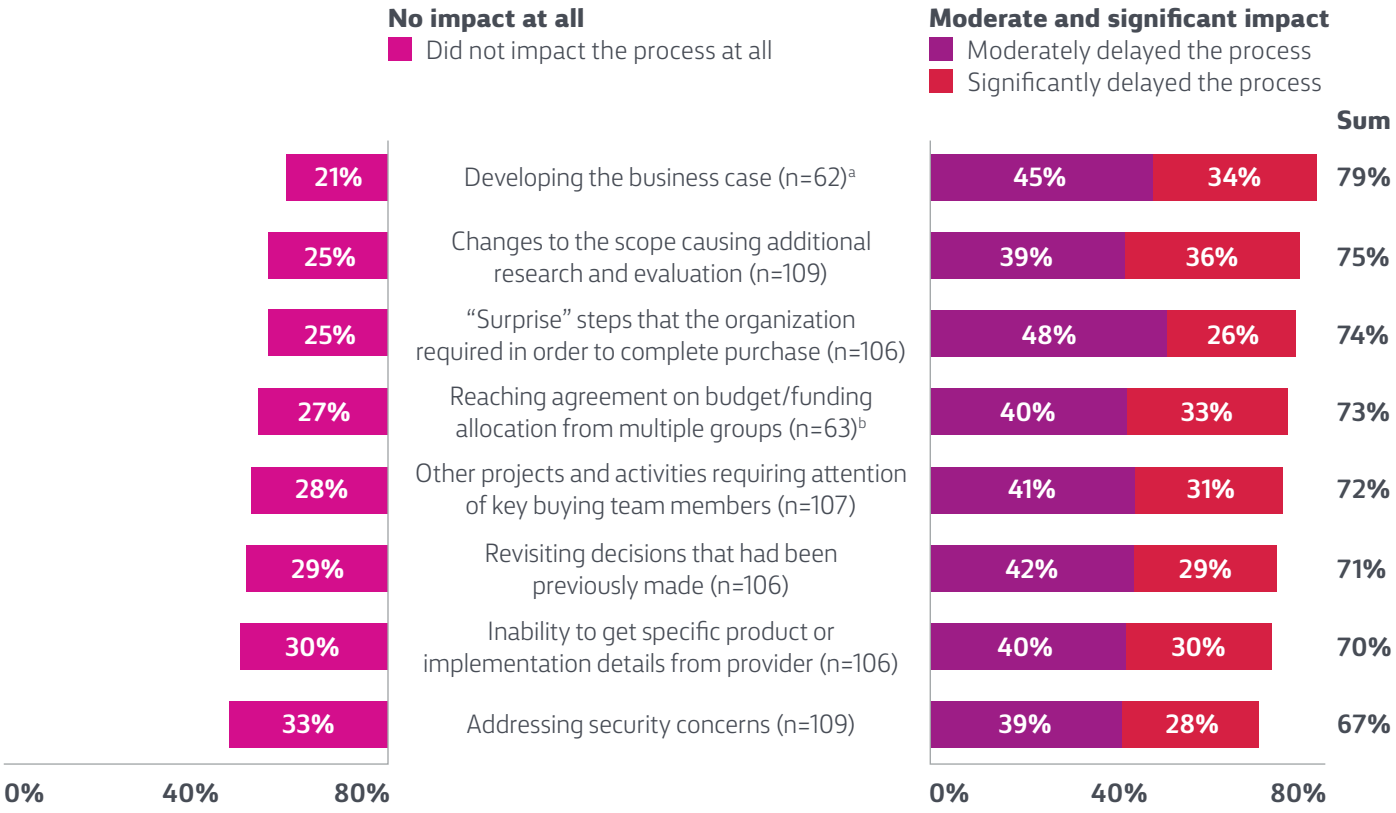
Research from Gartner[19] shows that nearly three-quarters (71%) of companies surveyed reported delays in the buying effort because of "surprise steps" and generally being unaware of the required steps in the purchasing process.

In this section

We will outline a high-level framework specific to the purchasing process for a converged SASE solution that you can apply to the specific needs or processes of your organization. We will also look at the individual roles within the purchasing team, where they sit in the decision process and key considerations and questions for each, specific to the purchase.

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

Delay causes in the purchase process[20]



n varies; Based on excluding "does not apply"

Q: How, if at all, did the following activities impact the length of time needed to complete the purchase?

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

Buyer roles: Key considerations checklist by functional team member

Chief Information Officer

Role responsibility

The primary source of sponsorship for SASE initiatives is typically the CIO, who has the authority to break down organizational barriers and facilitate the implementation of a SASE architecture. The driving force behind many SASE projects is the goal of simplifying policy management and enforcement, as well as enhancing the overall security posture of the organization. These initiatives may be spearheaded by networking and branch office transformation efforts, or by security concerns related to supporting a hybrid workforce. As SASE solutions encompass both network and security capabilities, it is advisable to establish a joint team comprising members from both networking and security departments to develop a comprehensive strategic roadmap for enterprise adoption of SASE.

Key questions to ask

- What security breaches or close calls have we encountered in the last year and what were/could have been the reputational or financial consequences?
- What is our benchmark for measuring improvement in threat detection and deterrence post-installation?
- Can you examine our current IT landscape and determine the best path forward when it comes to migrating to a SASE solution vs. a full rip and replace of all network and security contracts and software?
- Can you help me identify the ROI easily so I can brief the board?
- How will the SaaS solution integrate with our existing security infrastructure and IT environment? Is it compatible with our current operating systems and endpoint types?
- As SASE is continuing to evolve and improve, does the solution go beyond the five traditional components outlaid by Gartner to include DLP, IPS, NGAM, MDR, RBI and SaaS API?

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

Chief Information Security Officer

Role responsibility

The CISO/CSO is all about data security and breach prevention and reduction and elimination of threats. The CISO focuses on creating and maintaining a safe information environment while educating the staff on the same. The CISO is typically a senior executive who reports to the CIO or the Chief Executive Officer (CEO) and is responsible for managing and directing the organization's information security program, so this is one of the most critical roles in contributing to the buying process of any cybersecurity solution.

Key questions to ask

- What is the range of security services provided by the SASE solution? Does it include FWaaS, SWG, ZTNA and CASB, as well as SD-WAN?
- What is the scalability of the SASE solution? Can it easily accommodate changes in the organization's network and security requirements, as well as increased traffic volume?
- Does the SASE solution support multi-cloud environments? Can it integrate with different cloud providers and workloads, such as my existing SaaS and IaaS tools?
- What are the performance and latency guarantees of the SASE solution? How does it ensure consistent and reliable network connectivity, even in challenging network conditions or high-traffic situations?
- How does the SASE solution ensure compliance with regulatory requirements, such as GDPR, HIPAA and PCI DSS? Does it provide compliance reporting and auditing features?
- What is the level of visibility and control provided by the SASE solution? Can it provide granular visibility into network traffic, user behavior and application usage? Can it enforce policy-based access control and apply adaptive security measures based on user and device context?

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

IT Leaders, VP, Director and Manager

Role responsibility

In the context of purchasing a technology platform, IT leader roles like IT VP, Director or Manager, which may also include the Network Engineers, are the boots on the ground agents that can help kickoff the purchasing process. These roles are often first to expose an issue with existing technology, be on the forefront of researching new trends and are directly exposed to the effects of poor platform performance and employee feedback. These roles are often tasked with doing the initial research for a new technology purchase, which may include sourcing/vetting vendors, attending industry events and conferences and bringing initial options to the table.

Key questions to ask

- What is the pricing structure? Does it offer a subscription-based model, a one-time license fee, or other pricing options? What are the ongoing maintenance and support costs? Do we have good, better, best options?
- What is the level of customization and integration? Can it be easily customized to meet the organization's specific needs and integrate with other systems and applications?
- What is the level of support, training and service provided?
- What is the level of user adoption and training required? Can it provide user-friendly interfaces and intuitive workflows? Does it offer training and support materials to help users become proficient in using the technology?
- What are the key differentiators between this SASE platform and the others I'm reading about?
- Do you have customer evidence to support the success that I can deliver to my buying team?

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

Infrastructure and Operations Leader

Role responsibility

I&O leaders are broadly responsible for the administration and management of technology, information and data. These teams manage a variety of elements including computers, servers, processes, networking, storage, data, software, security and cloud-based services. From a buying perspective, I&O leaders are concerned with the solution's impact on operational priorities, such as availability, reliability, scalability, flexibility, cost optimization and user experience.

Key questions to ask

- What are the unique requirements of both the network and security teams that we can gather to ensure we have cohesiveness in the solution and a network that is both secure and well-performing?
- How can we ensure that the solution will not need continual reconfiguring and redesign—can we future-proof elements now to avoid changes down the road?
- How can we bring together both the network and security teams within the company to align on goals and ensure they're being met throughout the buying journey—from strategy, design, implementation and operations?
- As the likely responsible party for operations, how can you as the single provider MSP assist me in augmenting the capabilities of our internal teams so that we're not overburdened in any one area.

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

Chief Financial Officer

Role responsibility

The CFO wants to ensure that the enterprise runs in the most cost-effective manner. They are responsible for making finance easy to understand for both managers and their board. The CFO likes to demonstrate their financial, technical and clinical acumen. Collaboration, strategy and quality figure heavily with CFOs in all vertical industries.

Key questions to ask

- Can you demonstrate the ROI of a SASE implementation?
- How long do you predict it will take to realize a ROI on this investment?
- Does this SASE solution allow for a migration to full implementation, allowing us to leverage previous investments in technology that is still tied to contracts?
- What customers do you already have that look similar to our enterprise and what cost savings or efficiencies have they realized already?

Chief Experience Officer

Role responsibility

The CXO is responsible for making sure every aspect of the enterprise and the products and services it delivers consistently meets and/or exceeds the expectations of its customers, employees and partners. The CXO is involved in loyalty drivers and associated analytics while creating an environment that promotes positive experience both inside and outside of the company.

Key questions to ask

- How does SASE impact the KPIs that our enterprise uses as benchmarks for success?
- How can the implementation of SASE contribute to a positive experience for our customers and is there a way to quantify that?
- How can your technology help identify and act on opportunities to improve?
- How does SASE tie in and protect the methods we use to contact customers and resolve issues, such as the contact center platform, CRM and even social media platforms?

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

Chief Procurement Officer

Role responsibility

The CPO heads up buying groups and processes for the enterprise, including all vendor relationships. This role has traditionally been supply chain-driven, but is evolving quickly as more emphasis is put on digital innovation, sustainability/ESG, business insights generation and partnerships. The CPO plays a critical role in ensuring the organization has access to the products and services it needs to operate effectively, efficiently and in compliance with applicable laws and regulations. This group will ultimately enable the purchase of the SASE platform, with approval from the rest of the C-suite.

Key questions

- Can you clearly outline the buying process for this platform, including milestones and prerequisite technologies needed?
- What is the level of support and service provided for the SASE platform? Does it offer 24/7 customer support, professional services to help with implementation and integration and ongoing maintenance and upgrades?
- What is the level of scalability and flexibility provided? Can it accommodate changes in the organization's requirements and adapt to new technologies and business processes?
- Why not buy from the lowest bidder?
- Do you offer innovative contracting agreements, such as discounts for scale or agreement length?

Team purchasing for enterprise network connectivity and security: Trends, roles and buying process

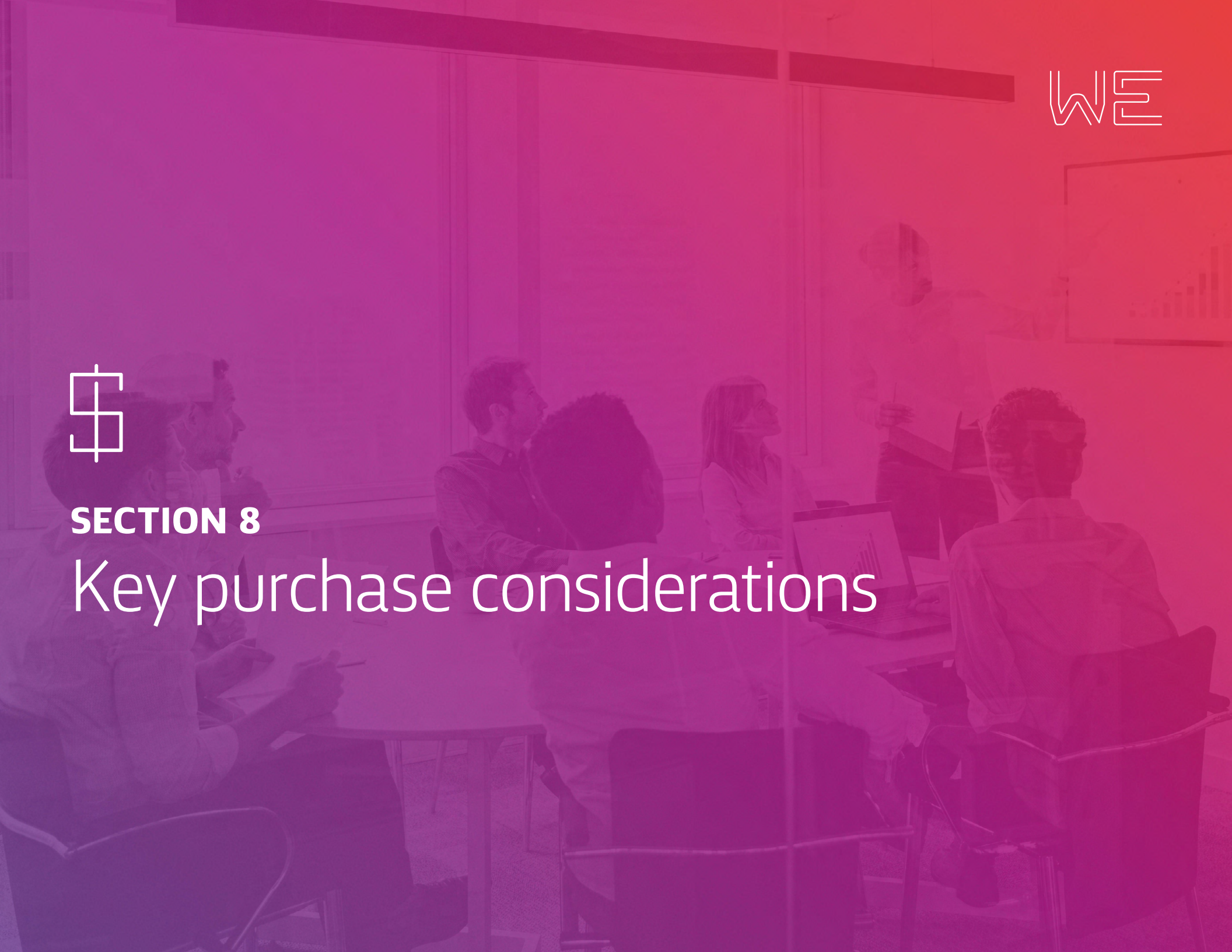
VP Network Operations/Network Infrastructure

Role responsibility

The VP of Network Operations typically reports to the CIO or CTO and is responsible for managing an organization's network infrastructure, ensuring it is secure, reliable and efficient. This role is a critical contributor to the SASE purchasing process as it will require a migration to SD-WAN from the enterprise's legacy network delivery method. While this person will be interested in the solution as a whole, most of the focus will be on the network component.

Key questions

- Does it meet our organization's network requirements and business goals, such as improved network performance, increased security and reduced costs? What quantifiable data can we show to back it up?
- What are the disaster recovery and business continuity capabilities?
- What is the level of customization and integration provided by the SD-WAN solution? Can it be easily customized to meet our specific needs and integrate with other systems and applications?
- What is the level of support and service provided? Do you offer 24/7 customer support, professional services to help with implementation and integration and ongoing maintenance and upgrades?
- What is the level of scalability and flexibility? Can it accommodate changes in the organization's requirements and adapt to new technologies and business processes?
- What is the level of network visibility and control? Can it provide granular visibility into network traffic, user behavior and application usage? Can it enforce policy-based access control and apply adaptive security measures based on user and device context?



SECTION 8

Key purchase considerations

Key purchase considerations

1

Needs based on organization size

No security platform is one size fits all, but the biggest determining factors for the scale, complexity and adaptability of the platform is the size of your organization, the amount of network traffic used and the level of security of the data being transferred. It is important for organizations to understand their specific needs and evaluate the different options available in order to make an informed decision when selecting a SASE platform. This article will provide an overview of the key buying considerations for a SASE platform, including organization size, scalability, cost-effectiveness and more.

Small/Medium >100 employees	**Mid-market** 100-999 employees Multiple offices	**Enterprise** +1,000 employees Multiple regions/countries
+ Simple purchasing process—online sales support + Onboarding/ implementation support without additional pro services packages + Cost-accessible packages available + Assistance with consolidation of existing platforms, migration plans, API integrations with existing SaaS tools + Cost-savings angle, without compromising on features or nickel and diming + Zero-touch provisioning	+ Full featured SASE suite, including comprehensive SD-WAN solution + Ability to implement individual elements of the SASE solution in order to maximize existing vendor contracts + Secure connectivity options for cloud-based services to support remote employees + Robust professional services offerings + Thorough onboarding, implementation and training protocols	+ Real-time access to account management functions, plus visibility and control over your network, all in one portal + Advisory and deployment services from the SASE provider + Full customization capabilities + Enterprise-grade security features in each element of SASE

Key purchase considerations

2

SLAs

Network uptime can make or break a business, as it affects customer satisfaction and the ability to deliver services. With SASE, businesses can ensure that their customers have access to the services they need. SASE provides a secure connection between users and applications, ensuring that data is always available when needed. Uptime is often over-promised and under-delivered, so it is important to have a conversation with potential providers around SLAs offered.

Here are some talking points to bring up:

How do you ensure my network stays online at all times?

- No network connection is 100% safe from downtime, so the best way to ensure connectivity is to set up network redundancy and immediate failover using SD-WAN with multiple access connections in an active/active configuration. In an SD-WAN configuration, networking hardware is decoupled from the physical control layer, enabling enterprises to enable multiple connections through low-cost, readily available broadband Internet and wireless internet for remote locations.
- SD-WAN simplifies WAN operation and management by combining functions at the edge, ensuring performance and availability for cloud-based workloads. Ask your provider how they are able to leverage SD-WAN for network redundancy. Potential red flags should be if they are still limited to outdated MPLS technology, or do not offer any kind of network connectivity or professional services around networking at all.

What is your uptime percentage? How many "nines?"

You will often see network and platform uptime calculated and marketed in terms of how many nines (i.e., 99.999%) the company can guarantee their customers as part of their SLA. This calculation is also known as availability.

Here are a few considerations and questions you should ask regarding uptime:

- While most companies will market themselves as four nines (99.99%) and above, even 3 nines does not equate to much downtime at all when spread across the year (99.9% = 52 minutes and 36 seconds of downtime per year).
- Remember that an uptime SLA is a guarantee that you will be credited for any downtime that exceeds the amount stated in the SLA—not that the uptime number will be achieved.
- Ask your potential provider if the uptime SLA includes maintenance windows—there could be a clause in the SLA excluding scheduled maintenance.
- When in doubt, consider a provider with 100% uptime SLAs, such as Windstream Enterprise, who backs the uptime with diverse, redundant connections at each location with automatic failover configurations.
- For the most critical locations deploying two SD-WAN edge devices in parallel delivers a true High Availability configuration.

Key purchase considerations

3

SASE application management

Control over aspects of the SASE solution is available via a portal, which is unique to each software vendor you will analyze in the buying process. Oftentimes, the UI and functionality of these portals are not widely marketed publicly, making it even more important to get a thorough demo and understanding of its usability, as both users and admins will be spending a considerable amount of time there.

Here are several considerations when assessing a SASE management portal:

- Although they commonly share the same back end, portals will differ slightly between end user and admin profiles, so it is important to be shown the unique aspects of both.
- Does the portal include or can it iframe in network performance for a singular view? This would include network latency, packet loss and jitter by site, plus easy-to-customize reports.
- Does the mobile app allow user management functions natively? If so, does it have full admin parity with the web-based portal?
- Can reports be adjusted, automated and customized within the analytics section? Are you able to build customized dashboards per user?
- Are all SASE functions (FWaaS, CASB, ZTNA, SWG, SD-WAN) accessible from one portal? Or are there different portals for each point solution?
- Which languages does the portal support? Will international employees easily be able to use the portal?

Key purchase considerations

4

How much does SASE cost?

The cost of a SASE solution is one of the most important factors in the decision process, especially when forecasting how it will impact budget and ROI during annual planning cycles. Determining overall monthly cost is not always easy, unfortunately. Because of the convergence of the five security tools into a single solution, including the network—which can function as a metered service—you may find that costs differ greatly between vendors depending on how the initial solution is designed by each vendor.

Other cost savings are achieved by eliminating the need for IT staff to manage and patch on-premises equipment as everything is in the cloud. The online management portal also make the monitoring and troubleshooting a much easier process, and with the right MSP, any issues will be proactively resolved on your behalf.

This section will cover basic pricing elements of a SASE solution and should be used to guide pricing conversations with your provider.

Elements of cost

SASE price model—all costs fixed rate MRC

- Base Package includes SD-WAN, SWG and FWaaS—priced per site
- ZTNA priced per user
- Additional components to protect all users and are priced per site: and they protect all users: CASB, Threat Prevention, DLP, RBI, SaaS API, EPP and MXDR

What else do I need to make SASE work?

- Base package includes an SD-WAN socket for each location
- An Internet access connection for the socket—bring your own or let us provide
- Suggest second access connection for active/active configuration to maximize uptime

Non-tangible benefits that can impact cost

SASE carries with it benefits and implications that cannot be assigned as a line item. Be sure to address these elements with your provider when assessing how a new system will impact your organization, both from cost and culture standpoints.

Change management implications

Large-scale changes to a technology that every employee and patient touches can cause experience and process issues if not implemented properly, so having the conversation with your SASE provider around their strategy for facilitating customer change is essential. 47% of organizations that integrate change management are more likely to meet their objectives than the other 30% that did not incorporate it[21].

This strategy should include:

- Access to onsite and virtual training on the platform
- An internal communication plan to set expectations and deliver updates on the new rollout
- Measurement of user adoption and platform use
- Phased deployment according to unique business needs

Key purchase considerations

Extension of IT team/FTE management
The SASE provider should become an extension of your IT team, and they should be actively marketing that value. Through professional services packages and native support included in license fees, the provider will take over tasks, such as:

- Moves, adds and changes between personnel and licenses (ZTNA)
- Integration of the SASE platform and tools with any existing or legacy holdover technologies—network, firewalls, etc.
- Proactive network and system monitoring and troubleshooting

While these services are not designed to explicitly replace full-time IT employees, it will allow the organization to have them focused on more strategic, revenue-generating activities rather than perform mundane, daily maintenance and management tasks.

5

Vendor strengths and weaknesses

Can the vendor provide all the capabilities that are part of the SASE definition? If not, where do the shortcomings lie? If the vendor claims to offer all the features, what are their strengths and weaknesses? Moreover, how does the maturity of their SASE offerings align with your priorities, strengths and weaknesses?

A vendor's strengths may include their ability to provide a complete SASE solution that is easy to deploy and manage. However, their weaknesses could include a lack of customization options or poor integration with other security tools.

Finally, you must evaluate the maturity of the vendor's SASE offerings and how well they align with your priorities, strengths and weaknesses. If your organization's primary focus is Zero Trust, but the vendor's strength is in cloud access security broker, then their offerings may not mesh well with your needs. Therefore, it is crucial to consider all these factors when evaluating a vendor's SASE capabilities to ensure you choose the right solution for your organization.

Key purchase considerations

6

Dense private backbone and network of POPs

SASE relies on a cloud delivery architecture that operates on a distributed network of interconnected POPs. However, not all SASE vendors are equally equipped to provide coverage to any enterprise, regardless of location. This is especially true for highly geographically distributed enterprises and those with presences in parts of the world, such as China and the Middle East. To comply with performance and regulatory requirements while maintaining data privacy, a dense network of SASE POPs is necessary to support the CSP's managed service offering.

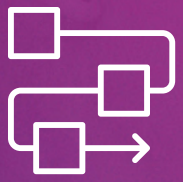
A robust fabric of SASE POPs can help organizations strike a balance between cybersecurity, network performance and regulatory compliance. This can significantly simplify adherence to compliance requirements. Investigate not only the number and location of POPs a SASE partner has but also where SASE data is managed and secured as they develop their managed SASE offerings.

The more POPs a provider has, the better the coverage they can offer, and the more opportunities they have for optimizing routing and delivering maximum throughput. Additionally, the location of the POPs should align with the location of your branch offices to ensure the best possible user experience.

Inadequate POP locations and architecture can lead to some users or applications experiencing higher latency, jitter and packet loss due to their distance from the nearest POP.

Going further, it is essential to ensure that each POP can run the full set of SASE capabilities. This means that they should be able to provide secure access service edge, secure web gateway, cloud access security broker, firewall as a service and zero-trust network access. Running the full set of capabilities at each POP helps to ensure minimal latency for connected users and locations.

Another critical factor to consider when evaluating a network provider is the backbone's self-healing capabilities and routing optimization. These features help to ensure maximum uptime and network resiliency in the event of a failure or outage. Additionally, WAN and cloud optimization should be provided to ensure that users can access cloud resources with minimal latency and full encryption to keep data secure.



SECTION 9

Model engagement/solution purchasing process

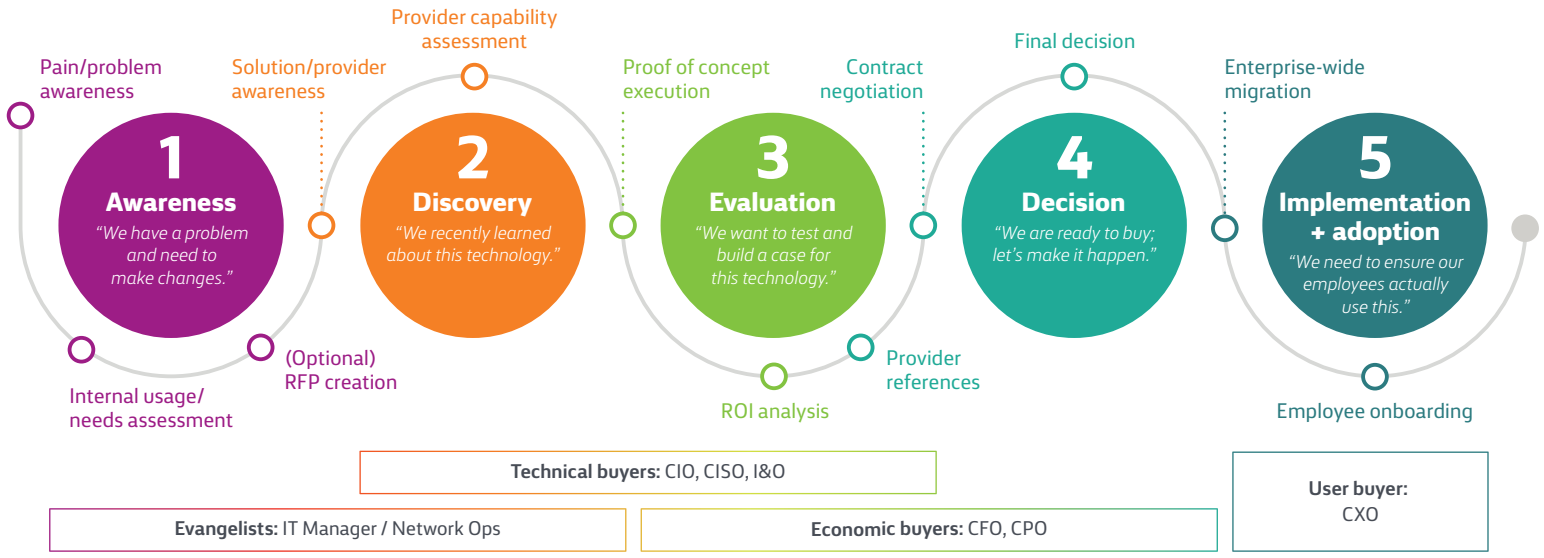
Model engagement/solution purchasing process

Buying processes for SASE vary depending on the size, scale and maturity of the organization and the history and composure of the overall composure of the cybersecurity strategy. Some will have extensive and detailed procurement processes, while others encounter a different buying process with every solution.

It is important to remember that the move to SASE is also more of a migration or evolution as opposed to a complete "rip and replace," as echoed by Gartner in the 2022 Strategic Roadmap for SASE Convergence.[22] Not every vendor claiming to offer a SASE product currently delivers all of the required and recommended SASE capabilities. Even then, not all of the SASE vendor's capabilities are at the same level of functionality and maturity.

Here we outline a model engagement and purchasing process for an enterprise buying process by role, designed to provide a framework on which to base a SASE purchase.

Job titles described in the previous section are categorized into buying roles as outlined in the Miller Heiman process, a framework that defines distinct roles and outlines each role's responsibilities. In this framework, each team member should understand their part to ensure they help choose the best technology for the organization.



Model engagement/solution purchasing process

1

Awareness

"We have a problem and need to make changes."

Pain/problem awareness

It is at this point that members of the organization realize they have a problem, often before they even realize they need a technology solution. This could be a problem with the status quo, a process or tool that's broken, or an impending upgrade of an often-used software platform. In the case of cybersecurity, this could also come from a breach, attempted attack or by seeing an incident occur with a competitor or partner that alerts the company to take action.

Internal usage/needs assessment

The discovery team, usually residing in the IT organization, reacts to the feedback by formalizing a strategic needs assessment of their internal cybersecurity and connectivity issues that could be causing the problem. This can include network downtime, difficulty with the management portal, attempted breaches or security incidents or anecdotal employee interviews and/or focus groups.

(Optional) RFP creation

Depending on the size and procurement requirements of the organization, the next step may be to organize a Request for Proposal (RFP) that outlines the perceived issues from the internal discovery, as well as any specific security or connectivity requirements. SASE providers are adept at responding to RFPs, but you can also initiate the sales process through a simple website inquiry or phone call directly to the provider.

Buyer roles at this stage:

Evangelist: IT Engineer, Network Operations Manager

With "boots on the ground" within the IT landscape, IT engineers and/or network operations managers are generally tasked with the discovery of new software for purchase, and then bringing possible solutions to upper IT leadership once they have been vetted.

The evangelist offers compelling reasons for the organization to apply time and attention to evaluation, acquisition and deployment of the software or services. At this stage, a detailed business case is not necessarily required to get started, although it will be needed later in the buying process.

Model engagement/solution purchasing process

2

Discovery

"We recently learned about this technology."

Solution/provider awareness

We have proof points somewhere that the majority of the research is done via website research before they ever talk to a potential provider. It is at this point that the IT managers begin to interact with possible solution providers, either through RFP responses or direct research of possible solution offerings. This research can be done digitally, although IT leaders report that tradeshows and conferences are where many discoveries and connections are made.

Provider capability assessment

Technical buyers, which include stakeholders from IT leadership, are brought in once solutions and their providers are narrowed down to single digits. There is no set number of candidates, although it should be fairly easy to disqualify or approve candidates that do not meet your specific needs during the Provider Awareness Stage.

Most providers will have a sales process in which they assist you with a capability assessment, but you should do some homework before the engagement to ensure preparedness. Gather input from any relevant departments and determine an immediacy rank for solving those issues—this can help with the eventual scope of the SASE project, ensuring you right-size the solution for your business needs.

Buyer roles at this stage:

Evangelist: IT Engineer, Network Ops Mgr

Technical buyer: CIO, CISO, I&O Manager

The technical buyer evaluates both the technology and the provider to see if the investment is justifiable technologically and allowable at the organizational level. They must question whether it can deliver on the defined requirements from the needs assessment, as well as future-proof the organization through scalability and extensibility. Stakeholders from the cybersecurity and medical information departments are essential here to ensure the technology solves for the organization's healthcare-specific challenges, while aligning with the long-term goals of the organization as a whole.

To be successful when serving in the technical buyer role, IT professionals need to be detail-oriented and present-minded: "Does it do what we need it to do now, and what we know we need it to do soon?" In addition, they should identify all the requirements that the product or service needs to satisfy.

Model engagement/solution purchasing process

3

Evaluation

"We want to test and build a case for this technology."

Proof of concept execution

Unlike a free trial, a proof-of-concept (POC) is a partial rollout of the full SASE solution in your unique environment. POCs must have predetermined goals for success or failure and must be conducted during a set time frame. Ensure that direct user and client feedback is accessible during the POC and that it is not siloed within the decision-making group. Again, SASE providers will have their own process for assisting you with the POC but be sure to have any goals or requirements unique to your organization clearly outlined prior to rollout.

ROI analysis

A clear Return on Investment outlook should be established prior to signing any contract, and again, most providers will be able to apply an ROI tool to your needs and run a model that shows break-even points based on your cybersecurity costs. These can be delivered via software but are also sometimes done using spreadsheets—so do not be turned off to that approach. They can also be implemented by third parties on behalf of a provider. More broad Total Economic Impact reports from analyst groups, such as Forrester can also be made available by certain providers.

Buyer roles at this stage:

Technical buyer: CIO, CISO, I&O

Economic buyer: CFO, CPO

At this stage we introduce the economic buyer, which assumes that the technical needs have been assessed by the technical buying group and is interested in the financial impact of the new solution on the company's bottom line.

This group usually has direct veto power over the purchase and is concerned with the income sources that support the organization, the ways in which IT supports revenue and profit and the ways in which the new platform will potentially affect revenue and profits.

Model engagement/solution purchasing process

4

Decision

"We are ready to buy, let's make it happen."

Provider references

References are essential to building credibility for a SASE solution, so providers should be more than willing to give you the customer references and stories you need to build a business case for their solution. References are often delivered in 3 ways:

1. Providers will publish customer stories and case studies on their websites, usually in their Resources section. See this example of an archive from Windstream Enterprise.
2. Sales reps may also have customer references from logos that are not made publicly available. They may even be able to facilitate conversations with existing customers via video conference in order to address specific needs allow for open conversation.
3. If you are a client of an advisory firm, such as Gartner, Forrester or Frost & Sullivan and have contracted with them to assist in your search, they can provide customer references per provider under NDA in certain cases.

Contract negotiation

At this stage, you have narrowed providers down to one or two and received contracts, which are then sent to each company's legal departments for review. It is not uncommon for this stage to take a long time, up to several months, with many reviews and redlines involved. It is important not to lose sight of the original goals and intentions of the solution identified in early stages, especially if concessions are made or features are reduced to accommodate budgets.

Final decision

Once the final decision is made, contracts are signed, usually electronically, and the handoff of your account is made from the sales team to the implementation and account management teams. During this stage, it is important to work with the provider to establish POCs as the provider transitions into their own procurement processes, so you are able to have constant updates of where you stand in that process.

Buyer roles at this stage:

Economic Buyer: CFO, CEO, CPO
Ultimate decision makers are required for final sign-off of contracts.

Model engagement/solution purchasing process

5

Implementation and adoption

"We need to ensure our employees actually use this."

Enterprise-wide migration

Changeover to the new solution will not happen overnight. As we discussed earlier, implementation means replacing one or two security capabilities with plans to complete the rest later. You should have already addressed this during the Evaluation stage, but ensure that there is minimal downtime or failover procedures in place as the transition is made to any new security tool and that there is no impact to revenue as a result.

Employee onboarding

User onboarding is one of the biggest hurdles in the transition to a new software platform. This includes ensuring that the departments using the SASE platform are well-trained on its function, as well as providing the tools they need to solve any post-training issues. The SASE provider should have training and adoption services included in any professional services package you have committed to, as well as extensive documentation in Help Centers that end users can refer to without having to contact the IT department in case of an issue.

Buyer roles at this stage:

User Buyer: CXO

Experience should be part of the decision-making process, but their key responsibilities will lie in the onboarding and rollout process. HR leadership may be brought in in some cases as well. User buyers determine what makes a tool "fit for use" and are the organization's means of filtering out options that do not satisfy requirements beyond technical capabilities. The software may fulfill its role at a technical level but could be challenging to use or complex to manage.

User experience stakeholders should focus their attention on how new software would fit into employees' workflow, both outside and inside IT. So, they will talk to other users, ask the right questions and be their voice in the overall purchasing process.

SECTION 10

Additional resources

Additional resources: SASE success stories

Help at Home®
Care to Live Your Life.

Nation's largest provider of in-home care implements SASE with SD-WAN to strengthen their network security

Challenge

Now more than ever, top-quality healthcare demands reliable technology. The digitization of the healthcare ecosystem—from digital EMRs to remote admin work and dispersed care—has underscored the need and increased the urgency for network security and 100% uptime.

In-home healthcare provider Help at Home knows how important digital innovation is to providing great patient care from anywhere. The collection of disparate IT systems and point solutions acquired as the result of multiple acquisitions was creating inefficiencies and complexity that consumed unnecessary resources and required frequent intervention to maintain the IT environment.

Legacy LAN services and wiring in branch locations caused frequent connection issues. Single-threaded Internet access with redundancy was causing unwanted outages.

As a result, the IT team was constantly in a state of reaction, putting out fires while also manually managing 150+ on-premises firewalls, multiple vendors and disparate point solutions. This made it difficult to support the environment and provide the level of visibility needed to better protect the network from cybersecurity threats.

Solution

Windstream Enterprise proved to be the all-in-one technology partner Help at Home was looking for. With SASE, the entire network is strong and secure, and the team can power up new sites quickly, without disrupting business.

The Windstream Enterprise SASE solution is powered by Cato Networks and all security components are cloud-based, enabling Help at Home to manage security services from a centralized portal.

WE Connect from Windstream Enterprise, the customer management portal, offers real-time visibility for the IT team to monitor services, view logs and make changes in real time, all from a single pane of glass.

Help at Home counts on the security experts in the Windstream Enterprise Cyber Security Operations Center (CSOC) to proactively alert them to security issues and to take immediate remediation measures.

Result

Help at Home now has a more secure, strong and resilient network foundation, thanks to leveraging Windstream Enterprise's SASE solution, powered by Cato Networks.

The new solution has been an incredible time saver for the IT team, allowing them to focus on moving the business forward instead of managing the security platform, myriad vendors and putting out fires.

Read full Help at Home case study →

View all case studies →

Additional resources: SASE success stories

Oil and gas company implements SASE to energize IT resiliency, connection speed and network security.

Challenge

Ranger Energy Services, a major player in the oil and gas industry, faced a fragmented network infrastructure ill-equipped to meet the demands of their operation. Their legacy MPLS and point-to-point networks lacked reliability and were vulnerable to cybersecurity threats. A lack of centralized control hampered their IT team who were overwhelmed with network-related tickets and burdened by slow, manual processes for even basic changes. Further, their legacy firewall setup required tedious, manual updates providing insufficient protection in a rapidly evolving threat landscape. Ranger needed a swift and comprehensive solution to deliver both reliability and security while easing the burden on their IT staff.

Solution

Ranger Energy Services partnered with Windstream Enterprise to implement a comprehensive SASE (Secure Access Service Edge) solution. First, they replaced their legacy VPN with Windstream Enterprise's Software Defined Perimeter (SDP), a core component of SASE that embraces Zero Trust Network Access (ZTNA) principles. This transition provided a significant boost to their security posture. Encouraged by the successful SASE proof of concept, Ranger rapidly deployed the solution across all of their nationwide locations.

Windstream Enterprise's SASE solution also integrated cloud-based Firewall as a Service (FWaaS) and Secure Web Gateway (SWG) functionality. These seamlessly replaced Ranger's on-premises firewalls, offering enhanced protection and centralized management.

Result

Ranger Energy Services reaped immediate benefits from their SASE implementation. Remote users and work-from-home employees experienced a significant performance boost with the new ZTNA clients, leading to a sharp reduction in network trouble tickets. Overall network stability and uptime dramatically increased across all locations. Ranger's IT staff were empowered by Windstream Enterprise's SASE portal, allowing them to self-deploy and rapidly scale according to their needs.

Security also saw major gains. The centralized, cloud-based controls made it simple to enforce consistent policies and respond to threats in real-time. Additionally, the Windstream Enterprise Cyber Security Operations Center (CSOC) provided proactive monitoring and alerting, giving Ranger peace of mind. The company's leadership and IT team alike were highly satisfied with the results.

Read full Ranger Energy Services case study →

View all case studies →

Additional resources

If you would like to dive even further into SASE, check out the following links for thought leadership, analyst insights and real-world customer stories:

SASE brochure

The convergence of SD-WAN and security →

SASE eBooks

Let's get SASE: Your quick guide to this security must have →

The top seven use cases for SASE →

7 compelling reasons why analysts recommend SASE →

Security as a Service →

SASE fact sheet

Integrated network and security. Managed your way. →

SASE videos

End-to-end protection in the cloud →

Keep IT simple with SASE →

The convergence of network and security with Cato Networks →

SASE webinars

Prevent data loss with SASE →

SASE is transforming the enterprise network →

SSE vs. SASE: What's the difference? →

What to expect with SASE →

When SASE is not really SASE →

SASE whitepapers

The unification of network and security →

What to consider before renewing your SD-WAN contract or service →

ROI of doing nothing →

Keeping your IT staff happy: How CIOs can turn the burnout tide in 6 steps →

Single-vendor SASE vs alternative SASE solutions →

Why Windstream Enterprise for a SASE solution?

- First and only MSP in North American to deliver a cloud-native SASE solution
- Fully integrated network and security solution—no multi-vendor point solutions
- Trusted by thousands of organizations as a market leader in SD-WAN
- White glove support and security experts in our Cyber Security Operations Center (CSOC)
- Managed Service integration with unified communications and LAN Services
- Fully managed access services—flexibility to enable bring your own access
- Award-winning WE Connect portal for complete visibility and co-management control

Citations:

1. Gartner. "Secure Access Service Edge (SASE)".
2. Gartner. "Security Service Edge (SSE)".
3. Gartner. "Magic Quadrant for Security Service Edge", April 10, 2023. Charlie Winckless, Aaron McQuaid, John Watts, Craig Lawson, Thomas Lintemuth, Dale Koeppen.
4. Gartner. "2022 Strategic Roadmap for SASE Convergence", June 24, 2022, Neil MacDonald, Andrew Lerner, John Watts.
5. Gartner. "Forecast Analysis: Secure Access Service Edge, Worldwide," July 21, 2021. Joe Skorupa, Nat Smith.
6. Gartner. "Forecast Analysis: Secure Access Service Edge", October 10, 2023, Nat Smith, Neil MacDonald, Christian Canales, Andrew Lerner, Jonathan Forest, John Watts, Shailendra Upadhyay, Charlie Winckless.
7. Verizon. "2023 Data Breach Investigations Report".
8. Gartner. "Press Release: More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025", February 9, 2022.
9. Gallup. "Remote Work Stable at Higher Rate Post-Pandemic", September 15, 2023. Jeffrey M. Jones.
10. Cybercrime Magazine. "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031", June 3, 2021.
11. University of Maryland. "Study: Hackers Attack Every 39 Seconds".
12. Trend Micro. "Cyber-Risk Declines But 78% of Organizations Predict Successful Attacks in Coming Year", May 2, 2023.
13. Forrester. "Shift Your Network Thinking To SD-WAN And Security", March 2022.
14. Gartner. "Magic Quadrant for Single-Vendor SASE", August 16, 2023.
15. By Analyst(s): Andrew Lerner, Jonathan Forest, Neil MacDonald, Nat Smith, Charlie Winckless.
16. Gartner. "Top Strategic Cybersecurity Trends for 2023", April 19, 2023. Lori Perri.
17. Gartner. "Gartner Identifies Three Factors Influencing Growth in Security Spending", October 13, 2022.
18. Gartner. "Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024", September 28, 2023.
19. Trend Micro. "2H'2022 Cyber Risk Index (CRI)".
20. Tech Buying: Key Jobs and Challenges in the IT Services Buying Process, 2022: Gartner. Katie Gove, Derry Finkeldey, Neil McMurchy. Page 5. Aug 19, 2022.
21. Gartner. Tech Buying: Key Jobs and Challenges in the Security Buying Process, 2022. September 2022, Swati Rakheja, Derry Finkeldey, Neil McMurchy.
22. WalkMe. "Change Management Statistics You Need to Know in 2023", October 31, 2022.
23. Gartner. "2022 Strategic Roadmap for SASE Convergence". June 24, 2022. Neil MacDonald, Andrew Lerner, John Watts.

Managed cloud connectivity, communications and security—guaranteed.

Windstream Enterprise drives business transformation through the convergence of our proprietary software solutions and cloud-optimized network to unlock our clients' revenue and profitability potential. Our end-to-end IT managed services modernize technology infrastructure, optimize operations, eliminate resource constraints and elevate the experience of our clients and their end users, while securing their critical data and brand reputation. Analysts recognize Windstream Enterprise as a market leader for our product innovation, and clients rely on our first-in-the-industry service guarantees and best-in-class management portal. Businesses trust Windstream Enterprise as their single-source for a high-performance network and award-winning suite of connectivity, collaboration and security solutions—delivered by a team of technology experts whose success is directly tied to our clients' complete satisfaction.

To learn more about Windstream Enterprise SASE, visit windstreamenterprise.com

WINDSTREAM ENTERPRISE