2022 Strategic Roadmap for SASE Convergence

Published 24 June 2022 - ID G00770805 - 30 min read

By Analyst(s): Neil MacDonald, Andrew Lerner, John Watts

Initiatives: Infrastructure Security

Work from anywhere and the relentless shift to cloud computing services have accelerated SASE offerings to enable anywhere, anytime access from any device. Security and risk management leaders should build a migration plan, from legacy perimeter and hardware-centric offerings to a SASE architecture.

Overview

Key Findings

- To enable and secure anywhere, anytime access, network and network security must become software-defined and cloud-delivered, forcing changes in architecture and vendor selection.
- The adoption of zero trust security architectures and branch office transformation projects — including software-defined WAN (SD-WAN), Multiprotocol Label Switching (MPLS) offload, internet-only branch — are accelerating the adoption of secure access service edge (SASE).
- Traditional perimeter-based approaches to securing anywhere, anytime access force rigid routing of network traffic through multiple disparate on-premises security chokepoints. This results in complexity for security administrators and inconsistent security experiences for users.
- Enterprises can reduce SASE adoption time by considering existing skill sets, vendors, and timing of hardware refresh cycles in their strategic roadmap for SASE adoption.

Recommendations

Security and risk management (SRM) leaders responsible for infrastructure security should include the following activities in their SASE roadmap:

Short term:

- Actively engage with initiatives for branch office transformation and MPLS offload to integrate cloud-centric security edge services into the scope of project planning.
- Inventory equipment and contracts to implement a multiyear phaseout of legacy on-premises perimeter and branch hardware, in favor of cloud-centric delivery of SASE capabilities within a thin-branch, heavy-cloud SASE architecture.
- Avoid point solution projects. Instead, opt for consolidation by using the converged security service edge (SSE) market at renewal time for CASB, SWG or VPN to remove complexity.
- Evaluate multiple approaches for SASE adoption — a single vendor, two explicitly partnered vendors or a managed SASE offering — to provide the most flexibility in selection and timing.

Longer term:

- Consolidate SASE offerings to a single vendor, two explicitly partnered networking and security vendors with deep integration, or a managed SASE offering to reduce complexity.
- Implement zero trust network access (ZTNA) within a SASE/SSE strategy to deliver consistent, contextual application access for all users, regardless of location (including in the office or branch).
- Choose SASE offerings that allow control of where inspection takes place, how traffic is routed, what is logged, and where logs are stored to meet privacy and compliance requirements.
- Create a dedicated team of security and networking experts with a shared responsibility for secure access engineering, spanning on-premises, remote workers, branch offices and edge locations to reduce implementation times and to facilitate successful implementation.

Strategic Planning Assumptions

By 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services and private application access using a SASE/SSE architecture, up from 20% in 2021.

By 2025, 65% of enterprises will have consolidated individual SASE components into one or two explicitly partnered SASE vendors, up from 15% in 2021.

By 2025, 50% of SD-WAN purchases will be part of a single vendor SASE offering, up from less than 10% in 2021.

Introduction

Traditionally, most network and security architectures were designed with the enterprise data center as the focal point for access needs, supporting users that were relatively static. But digital business has driven requirements for new digital capabilities — such as cloud and edge computing and work-from-anywhere initiatives — which have, in turn, inverted access requirements. There are now more users, devices, applications, services and data located outside of an enterprise perimeter than inside.

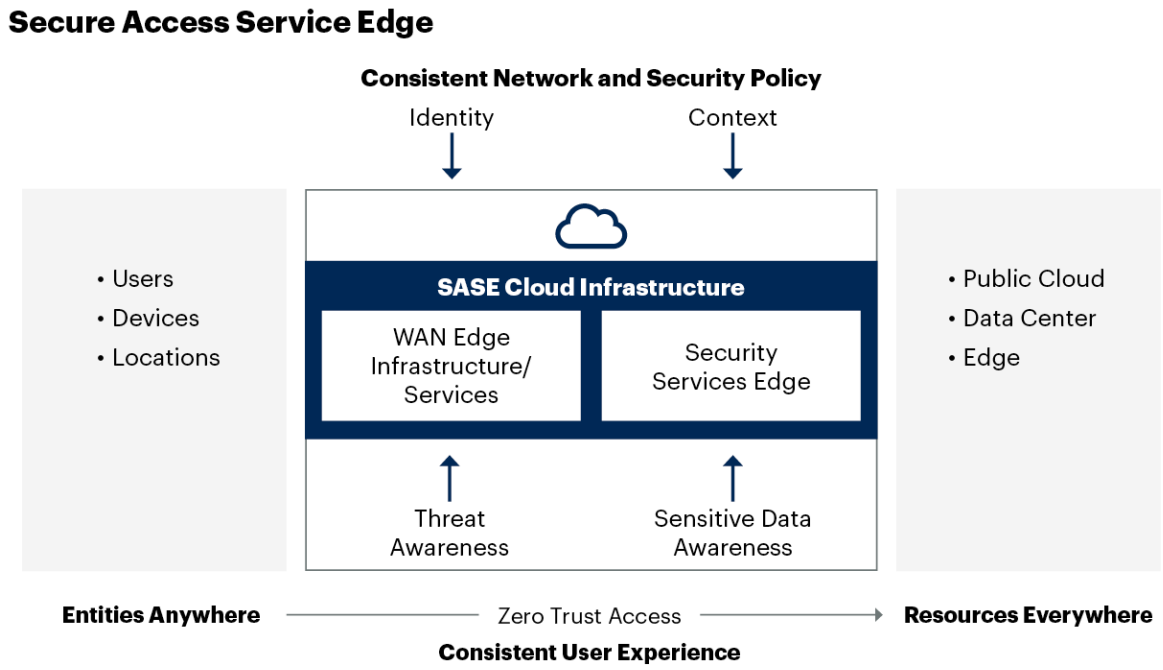
Network security designs based on a collection of perimeter security appliances are ill-suited to address the dynamic anywhere, anytime needs of a modern digital business and its hybrid digital workforce.

The legacy perimeter must transform into a set of user- and application-centric converged capabilities, managed from the cloud and enforced when and where an enterprise needs them — that is, a dynamically created, policy-based SASE.

At the same time, enterprises are increasingly pursuing zero trust strategies, but finding meaningful implementations of zero trust principles challenging. Delivering a zero trust security posture is an integral part of a SASE architecture and integral to emerging SASE offerings. Zero trust networking models replace implicit trust with continuously assessed risk/trust levels (see Quick Answer: How to Explain Zero Trust to Technology Executives). Zero trust architectures adapt the amount of explicit trust granted for interactions as the context surrounding the interactions changes.

The need to agilely support digital business transformation efforts with a zero trust security posture while keeping complexity manageable is a significant driver for the emerging SASE market, primarily delivered as a cloud-based service (originally described in The Future of Network Security Is in the Cloud). The SASE architecture (see Figure 1) converges network (most notably, SD-WAN) and network security services (most notably SWG, CASB, ZTNA).

Figure 1: Secure Access Service Edge



Source: Gartner
741491_C

Gartner

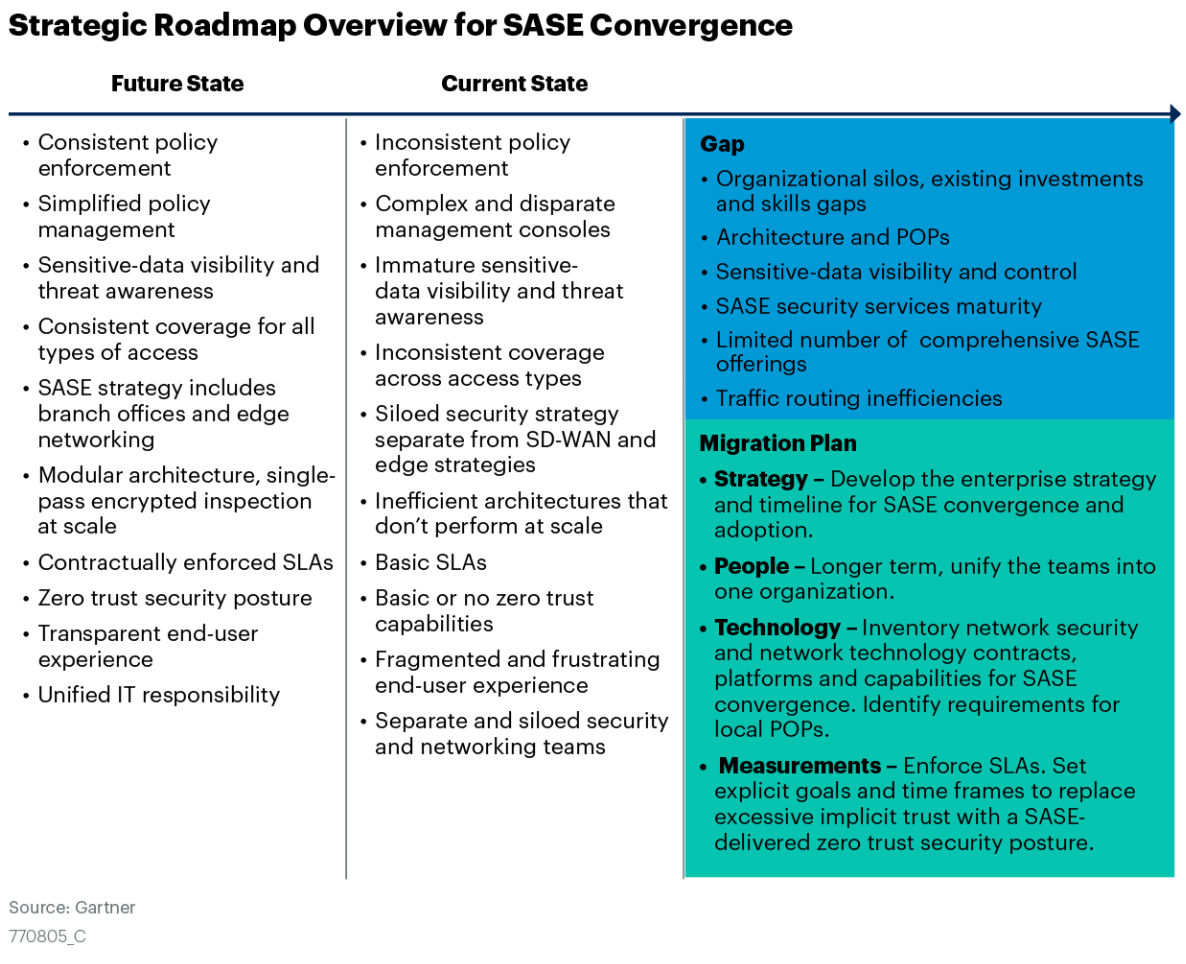
Since defining the emerging SASE market in 2019, industry and client interest in SASE has exploded, primarily driven by existing enterprise needs not being met by existing vendors. End-user client inquiries on SASE grew 89% in 2021, as compared to 2020, with growth continuing into the first quarter of 2022. In the 2022 Gartner CIO and Technology Executive Survey, SASE was the third most commonly cited technology investment (deployed or planning to deploy within 12 months) after AI/ML and distributed cloud, providing further evidence that momentum around SASE is growing among enterprise buyers. [1]

In the 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey, over one-third of respondents indicated they will have SASE implemented by the end of 2022, and 75% of respondents either have or will have SASE by 2024 or later. [2] In the last 18 months, there have been a number of significant vendor consolidation, acquisitions and announcements to build out a complete SASE portfolio, including multiple managed SASE offerings (see Note 4). Our Forecast Analysis: Secure Access Service Edge, Worldwide research indicates that over the next four years, the market for SASE will grow at a CAGR of 32%, reaching almost $15 billion by 2025.

However, enterprise transition to a complete SASE architecture will take time. The reality is that enterprises have existing investments in hardware and software with time and value remaining. Hardware refresh cycles at branch offices average four to seven years. Relationships and staff expertise with incumbent vendor offerings is another factor. Moreover, most larger enterprises have separate network security and network operations teams, further complicating SASE adoption.

Finally, many vendors claim to offer a SASE product but don't deliver all of the required and recommended SASE capabilities (see Note 1). Even where more capabilities are available, not all of the vendor's SASE capabilities are at the same level of functionality and maturity. We analyzed the gaps between the future and current state of SASE offerings in the market to enable SRM leaders with a strategic roadmap, a migration plan and implementation advice for SASE adoption over the next several years (see Figure 2).

Figure 2: Strategic Roadmap Overview for SASE Convergence

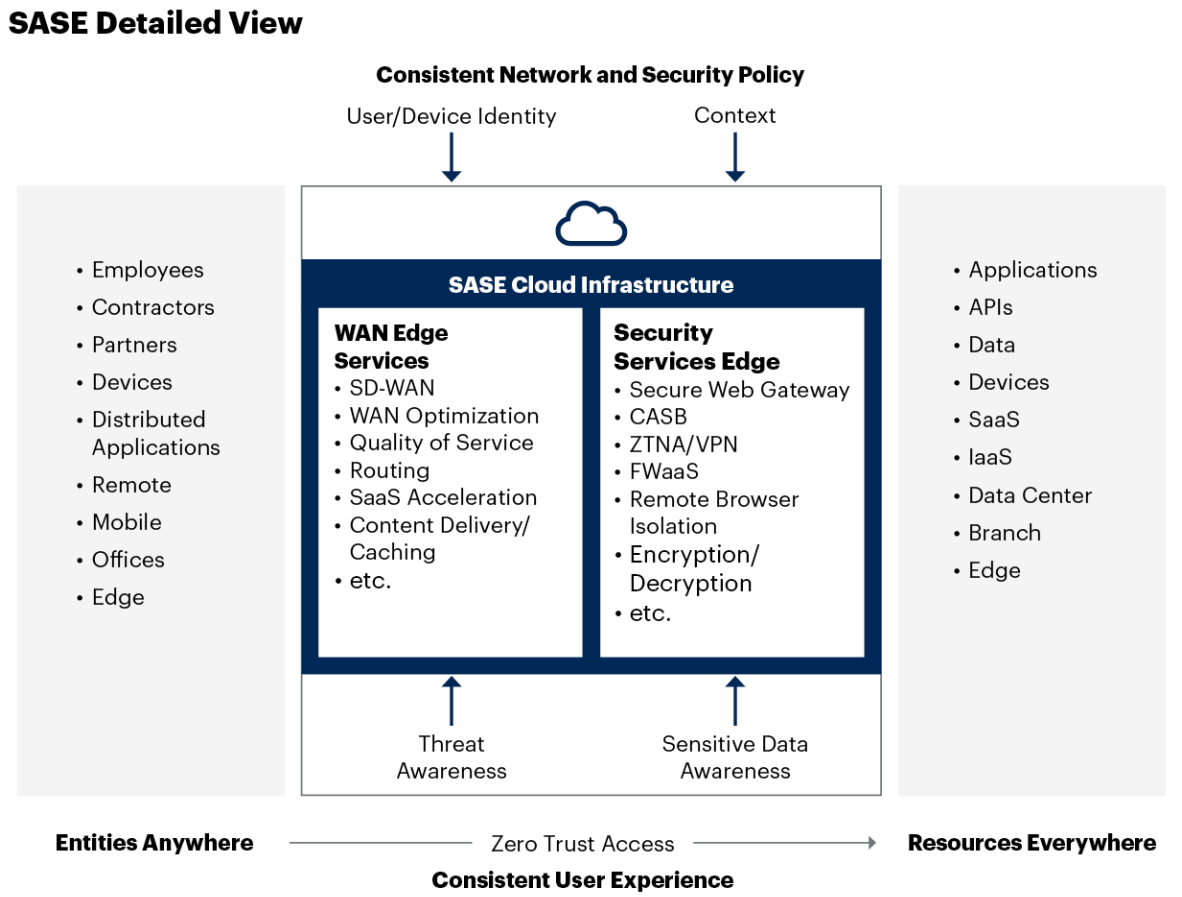


Source: Gartner
770805_C

Future State

Figure 3 shows a more detailed view of the future state of SASE.

Figure 3: SASE Detailed View



Source: Gartner
741491_C

Gartner

Your users and edge devices can be located anywhere and most of your users' network access is via the internet. Even on your internal network, a zero trust security posture treats the network as untrusted. Users, branch offices and edge devices need secure access to your data and applications that are spread everywhere throughout the cloud and data centers. SASE offerings deliver and protect this future state (i.e., 2025 and beyond; see Table 1).

Table 1: SASE Offerings Future State

(Enlarged table in Appendix)

Future State	Description
Consistent policy enforcement, regardless of location, with support for local decision making	A SASE architecture enables distributed policy enforcement to the enforcement "edge" that makes the most sense. Enforcement points can be in the public cloud, internet edge, vendor points of presence (POPS) or even at the endpoint itself. This will require a software-based, hardware-neutral architecture deployed across globally distributed POPs, with policy enforcement as close to the point of consumption (typically users) as needed. Customers can choose traffic to be inspected and directed to specific enforcement points based on business policy and compliance requirements. A fully distributed cloud architecture allows some security decisions to be made locally — addressing latency-sensitive, compliance, data sovereignty and intermittent access use cases — and other decisions to be made in the cloud. For branch office and edge locations, small hardware or virtual appliances are supported, but managed as part of a distributed cloud and implemented with a thin-branch, heavy-cloud architecture. Policies are applied consistently whether the user is remote, in a branch location, or in a campus or main office.
Ease of administration via a consolidated policy control plane	The SASE management control plane is decoupled from the enforcement nodes, allowing centralized administration, data storage and advanced analytics to be performed. The administrative interface will allow security and network policy to be managed from a single console and centralized dashboard for troubleshooting, reporting, analytics and configuration. It must also implement a robust set of APIs so that it can be programmatically interacted with other security tooling to address specific use cases. Machine learning (ML) is integral to automating policy creation and management.
Sensitive-data visibility and control as well as threat detection	Sensitive-data visibility and control is a critical core competency of SASE. This can be enabled using a combination of local agents, in-line traffic inspection and API-based inspection of cloud services. Advanced data security techniques and data loss prevention (DLP) engines will detect and protect sensitive data with minimal false positive and false negative rates. Visibility and protection from malicious content and network attacks is also provided.
Consistent policy enforcement covering all types of access	SASE offerings provide policy-based access to the internet, cloud services and enterprise private apps (hosted on-premises or in the cloud) all at the same time. SASE consolidates previously disparate network and security access policy enforcement points — i.e., SWG, CASB, SD-WAN and ZTNA — into a single-vendor, cloud-based offering. Security policies such as sensitive data and malware inspection are consistently applied across all access methods. For applications and APIs accessed via SASE, platforms will include network-based security controls (such as basic web application and API protection) to further protect applications from attacks. This is especially important for unmanaged devices that must be assumed hostile.
Consistent coverage for all types of entities, including users and devices at branch office, campus and edge locations	SASE offerings protect the access of users, collections of users (branch offices) and edge devices, as well as managed and unmanaged devices. For managed devices, agents will often be used; however, unmanaged devices are also supported when needed without the use of an agent (for example, for contractor or third-party access). At branch offices, a local appliance — typically SD-WAN hardware — acts as a shared agent for the branch for devices without agents (for example, printers). This provides traffic prioritization, connectivity failover, and local security capabilities such as firewalling and segmentation.
Single-pass inspection of encrypted traffic and content at line speed	Encrypted network sessions and content are inspected at line speed and support the latest versions of SSL/ TLS. Rather than scan a given piece of content once for malware/attacks and again using a separate engine for sensitive data, the session and its content will be decrypted once and scanned for malware and sensitive data using a single-pass, parallelized architecture.
Highly available, low-latency services with contractually enforced SLAs	SASE offerings will be built using an elastically scalable, composable architecture to deliver high performance and resilient service that can adapt to customer demand dynamically. Multiple and geographically dispersed enforcement points (most SASE vendors have dozens of POPs worldwide) enable the SASE provider to commit to contractual SLAs for high availability and low latency, without exceptions for inspecting encrypted traffic or inspecting for sensitive data.
Delivers a zero trust networking security posture	SASE offerings replace the implicit trust in legacy networking models with explicit, continuously assessed adaptive risk and trust levels based on identity and context of users. This zero trust security posture should extend to all devices when making connections to enterprise resources regardless of location — remote, on campus, in a branch or in the headquarters — i.e., "universal zero trust access." Once connected, the entity, device, session and associated behaviors are monitored for anomalous or risky behaviors. Based on risk, adaptive actions are taken such as modifying access.
Seamless end-user experience	SASE offerings provide the same user and access experience regardless of location or device. SASE offerings will use a unified endpoint agent that hides the access complexities from the user (e.g., forward proxy, tunnel creation where needed, device security posture). All common OSs and device types will be supported — Windows, macOS, Linux, iOS and Android. End-to-end measurement of user digital experience monitoring (DEM) will be integrated.
Unified IT responsibility for access engineering	In a SASE architecture, a single cross-functional IT team has responsibility for access design, selection, engineering and operations, spanning network security and networking and enabling secure access for all entities everywhere. Wide-area network engineering and network security engineering evolve into an emerging composite role of "access engineering" (a complement to the emerging IT role of platform engineering supporting application creation).

Source: Gartner

Current State

A mix of legacy perimeter-based security appliances, the use of different vendors for CASB, SWG, ZTNA, firewall and SD-WAN functions, and separate organizational structures for networking security and networking has created a complex and unmanageable collection of vendors, agents, consoles and traffic pingpongs and hairpinning (see Table 2).

Table 2: SASE Offerings Current State

(Enlarged table in Appendix)

Current State	Description
Inconsistent policy enforcement that is location-dependent	Some vendors with a legacy-appliance-based security business have been slow to deliver solutions natively from the cloud. Offerings built from multiple acquisitions have different policy enforcement options. Some SASE offerings are built on one or more hyperscale IaaS platforms. Other SASE vendors built their own POPs using colocation facilities. Some SASE architectures use both strategies to increase coverage (see Note 3). A few cloud-centric SASE offerings provide a locally installed enforcement point (typically a software appliance) for low-latency local policy enforcement. None yet support IaaS provider's distributed cloud hardware platforms such as AWS Outposts.
Complex administration using disparate management consoles and policies	Some vendors that are integrating a portfolio of SASE capabilities from a set of acquisitions have different consoles (or different tabs within the same console) for the different capabilities. These separate consoles increase the chance of error and complexity, reducing security while limiting efficiency. Others use service chaining to partners or network function virtualization (NFV) for services they don't yet offer, or they stitch together their acquired technologies, complicating administration and policy management. Some vendors with a legacy appliance-centric business model use different architectures on-premises versus in the cloud, with different management consoles and different capabilities.
Rudimentary or nonexistent sensitive-data visibility and control, and basic threat detection capabilities	Some vendors offer no sensitive-data discovery capabilities, others partner, while others offer only basic pattern matching. Leading SASE and SSE vendors offer consistent coverage for all channels and all security features, but not all vendors offer this. Very few offer optional sensitive data scanning for on-premises systems or endpoints. Some SASE vendors don't own their threat intelligence and detection capabilities, and instead license threat intelligence feeds from third parties. Finally, not every vendor includes remote browser isolation (RBI) and network sandboxing capabilities.
Immature or nonexistent capabilities in the security parts of the SASE portfolio	Some SASE offerings started with SWG, and later added CASB and ZTNA. Some started with CASB, and later added SWG and ZTNA. Some built SASE from their advanced SD-WAN and firewall offerings, adding cloud security through OEM partners with basic SWG, ZTNA and in-line-only CASB controls. The result is that even a vendor with a full set of SASE capabilities may be immature in some areas, while being advanced in other areas.
Not all vendors address the full set of required and recommended SASE capabilities (listed in Note 1)	Some SASE offerings only focus on cloud-delivered SSE capabilities (right side of Figure 3), and avoid the networking (left side of Figure 3) and partner for SD-WAN. Likewise, some SASE vendors focus on SD-WAN and have only basic security capabilities, and partner for cloud-delivered SSE capabilities. Few vendors address Internet of Things (IoT)/OT needs currently, and those serving edge computing and distributed composite application use cases are embryonic.
Inefficient architectures with multiple inspection points that ignore encrypted traffic or incur a significant performance hit	SASE vendors that came from an appliance background typically have monolithic architectures in the form of virtual appliances that have difficulty dynamically expanding to support higher-throughput connections. SASE vendors that partner to fill out capabilities often pingpong traffic across different services en route to their final destination. SASE vendors have used different approaches to inspecting encrypted traffic, and enterprises need to test this functionality to determine its impact on latency and throughput.
Basic SLAs, rarely with contractual penalties	Several vendors offer contractual SLAs for availability. SLAs for latency are less common, and, if offered, tend to address only regional access performance or only one channel of access (e.g., SWG). Some vendors have exceptions when inspecting for sensitive data or when the service is unavailable for maintenance. SLAs should be applied worldwide across all access mechanisms and enforcement policies with no exceptions.
Basic or no zero trust capabilities, lacking inspection and limited integration into endpoint security and management tools	Some ZTNA components of SASE don't have the option to remain in line the entire session, eliminating the capability to do sensitive data and malware inspection on these connections. Some agent-based ZTNA offerings have only basic device security posture assessment capabilities. A few integrate with local endpoint protection platform (EPP), endpoint detection and response (EDR) or unified endpoint management (UEM) agents. Many, but not all, offer agent and agentless ZTNA, satisfying employee and third-party or bring your own device (BYOD) access use cases.
Fragmented and frustrating end-user experience	For SASE offerings that provide only a partial set of capabilities, or have cobbled together from different acquisitions, multiple agents may be required. Some support ZTNA for remote users, but don't support this model when remote users go on-premises. Some vendors offer agents, but only for Windows/macOS and not Linux or mobile. Very few SASE vendors offer integrated DEM, even as an option.
Separate and siloed teams responsible for security versus network engineering	Most larger enterprises have separate teams for network security versus networking. Some very large enterprises may even have separate teams for SWG, CASB and remote access (VPN and ZTNA). While many SD-WAN implementations solicit security input, the branch office access transformation decisions are rarely from a unified cross-functional team.

Source: Gartner (June 2022)

Gap Analysis and Interdependencies

The most significant gaps that will inhibit SASE migration include:

- **Organizational silos, existing investments and skills gaps —** These are the biggest gaps that must be considered in migration planning. A full SASE implementation requires a coordinated and cohesive approach across security and the networking teams. For midsize enterprises (MSEs), this is an easier problem to address, as a separate security team may not exist. Within large organizations, these organizational structures, budgeting processes and responsibilities are quite rigid. Some vendors will be replaced and those associated skill sets will need to be repurposed toward policy creation in collaboration with business process and application owners.

- **Architecture and POPs —** SASE solutions are cloud-delivered, but vendors vary in the degree of "cloud nativeness" of their architecture. Legacy appliance and virtual appliance architectures need to be broken down into smaller, scalable components (see Note 2). Use of public cloud IaaS for POPs versus owning POPs is a difference among SASE providers that may impact adoption for some regions (see Note 3). Hairpinning of traffic and ping-ponging across multiple cloud POPs is an issue for both non-SASE deployments, multi-vendor SASE implementations and even some single-vendor SASE offerings. Every enterprise has different requirements for compliance, and has privacy requirements for the inspection of data, storage of logs and routing of traffic. A lack of geographic dispersion and number of enforcement points will also impact the ability of a SASE provider to commit to availability and latency SLAs.

- **Sensitive-data visibility and control —** This is a high-priority capability, but one of the most difficult problems for SASE vendors to address. Even vendors with strong data security may have gaps in coverage — for example, on-premises data stores and sensitive data stored at endpoints. Sending data to a third party for sensitive-data identification is not a sustainable or cost-effective option. This capability must be delivered natively by the SASE offering, and provide options for where the sensitive data is inspected.

- **SASE security services maturity —** For the next several years, SASE capabilities will vary widely. Enterprises need to prioritize their needs for converged capabilities versus the need for continued best-of-breed capabilities until the gaps are closed. Some vendors positioning themselves as a SASE offering fill gaps of core SASE functionality with partnerships, but daisy chaining of services and/or network function virtualization to deliver core services is not a sustainable long-term option. Partnerships are tenuous as markets merge and former partners begin competing directly.

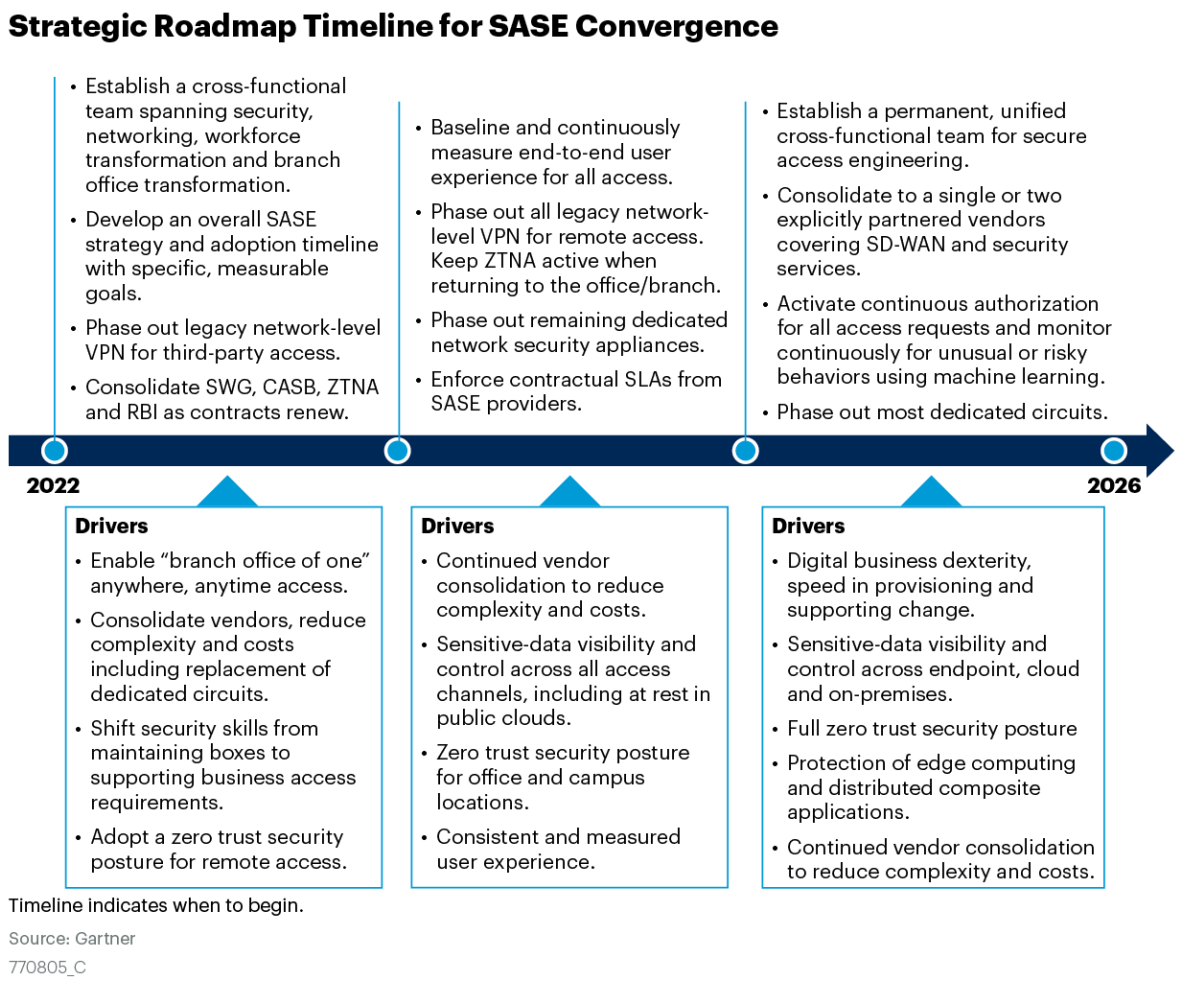
- **Limited number of comprehensive SASE offerings —** At the start of 2022, approximately 10 SASE offerings provide all of the core capabilities outlined in Note 1. Over the next five years, acquisitions and further market consolidation will address these gaps. As an interim step, even converged SSE vendors that avoid the direct requirements of SD-WAN are being pressured by customers to address branch office access needs and could provide a subset of SD-WAN capabilities, such as application-based bandwidth prioritization, path selection and content inspection.

- **Traffic routing inefficiencies —** Hairpinning of traffic and ping-ponging across multiple cloud POPs is an issue for both non-SASE deployments, multi-vendor SASE implementations and even some single-vendor SASE offerings. This increases latency and decreases throughput for users.

Migration Plan

Based on the gap analysis, we propose the following roadmap and action items over the next several years to be used as a template for SASE adoption and migration planning suitable for most enterprises. While a single-vendor approach for providing everything detailed in Figure 3 may be possible, every enterprise must determine if a fully converged approach makes sense for its requirements and, if so, in what time frame. Enterprises can't flip a switch and adopt SASE. As such, many larger organizations will use explicitly partnered network and security vendors in the short term. The vast majority of enterprise SASE adoption will occur over several years, prioritizing areas of greatest opportunity in terms of simplifying network security policy management, eliminating complexity and redundant vendors, and reducing risk through adoption of a zero trust security posture [3] (see Figure 4).

Figure 4: Strategic Roadmap Timeline for SASE Convergence



Accordingly, we have divided the recommendations into high-, medium- and lower-priority sections, based on the expected timeline for typical enterprise SASE adoption.

Higher Priority

In the next 18 months:

- Engage with digital workforce transformation teams to enable anywhere, anytime access for a remote and mobile workforce via SASE. Adopt a unified vision to enable a "branch office of one" for all remote/mobile workers, regardless of location and regardless of the location of applications.

- Form a joint network and security team/task force to develop a three- to five-year roadmap for SASE transformation, covering secure access strategies for users, branches, edge locations and distributed applications. Map and consolidate zero trust networking initiatives within the SASE roadmap:
  - Make sure this team includes the personnel responsible for branch office transformation and WAN redesign for direct internet access and MPLS offload projects.
  - Jointly establish a vision for the secure digital branch of the future that embraces a thin-branch, heavy-cloud architecture.

- Set a two- to four-year goal to replace 95% of legacy network-level VPN access with zero trust network access. Adopt cloud-based ZTNA (typically within an SSE deployment) to augment legacy VPN access for higher-risk use cases such as:
  - Contractor and third-party access
  - Unmanaged device access
  - Cloud administrator and developer access

- Set a two- to four-year goal to replace 95% of demilitarized zone (DMZ)-based services, using zero trust access (typically using ZTNA within SASE/SSE). Begin phasing out DMZ-based services for named user access and move internet-facing services to public cloud IaaS or colocation facilities.

- Capitalize on every refresh opportunity of security and branch office appliances/hardware to adopt SASE:
  - Where physical SWG, CASB and VPN appliances are used, we advise enterprises to move off these appliances at the soonest refresh possible and shift to SASE or SSE.
  - Sign no more than three-year contracts with net new providers that address your SASE roadmap. Set a goal to reevaluate the SASE provider landscape in Year 2 to verify the chosen SASE provider is still aligned with long-term business needs. However, plan for high costs if the decision is made to switch vendors. Make changes based on business need, not just to reduce subscription pricing.
  - If a branch refresh occurs in 2022, accelerate deployment of SSE and extend zero trust network access to managed devices in the branch and consider adoption of firewall as a service (FWaaS).
  - Include the providers' broader SASE capabilities in your pilot. For example, even if you don't have an immediate need for SaaS security (CASB), you should include it in the criteria. This helps to pick an optimal long-term solution, and selecting SSE over a dedicated CASB is preferred.
- Cut costs and reduce complexity by consolidating vendors when renewing SWG, CASB and ZTNA. All three are commonly offered now by a single vendor in a competitive market for SSE (the right side of the cloud services in Figure 1 and Figure 3; see Magic Quadrant for Security Service Edge). Evaluate single-vendor offerings, ideally including remote browser isolation capabilities:
  - Make sensitive-data discovery and protection a high-priority selection criterion when evaluating converged offerings.
  - Favor SASE architectures that inspect traffic only once for malware and sensitive data.
- Expand SASE RFI/RFP requirements with specific questions on the number and location of POPs mapped to enterprise requirements, peering relationships, encrypted traffic inspection performance and the ability to scale:
  - Demand contractual SLAs with penalties. SLAs should address latency, throughput and service availability without exceptions.

- MSEs should evaluate consolidated SD-WAN and cloud-based security edge services from a single provider.
- Larger organizations should evaluate the pros and cons of using a single vendor for SD-WAN and security services versus a partnership approach, and the timeline for consolidation. In both cases, consider the time to amortize investments and staff skills, as well as the maturity of the provider's SASE capabilities in this decision.
- Require explicit partnerships with console integration and technical support, when multiple vendors are used.
- Ignore vendor hype, as there is rampant "SASE washing" occurring, and focus on delivering against specific business and user outcomes.

Medium Priority

Over the next 18 to 36 months, enterprises should:

- Reevaluate the SASE architecture and roadmap if multiple vendors are still used. A single-vendor-provided SASE offering is now viable for most enterprises, although some organizations with separate network and network security teams will still pursue best-of-breed strategies and target consolidation to two providers:
  - Extend the enterprise SASE strategy to include edge computing use cases.
  - If multiple vendors are used, require explicit partnerships, with engineering and technical support backing up the integration.
- Deactivate remaining dedicated SWG, CASB and VPN appliances as they reach end of life, and replace them with cloud-based SSE if security best of breed is required.
- Pilot FWaaS for branch office protection, ideally for inbound and outbound traffic, to eliminate the need for physical branch office firewalls:
  - Phase out the use of separate physical firewalls at branch offices.
  - Adopt a deny-all, zero trust security posture for branch offices.

- Phase out the use of MPLS and adopt internet-only access for the majority of branches:
  - As part of this, evaluate emerging hyperscale offerings for WAN connectivity for branches, as they become an alternative for WAN services.
- In the context of a SASE or SSE deployment plan, move beyond initial ZTNA deployments, and implement a systematic and risk-based approach for phasing out all network-level VPN and DMZ-based services:
  - Use ML-based approaches to learn application access requirements to build policies and manage ongoing operations.
  - Expand ZTNA to more use cases, such as unified on-premises and remote policy enforcement, cloud application access and IoT/OT access.
  - Extend ZTNA to include session inspection for threats, sensitive data and unusual behavior.
- Extend sensitive-data visibility and control to data at rest in public clouds and for cloud-to-cloud services where the enterprise has no visibility.
- Phase out remaining DMZ-based applications and shift to SASE-based access for named users (e.g., partners and suppliers).
- Create an “access center of excellence” — a standing, single, unified secure access engineering team, combining team members from network architecture and network security teams into a unified secure access architecture team.
- Extend SASE capabilities to include integrated DEM.
- Implement a single agent for all access needs by leveraging an SSE solution that converges CASB, SWG and ZTNA capabilities.

Note: The recommendations listed may be accelerated to coincide with hardware refresh cycles and branch office transformation initiatives.

Lower Priority

At three to five years out, the SASE future strategic target state is achievable for most organizations. Specifically, a unified strategic approach for branch, edge, campus, headquarters and remote access needs covering private applications, the internet and cloud application access:

- Revisit the SASE migration plan, as the market will have matured and the technology is expected to be mainstream. Set a strategic goal of using no more than one or two SASE providers, using either a single vendor or tightly integrated explicit partnership.
- Extend the SASE migration strategy to address the needs of distributed composite applications, which have similar network and network security policy requirements (see Innovation Insight for Comprehensive Secure Connectivity for Composite Applications).
- Deliver against defined, measurable SASE goals that were committed to at the beginning. Specific examples include:
  - 95% of network-level VPN access eliminated
  - 95% of DMZ services eliminated for internal and third-party services
  - 80% reduction in the number of dedicated circuits, as much of this shifts to the internet
  - Percentage of applications isolated and secured with zero trust access controls
  - Improvements in end-user satisfaction
  - Improvements and stability (e.g., reduced latency) from DEM
- Adopt internet-only access as the default for most remote location use cases and continue with the phaseout of dedicated circuits. Make dedicated circuits an approved exception.
  - Replace all end-user access (even when on-premises in campus and headquarter locations) with a ZTNA-based approach.
- Extend the enterprise zero trust networking strategy “end to end” from the edge to the back end of applications to segment service creation based on identities using identity-based, zero trust segmentation (microsegmentation).

- Extend sensitive-data visibility and control to on-premises legacy data stores and to endpoints.
- Create a single, unified team and role responsible for access engineering that unifies networks and network security policy across all access methods (much like the emerging role for platform engineering with IaaS and DevOps).

Evidence

[1] **2022 Gartner CIO and Technology Executive Survey.** This survey was conducted online from 3 May through 19 July 2021 among Gartner Executive Programs members and other technology executives, to help CIOs and technology executives adopt business composability as a means to thrive during periods of volatility and uncertainty. Qualified respondents were each the most senior IT leader for their overall organization or a part of their organization (e.g., a business unit or region). The total sample was 2,387, with representation from all geographies and industry sectors (public and private). Disclaimer: Results do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[2] **2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey.** This study was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, expected or realized benefits of vendor consolidation, and how those who are consolidating are prioritizing their consolidation efforts. A primary purpose of this survey was to collect objective data on extended detection and response (XDR) and secure access service edge (SASE) for consolidation of megatrend analysis. The research was conducted online during March and April 2022 among 418 respondents from North America (n = 277; U.S., Canada), Europe (n = 104; France, Germany, U.K.) and the Asia/Pacific region (n = 37; Australia, Singapore). Results were from respondents with $50 million or more in 2021 enterprisewide annual revenue. Industries surveyed included manufacturing, communications and media, information technology, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences. Respondents were screened for job title, company size, job responsibilities to include information security/cybersecurity and IT roles, and primary involvement in information security. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[3] In the 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey, respondents contributed these key findings:

- SASE adoption for most organizations will take several years.
- Most organizations pursue SASE projects to simplify network security policy management and improve security posture, not to save on budget.

Note 1: SASE Capabilities

Core SASE capabilities:

(note: remote browser isolation was originally an optional SASE capability in 2019, but its use has become widespread for certain use cases and its inclusion must now be considered core)

- SWG
- CASB
- ZTNA
- SD-WAN
- Remote browser isolation
- FWaaS (including intrusion prevention system [IPS]/intrusion detection system [IDS])
- Sensitive-data and malware inspection capabilities
- Line rate operation

Recommended SASE capabilities:

- Network sandbox
- DNS protection
- API-based access to SaaS for data context
- Support for managed and unmanaged devices
- Web application and API protection

- Enhanced internet and/or private backbone transport
- CDN
- External DNS

Optional SASE capabilities:

- Wi-Fi hot spot protection
- Network obfuscation or dispersion
- Legacy VPN
- Edge compute protection

Note 2: Monolithic Versus Microservices Architectures

For example, monolithic virtual appliance architectures may have restrictions on the maximum bandwidth that can be inspected on a single connection. The use of virtual appliances may also affect the price/performance of the SASE offering, which may result in higher pricing for customers. SASE providers using public cloud IaaS also incur egress costs for traffic, which may result in higher pricing for customers and lower margins for the SASE provider.

Note 3: More POPS, More Coverage

The increasing fragmentation of the internet favors providers that can provide local access and local inspection within a country (including China and Russia) that may restrict access and data processing outside its borders.

Note 4: Notable SASE Announcements

In the past 18 months, many notable SASE announcements were made, many around managed SASE offerings:

- Adding a CASB to Cloudflare Zero Trust, Cloudflare.
- Aryaka Acquires Cloud-Based SASE Platform Secucloud GmbH, Aryaka.
- AT&T SASE Branch With Fortinet, AT&T Cybersecurity.
- AT&T SASE With Cisco, AT&T Cybersecurity.

- AT&T SASE With Palo Alto Networks, AT&T Cybersecurity.
- Cato Networks Partners With Horizon Telecom to Deliver SASE Services Across Europe, Cato Networks.
- Comcast Business Closes Masergy Acquisition, Comcast.
- Comcast Business Partners With Versa Networks to Extend ActiveCore to Deliver SASE Services, Comcast.
- Expereo Selects Cato for Delivering Managed SASE Services Worldwide, Expereo.
- KDDI Partners With Cato Networks to Deliver Cloud-Native SASE Services Worldwide, Cato Networks.
- MetTel and VMware to Deliver Cloud-Based Security, Networking and Compute Services at the Edge, VMware.
- MetTel Launches Global Cloud Network to Deliver SASE Managed Services to Safeguard Network Data in the Borderless Enterprise, MetTel.
- Orange Business Services and Fortinet Partner on SASE to Create a Secure, Seamless and Scalable Cloud-Native Network, Delivering Improved User Experience, Fortinet.
- Palo Alto Networks Partners With BT to Offer Managed SASE, Palo Alto Networks.
- Verizon Business Launches Advanced SASE Solution, Verizon.
- Versa Networks: Enable Agile and Secure Networks, Verizon.
- VMware SASE Launched by BT as a Managed Service, VMware.
- Windstream Enterprise and VMware Partner on SASE to Simplify Security and Deliver a Superior Customer Experience, Windstream Enterprise.
- Windstream Enterprise Partners With Cato Networks to Deliver Cloud-Native SASE to Organizations in North America, Cato Networks.

Document Revision History

2021 Strategic Roadmap for SASE Convergence - 25 March 2021

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

SASE Will Improve Your Distributed Security Everywhere

Magic Quadrant for WAN Edge Infrastructure

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Market Guide for Zero Trust Network Access

Forecast Analysis: Secure Access Service Edge, Worldwide

Market Insight: CSPs Must Augment Managed SD-WAN Services With Managed SASE

Table 1: SASE Offerings Future State

Future State	Description
Consistent policy enforcement, regardless of location, with support for local decision making	A SASE architecture enables distributed policy enforcement to the enforcement "edge" that makes the most sense. Enforcement points can be in the public cloud, internet edge, vendor points of presence (POPS) or even at the endpoint itself. This will require a software-based, hardware-neutral architecture deployed across globally distributed POPs, with policy enforcement as close to the point of consumption (typically users) as needed. Customers can choose traffic to be inspected and directed to specific enforcement points based on business policy and compliance requirements. A fully distributed cloud architecture allows some security decisions to be made locally — addressing latency-sensitive, compliance, data sovereignty and intermittent access use cases — and other decisions to be made in the cloud. For branch office and edge locations, small hardware or virtual appliances are supported, but managed as part of a distributed cloud and implemented with a thin-branch, heavy-cloud architecture. Policies are applied consistently whether the user is remote, in a branch location, or in a campus or main office.
Ease of administration via a consolidated policy control plane	The SASE management control plane is decoupled from the enforcement nodes, allowing centralized administration, data storage and advanced analytics to be performed. The administrative interface will allow security and network policy to be managed from a single console and centralized dashboard for troubleshooting, reporting, analytics and configuration. It must also implement a robust set of APIs so that it can be programmatically

	interacted with other security tooling to address specific use cases. Machine learning (ML) is integral to automating policy creation and management.
Sensitive-data visibility and control as well as threat detection	Sensitive-data visibility and control is a critical core competency of SASE. This can be enabled using a combination of local agents, in-line traffic inspection and API-based inspection of cloud services. Advanced data security techniques and data loss prevention (DLP) engines will detect and protect sensitive data with minimal false positive and false negative rates. Visibility and protection from malicious content and network attacks is also provided.
Consistent policy enforcement covering all types of access	SASE offerings provide policy-based access to the internet, cloud services and enterprise private apps (hosted on-premises or in the cloud) all at the same time. SASE consolidates previously disparate network and security access policy enforcement points — i.e., SWG, CASB, SD-WAN and ZTNA — into a single-vendor, cloud-based offering. Security policies such as sensitive data and malware inspection are consistently applied across all access methods. For applications and APIs accessed via SASE, platforms will include network-based security controls (such as basic web application and API protection) to further protect applications from attacks. This is especially important for unmanaged devices that must be assumed hostile.
Consistent coverage for all types of entities, including users and devices at branch office, campus and edge locations	SASE offerings protect the access of users, collections of users (branch offices) and edge devices, as well as managed and unmanaged devices. For managed devices, agents will often be used; however, unmanaged devices are also supported when needed without the use of an agent (for example, for contractor or third-party access). At branch offices, a local appliance — typically SD-WAN hardware — acts as a shared agent for the branch for devices without agents (for example, printers). This provides traffic

	prioritization, connectivity failover, and local security capabilities such as firewalling and segmentation.
Single-pass inspection of encrypted traffic and content at line speed	Encrypted network sessions and content are inspected at line speed and support the latest versions of SSL/TLS. Rather than scan a given piece of content once for malware/attacks and again using a separate engine for sensitive data, the session and its content will be decrypted once and scanned for malware and sensitive data using a single-pass, parallelized architecture.
Highly available, low-latency services with contractually enforced SLAs	SASE offerings will be built using an elastically scalable, composable architecture to deliver high performance and resilient service that can adapt to customer demand dynamically. Multiple and geographically dispersed enforcement points (most SASE vendors have dozens of POPs worldwide) enable the SASE provider to commit to contractual SLAs for high availability and low latency, without exceptions for inspecting encrypted traffic or inspecting for sensitive data.
Delivers a zero trust networking security posture	SASE offerings replace the implicit trust in legacy networking models with explicit, continuously assessed adaptive risk and trust levels based on identity and context of users. This zero trust security posture should extend to all devices when making connections to enterprise resources regardless of location — remote, on campus, in a branch or in the headquarters — i.e., "universal zero trust access." Once connected, the entity, device, session and associated behaviors are monitored for anomalous or risky behaviors. Based on risk, adaptive actions are taken such as modifying access.
Seamless end-user experience	SASE offerings provide the same user and access experience regardless of location or device. SASE offerings will use a unified endpoint agent that hides the access complexities from the user (e.g., forward proxy, tunnel creation

	where needed, device security posture). All common OSs and device types will be supported — Windows, macOS, Linux, iOS and Android. End-to-end measurement of user digital experience monitoring (DEM) will be integrated.
Unified IT responsibility for access engineering	In a SASE architecture, a single cross-functional IT team has responsibility for access design, selection, engineering and operations, spanning network security and networking and enabling secure access for all entities everywhere. Wide-area network engineering and network security engineering evolve into an emerging composite role of “access engineering” (a complement to the emerging IT role of platform engineering supporting application creation).

Source: Gartner

Table 2: SASE Offerings Current State

Current State	Description
Inconsistent policy enforcement that is location-dependent	Some vendors with a legacy-appliance-based security business have been slow to deliver solutions natively from the cloud. Offerings built from multiple acquisitions have different policy enforcement options. Some SASE offerings are built on one or more hyperscale IaaS platforms. Other SASE vendors built their own POPs using colocation facilities. Some SASE architectures use both strategies to increase coverage (see Note 3). A few cloud-centric SASE offerings provide a locally installed enforcement point (typically a software appliance) for low-latency local policy enforcement. None yet support IaaS provider's distributed cloud hardware platforms such as AWS Outposts.
Complex administration using disparate management consoles and policies	Some vendors that are integrating a portfolio of SASE capabilities from a set of acquisitions have different consoles (or different tabs within the same console) for the different capabilities. These separate consoles increase the chance of error and complexity, reducing security while limiting efficiency. Others use service chaining to partners or network function virtualization (NFV) for services they don't yet offer, or they stitch together their acquired technologies, complicating administration and policy management. Some vendors with a legacy appliance-centric business model use different architectures on-premises versus in the cloud, with different management consoles and different capabilities.
Rudimentary or nonexistent sensitive-data visibility and control, and basic threat detection capabilities	Some vendors offer no sensitive-data discovery capabilities, others partner, while others offer only basic pattern matching. Leading SASE and SSE vendors offer consistent coverage for all channels and all security features,

	but not all vendors offer this. Very few offer optional sensitive data scanning for on-premises systems or endpoints. Some SASE vendors don't own their threat intelligence and detection capabilities, and instead license threat intelligence feeds from third parties. Finally, not every vendor includes remote browser isolation (RBI) and network sandboxing capabilities.
Immature or nonexistent capabilities in the security parts of the SASE portfolio	Some SASE offerings started with SWG, and later added CASB and ZTNA. Some started with CASB, and later added SWG and ZTNA. Some built SASE from their advanced SD-WAN and firewall offerings, adding cloud security through OEM partners with basic SWG, ZTNA and in-line-only CASB controls. The result is that even a vendor with a full set of SASE capabilities may be immature in some areas, while being advanced in other areas.
Not all vendors address the full set of required and recommended SASE capabilities (listed in Note 1)	Some SASE offerings only focus on cloud-delivered SSE capabilities (right side of Figure 3), and avoid the networking (left side of Figure 3) and partner for SD-WAN. Likewise, some SASE vendors focus on SD-WAN and have only basic security capabilities, and partner for cloud-delivered SSE capabilities. Few vendors address Internet of Things (IoT)/OT needs currently, and those serving edge computing and distributed composite application use cases are embryonic.
Inefficient architectures with multiple inspection points that ignore encrypted traffic or incur a significant performance hit	SASE vendors that came from an appliance background typically have monolithic architectures in the form of virtual appliances that have difficulty dynamically expanding to support higher-throughput connections. SASE vendors that partner to fill out capabilities often pingpong traffic across different services en route to their final destination. SASE vendors have used different approaches to inspecting encrypted traffic, and enterprises need to test this functionality to determine its impact on latency and throughput.
Basic SLAs, rarely with contractual penalties	Several vendors offer contractual SLAs for availability. SLAs for latency are

	less common, and, if offered, tend to address only regional access performance or only one channel of access (e.g., SWG). Some vendors have exceptions when inspecting for sensitive data or when the service is unavailable for maintenance. SLAs should be applied worldwide across all access mechanisms and enforcement policies with no exceptions.
Basic or no zero trust capabilities, lacking inspection and limited integration into endpoint security and management tools	Some ZTNA components of SASE don't have the option to remain in line the entire session, eliminating the capability to do sensitive data and malware inspection on these connections. Some agent-based ZTNA offerings have only basic device security posture assessment capabilities. A few integrate with local endpoint protection platform (EPP), endpoint detection and response (EDR) or unified endpoint management (UEM) agents. Many, but not all, offer agent and agentless ZTNA, satisfying employee and third-party or bring your own device (BYOD) access use cases.
Fragmented and frustrating end-user experience	For SASE offerings that provide only a partial set of capabilities, or have cobbled together from different acquisitions, multiple agents may be required. Some support ZTNA for remote users, but don't support this model when remote users go on-premises. Some vendors offer agents, but only for Windows/macOS and not Linux or mobile. Very few SASE vendors offer integrated DEM, even as an option.
Separate and siloed teams responsible for security versus network engineering	Most larger enterprises have separate teams for network security versus networking. Some very large enterprises may even have separate teams for SWG, CASB and remote access (VPN and ZTNA). While many SD-WAN implementations solicit security input, the branch office access transformation decisions are rarely from a unified cross-functional team.

Source: Gartner (June 2022)