2021 Strategic Roadmap for SASE Convergence

Published 25 March 2021 - ID G00741491 - 25 min read

By Neil MacDonald, Nat Smith, **and 2 more**

Digitalization, work from anywhere and cloud-based computing have accelerated cloud-delivered 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-based offerings to a SASE model.

Overview

Key Findings

- To protect anywhere, anytime access to digital capabilities, security must become software-defined and cloud-delivered, forcing changes in security architecture and vendor selection.
- Perimeter-based approaches to securing anywhere, anytime access has resulted in a patchwork of vendors, policies, and consoles creating complexity for security administrators and users.
- Enterprises that consider existing skill sets, vendors, and products and timing of hardware refresh cycles as migration factors will reduce their secure access service edge (SASE) adoption time frame by half.
- Branch office transformation projects (including software-defined WAN [SD-WAN], MPLS offload, internet-only branch and associated cost savings) are increasingly part of the SASE project scope.
- SASE is a pragmatic and compelling model that can be partially or fully implemented today.

Recommendations

Security and risk management leaders responsible for infrastructure security should develop a roadmap for the adoption of SASE capabilities and offerings:

Short term:

- Deploy zero trust network access (ZTNA) to augment or replace legacy VPN for remote users, especially for high-risk use cases.

- Inventory equipment and contracts to implement a multiyear phase out of on-premises perimeter and branch hardware in favor of cloud-based delivery of SASE capabilities.
- Consolidate vendors and cut complexity and costs as contracts renew for secure web gateways (SWGs), cloud access security brokers (CASBs) and VPN. Leverage a converged market that emerges combining these security edge services.
- Actively engage with initiatives for branch office transformation and MPLS offload in order to integrate cloud-based security edge services into the scope of project planning.

Longer term:

- Consolidate SASE offerings to a single vendor or two explicitly partnered vendors.
- Implement ZTNA for all users regardless of location, including when 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.

Strategic Planning Assumptions

By 2024, 30% of enterprises will adopt cloud-delivered SWG, CASB, ZTNA and branch office firewall as a service (FWaaS) capabilities from the same vendor, up from less than 5% in 2020.

By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch and edge access, up from 10% in 2020.

By 2023, to deliver flexible, cost-effective scalable bandwidth, 30% of enterprise locations will have only internet WAN connectivity, compared with approximately 15% in 2020.

Introduction

Current network security architectures were designed with the enterprise data center as the focal point for access needs. Digital business has driven new IT architectures like cloud and edge computing and work-from-anywhere initiatives, which have, in turn, inverted access requirements, with more users, devices, applications, services and data located outside of an enterprise than inside. The COVID-19 pandemic accelerated these trends. [1]

Network security models based on data center perimeter security using a collection of security appliances are ill-suited to address the dynamic needs of a modern digital business and its distributed

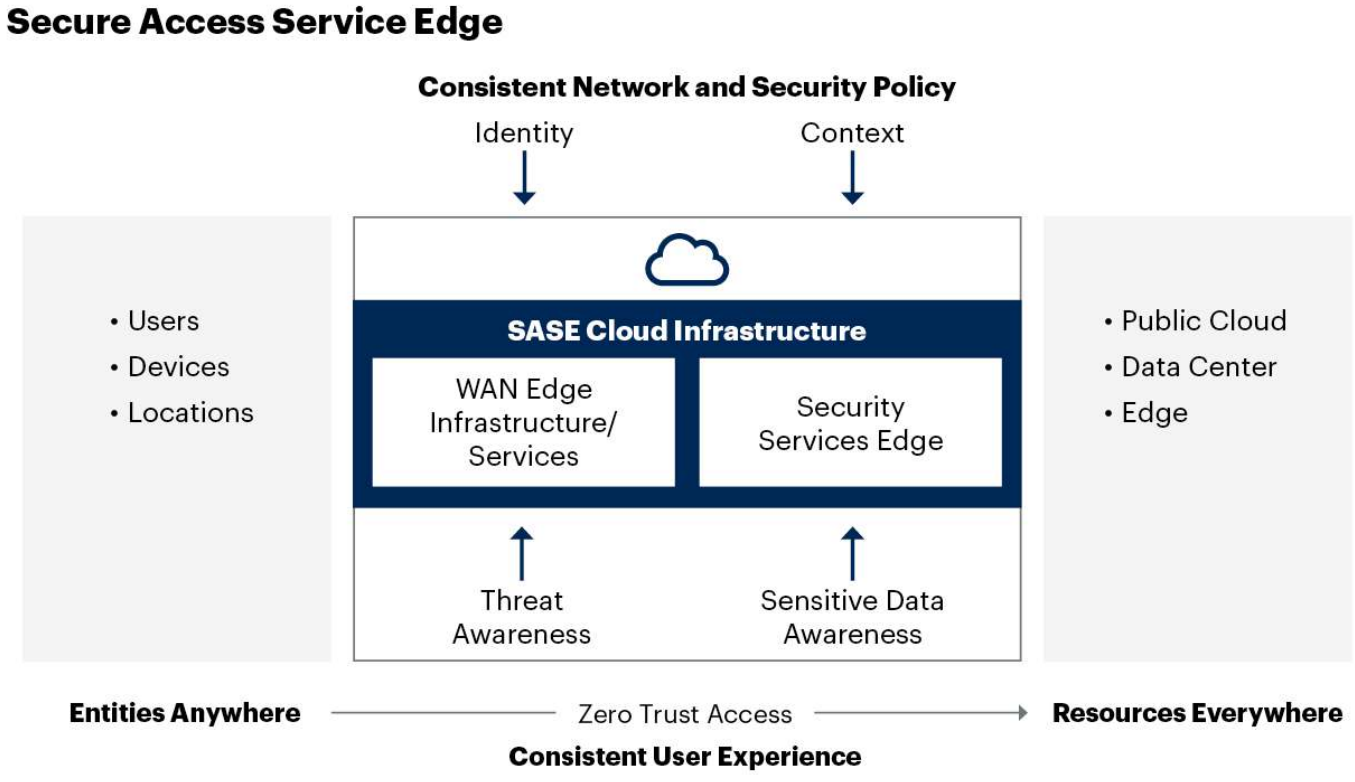
digital workforce.

The legacy perimeter must transform into a set of cloud-based, converged capabilities created when and where an enterprise needs them — that is, a dynamically created, policy-based secure access service edge .

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 emerging SASE offerings. Zero trust networking models replace implicit trust (zero implicit trust is the goal) with continuously assessed risk/trust levels (see Zero Trust Is an Initial Step on the Roadmap to CARTA). They adapt the amount of explicit trust granted for interactions as 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 (see The Future of Network Security Is in the Cloud). This market converges network (for example, SD-WAN) and network security services (such as SWG, CASB, ZTNA and FWaaS; see Figure 1).

Figure 1. Secure Access Service Edge

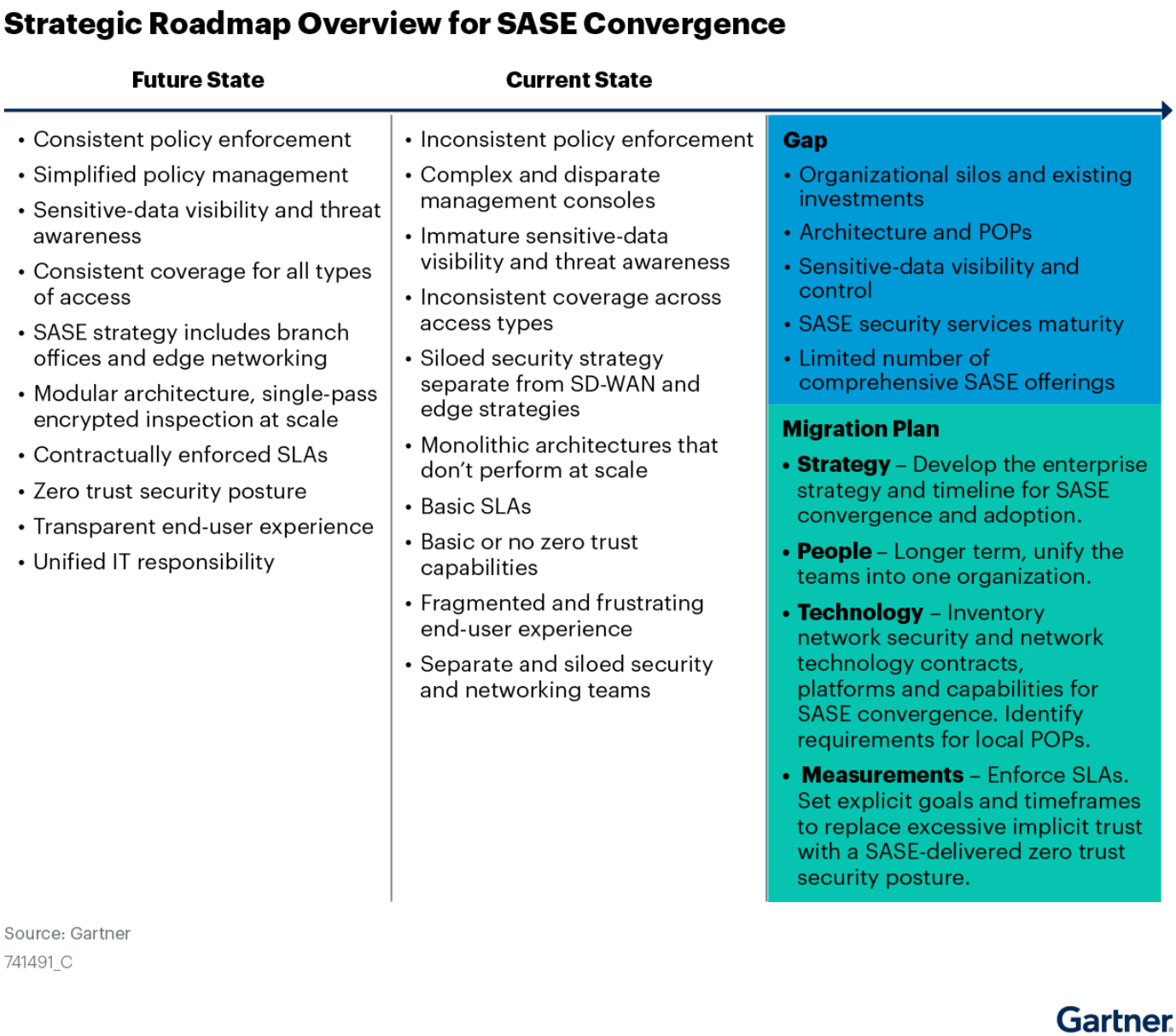


Source: Gartner
741491_C

Since defining the emerging SASE market in July 2019, industry and client interest in SASE has exploded primarily driven by existing enterprise needs being unmet by existing vendors. But vendor hype complicates the understanding of the SASE market. Since publishing the initial research, the percentage of end-user inquiries mentioning SASE grew from 3% to 15% when comparing the same time period in 2019 to 2020 across the total number of end-user conversations on related security topics. [2] The growth in interest continues in January 2021, with 17% of end-user calls mentioning SASE across the same set of related markets. Significant vendor consolidation, acquisitions and announcements to build out a complete SASE portfolio have increased, [3] with more expected over the next 12 to 24 months.

However, enterprise transition to a complete SASE model will take time. The reality is enterprises have existing investments in hardware that is not fully amortized and in software contracts with time remaining. Hardware refresh cycles at branch offices average five to seven years. Relationships and staff expertise with incumbent vendor offerings is another factor. Complicating SASE adoption is that most larger enterprises have separate network security and network operations teams. Finally, not every vendor claiming to offer a SASE product currently delivers all of the required and recommended SASE capabilities (see Note 1). Even then, not all of the SASE vendor's capabilities are at the same level of functionality and maturity. By analyzing the gaps between the future and current state of SASE offerings, we provide a strategic roadmap, migration plan and implementation advice for SASE adoption over the next several years (see Figure 2).

Figure 2. Strategic Roadmap Overview for SASE Convergence

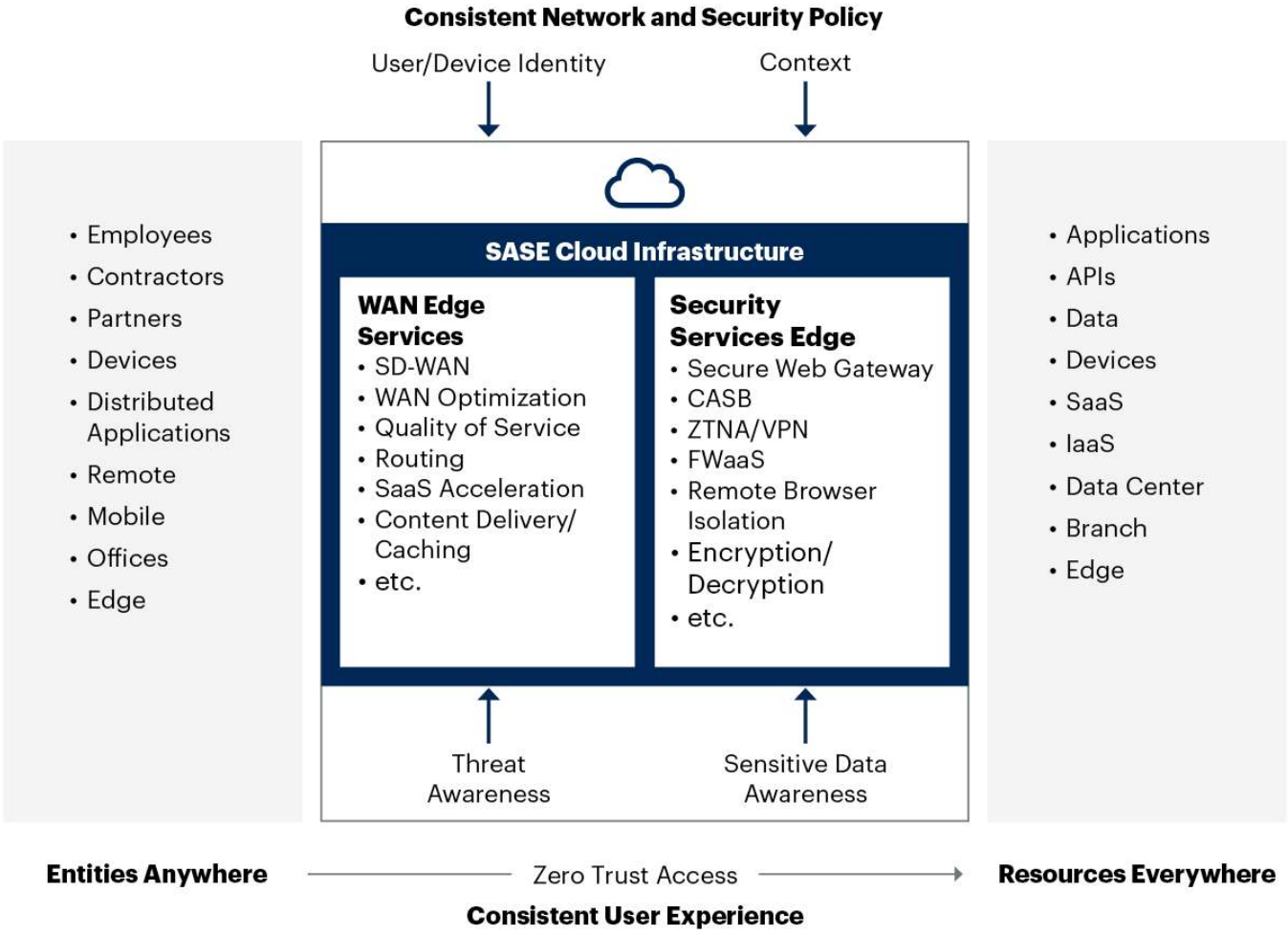


Future State

A more detailed view of the future state of SASE is shown in Figure 3.

Figure 3. SASE Detailed View

SASE Detailed View



Source: Gartner
741491_C

Gartner

Your users and edge devices can be located anywhere and your access network is the internet. These entities need secure access to your data and applications that are spread everywhere throughout the cloud. SASE offerings deliver and protect this future state (i.e., 2024 and beyond; see Table 1).

Table 1: SASE Future State

Future State	Description

Consistent policy enforcement, regardless of location, with support for local decision making	SASE security policy enforcement is dispersed in the cloud. This requires a software-based, hardware-neutral architecture deployed across multiple points of presence (POPs) with policy enforcement close to the point of consumption. Customers can choose traffic to be inspected and directed to specific POPs based on business policy and compliance requirements. A distributed cloud architecture allows some security decisions to be made locally (addressing latency-sensitive and intermittent access use cases). For branch office and edge locations, small hardware or virtual appliances are supported but managed as a 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. The administrative interface will allow security and network policy to be managed from a single console and applied regardless of the location of the user, the application or the data. Artificial intelligence (AI) and machine learning (ML) will be integral to automate policy creation. Full API enablement allows automation and integration with existing processes and tools.
Sensitive-data visibility and control as well as threat detection	Sensitive-data visibility and control is a critical capability of SASE. This is enabled using a combination of techniques including local agents, in-line traffic inspection and API-based inspection of cloud services. 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, SaaS apps and enterprise private apps (on-premises or in IaaS) 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 exposed applications and APIs, optional web application firewall (WAF) and API protections are provided.

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 be used; however, unmanaged devices are also supported when needed. At branch offices, a local appliance (typically SD-WAN hardware) acts as an “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” architecture.
Highly available, low-latency services with contractually enforced SLAs	SASE offerings will be built using an elastically scalable, multitenanted microservices-based architecture to deliver a high performance and resilient service that can adapt to customer demand dynamically. Multiple and geographically dispersed POPs enable the SASE provider to commit to contractual SLAs for high availability and low latency.
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 for all connections — remote, on campus, in a branch or in the headquarters. Following the Gartner continuous adaptive risk/trust assessment (CARTA) approach, once connected, the entity, device, session and associated behaviors are monitored for anomalous or risky behaviors. Based on policy, adaptive actions are taken such as dynamically modifying access.
Transparent and simplified end-user experience	SASE offerings provide exactly the same user and access experience regardless of location. 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, etc). All common OSs and device types will be supported — Windows, Mac, Linux, iOS and Android. End-to-end user-experience monitoring in terms of latency and performance will be integrated.

Unified IT responsibility for access engineering	In a SASE model, a single unified 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 hardware, the use of different vendors for CASB, SWG, ZTNA and SD-WAN functions, and separate organizational structures for networking security and networking have created a complex and unmanageable collection of vendors, agents, consoles and traffic hairpinning (see Table 2).

Table 2: SASE Current State

Current State	*Description*
Inconsistent policy enforcement that is location dependent.	Some vendors with a legacy-hardware-based security business have been slow to embrace cloud-based delivery of services. 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). Only a few cloud-based SASE offerings provide a locally installed enforcement point for low-latency local decisions in remote locations. None yet support distributed cloud architectures or platforms (see Differences Between AWS Outposts, Google Anthos, Microsoft Azure Stack and Azure Arc for Hybrid Cloud).
Complex administration using disparate management consoles and policies.	Some vendors that are integrating SASE capabilities from a set of acquisitions have different consoles for the different capabilities. Others use service chaining to partners or network function virtualization (NFV) for services they don’t yet offer, complicating administration and policy management. Some vendors with a legacy hardware business use different architectures on-premises versus in the cloud, with different management consoles and different capabilities.

Current State	*Description*
Rudimentary or nonexistent sensitive-data visibility and control. Basic threat detection capabilities.	Some offer no sensitive-data discovery capabilities, others partner, while others offer only basic pattern matching. Some vendors offer data loss prevention (DLP) and malware scanning for SWG and CASB access, but not for ZTNA. 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. 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 currently address the full set of required and recommended SASE capabilities listed in Note 1.	Some SASE offerings only focus on cloud-delivered security edge services, (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 security edge services. Few vendors address Internet of Things (IoT) needs today, and serving edge computing and distributed composite application use cases are embryonic.

Current State	*Description*
Monolithic architectures with multiple inspection points that ignore encrypted traffic or incur a significant performance hit.	SASE vendors that came from a physical appliance background may have monolithic architectures in the form of virtual appliances that have difficulty dynamically expanding to support larger throughput connections. SASE vendors have used different approaches to inspecting encrypted traffic, and enterprises need to test this functionality to determine its impact on latency.
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). The SLAs should be applied worldwide across all access mechanisms and enforcement policies.
Basic or no ZTNA capabilities lacking inspection and limited integration into endpoint security and management tools.	Some offerings identifying as SASE don't yet include ZTNA. Some SASE vendors that have ZTNA 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 master data management (MDM) 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/Mac and not Linux or mobile. Very few SASE vendors offer integrated user experience monitoring, even as an option.

Current State	*Description*
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

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 network security and the networking teams. For midsize enterprises, 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.** 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). Every enterprise has different requirements for compliance, and has privacy requirements for the inspection of data, storage of logs and routing of traffic. 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. Of the vendors converging on the SASE opportunity, CASB providers have the most experience in dealing with sensitive-data visibility and control. Even then, gaps remain — 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.

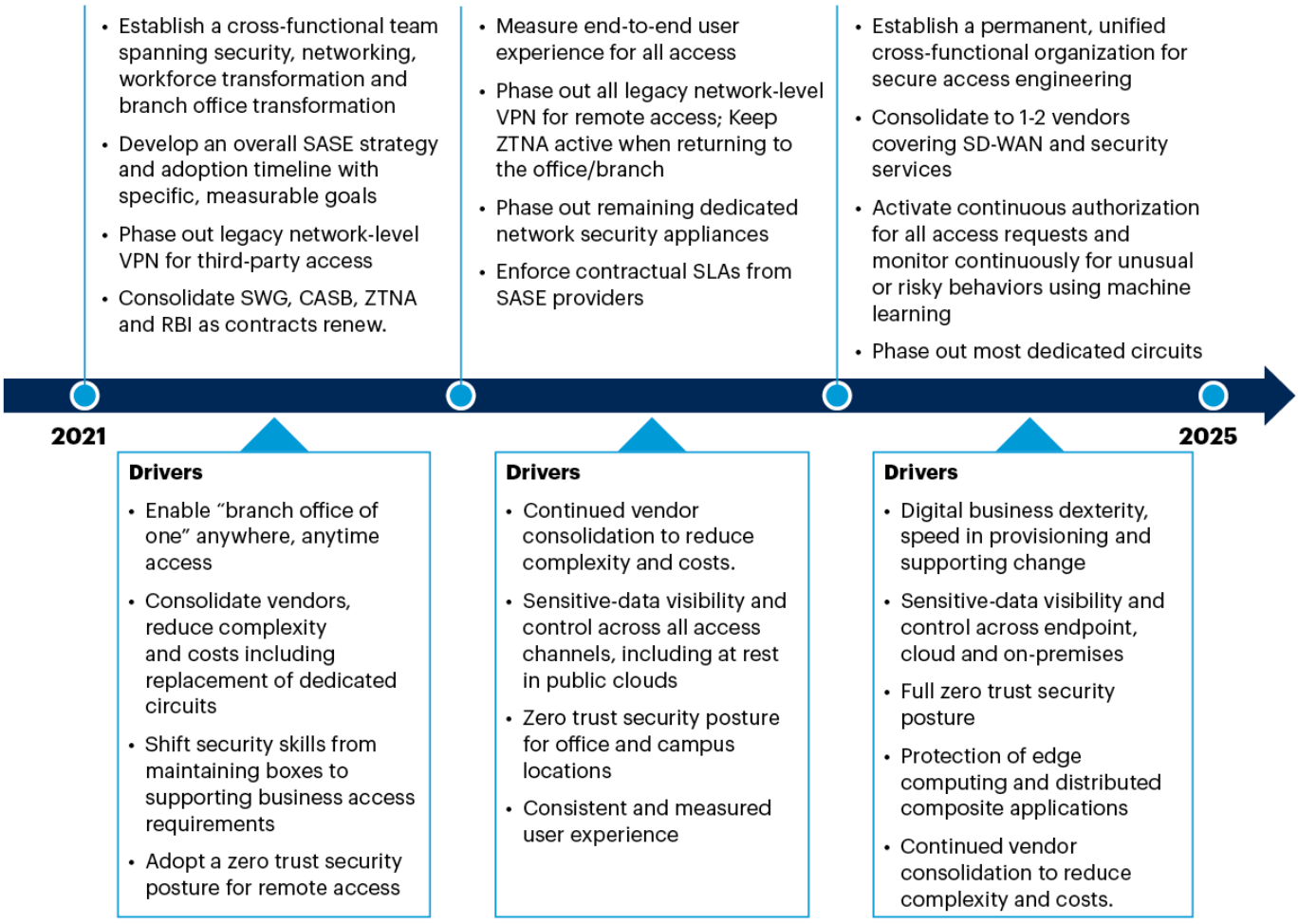
- **SASE security services capability maturity.** For the next several years, SASE capabilities will vary widely. Enterprises need to prioritize their needs for converged capabilities versus the need for continued best-of-breed capabilities until the gaps are closed. Some vendors positioning themselves as offering SASE to fill gaps with partnerships, but daisy chaining of services and/or network function virtualization to deliver this 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 2021, less than 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 security 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 bandwidth prioritization and content inspection.

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 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. The vast majority of enterprise SASE adoption will occur over several years, prioritizing areas of greatest opportunity in terms of cost savings, eliminating complexity and redundant vendors, and risk reduction through adoption of a zero trust secure posture (see Figure 4).

Figure 4. Strategic Roadmap Timeline for SASE Convergence

Roadmap Timeline for SASE Convergence



Timeline indicates when to begin.

Source: Gartner

741491_C

Gartner

Given this, 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 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 three- to five-year goal to replace 90% of legacy network-level VPN access with zero trust network access over the next five years. Adopt cloud-based ZTNA 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 three- to five-year goal to replace 90% of demilitarized zone (DMZ)-based services with ZTNA access over the next three years. 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 hardware to adopt SASE:
  - Where physical SWG, CASB and VPN appliances are used, we advise enterprises move off these appliances at the soonest refresh possible and shift to cloud offerings.
  - 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 two to verify the chosen SASE provider is still aligned with long-term business needs.
  - If a branch refresh occurs in 2021, accelerate deployment of ZTNA for managed devices in the branch and consider adoption of FWaaS.

- 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 security edge services (the right side of the cloud services in Figure 2 and Figure 3). Evaluate single vendor offerings, ideally including remote browser isolation capabilities:
  - Make sensitive-data discovery and protection a high-priority selection criteria 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 for SASE availability and latency performance.

- Midsize enterprises (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. If multiple vendors are used, require explicit partnerships with console integration and technical support.

Medium Priority

Over the next 18 to 36 months (note that the recommendations in this section may be accelerated to coincide with hardware refresh cycles and branch office transformation initiatives), enterprise 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/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 their end of life, and replace with cloud-based services.
- 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.

- 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.
    - Expand ZTNA to more use cases, such as cloud application access and IoT/OT access.
    - Use ZTNA agents on managed endpoints when in the branch.
    - 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 user experience monitoring.
- Implement a single agent for all access needs (ZTNA, SWG, SASE and CASB).

Lower Priority

At three to five years out, the SASE future strategic target state is achievable for most organizations — a unified strategic approach for branch, edge, campus, headquarters and remote access needs:

- The SASE migration plan should once again be revisited 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 Emerging Technologies: Applying SASE’s Architectural Model to Secure Distributed Composite Apps).
- Deliver against defined, measurable SASE goals that were committed to at the beginning. Specific examples include:

    - 90% of network-level VPN access eliminated
    - 95% of DMZ services eliminated for internal and third-party services
    - 80% reduction in dedicated MPLS circuit cost

- Adopt internet-only access as the default for most remote location use cases and continue with the phase out of MPLS. 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] The 2021 Gartner View From the Board of Directors Survey found that boards of directors are prioritizing digital technology initiatives as a response to the COVID-19 pandemic. When asked to indicate what kind of impact COVID-19 had on their digital business initiatives, the most frequently selected impact was an acceleration of digital business initiatives, with 69% of survey respondents selecting this (n = 260; see Survey Analysis: Board Directors Say Pandemic Drives Increased Investments in IT).

[2] Data was analyzed from Gartner conversations with end-user clients during the time period of 1 August 2019 through 31 December 2019, and compared to the same time period in 2020. This time period was used because the first research on SASE was published in July 2019. For 2021, the dataset analyzed covered 1 January 2021 through 31 January 2021. SASE inquiries are calculated as a percentage of the total number of end-user, security-related inquiries across these related topic areas: SASE, SWG, CASB, ZTNA, SD-WAN, WAF and FWaaS.

[3] In 2020, multiple acquisitions and announcements demonstrated vendor interest in building out complete SASE offerings:

- Barracuda acquired Fyde for ZTNA capabilities.

- Cisco acquired Portshift to extend its zero trust and identity-based segmentation strategies into cloud-native applications.
- Palo Alto Networks acquired SD-WAN vendor CloudGenix (see Magic Quadrant for WAN Edge Infrastructure).
- Fortinet acquired OPAQ for cloud-based security delivery and ZTNA capabilities.
- Check Point Software Technologies acquired Odo Security for ZTNA capabilities.
- McAfee acquired Light Point Security for RBI capabilities.
- Cloudflare acquired S2 Systems for RBI capabilities.
- Zscaler acquired Edgewise Networks to extend its zero trust networking policies into workloads and Cloudneeti to strengthen its API-based CASB, cloud security posture management (CSPM) and SaaS security posture management (SSPM) capabilities.
- VMware announced a two-pronged SASE strategy, partnering its VeloCloud SD-WAN offering with Zscaler for customers that use both, and an OEM of Menlo Security's software-based security stack to build out VMware's own SASE capabilities for customers wanting a single-vendor strategy.

Note 1. SASE Capabilities

Core SASE capabilities:

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

Recommended SASE capabilities:

- Remote browser isolation
- Network sandbox

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

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.

Note 3. More POPS, More Coverage

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