The Future of Network Security Is in the Cloud - Gartner

Published 30 August 2019 - ID G00441737 - 32 min read

Digital business transformation inverts network and security service design patterns, shifting the focal point to the identity of the user and/or device — not the data center. Security and risk management leaders need a converged cloud-delivered secure access service edge to address this shift.

Overview

Key Findings

- Network security architectures that place the enterprise data center at the center of connectivity requirements are an inhibitor to the dynamic access requirements of digital business.
- Digital business and edge computing have inverted access requirements, with more users, devices, applications, services and data located outside of an enterprise than inside.
- Complexity, latency and the need to decrypt and inspect encrypted traffic once will increase demand for consolidation of networking and security-as-a-service capabilities into a cloud-delivered secure access service edge (SASE, pronounced “sassy”).
- Inspecting and understanding data context will be required for applying a SASE policy.
- To provide low-latency access to users, devices and cloud services anywhere, enterprises need SASE offerings with a worldwide fabric of points of presence (POPs) and peering relationships.

Recommendations

Security and risk management leaders responsible for security of networks and endpoints should:

- Position the adoption of SASE as a digital business enabler in the name of speed and agility.
- Architect to move inspection engines to the sessions, not to reroute the sessions to the engines.
- Shift security staff from managing security boxes to delivering policy-based security services.
- Engage with network architects now to plan for SASE capabilities. Use software-defined WAN and MPLS offload projects as a catalyst to evaluate integrated network security services.
- Reduce complexity now on the network security side by moving to ideally one vendor for secure web gateway (SWG), cloud access security broker (CASB), DNS, zero trust network access (ZTNA), and remote browser isolation capabilities.

Strategic Planning Assumptions

By 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor up from less than 5% in 2019.

By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.

By 2025, at least one of the leading IaaS providers will offer a competitive suite of SASE capabilities.

Analysis

Network and network security architectures were designed for an era that is waning, and they are unable to effectively serve the dynamic secure access requirements of digital business. The enterprise data center is no longer the center of access requirements for users and devices. Digital business transformation efforts, the adoption of SaaS and other cloud-based services, and emerging edge computing platforms have turned the enterprise network "inside out," inverting historical patterns. Digital enterprises are characterized by:

- More user work performed off of the enterprise network than on the enterprise network
- More workloads running in IaaS than running in the enterprise data center
- More applications consumed via SaaS than consumed from enterprise infrastructure
- More sensitive data located outside of the enterprise data center in cloud services than inside
- More user traffic destined for public cloud services than to the enterprise data center
- More traffic from branch offices heading to public clouds than to the enterprise data center

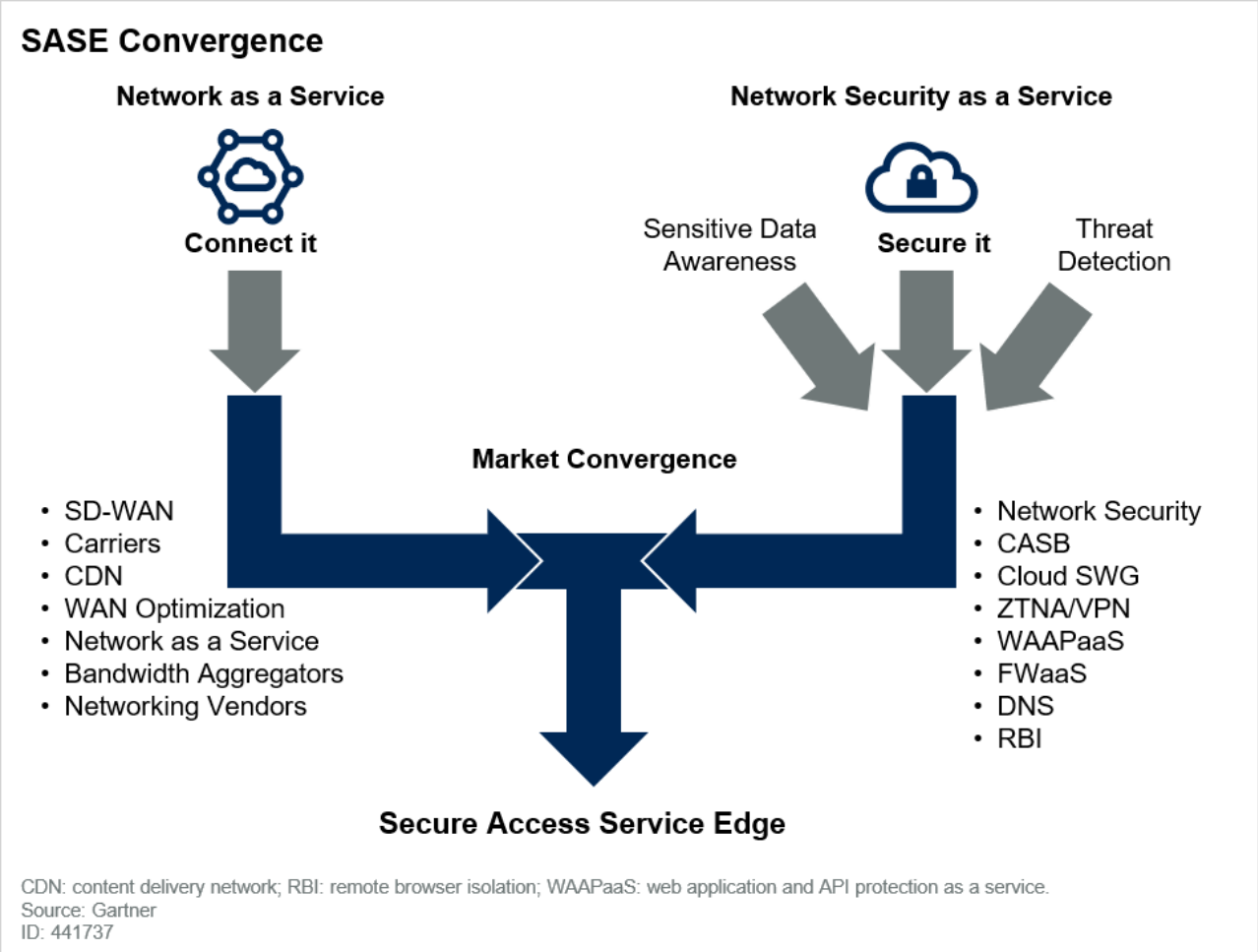
Digital business transformation requires anywhere, anytime access to applications and services — many of which are now located in the cloud. While the enterprise data center will continue to exist for years to come, the percentage of traffic destined to and from its remnants will continue to shrink.

The legacy "data center as the center of the universe" network and network security architecture is obsolete and has become an inhibitor to the needs of digital business.

The digital inversion of usage patterns will expand further with the growing enterprise need for edge computing capabilities that are distributed and closer to the systems and devices that require low latency access to local storage and compute, with 5G acting as a catalyst to accelerate edge computing adoption. (See "Exploring the Edge: 12 Frontiers of Edge Computing.")

The need to agilely support digital business transformation efforts while keeping the complexity manageable to support the inversion of access patterns will be the primary drivers for a new market. This market converges network (for example, software-defined WAN [SD-WAN]) and network security services (such as SWG, CASB and firewall as a service [FWaaS]). We refer to it as the secure access service edge (see Figure 1 and Note 1) and it is primarily delivered as a cloud-based service.

Figure 1. SASE Convergence



SASE offerings will provide policy-based “software defined” secure access from an infinitely tailorable network fabric in which enterprise security professionals can precisely specify the level of performance, reliability, security, and cost of every network session based on identity and context. The emergence of SASE will create a significant opportunity for security and risk professionals to securely enable the dynamic access requirements of digital transformation, providing secure access capabilities to a variety of distributed users, locations and cloud-based services. Enterprise demand for cloud-based SASE capabilities, and market competition and consolidation, will redefine enterprise network and network security architectures and reshape the competitive landscape.

The future of network security is in the cloud.

Definition*

The secure access service edge is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure access needs of digital enterprises.

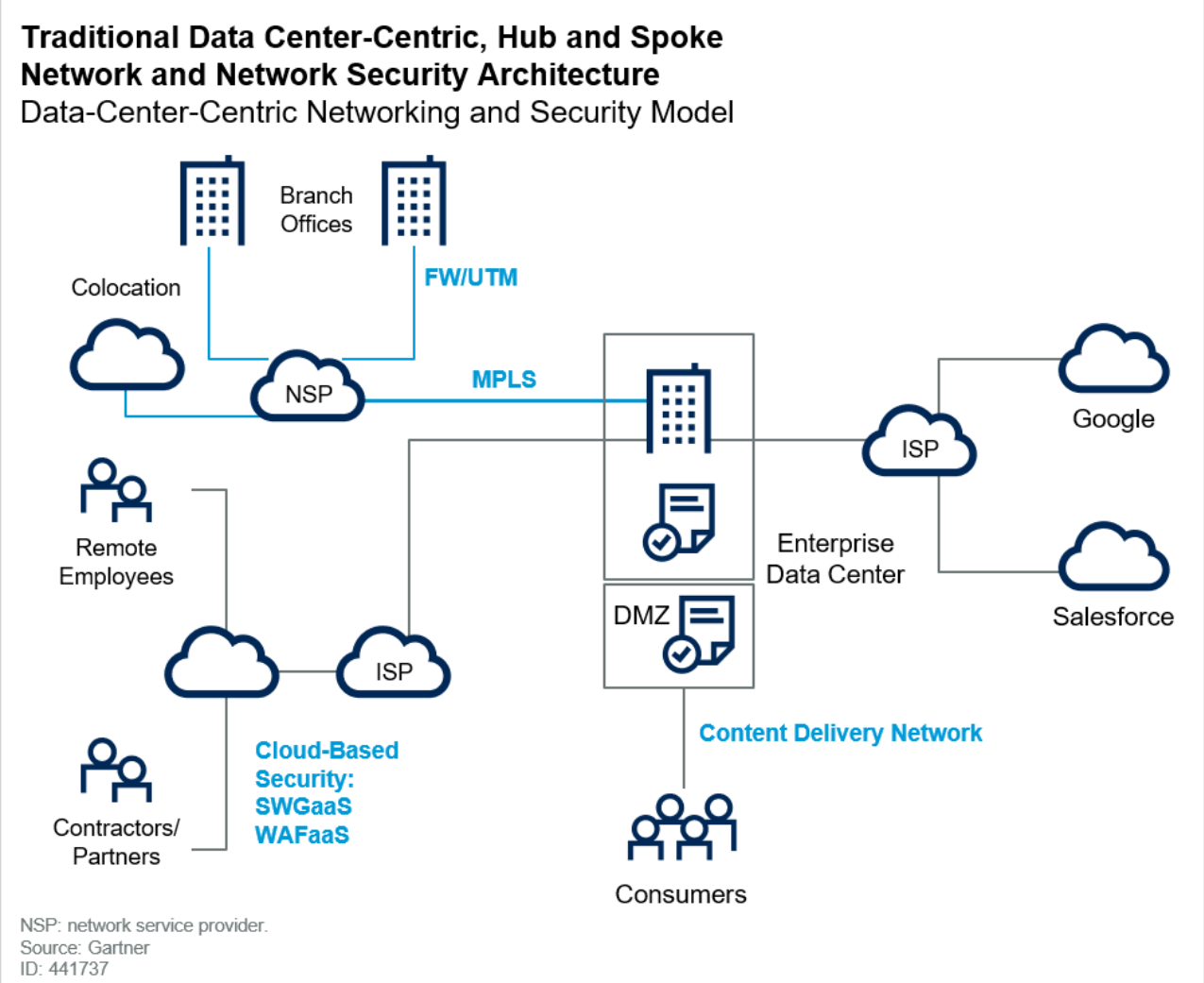
SASE capabilities are delivered as a service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions. Identities of entities can be associated with people, groups of people (branch offices), devices,

applications, services, IoT systems or edge computing locations (see “Zero Trust Is an Initial Step on the Roadmap to CARTA”).

Description*

Traditional enterprise network and network security architectures that place the enterprise data center as the focal point for access are increasingly ineffective and cumbersome in a world of cloud and mobile. Even with the adoption of some cloud-based services (such as cloud-based SWG, content delivery network [CDN], web application firewall [WAF] and others), the data center is still the center of most enterprise network and network security architectures (see Figure 2).

Figure 2. Traditional Data-Center-Centric, Hub-and-Spoke Network and Network Security Architecture



In a modern cloud-centric digital business, users, devices and the networked capabilities they require secure access to are everywhere. As a result, secure access services need to be everywhere as well. The data-centric model of Figure 1 won’t scale. Network gymnastics to route traffic to and from the enterprise data center make no sense when very little of what a user needs remains in the data center. Worse, we impact user productivity, user experience and costs by restricting access to SaaS only if a user

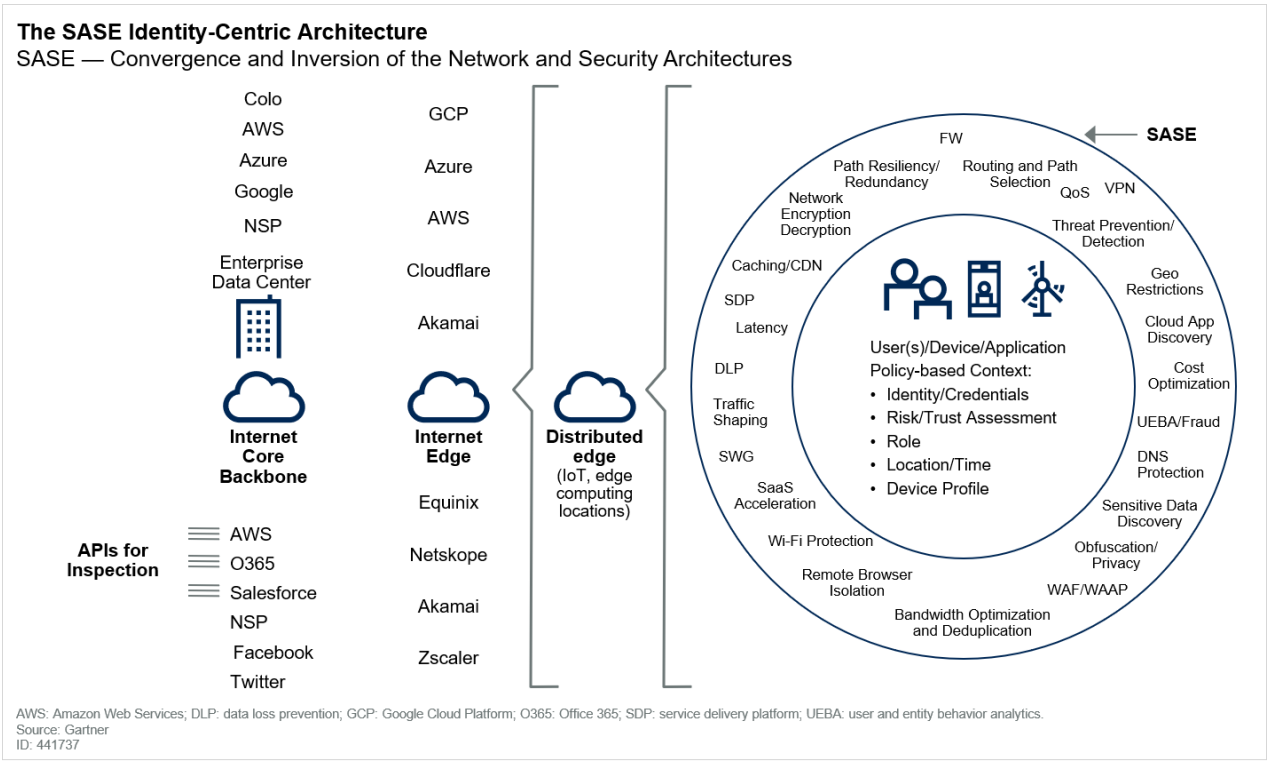
is on the enterprise network or has used a VPN, or requiring different agents for SWG, CASB and VPN, which creates agent bloat and user confusion. In other cases, branch-office traffic is forced through the data center for inspection when users access any cloud-based resource, increasing latency and the cost associated with dedicated MPLS circuits.

What security and risk professionals in a digital enterprise need is a worldwide fabric/mesh of network and network security capabilities that can be applied when and where needed to connect entities to the networked capabilities they need access to.

Instead of forcing (via "tromboning") various entities' traffic to inspection engines entombed in boxes in the data center, we need to invert our thinking to bring the inspection engines and algorithms closest to where the entities are located.

Whether we are connecting users to internal apps, cloud-based apps, SaaS, or the internet in general, these all present variations of the same secure access problem. A branch office is simply a place where multiple users are concentrated. Likewise, a salesperson in a car accessing Salesforce is a branch office of one. An IoT edge location is a branch office of devices. All of these are endpoint identities needing access to networked capabilities spread throughout the internet. In a digital business, secure access decisions must be centered on the identity of the entity at the source of the connection (user, device, branch office, IoT device, edge computing location and so on). As shown in Figure 3, identities are the new center for access decisions, not the data center.

Figure 3. The SASE Identity-Centric Architecture



The identity of the user/device/service is one of the most significant pieces of context that can be factored into the policy that is applied. However, there are other relevant sources of context that should

be available for input into policy application. These include the location of the identity, time of day, risk/trust assessment of the device the user is accessing from, and the sensitivity of the application and/or data being accessed. The enterprise data center is still there, but it is not the center of the architecture. It is just one of many of the internet-based services that users and devices will need access to.

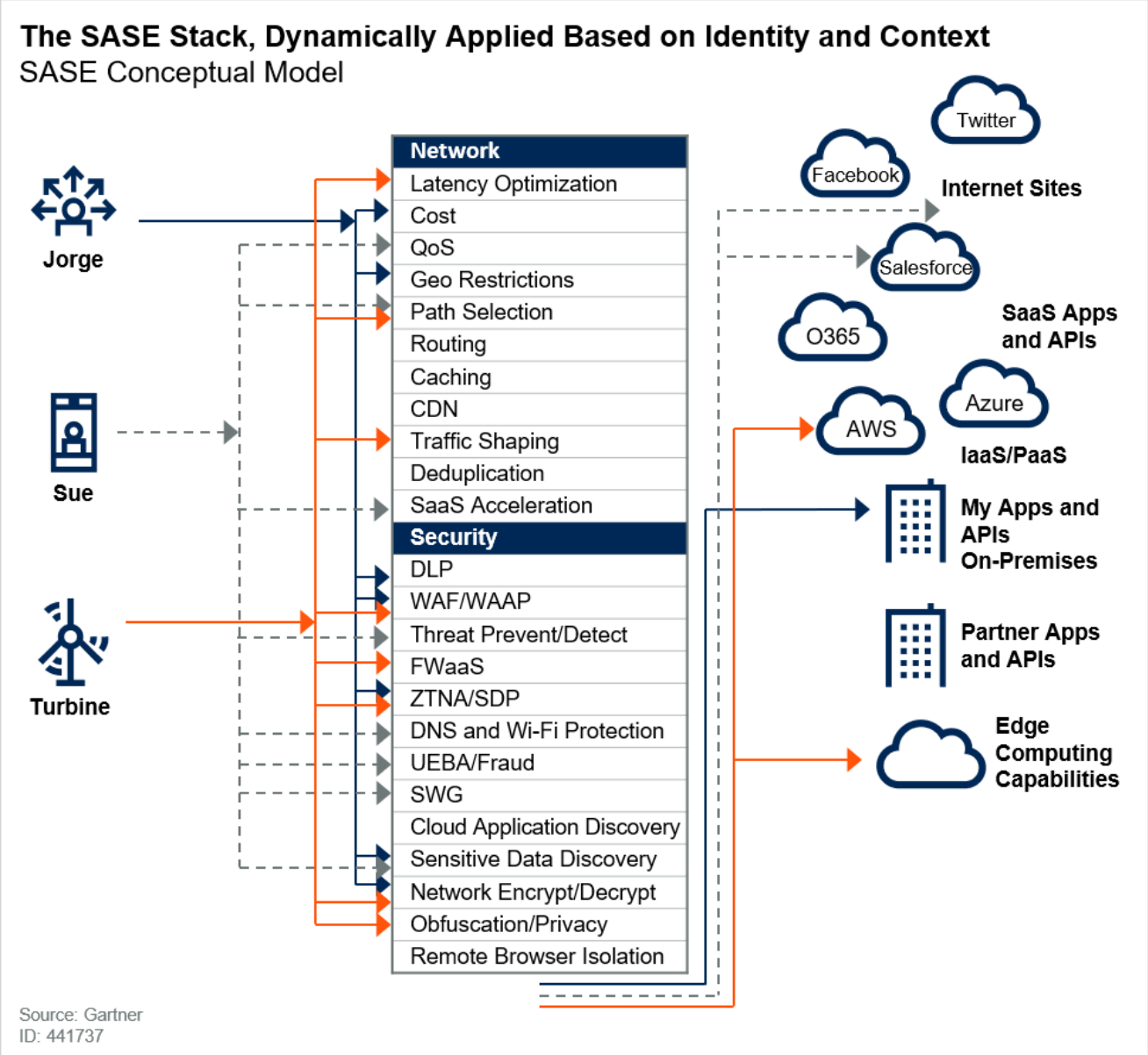
These entities need access to an ever-increasing number of cloud-based services, but how they are connected and the types of network security policies applied will vary based on regulatory requirements, enterprise policies and a given business leader's risk appetite. Much like an intelligent switchboard, identities are connected to networked capabilities via the SASE vendor's worldwide fabric of secure access capabilities.

Consider these scenarios:

- Sue, a salesperson, needs access to Salesforce CRM after hours from airport Wi-Fi on her managed device, while also browsing the internet. (SASE delivers a quality of service [QoS]-optimized and SaaS-accelerated connection to Salesforce with DLP, malware inspection, UEBA, and Wi-Fi protection. For internet browsing, SWG protection with DLP is provided.)
- Jorge, a contractor, needs access to an enterprise web-enabled app, hosted in an on-premises data center, from an unmanaged device. (SASE delivers ZTNA, restricts access to specific locations, protects the web-enabled application from attack with WAAP services, and monitors for sensitive data loss by inspecting the encrypted traffic stream.)
- A set of wind turbines needs edge-computing-based network and compute access for data analytics on sensor data, then needs to stream the results to AWS, but obscuring the location of the turbines. (SASE delivers low-latency ZTNA access for the turbines to edge computing resources, obfuscating their IP addresses and establishing a less-latency-sensitive, encrypted connection to AWS with API protection. The edge computing location is protected from inbound attacks via a SASE-provided FWaaS.)

SASE delivers the required services and policy enforcements on demand, independent of location of the entity requesting the service (left side of Figure 4) and the access to the capability (right side of Figure 4).

Figure 4. The SASE Stack, Dynamically Applied Based on Identity and Context



The result is the dynamic creation of a policy-based, secure access service edge, regardless of the location of the entities requesting the capabilities and regardless of the location of the networked capabilities they are requesting access to.

Instead of the security perimeter being entombed in a box at the data center edge, the perimeter is now everywhere an enterprise needs it to be — a dynamically created, policy-based secure access service edge.

Further, a given entity will need multiple simultaneous secure connections. For example, a user might simultaneously have:

- Connections to Office 365 that are not inspected, but routed with lowest latency

- A connection to Facebook where the chat sessions are inspected for sensitive data, but where latency is not a factor
- A connection to Salesforce where the session is monitored for sensitive data and malware
- A connection to an enterprise's private application in the data center that is monitored
- A connection to the user's personal internet banking application, which is not inspected

The enterprise perimeter is no longer a location; it is a set of dynamic edge capabilities delivered when needed as a service from the cloud.

Once again, these are all variations of the same underlying need for secure access. The difference is the real-time network and network security policy applied. Further, where applied by policy, the inspection capabilities applied will be consistent, regardless of what the entity is accessing; for example, inspecting content across all connections for sensitive data and malware. To reduce latency, SASE offerings should inspect using a "single pass" architecture where the traffic stream is opened up (potentially decrypted) and inspected one time using the multiple policy engines in parallel, ideally in-memory, without requiring chaining of inspection services.

Finally, emerging leaders in SASE will embrace the continuous adaptive risk and trust assessment (CARTA) strategic approach (see "Seven Imperatives to Adopt a CARTA Strategic Approach" and Note 2), ensuring that the session is monitored continuously. By remaining in the data path, the session can be analyzed for indications of excessive risk (such as compromised credentials or insider threat) using embedded UEBA capabilities. The SASE offering should be capable of adaptive responses as a user's behavior is analyzed and subsequent risk increases, or as device trust decreases (for example, requiring additional authentication from the user).

Benefits and Uses*

SASE will enable security teams to deliver a rich set of secure network security services in a consistent and integrated manner to support the needs of digital business transformation, edge computing and workforce mobility. The adoption of SASE should offer the following benefits:

- Reduction in complexity and costs. By consolidating secure access services from a single provider, the overall number of vendors will be reduced, the number of physical and/or virtual appliances in a branch will be reduced, and the number of agents required on an end-user device will be reduced. Costs should also be reduced over the longer term as more SASE services are adopted; savings will come from the consolidation of vendors and technology stacks.
- Enable new digital business scenarios. SASE services will enable enterprises to make their applications, services, APIs and data securely accessible to partners and contractors, without the bulk risk exposure of legacy VPN and legacy demilitarized zone (DMZ) architectures.
- Improvement in performance/latency. Leading SASE vendors will provide latency-optimized routing across worldwide points of presence. This is especially critical for latency-sensitive apps such as collaboration, video, VoIP, and web conferencing. Based on policy, users can be routed through the SASE provider's high-bandwidth backbones (and its peering partners).

- Ease of use/transparency for users. Implemented correctly, SASE will reduce the number of agents required on a device (or the amount of customer premises equipment [CPE] at a branch) to a single agent or device. It reduces agent and appliance bloat and should automatically apply access policy without requiring user interaction. This provides a consistent access experience for users, regardless of where the user is, what they are accessing and where it is located.
- Improved security. For SASE vendors that support content inspection (identification of sensitive data and malware), any access session can be inspected and the same set of policies applied. An example is scanning for sensitive data in Salesforce, Facebook and cloud-hosted applications all using a consistent policy that is applied consistently regardless of where the user/device is located.
- Low operational overhead. As threats evolve and new inspection mechanisms are needed, the enterprise is no longer limited by hardware capacity and multiyear hardware refresh rates to add new functionality. With cloud-based SASE offerings, updating for new threats and policies requires no new deployments of hardware or software by the enterprise and should allow quicker adoption of new capabilities.
- Enable zero trust network access. One of the principles of a zero trust networking approach is that network access is based on the identity of the user, the device and the application — not on the IP address or physical location of the device. (See "Zero Trust Is an Initial Step on the Roadmap to CARTA.") This shift to logically defined policies greatly simplifies policy management. SASE provides protection of the entity's session seamlessly and consistently on and off of the enterprise network. Further, assuming the network is hostile, SASE offerings will provide end-to-end encryption of the entire session and optional web application and API protection (WAAP) services (see "Defining Cloud Web Application and API Protection Services"). Leading SASE vendors will extend this all the way to the endpoint device with public Wi-Fi network protection (coffee shop, airport and so on) by tunneling to the nearest POP.
- Increased effectiveness of network and network security staff. Instead of the routine tasks of setting up infrastructure, network security professionals can focus on understanding business, regulatory, and application access requirements and mapping these to SASE capabilities.
- Centralized policy with local enforcement. SASE allows cloud-based centralized management of policy with distributed enforcement points logically close to the entity and including local decision making where needed; for example, local to a branch office using a CPE appliance. Another example is local agents on managed devices for local decision making.

Adoption Rate

SASE is in the early stages of development. Its evolution and demand are being driven by the needs of digital business transformation due to the adoption of SaaS and other cloud-based services accessed by increasingly distributed and mobile workforces, and to the adoption of edge computing. Early manifestations of SASE are in the form of SD-WAN vendors adding network security capabilities and cloud-based security vendors offering SWG, ZTNA and CASB services.

In the "Hype Cycle for Cloud Security, 2019," SASE was placed on the far left of the Hype Cycle at the post-trigger 20% position, with five to 10 years until the technology approach reaches mainstream.

Comprehensive SASE offerings are only now emerging, with adoption rates at less than 1%. However, the next three years will provide significant opportunities for enterprise security and risk management leaders to simplify their network security architectures.

While adoption of SASE will occur over the next several years, successful vendors will be easy to identify within three years, with several incumbents at risk of irrelevance.

Risks*

With the emergence and adoption of SASE, there will be risks that security and risk management professionals should consider:

- Siloed teams, culture and politics. Network and network security architectures are typically different siloed teams. Even in information security, the buyers for SWG, CASB and network security may be different. Different teams may fight the adoption of SASE as a matter of turf protection, or one team may attempt to control the SASE offering and block the participation of the other teams. To address this, SASE must be a CISO- and CIO-level cross-silo transformational value proposition in the name of speed, agility, and reduction of complexity.

- Good enough may not be good enough. Some SASE offerings will be developed and delivered by network-centric providers that are new to the security protection market. Likewise, security-centric providers may not have the full SD-WAN functionality expected of a leading WAN edge solution. This is an area where independent testing will play a critical role, with organizations like ICSA Labs and NSS Labs extending evaluations to cloud-based services.

- Complexity. For enterprises that attempt to build their own SASE stack out of disparate vendors and cloud offerings, stitching this together will lead to inconsistent management and enforcement, poor performance, and expensive deployments. A similar problem occurs if the SASE offering is stitched together by the vendor from multiple acquisitions and/or partnerships.

- Legacy vendors don’t have a cloud-native mindset. Hardware-centric network and network security vendors will have difficulty adjusting to cloud-native and cloud-based services delivery. Business models as well as salesforce and channel compensation will change. Vendors that previously sold dedicated hardware on-premises will likely follow a path of least resistance and deliver initial SASE offerings based on single-tenant architectures (virtual appliances dedicated for each customer).

- Network and firewall vendors have a lack of proxy expertise. Many of the capabilities of SASE will use a proxy model to get in the data path and secure the access. Legacy in-line network and enterprise firewall vendors lack the expertise to build distributed, in-line proxies at scale, risking higher costs and/or poor performance for SASE adopters.

- Investments required in POPs and peering relationships. SASE policy decision and enforcement capabilities need to be everywhere the endpoint identities will be located. For larger organizations supporting a mobile workforce and a distributed digital ecosystem, this means worldwide access. Smaller SASE providers won’t be able to sustain the investments necessary to be competitive, resulting in degraded performance. SASE offerings that use only the internet

backbone capacity of IaaS, but without local POPs/edge capabilities, risk latency, performance issues and resultant end-user dissatisfaction.

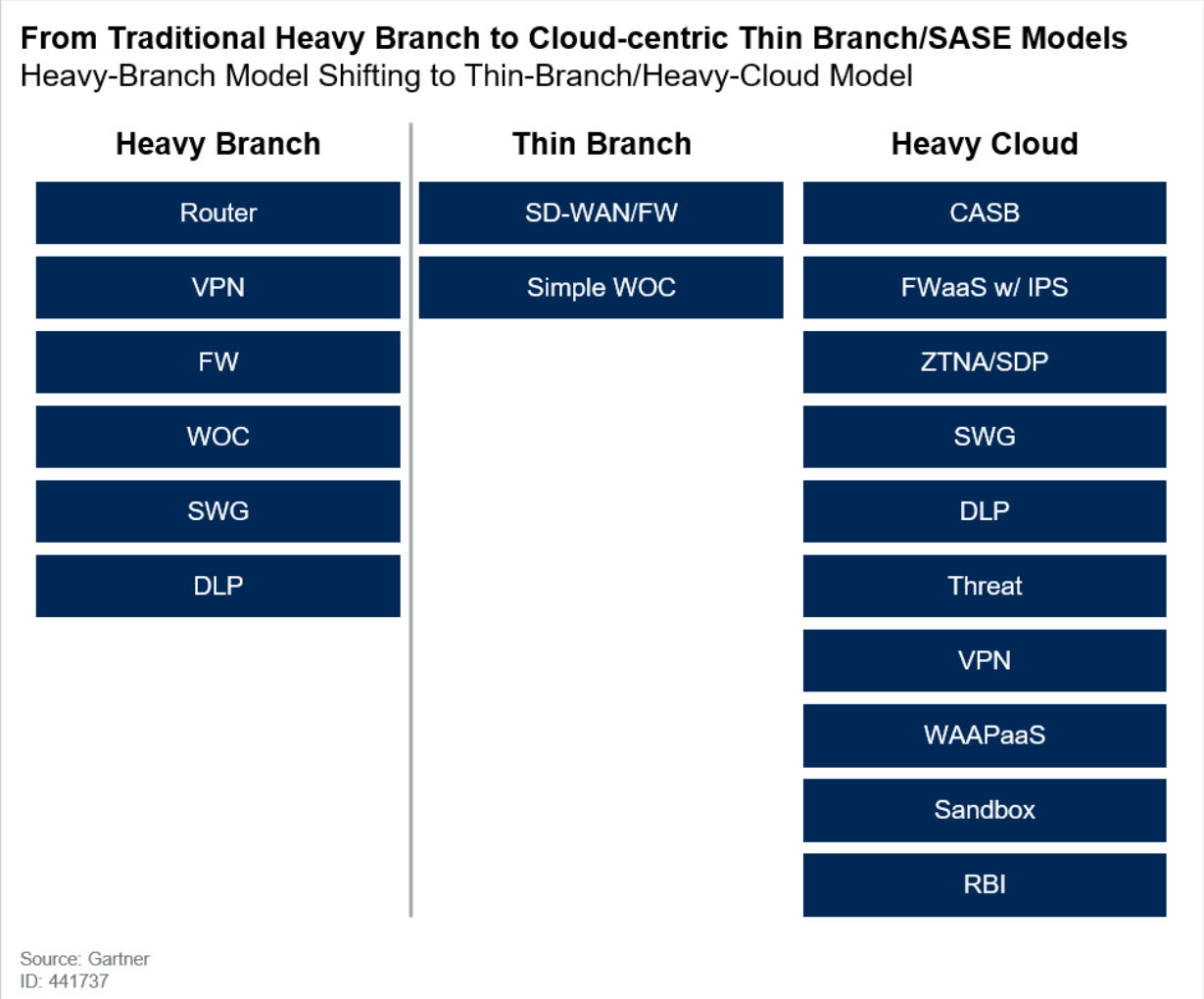
- Switching vendors. For some enterprises, the shift to SASE will require a switch in vendors and the resultant retraining of staff, development of new skills, and learning a new management and policy definition console.
- Lack of data context. Many network-focused vendors' solutions do not understand the context of the data — whether the content is sensitive or malicious. Data context is critical to setting policies on access, understanding and prioritizing risk, and adapting the access policies accordingly. Vendors that don't have this context will be limited in their capability to make rich context-aware adaptive SASE decisions.
- Investing in API inspection into leading cloud providers. Since many of the user-endpoint access decisions will be to connect to SaaS, SASE vendors will need understanding of data context. This data context can't be completely based on in-line inspection. In-line inspection misses partner uploads/shares and cloud-to-cloud content exchanges. API inspection is such a critical capability that it was a minimum requirement to appear in every CASB Magic Quadrant (see "Magic Quadrant for Cloud Access Security Brokers"). However, some SWG and network-focused providers do not yet have this expertise.
- Leading SASE offerings will require an agent. To integrate with forward-proxy-based architectures and to handle some legacy application protocols, a local agent will be required (for example, SWG, ZTNA for older applications, local Wi-Fi protection, and local device security posture assessment). Additionally, SASE vendors get much more device context using local agents. However, agents increase the complexity issues for enterprise SASE deployments if multiple agents have to be used to support access. Integration with existing endpoint protection platform (EPP) and unified endpoint management (UEM) agents will be needed for context. (See "The Long-Term Evolution of Endpoints Will Reshape Enterprise Security.") Further, if the SASE vendor has limited expertise in developing end-user device agents, stability and manageability may be an issue or platform support may be limited.
- Paying too much and SASE market turmoil. The SASE market will undergo significant changes over the next five years, with further consolidation and acquisitions expected. Because of the early stage of this market, we recommend one- to two-year contracts only with appropriate acquisition protection clauses. As the market consolidates and starts to favor the economies of scale for larger providers, the entire SASE market will experience downward pricing pressures. In addition, it will shift away from bandwidth-based models for WAN edge/SD-WAN to entity-based subscription models with pricing based on the types of inspection applied.

Evaluation Factors

When evaluating the specific SASE capabilities (SD-WAN, SWG, CASB, FW and so on), we have provided links to the corresponding Market Guides and Magic Quadrants in the Gartner Recommended Reading section. For the purposes of this research, we will focus on SASE-specific evaluation criteria:

- Breadth of SASE services offered. Not every vendor will deliver on every capability. Some vendors will start with networking-centric functionality, others will start with security-centric capabilities. Emerging SASE leaders should offer most or all of the services in Figure 3.
- Location of the SASE policy decision points. Most of the SASE decisions can and should be cloud-based using a cloud-based delivery and management model. However, some decisions should be local at the endpoint — in the agent for policy-based access (for devices) or in the physical/virtual appliance (in the case of QoS and path selection in the CPE at a branch office). However, these should be centrally managed from a cloud-based service. Leading SASE architectures will use a cloud-based policy decision engine that can be applied in cloud-based or local policy enforcement points using a CPE thin-branch/heavy-SASE cloud model (see Figure 5).

Figure 5. From Traditional Heavy Branch to Cloud-Centric Thin Branch/SASE Models



- Location of the SASE management/control plane. Even with local enforcement points in the form of agents and CPE, the SASE management console should be delivered as a cloud-based service. Policies should be cloud-managed and distributed to local enforcement points.

- Architecture. SASE architecture matters. Ideally, the offering is cloud-native, built on microservices with the ability to scale out as needed. To minimize latency, packets should be copied into memory, acted upon and forwarded/blocked, not passed from virtual machine (VM) to VM or from cloud to cloud. The software stack should have no specific hardware dependency and be instantiated when and where needed to deliver the risk-optimized and policy-based capabilities to the endpoint identity.

- On-premises CPE deployment options. Acknowledge and accept that an on-premises footprint (physical or virtual) is still needed — but using a cloud-based management and provisioning model. The design pattern should be turnkey black box — turn it on and forget it. As a part of the assessment, evaluate the vendor's architecture for secure birth-to-death life cycle provisioning updates and retirement of CPE. Some enterprises will prefer hardware for use as SASE CPE. The hardware should be commodity with an architecture for secure boot and secrets protection (such as encryption keys and certificates) that are not possible with a virtual appliance form factor.

- Tenancy model. Cloud-native SASE architectures will almost always be multitenant with multiple customers sharing the underlying data plane. Some providers will instead use a dedicated instance per customer. The enterprise customer may not know or care which is used, but the architecture may affect the SASE provider's ability to scale. Single tenancy typically results in lower densities with potentially higher costs that are passed on to enterprises. However, some enterprises prefer the stronger isolation of single-tenancy models.

- Location/number of POPs and peering relationships. With SASE, latency will matter for some applications. The SASE solution should offer distributed points of presence and a portfolio of traffic-peering relationships that align with the digital enterprise's access latency and data residency requirements. This is also critical for localized end-user experiences. Enterprise traffic should rarely traverse the public internet. Instead, the internet is used for a short hop to the SASE fabric, where it is then inspected based on policy and optimized for best performance using fast-path routing and peering arrangements. Further, SASE vendors must be able to show the ability to handle distributed denial of service (DDoS) attacks because the attack surface moves to the SASE vendor.

- Use of IaaS generic compute for non-latency-sensitive operations. Some SASE vendors will use a hybrid model with internet edge/POPs for low-latency in-line inspection and use commodity compute (CPU/GPU) and storage from IaaS providers for less-latency-sensitive operations such as network sandboxing, remote browser isolation, and audit log storage and analytics.

- Encrypted traffic inspection at scale. SASE offerings must be able to deliver in-line encrypted traffic inspection (decryption and subsequent re-encryption) at scale, ideally delivered from the cloud and without the use of proprietary hardware. This must support the latest versions of TLS.

- Single-pass scanning. A given session's traffic and embedded content should be opened and inspected once. Once decrypted, multiple scanning and policy engines can operate in parallel in a scale-out fashion, ideally without have to service chain inspection services. For example, content should be inspected once for both sensitive data and malware in a single pass.

- Traffic redirection, inspection and logging options. An increase in worldwide regulatory requirements on data privacy such as General Data Protection Regulation (GDPR) will create enterprise demand for SASE policy-based traffic handing for inspection, routing and logging to a specific geographic jurisdiction.
- Support for IoT/edge computing use cases. An IoT edge computing platform is just another endpoint identity to be supported with SASE. The key difference will be the assumption that the edge computing location will have intermittent connectivity and the risk of physical attacks on the system. Thus, the SASE architecture should support offline decision making (for example, caching access policies) with local protection of the data and secrets. Since IoT and edge devices may not support agents, a local SASE gateway/CPE may be required. Network access control for remote devices is a value-add.
- Threat protection. Examples include scanning of content in sessions for malware and content sandboxing. On public Wi-Fi networks, SASE solutions should offer DNS-based protection services and encryption of the session to local POPs to prevent eavesdropping. If content the user is handling represents risk, adaptive actions can be taken (for example, quarantining content or blocking downloads). More advanced threat protection should be available at additional cost (see Note 3).
- Ability to identify sensitive data and adapt. SASE offerings should understand the context of the data/applications that are being accessed and be able to take adaptive actions if excessive risk is detected; for example, block the upload/download of sensitive data. A critical evaluation criterion will be the richness in how sensitive data policies are defined. To understand sensitive data in clouds, the use of APIs to inspect data will be critical to understanding data context and to applying useful policies (such as encryption or watermarking) as data leaves the cloud.
- User privacy. SASE vendors should offer the option to not inspect traffic based on policy (for example, GDPR, Health Insurance Portability and Accountability Act [HIPAA] and similar personal privacy protection regulations). This noninspection policy may be combined with remote browser isolation to further isolate the session from enterprise systems and logging.
- Agents supported. End-user-facing endpoint devices will be a combination of Windows, Mac, and specific Linux distributions. Android- and iOS-based devices must be supported as well. Further, by using either the SASE vendor's agent or integration with a UEM provider, the SASE offering should be able to gather device context (e.g., health, status, odd behavior and so on) for improved secure access decision making (see "Magic Quadrant for Unified Endpoint Management Tools").
- Support for unmanaged devices. Enterprises can't always dictate the use of an agent, especially on systems they don't own or control. A lightweight mobile app or browser plug-in might be used for additional visibility (see "Market Guide for Mobile Threat Defense"). Or, unmanaged devices should be supported with a reverse proxy or by redirecting them through a remote browser isolation service (essentially creating a managed session where policy can be applied within an unmanaged endpoint).

- Granular visibility and detailed logging options. SASE offerings should provide granular activity monitoring of the user when accessing applications and services (and ideally bring this visibility to enterprise applications when protected with ZTNA). All activities within a session should be logged, requiring the SASE offering to create and manage distributed logs at scale, keeping logs of users and devices in the customer's preferred geography based on policy.
- Monitoring of behaviors during sessions. Following Gartner's CARTA strategic approach, SASE-brokered sessions should be continuously monitored for excessive risk and anomalies using embedded UEBA. If excessive risk is detected, the ability to raise an alert should be provided at a minimum. Integration with the enterprise security information and event management (SIEM) tool should be standard.
- Role-based management console and dashboard. Ultimately, the security architect, network operation manager or CISO may want to get a snapshot view of all secure access sessions. The SASE provider should offer a role-based, customizable risk dashboard/heat map for specific roles to gain visibility into overall network performance (for network operations) and cloud risk and security posture (for security operations).
- Licensing model. WAN edge/SD-WAN offerings are typically licensed by bandwidth. However, offerings such as CASB, SWG and remote browser isolation are licensed per user, per year. Since SASE converges both, SASE vendors will experiment with licensing models as bandwidth-based pricing is phased out. Most models will be subscriptions based on the number of entities protected — either individual entities (devices, users, apps, systems) or aggregation of entities (branch office/IoT and edge locations).

SASE Alternatives

- Status quo using a hardware-based branch office. This is the model that most enterprises today find constraining, due to changing access patterns and the rigidity and high cost of hardware-centric appliances with plug-in hardware blades for specific network security functions. Inspection is limited by local computing capacity and hardware refresh cycles and hardware-based form factors are inefficient in supporting the traffic patterns of the digital enterprise.
- Software-based branch office. By using a software-based blade approach to an on-premises branch CPE, a vendor with a set of partners could deliver many of the services in Figure 3. Alternatively, the CPE could call out to cloud-based services when and where needed (for example for security inspection). While a cloud-managed and cloud-delivered branch could deliver SASE, the branch office is just one type of edge service delivery problem to be addressed. Further, this approach still has the issue of multiple services, consoles and policies stitched together to build a complete portfolio.
- Build SASE yourself via service chaining. Some enterprises will attempt to stitch together their own SASE-like set of capabilities by service chaining the offerings from multiple disparate providers and using multiple endpoint agents. This approach risks unmanageable complexity, high costs and high latencies. Adoption of newer encryption standards such as TLS 1.3 will make service-chained inspection difficult.

- SD-WAN from one vendor, converged network security as a service from another. Another approach that some enterprises will adopt is to separate the “connect it” infrastructure from the “secure it” infrastructure shown in Figure 1, but move both to cloud-based services. This has the advantage of solving organizational politics, but with higher complexity and costs than if a single SASE provider was used.
- Provider-orchestrated service chaining. Another alternative for enterprises will be to turn to a dominant provider in networking, network security or a carrier and let the vendor perform the service chaining needed on behalf of the customer. Using service chaining and network function virtualization, the dominant provider can become the broker or general contractor responsible for stitching together the disparate services. The issue of multiple vendors’ management consoles, who manages and controls these consoles, and disparate policy frameworks complicates this strategy.

Recommendations*

SASE will be as disruptive to network and network security architectures as IaaS was to the architecture for data center design. SASE offers security and risk management professionals the opportunity to completely rethink and redesign network and network security architectures over the next decade. Digital business transformation, adoption of cloud-native computing and increasing adoption of edge computing platforms will require SASE. Even though SASE is just emerging, there are specific actions security and risk management professionals can take today:

- Get involved now with SD-WAN architecture and planning meetings. Use the opportunity to include network security services as a part of the architecture where possible:
    - Include network security providers in enterprise SD-WAN evaluations. For example, Barracuda, Cisco, Forcepoint and Fortinet are well known security vendors with competitive SD-WAN offerings (see “Magic Quadrant for WAN Edge Infrastructure”).
    - Require SASE vendors to provide evidence of third-party testing of SD-WAN capabilities and security capabilities, ideally using a known reputable and independent testing firm.
- Evaluate ZTNA as an immediate opportunity to adopt SASE solutions and to apply zero trust concepts (see “Market Guide for Zero Trust Network Access”). Start with specific digital-business-enabled projects such as precise identity and application-aware access for unmanaged devices used by partners or contractors.
- Evaluate the short-term opportunities for SASE service consolidation and complexity now; for example, partial or full consolidation across CASB, SWG, ZTNA, VPN and remote browser isolation capabilities as these contracts come up for renewal.
- Start requiring network security vendors to show a roadmap for SASE capabilities, including SD-WAN. Likewise, require SD-WAN vendors to start adding network security services. Require both to demonstrate existing and planned investments in POPs and peering relationships.
- Avoid SASE offerings that are stitched together. A large vendor may have all the individual SASE elements from acquisitions or partnerships. However, closely evaluate the integration of the

services and its ability to be orchestrated as a single experience from a single console and a single method for setting policy.

- Involve your CISO and lead network architect when evaluating offerings and roadmaps from incumbent and emerging vendors because the technology transition to SASE cuts across traditional organizational boundaries. Expect resistance from team members that are wedded to appliance-based deployments.
- Enter into short-term SASE contracts of one to two years maximum as licensing models are in flux. Favor SASE vendors that offer the simplicity of identity-/entity-based subscription licensing (not based on bandwidth) across all offerings.

Representative Providers

As the SASE market is emerging, there is no single vendor yet that offers the entire SASE portfolio, although several vendors have a majority of the necessary functionality. By year-end 2020, we expect several vendors will offer complete portfolios. Because this market crosses previously separate markets and involves the transformation of how capabilities are delivered, it is not possible to include a comprehensive list. Consequently, this list includes representative vendors across categories that we expect will compete to provide SASE:

- Akamai
- Cato Networks
- Cisco
- Cloudflare
- Forcepoint
- Fortinet
- McAfee
- Netskope
- Palo Alto Networks
- Proofpoint
- Symantec
- Versa
- VMware
- Zscaler

The major IaaS providers (AWS, Azure, and GCP) are not yet competitive in the SASE market. We expect at least one will move to address the majority of the market requirements for SASE shown in Figure 3 in the next five years as they all expand their edge-networking presence and security capabilities.

Note 1SASE Components

Core Components: SD-WAN, SWG, CASB, ZTNA and FWaaS, all with the ability to identify sensitive data/malware and all with the ability to encrypt/decrypt content at line speed, at scale with continuous monitoring of sessions for risk/trust levels.

Recommended Capabilities: Web application and API protection, remote browser isolation, recursive DNS, network sandbox, API-based access to SaaS for data context, and support for managed and unmanaged devices.

Optional Capabilities: Wi-Fi hot spot protection, network obfuscation/dispersion, legacy VPN, and edge computing protection (offline/cached protection).

Note 2CARTA

Continuous adaptive risk and trust assessment is a strategic framework for the evolution of information security, where the organization's cybersecurity posture is continuously adapted and risk-optimized to desired levels. This is achieved by the continuous assessment of all digital entities, their attributes, their configuration, their environment and their behaviors for relative levels of risk and trust in development and in production. When the risk is too high, or the trust is too low, security infrastructure (and the resultant security posture) adapts to achieve desired risk levels.

Note 3Advanced Threat Protection

More advanced threat protection solutions are expected from SASE vendors. One example is remote browser isolation. Another example is network privacy protection (also referred to as network privacy as a service) and traffic dispersion. The goal is to make it difficult to find enterprise systems by hiding the underlying IP addresses and optionally dispersing the traffic into multiple, differentially encrypted streams, making it significantly harder for an attacker to eavesdrop.

By Neil MacDonald, Lawrence Orans, Joe Skorupa

independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."