Gartner.

# Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge

**Published:** 29 July 2019 **ID:** G00388951

**Analyst(s):** Joe Skorupa, Neil MacDonald

The WAN edge and network security markets will converge into a single market during the next seven to 10 years, dramatically reshaping the competitive landscape. This research guides TSPs in transforming their companies to prosper in this rapidly evolving market.

## Key Findings

- Digital transformation and adoption of mobile, cloud and edge deployment models fundamentally change network traffic patterns, rendering existing network and security models obsolete.
- Customer demands for simplicity, scalability, flexibility, low latency and pervasive security force convergence of the WAN edge and network security markets, creating the secure access service edge (SASE), *with a predominantly cloud-based, as-a-service delivery model*.
- Many emerging edge applications are latency-sensitive, requiring networking and security delivered in a distributed manner close to the endpoint device or user access. This requires a cloud-delivery-based approach, favoring providers with many points of presence (POPs).
- The winners and losers in SASE will be determined during the next three years. Networking and security vendors that fail to aggressively embrace this transition will lose influence with buyers and will find themselves relegated to market niches with limited prospects.

## Recommendations

To succeed in this market, technology and service providers (TSPs):

- Transform your offerings to a cloud-native architecture to deliver a broad set of integrated networking and security services, ideally via “single-pass” inspection.
- Transform your business models into an end-to-end, “cloud-native as-a-service” offering to best fit the emerging SASE market requirements.

- Develop and deliver to the market a clear vision of how your architectural approach and offering enables buyers to rapidly adapt their networking capabilities as their business needs change.
- Fill out your portfolio organically with the fewest acquisitions possible to minimize integration challenges and inconsistencies across services.
- Invest in distributed POPs, leveraging colocation facilities, service provider POPs and IaaS where appropriate, to place services as close to the entity access as required.

## Table of Contents

Introduction.......................................................2
Market Trend.......................................................4
To Continue to Grow in This Rapidly Evolving Market, Vendors Must Enhance Their Product Portfolio and Transform Their Delivery Model.......................................................4
New Application Deployment Models Are Forcing New Network and Security Models................4
SASE Adoption Will Be Delivered Primarily as an XaaS Offering, Obsoleting Device-Centric and Traditional CSP Offerings and Business Models.......................................................6
Emergence of SASE Will Force Vendors to Transform Their Business Models............................9
SASE Will Force Vendors to Rethink Their Technology Acquisition Strategies...........................11
Vendors to Watch.......................................................12
Gartner Recommended Reading.......................................................15

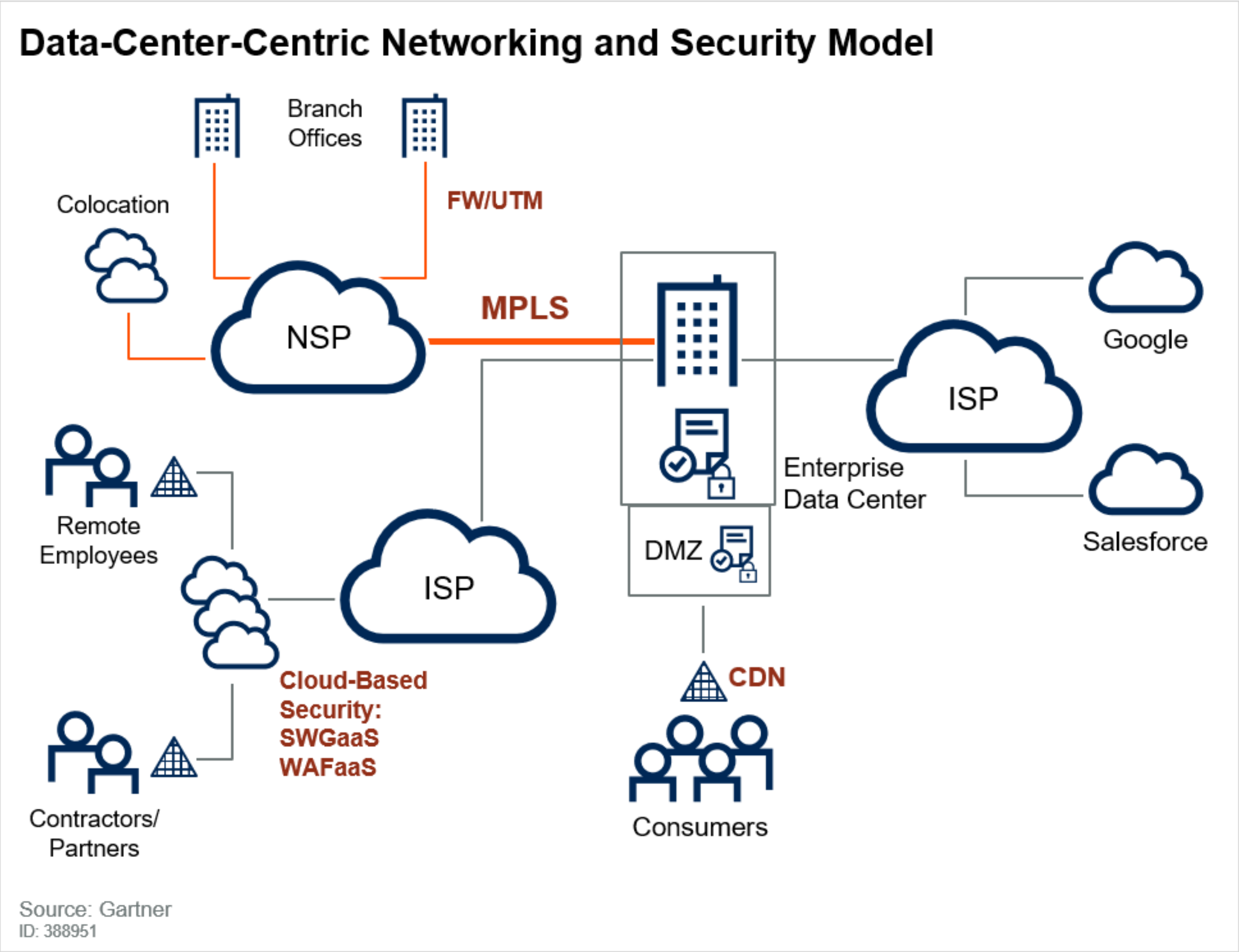
## List of Figures

Figure 1. Data-Center-Centric Networking and Security Model.......................................................3
Figure 2. SASE — Convergence and Inversion of the Network and Security Architectures......................5
Figure 3. Heavy-Branch Model Shifting to Thin-Branch/Heavy-Cloud Model..........................................7
Figure 4. SASE Conceptual Model.......................................................11

## Introduction

Networking and network security have coexisted as adjacent markets with minor overlap in the branch-office router/firewall/VPN space. While some large vendors offer products in both spaces, buying decisions were separate, with networking devices and security devices often procured from different vendors. The result was a complex hub-and-spoke network architecture, with the data center at the center (see Figure 1).

Figure 1. Data-Center-Centric Networking and Security Model



Source: Gartner
ID: 388951

However, the requirements of digital business and edge computing are inverting traditional traffic patterns, fundamentally transforming this model and forcing a convergence of the WAN edge and network security markets into the SASE (pronounced sassy). SASE typically combines products and services to delivery multiple capabilities such as SD-WAN, WOC, SWG, CASB, NGFW and ZTNA/SDP (see Note 1).

> While this transition will occur during the next five to 10 years, the long-term winners in the SASE market will be determined before 2022. Gartner believe that a number of vendors will announce and deliver early SASE offerings in 2H19.[1]

Market convergence is already underway as Gartner clients increasingly are linking WAN transformation and security refresh/transformation projects.[2] SD-WAN providers include multiple vendors that are network-security-focused, including Cato Networks, Fortinet, Forcepoint, Juniper Networks and Versa Networks. SD-WAN vendors that lack a cloud-delivered security have partnerships with Zscaler, Palo Alto Networks and others.

## Market Trend

### To Continue to Grow in This Rapidly Evolving Market, Vendors Must Enhance Their Product Portfolio and Transform Their Delivery Model

#### New Application Deployment Models Are Forcing New Network and Security Models

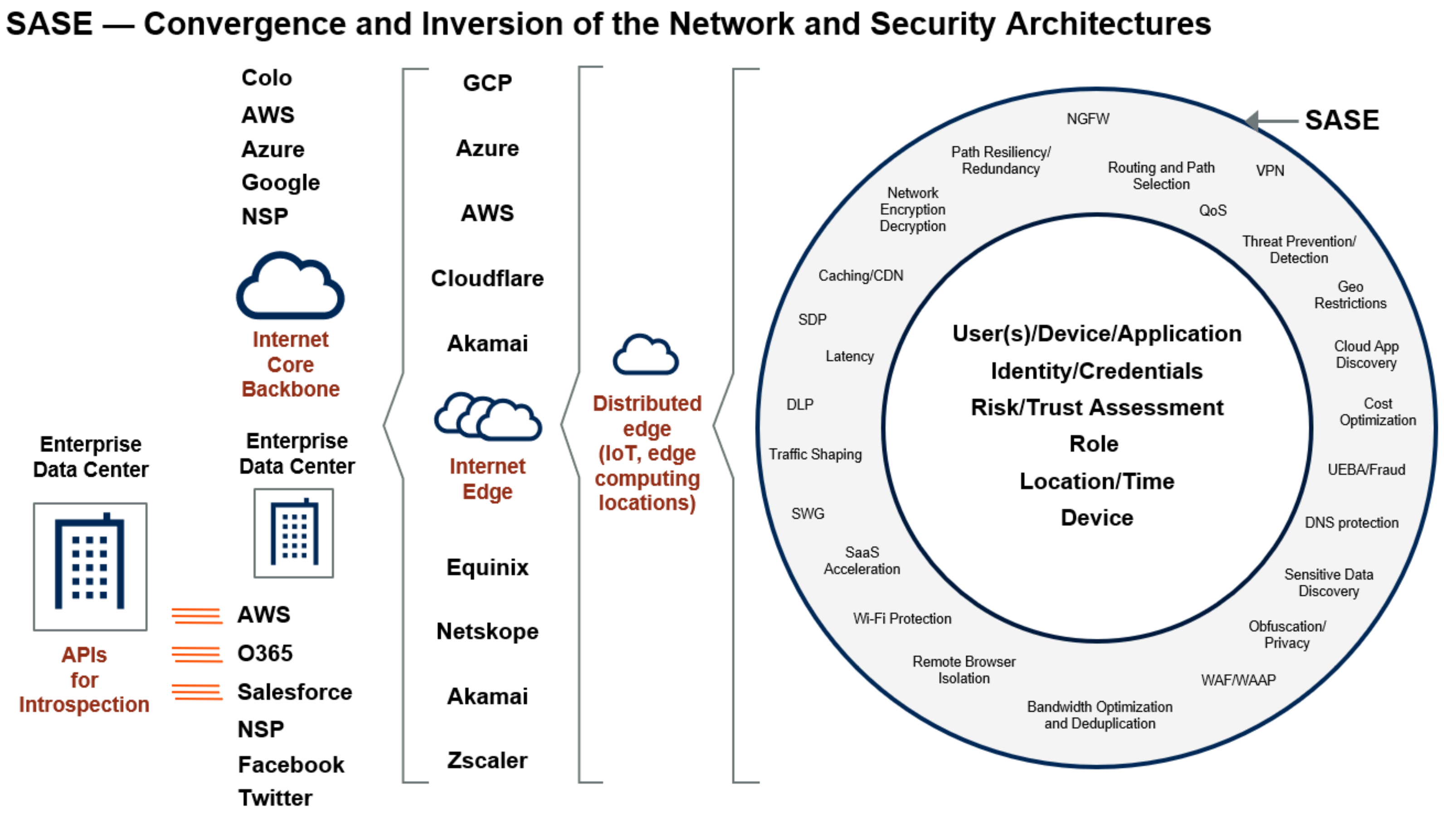
Digital transformation is driving new application deployment models, including cloud, edge and mobile. As organizations adopt these new deployments models, endpoints (users, programs and devices) no longer access a majority of applications and services from within the enterprise data center. [3]

> Instead of a data-center-focused hub-and-spoke model, traffic patterns are now becoming endpoint/entity-centric hub-and-spoke topologies. The endpoint is the individual user or device, or application represented by a single identity. The spokes are threads of secure access, established based on policy delivered from the provider's distributed mesh/fabric of network and security capabilities.

The traditional branch location is a proxy/aggregator for the device-centric hub described above.

The inversion is forcing companies to fundamentally change their network and security architectures from a data-center-centric model to an endpoint/entity/identity-centric model (see Figure 2).

Figure 2. SASE — Convergence and Inversion of the Network and Security Architectures



Source: Gartner
ID: 388951

## SASE Adoption Will Be Delivered Primarily as an XaaS Offering, Obsoleting Device-Centric and Traditional CSP Offerings and Business Models

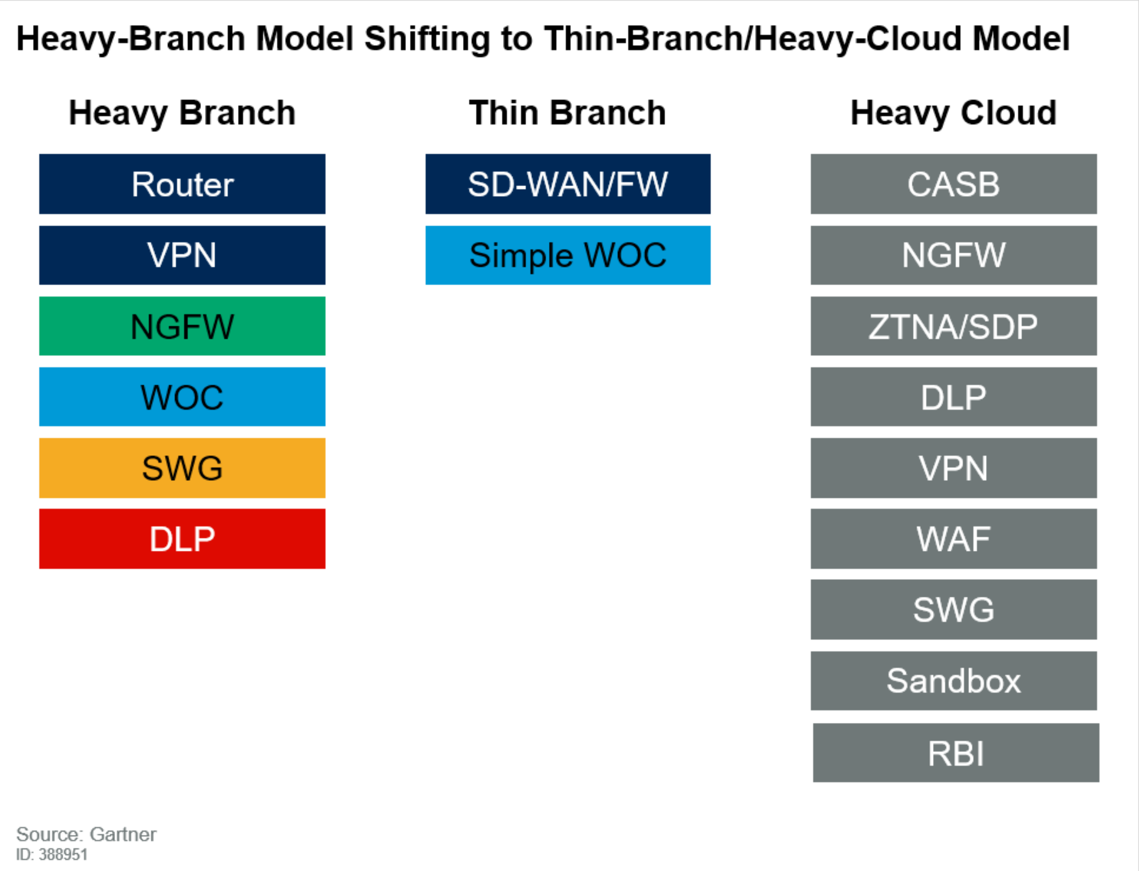
In this new model, a branch office is just another endpoint — a collection of individual users concentrated to leverage shared infrastructure and services such as redundancy and QoS. Likewise, a distributed edge computing location (such as one supporting a distributed local analytics application for a set of IoT devices) is also an endpoint needing secure access edge services when connecting to public clouds for data aggregation. A cloud-based delivery enables vendors to add new services to the stack or add more compute power to the stack dynamically.

> Vendors that are tied to an appliance-focused delivery model or a traditional CSP model will find it difficult to compete against more agile, service-rich providers.

### Endpoint Deployment Options and Drivers

Traditional branch office networking and security deployments have followed a “heavy branch” model, wherein each branch office deployed all, or nearly all, of the networking and security services that might be needed. For a branch with direct internet access, the stack might include a router, WOC, IDS/IPS, and SWG/sandbox. This resulted in a stack of appliances from multiple vendors, each with its own price, operational model, software upgrade cycle, hardware upgrade cycle and scalability (see Figure 3). This also resulted in a complex, inflexible, expensive and difficult to operate environment. Policy enforcement points were distributed across all branches, making it difficult to keep all endpoints consistent and up to date.

Figure 3. Heavy-Branch Model Shifting to Thin-Branch/Heavy-Cloud Model


Heavy-Branch Model Shifting to Thin-Branch/Heavy-Cloud Model

Source: Gartner
ID: 388951

As traffic patterns shift due to new application deployment models and as mobile/temporary endpoints became common, forward-leaning organizations have shifted to a light-branch/heavy-cloud approach. This is where endpoints (branch offices or individual user devices) deploy only the minimum required functions locally and the rest are cloud-based[3] (as shown in Figure 3).

Advantages of this approach include:

- Endpoint functions are limited (such as routing, path selection, QoS and L4 firewall), resulting in reduced capex and opex. The rest are delivered as a service from the cloud.
- The functions can be delivered via software appliances without requiring dedicated hardware because of the thinner stack. If hardware is requested, commodity hardware can be used.

- New endpoints, such as pop-up stores can be quickly and cost-effectively brought online.
- Branch offices and individual devices can share common policies and policy enforcement points.
- The infrastructure managed directly by the enterprise is simpler and less expensive.
- The policies managed by the enterprise are more consistent and managed via a cloud-based console, as-a-service offering from a single vendor.
- Latency-sensitive applications such as IoT edge to edge can be supported, even when the endpoints have minimal local resources.
- Cloud-native services such as more complex policy-based inspection for sensitive data, including malware, decryption and overall management, is performed in the SASE, which can easily scale up or down, as needed, when and where needed.
- Organizations can more quickly adopt new technological innovations via OTT cloud-delivered services, particularly to address the ever-evolving cybersecurity threat landscape.

Anywhere, anytime, high-performance delivery of secure access capabilities is the requirement. Enterprise buyers will favor a cloud-delivered SASE suite of dynamically linked services. This is because these services are invoked and billed on demand to match the secure access needs of the endpoint/entity and the policies of the enterprise, whether it is a human or a device. If the endpoint/entity supports a local agent, location-dependent services, such as path selection, and QoS decisions can be made locally via the agent (or, in the case of a branch office, a local SASE edge appliance).

In many cases, branch office SASE adoption will be driven by network and network security equipment refresh cycles and associated MPLS offload projects. However, other use cases will drive earlier adoption.

Vendors should identify use cases where SASE capabilities will drive measurable business value. Mobile workforce enablement, contractor access and edge computing applications that are latency-sensitive are three likely opportunities.

## Emergence of SASE Will Force Vendors to Transform Their Business Models

The shift to SASE architectures obsoletes legacy security and networking business models.

> To remain competitive, vendors will have to deliver an integrated, cloud-native set of services that can be delivered on demand, based on context and policy.

This will force vendors to transform their product portfolios and will drive acquisitions that result in consolidation across these previously adjacent, but distinct, markets.

The move to an on-demand service delivery model will force vendors to accelerate their move to SaaS-like, consumption-based billing models. The required adaptation will be determined by the vendor's place in the market.

- For traditional on-premises product providers, building a cloud-based delivery offering can be challenging. They need to retain existing customers and the margin-rich maintenance revenue streams that they provide. Introduction of a cloud-based model requires balancing the resources and focus needed to maintain the existing business, and building a new cloud-based one (see "Tech Go-to-Market: Four Crucial Product Management Steps to Transition Offerings to SaaS"). Understanding and mitigating potential adverse reactions from the sales channel is also critical, as the cloud delivery model can be seen as undercutting these partners.
- Existing OTT providers (security and CDN, for example) will have to add missing on-premises capabilities, which may force them into delivering and supporting on-premises hardware. Additionally, some have partnerships with SD-WAN providers that will undoubtedly view this incursion as a threat.
- Traditional CSPs are betting that the heavy-branch approach delivered via provider-managed universal CPE will reestablish account control, and deliver much needed margin and revenue growth. SASE is an existential threat to this strategy as CSPs will lack the ability to effectively compete with OTT SASE providers. This mirrors the loss of control CSPs have experienced with the introduction of OTT-delivered SD-WAN services.

Traditional appliance/bandwidth pricing models will not survive. Plentiful, cost-effective bandwidth means that small sites will have network links that map into midrange appliances costing more than $10,000. This issue favors a thin-branch/heavy-cloud delivery model since it allows for low-cost CPE that can deliver limited capabilities at very high throughput. Possible licensing alternatives include per user/identity or aggregate consumption across all sites/users. Further, we expect that some vendors will bundle hardware costs into the monthly service subscription and treat the CPE as part of the service, managed from the cloud — much like a cable TV set-top box.

### SASE Conceptual Model

With SASE, services are applied as needed on a per-endpoint-to-resource interaction basis, taking into consideration the context of the access request and the enterprise policy for protection (for example, inspecting for sensitive data). Endpoints serviced by SASE have an identity and can be people, groups of people (branch office), things (IoT devices and edge devices) or applications. Risk/trust, role, location, time and device are used to determine which services are needed (see Figure 4).

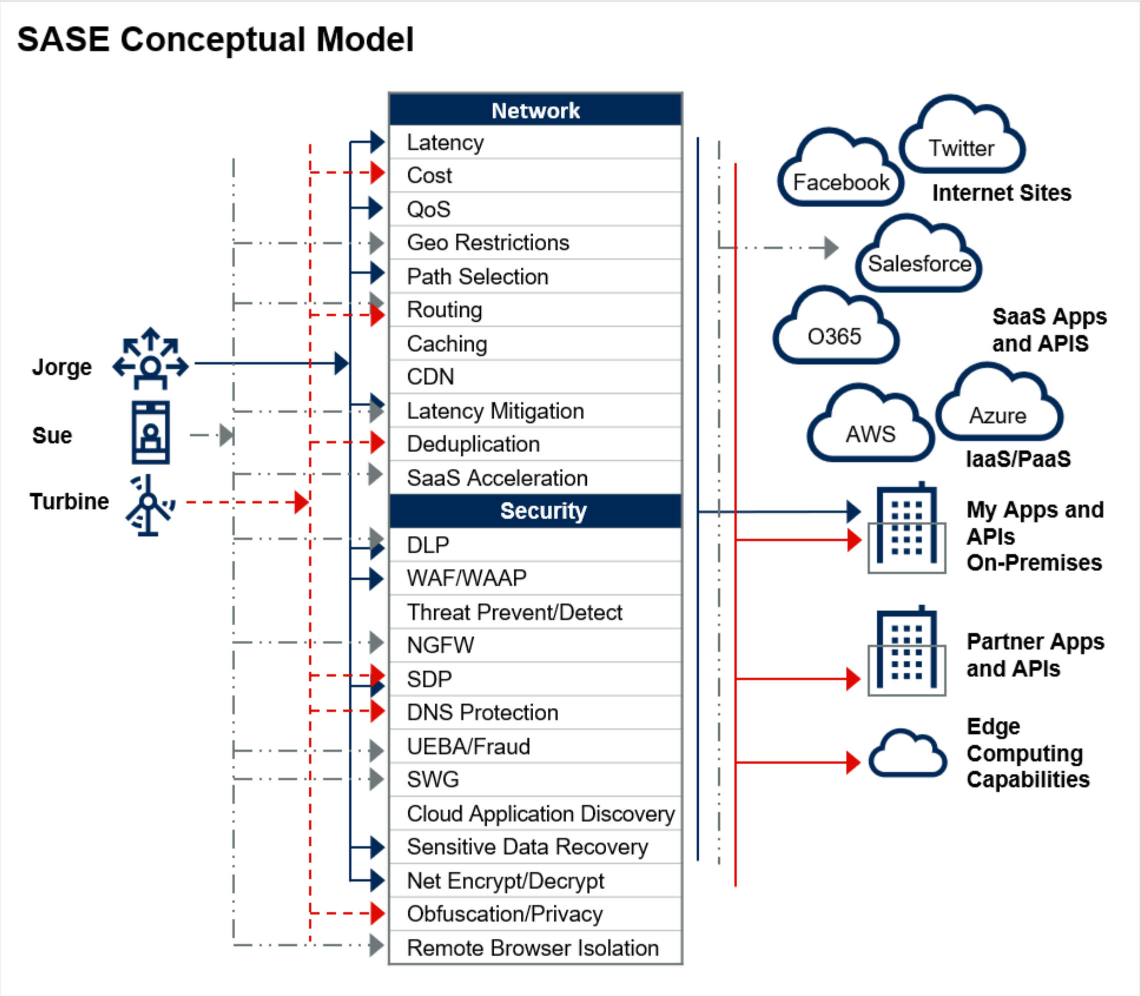
> Once the identity is authenticated, the result is much like a policy-based switchboard, connecting endpoint identities to services and applications securely and within desired performance levels from the services available in the SASE provider's fabric.

Consider these scenarios:

- Sue, in accounting, needs access to Salesforce CRM after hours from airport Wi-Fi on her managed device.
- Jorge, a contractor, needs access to an enterprise web-enabled app, hosted in an on-premises data center, from an unmanaged device.
- A set of wind turbines needs local network and compute access for data analytics on sensor data, then stream the results to AWS, but obscuring the location of the turbines.

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

Figure 4. SASE Conceptual Model



Source: Gartner
ID: 388951

## SASE Will Force Vendors to Rethink Their Technology Acquisition Strategies

A full SASE implementation requires a broad technology portfolio and few, if any, vendors can deliver the entire solution today. To remain competitive, vendors will have to deliver an integrated, cloud-native set of services that can be delivered on demand, based on context and policy. Organic development will be too slow and expensive for many companies, and partnerships involve the risk that the partner will be acquired by a competitor.

> This will drive a new wave of acquisitions that result in consolidation across these previously adjacent, but distinct, markets.

Some vendors will attempt to satisfy buyers' needs by stitching together a number of separate products or by acquiring a number of appliance-based point products that are then cloud-hosted and stitched together in a service chain. However, inconsistent policies across service elements will result due to inconsistencies in features, performance and management models.

This approach will also result in higher latency offerings, with greater capex and opex. Additionally, appliance-based products have functional and performance limitations, and cannot be adapted on demand. To avoid these problems, vendors will be well served by pursuing a very small number of acquisitions to minimize feature inconsistency and integration challenges.

Additionally, service chaining multiple VMs is very resource-intensive, which makes them expensive to host and operate, and limits scalability. Appliance-focused vendors may choose to deploy a heavy-branch, on-premises delivery model, but this will limit scalability (up and down) and will increase total cost of ownership. If the deployments are limited to public cloud IaaS provider data centers or colocation facilities, latency will be even worse. Dedicated internet edge processing capabilities will be a requirement from many enterprises.

### Advantages of a Single-Pass, Cloud-Native Approach

To deliver maximum flexibility with the lowest latency and resource requirements, a cloud-native single-pass architecture is advantageous. When considering the use cases in Figure 4, a well-designed implementation will perform the majority of services in parallel (single pass), ideally in the same cloud-service stack, at the same location, at the same time. The need to open, parse, and reencrypt and forward traffic should happen only once. This avoids expensive, high-latency packet copying and service inconsistency. Gartner is aware of multiple vendors that are pursuing the single-pass approach using modern cloud-native technologies such as scale-out via microservices and containers.

## Vendors to Watch

Because this market trend crosses previously separate markets and involves transformation of how capabilities are delivered, it is not possible to include a comprehensive list. Consequently, the information includes representative vendors across categories:

- Akamai is a global CDN provider that also provides cloud-delivered WAF, DDoS protection, DNS and bot mitigation, and ZTNA/SDP across multiple hundreds of POPs.

- AWS is a leading provider of IaaS/PaaS services that include networking and security, with presence in most major markets. However, its distributed edge locations don't support generic compute, only CDN, WAF, DDoS protection and Lambda at edge services.

- Cisco is a longtime provider of a broad set of networking (WAN edge and core switching) and security (NGFW, VPN, device authentication, SWG and CASB capabilities), some homegrown and many through acquisitions. Its cloud-based network security service platform, including its secure internet gateway, offers an increasing set of SASE-related services.

- Cato Networks offers secure SD-WAN, NGFWaaS and a ZTNA solution.

- Fortinet is a rapidly growing presence in the enterprise NGFW/UTM market, with credible WAN edge (SD-WAN and WAN optimization) capabilities.

- Forcepoint has many of the building blocks of SASE, including SWG, CASB, NGFWaaS, WAN edge and DLP.

- McAfee offers a broad set of security capabilities, including CASB, DLP and SWG, and is investing in its POPs for cloud-based delivery.

- Microsoft offers a rich set of security capabilities under the Microsoft Cloud App Security and Azure Security Center brands (including the Azure-centric distributed firewall), along with global network backbone services (Azure WAN).

- Netskope is a leading provider of cloud-delivered CASB and DLP, and also offers SWG and malware protection, with a rapidly expanding worldwide POP footprint. In June, it announced its ZTNA/SDP offering.

- Palo Alto Networks is a leading NGFW provider that also offers firewall as a service (built on AWS and Google Cloud Platform), behavioral analytics, threat intelligence and basic CASB capabilities.

- Symantec has a combination of SWG, CASB, remote browser, ZTNA/SDP from a large number of its own data centers and distributed POPs, and a Fortinet-based offering to deliver NGFWaaS capabilities.

- Versa offers a secure SD-WAN solution, uniting SD-WAN and NGFWaaS.

- VMware has a broad set of virtualization offerings, with an increasing emphasis on networking (WAN edge) and security with NSX and its service-defined firewall.

- Zscaler is a leading provider of cloud-based security services, including SWG, NGFW, route optimization for SaaS apps, sandboxing, bandwidth control, ZTNA/SDP and DLP delivered from over 100 POPs globally. It recently acquired a remote browser isolation technology.

## Acronym Key and Glossary Terms

| | |
|---|---|
| **AWS** | Amazon Web Services |
| **CASB** | cloud access security broker |
| **capex** | capital expenditure |
| **CDN** | content delivery network |
| **Colo** | colocation |
| **CPE** | customer premises equipment |
| **CSP** | communications service provider |
| **DDoS** | distributed denial of service |
| **DLP** | data loss prevention |
| **DMZ** | demilitarized zone |
| **FW** | firewall |
| **IaaS** | infrastructure as a service |
| **IDS/IPS** | intrusion detection system/intrusion protection system |
| **IoT** | Internet of Things |
| **ISP** | internet service provider |
| **MPLS** | Multiprotocol Label Switching |
| **NGFW** | next-generation firewall |
| **NGFWaaS** | next-generation firewall as a service |
| **NSP** | network service provider |
| **O365** | Office 365 |
| **opex** | operating expenditure |
| **OTT** | over-the-top |
| **PaaS** | platform as a service |
| **QoS** | quality of service |

| | |
|---|---|
| **RBI** | remote browser isolation |
| **SaaS** | software as a service |
| **SASE** | secure access service edge |
| **SDP** | software-defined perimeter |
| **SD-WAN** | software-defined WAN |
| **SWG** | secure web gateway |
| **SWGaaS** | secure web gateway as a service |
| **ZTNA** | zero trust network access |
| **UEBA** | user and entity behavior analytics |
| **UTM** | unified threat management |
| **WAAP** | web application and API protection |
| **WAF** | web application firewall |
| **WAFaaS** | web application firewall as a service |
| **WOC** | WAN optimization controller |

## Gartner Recommended Reading

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

“Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2016-2023, 2Q19 Update”

“Tech Go-to-Market: Four Crucial Product Management Steps to Transition Offerings to SaaS”

### Evidence

[1] Gartner regularly interacts with vendors from the WAN edge, network security and adjacent markets on the topic of corporate strategy and product roadmaps.

[2] Gartner conducted 768 SD-WAN-related inquiries and over 4,000 network security inquiry calls during the past 18 months.

[3] 77% of business Internet Protocol traffic is delivered across the internet. Source: "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper," Appendix G: Business IP Traffic.

### Note 1

We expect most SASE providers will offer SD-WAN, WOC, SWG, CASB, NGFW and ZTNA/SDP services. It is critical that SASE providers be able to terminate and inspect encrypted sessions where required based on policy with a scalable (ideally, software-based) architecture. To make policy-based access decisions, data, user and application context will be needed, requiring SASE vendors to be able to identify sensitive data and malware (including network sandboxing). Other important services include DNS protection, remote browser isolation, Wi-Fi hot spot protection, traditional VPN services, and web application and API protection services (including traditional web application firewall). Some vendors will offer network privacy as a service, hiding enterprise network infrastructure from visibility when using SASE services.

## This document is published in the following Market Insights:

Enterprise Network Infrastructure Worldwide

## GARTNER HEADQUARTERS

**Corporate Headquarters**
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

**Regional Headquarters**
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp