GIGAOM

Image credit: gorodenkoff

Chris Grundemann, Ivan McPhee
Jun 24, 2021

GigaOm Radar for Evaluating Secure Service Access v1.0

Vendor Assessment for Technology Decision Makers

Edge & Networking, Security & Risk

GigaOm Radar for Evaluating Secure Service Access

Vendor Assessment for Technology Decision Makers

Table of Contents

1. Summary

Due to the rapid adoption of cloud services, edge networks, and mobile workforces redefining the boundaries of the enterprise, digital transformation is changing the way organizations consume network security. Traditionally provided through legacy hardware-based networks and outdated architectures, security is shifting from location and VLAN-centric to user- and application-centric, with ubiquitous, unified policy management based on user identity instead of resource location.

This trend is accelerating the adoption of tightly integrated, multifunction cloud-native security solutions packaged as service offerings. Deploying cloud-based security services how and where they choose allows organizations to protect onsite and remote users with centralized control of application, data, device, and internet access without the need for additional hardware.

A relatively new concept, secure service access (SSA) represents a significant shift in the way organizations consume network security, enabling them to replace multiple security vendors with a single, integrated platform offering full interoperability and end-to-end resiliency. Encompassing secure access service edge (SASE), zero-trust network access (ZTNA), and extended detection and response (XDR), SSA shifts the focus of security consumption from the data center or network edge to ubiquitous users, apps, and devices everywhere.

SSA solution vendors enable organizations to roll out reliable and robust access controls for any user, device, or application anywhere in the world, thereby increasing organizational confidence in ubiquitous security without introducing new complexities or reducing performance.

This report provides an overview of the vendor landscape based on the following table stakes, which are mature, stable solution features common across all vendors:

- **Cloud-Native**
  Services are available in the cloud as a SaaS offering, independent of specific hardware requirements. Cloud-native refers to platforms specifically designed to take advantage of a cloud delivery model to increase speed, scalability, and agility.
- **User-Centric**
  Policies are enforced based on the identity and behavior of the user (application, device, or human) accessing the resource. Well-designed converged network and security systems should enable the user journey, providing authenticated users with authorized access to resources and services as easily and quickly as possible.
- **Location-Independent Service Delivery**
  Services are independent of user location and available to any user using any device anywhere in the world. With the recent shift toward a distributed workforce, remote users must have the same access to resources and services as they would if they were physically located in a corporate office.

- **Distributed Policy Enforcement**
  Instead of the enterprise data center being the access gateway to the network, policies are enforced and threats detected and eliminated at multiple data touchpoints. Ideally, defense-in-depth should be implemented within multiple layers of the OSI model, with Layer 3 and 4 firewalls filtering traffic at the packet level and Layer 7 firewalls filtering content for granular protection.

As you read this report, please do so with an open mind. The list of vendors included here is by no means exhaustive. As it is a new market sector meeting the demands of a distributed workforce, we anticipate rapid evolution in the next 18-36 months. As new agile players make inroads with lean, innovative solutions, established network and security vendors will continue to acquire point product vendors and expand critical partnerships. They will also focus on repackaging and integrating existing offerings to meet customer demand and retain market share.

We recommend using this report to explore the different architectures and delivery models available, identifying solutions and vendors matching your business requirements and capabilities. Then, contact the relevant vendors for more information on features and cost.

For additional information related to choosing a Secure Service Access solution, please read the report, *Key Criteria for Evaluating Secure Service Access: An Evaluation Guide for Technology Decision Makers*, published by GigaOm.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Solution Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

For a better understanding of the market and vendor positioning (**Table 1**), we categorized solutions for secure service access by the target market segment:

- **Cloud Service Providers (CSPs):** Service providers delivering pay-per-use, on-demand services to customers over the internet, including IaaS, PaaS, and SaaS.
- **Network Service Providers (NSPs):** Service providers selling network services—such as network access and bandwidth—provide access to backbone infrastructure or network access points (NAP). In this report, NSPs include data carriers, ISPs, telcos, and wireless providers.
- **Managed Service Providers (MSPs):** Service providers delivering application, IT infrastructure, network, and security services and support for businesses on customer premises, in the MSP's data center (hosting), or in a third-party data center.
- **Enterprises (Large, Medium, Small):** Enterprises refer to all businesses responsible for planning, building, deploying, and managing their applications, IT infrastructure, networks, and security in either an on-premises data center or a colocation facility.

We also recognize four deployment models for solutions in this report, shown in **Table 2**: private cloud, public cloud, hybrid cloud, and multi-cloud.

- **Private Cloud:** Used exclusively by one enterprise or organization, cloud computing resources are physically located in an on-premises data center or hosted by a third-party colocation service provider. Tailored to meet specific requirements, private clouds offer compliance, control, and flexibility.
- **Public Cloud:** Owned and operated by a third-party cloud service provider and delivered over the internet, public cloud providers offer cost-effective, scalable, and reliable on-demand resources for enterprises and SaaS vendors.
- **Hybrid Cloud:** Enabling data and apps to move seamlessly between environments, a hybrid cloud combines private on-premises infrastructure with a public cloud. Hybrid cloud allows compute to be brought closer to the edge where data resides—reducing latency and increasing reliability—while still meeting regulatory compliance and data sovereignty requirements.
- **Multi-Cloud:** Comprising multiple public cloud services performing different functions, multi-cloud allows enterprises and organizations to take advantage of different public cloud capabilities or geographies. Multi-cloud deployments may include private clouds, resulting in cloud deployment that is both hybrid and multi-cloud.

Table 1: Vendor Market Segments

	MARKET SEGMENT			
	Cloud Service Providers	Network Service Providers	Managed Service Providers	Enterprises
Ananda Networks	++	++	++	++
Cato Networks	–	–	++	++
Cisco	–	++	++	++
Citrix	–	++	++	++
Cloudflare	++	++	++	++
Dispersive	++	++	++	++
Fortinet	++	++	++	++
Masergy	–	–	–	++
Netskope	–	–	++	++
Palo Alto Networks	–	++	++	++
Symantec	++	++	++	++
Tempered	–	–	++	++
Versa Networks	++	++	++	++
VMware	++	++	++	++
Zscaler	++	++	++	++

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Source: GigaOm 2021

Table 2. Vendor Deployment Models

	DEPLOYMENT MODEL			
	Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
Ananda Networks	++	++	++	++
Cato Networks	++	++	++	++
Cisco	++	++	++	++
Citrix	++	++	++	++
Cloudflare	–	++	–	–
Dispersive	++	++	++	++
Fortinet	++	++	++	++
Masergy	++	++	++	++
Netskope	++	–	–	–
Palo Alto Networks	++	++	++	++
Symantec	++	++	++	++
Tempered	++	++	++	++
Versa Networks	++	++	++	++
VMware	++	++	++	++
Zscaler	++	++	++	++

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Source: GigaOm 2021

3. Key Criteria Comparison

Following the general indications introduced with the "*Key Criteria for Evaluating Secure Service Access*," **Tables 3, 4, and 5** summarize how each vendor included in this research performs in the areas that we consider differentiating and critical in this sector. The objective is to give the reader a snapshot of different solutions' technical capabilities and define the market landscape's perimeter.

Indicating each vendor's strengths and weaknesses, the tables provide the basis upon which organizations can create a shortlist, engage with various vendors, and make informed decisions on which solution to adopt for their particular needs. Attributes and capabilities will vary from one vendor to another and should be carefully evaluated based on each organization's needs and use cases.

Table 3. Key Criteria Metrics Comparison

	KEY CRITERIA							
	Software-Defined Architecture	Integrated Solution	Defense-in-Depth	Identity-Based Access	Dynamic Segmentation	Unified Threat Management	Autonomous Networking	IoT Support
Ananda Networks	+++	+	+++	+++	+++	++	++	–
Cato Networks	+++	++	++	+++	+++	+++	++	+
Cisco	+++	++	+++	++	++	+++	+++	++
Citrix	+++	++	+++	+++	+++	+++	++	++
Cloudflare	+++	+++	+++	+++	+	+	+++	++
Dispersive	++	+	++	++	+++	++	+	+
Fortinet	+++	++	+++	++	++	+++	++	+
Masergy	++	++	++	++	+++	++	+++	++
Netskope	+++	+++	++	+++	+++	+	+++	+
Palo Alto Networks	++	++	+++	+++	+++	+++	+++	+++
Symantec	++	+++	+++	++	++	+++	++	++
Tempered	++	+	++	++	+++	++	+	++
Versa Networks	+++	+++	+++	++	+++	++	++	+++
VMware	+++	++	++	+++	+++	++	++	++
Zscaler	+++	+++	+++	+++	++	+++	++	++

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Source: GigaOm 2021

Key criteria serve to differentiate one solution from another based on *features and capabilities*, outlining the primary criteria to be considered when evaluating secure service access solutions.

Table 4. Evaluation Metrics Comparison

	EVALUATION METRICS							
	Ease of Use	Performance	Interoperability	Redundancy	Visibility, Monitoring & Auditing	Pricing & TCO	Support	Roadmap & Vision
Ananda Networks	+++	+++	+++	+++	++	++	++	+++
Cato Networks	+++	++	+++	+++	+++	++	++	++
Cisco	+++	++	+++	+++	++	+	++	++
Citrix	++	++	+++	+++	+++	++	+	++
Cloudflare	+++	+++	++	+++	++	++	++	++
Dispersive	+++	+++	++	+++	++	++	++	++
Fortinet	+++	+++	++	++	+++	++	++	++
Masergy	++	+++	+++	++	++	++	++	++
Netskope	+++	+++	+++	+++	+++	++	++	++
Palo Alto Networks	++	++	++	+++	++	++	++	+++
Symantec	++	++	+++	+++	+++	++	++	++
Tempered	+++	++	++	++	+	+++	++	++
Versa Networks	++	++	+++	+++	++	++	++	++
VMware	+++	+++	+++	+++	+++	++	++	+++
Zscaler	+++	+++	+++	+++	+++	++	++	+++

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Source: GigaOm 2021

Evaluation metrics serve to differentiate one solution from another based on the *impact that the solution* may have on an organization, reflecting fundamental aspects like flexibility, ease of use, and total cost of ownership.

Table 5. Specific Security Capabilities

	SECURITY CAPABILITIES						
	Domain Name System Security	Secure Web Gateway	Firewall-as-a-Service	Cloud Access Security Broker	Zero-Trust Network Access	Endpoint Threat Detection & Response	Network Threat Detection & Response
Ananda Networks	+++	++	+++	++	+++	+	++
Cato Networks	+++	+++	+++	+++	+++	++	+++
Cisco	+++	+++	+++	+++	+++	++	++
Citrix	+++	+++	+++	++	+++	++	++
Cloudflare	+++	+++	+	+	+++	–	++
Dispersive	++	++	++	++	+++	++	+++
Fortinet	+++	+++	+++	+++	+++	++	++
Masergy	+	++	++	+++	++	++	++
Netskope	++	+++	+	+++	++	+	++
Palo Alto Networks	+++	+++	+++	+++	+++	+++	+++
Symantec	++	+++	+++	+++	+++	+++	+++
Tempered	++	+	++	++	++	++	++
Versa Networks	+++	+++	+++	+++	+++	+++	+++
VMware	+	++	+	++	+++	+++	+
Zscaler	++	+++	+++	+++	+++	+++	+++

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Source: GigaOm 2021

Specific security capabilities serve to differentiate one solution from another *based on specific functionality required to reduce the attack surface, detect threats, and mitigate risk.* These capabilities provide a comprehensive—but not exhaustive—list of functions enterprises and organizations require to take advantage of modern IT architectures. Indicating each vendor's strengths, **Table 5** also identifies converged platforms that can be tailored to meet unique requirements through in-house development or best-of-breed partnerships.

By combining the information provided in the tables above, the reader can develop a clear understanding of the technical solutions available in the market.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to create the GigaOm Radar graphic in **Figure 1**. The chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

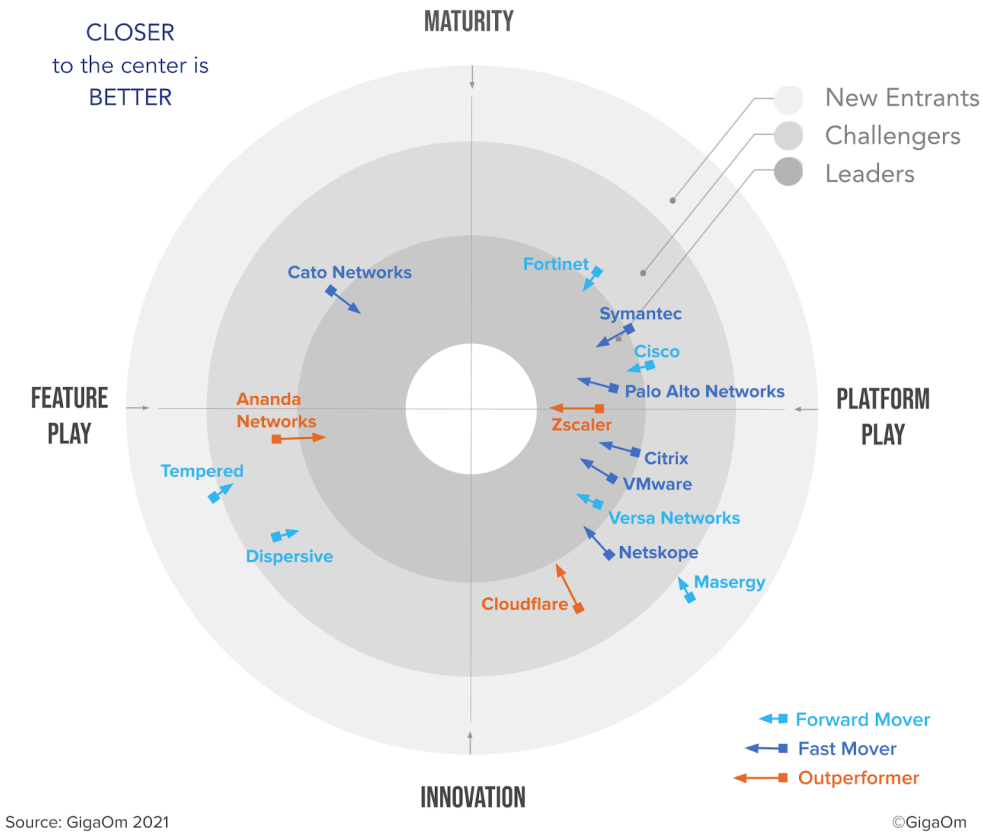

Figure 1. GigaOm Radar for Secure Service Access

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to the center judged to be of higher overall value. The chart characterizes each vendor on two axes—Maturity versus Innovation and Feature Play versus Platform Play—while providing an arrow that projects each solution's evolution over the coming 12 to 18 months.

As you can see in the Radar chart in **Figure 1**, the Platform Play side of the chart is extraordinarily active, with 11 of the 15 solutions in this report residing there. A total of five vendors earned Leader designation (again, all of them in the Platform Play side): Zscaler, Palo Alto Networks, VMware, Versa Networks, and Citrix. Symantec, meanwhile, is poised just outside of the Leader tier, while two vendors—Masergy and Tempered—are categorized as new entrants.

It is important to note that while SSA is a new sector, many vendors already have SSA capabilities

within their solution portfolio and are not, therefore, categorized as new entrants. These comprise end-to-end SSA platforms built from the ground up and solutions consisting of point products that are integrated to one degree or another.

You'll also note that some established networking and security vendors are positioned as challengers rather than leaders. Though many of these vendors have well-known point solutions recognized as leaders in their respective categories, we look at all capabilities in the context of an overarching SSA solution, with convergence and integration being crucial factors in establishing leadership. While all the vendors included in this report have SSA roadmaps, the speed at which they will be able to integrate their point solutions varies considerably, affecting their positioning as a leader or a challenger.

The longer orange arrows identify three outperformers. Ananda Networks and Cloudflare are gaining traction based on innovation, while Zscaler continues to extend its capabilities to meet the needs of its large installed base. At the same time, we expect Cisco, Citrix, and VMware to leverage new acquisitions to gain ground on the competition. While new entrants will expand through innovation, most of the more established players will focus on satisfying the needs of their existing installed base.

One area to keep an eye on is the managed service provider market. While Masergy is the only MSP included in this report, we expect to see new MSP entrants offering SSA solutions to their customers in the next 12-18 months. Also, watch out for emerging vendors—such as Ananda Networks, Dispersive, and Tempered—disrupting the sector with unique, high-performance, and cost-effective solutions that are quick and easy to roll out and manage.

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.
The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Ananda Networks – Ananda Secure Global LAN (SG-LAN)

Exiting stealth mode in August 2020, Ananda Secure Global LAN (SG-LAN) converges distributed network and security orchestration within a cloud-based control plane requiring zero hardware deployment. Replacing legacy networks and point products—including firewalls, MPLS, NAC, SD-WAN, and VPNs—SG-LAN is a cloud-managed, software-defined overlay network built from the ground up to enable enterprises to create and customize their own superfast private networks with end-to-end security and Slack-like ease of use.

At-a-Glance: Ananda Secure Global LAN (SG-LAN)

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Remote branch, employee, and third-party connectivity		Cloud enablement and migration	
Appliance elimination and cost reduction		MPLS and SD-WAN alternative	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Offering LAN-like connectivity by finding the optimal route between any two users, servers, devices, or cloud services located anywhere in the world, Ananda minimizes the threat surface. If required, Ananda dynamically spins up multi-cloud-based Nitro™ relays or waypoints—available in hundreds of different locations globally—to maximize link speed and quality. Eliminating most traffic backhaul caused by forcing traffic to pass through gateways or points of presence (PoPs), SG-LAN delivers speeds up to 25x faster than competitive solutions and legacy VPNs.

Ananda SG-LAN enforces tight security with authentication, end-to-end encryption, native segmentation, and zero-trust at the network level (Layer 3), blocking any type of network access or attack by any unauthorized node. Each user or node can only “see” other authorized nodes based on its private network membership and contextual access rules. Mediated by the Ananda control plane, end-to-end security from individual containers, devices, or servers to the destination is ensured, with best-of-breed content filtering, real-time inspection, sandboxing, and browser isolation provided via partner solutions.

Managed from the public cloud as a multi-tenant service, administrators simply deploy agents on endpoints and servers, or deploy gateways on private or public cloud instances to connect remote users and devices to applications on-premises or in the cloud. By eliminating the need for hardware infrastructure and multiple point products, Ananda Networks claims network and security savings of

90% or more compared to legacy MPLS-based solutions, and over 50% compared to competitive SD-WAN or SSA solutions.

Strengths: Ananda SG-LAN offers a unique unified approach for accelerating, orchestrating, and securing network traffic, with several patent-pending networking protocol and route selection innovations expected to boost network speeds and quality. Requiring no fixed infrastructure and with set up times of as little as 15 minutes, Ananda simplifies network design, deployment, and management, offering significant cost savings.

Challenges: Although currently being addressed by Ananda, troubleshooting overlay network issues can be a challenge. SG-LAN also relies on third-party integrations for ensuring device posture, browser isolation, content filtering, real-time inspection, and sandboxing. Clients should be aware of their needs and work with Ananda to ensure comprehensive threat coverage.

Cato Networks (Cato SASE Cloud)

Founded in 2015, Cato Networks was one of the first to launch a global cloud-native service converging SD-WAN and security-as-a-service. Developed from the ground up, Cato SASE Cloud allows enterprises to quickly migrate from MPLS and bundled solutions to a highly available and secure SD-WAN, backed up by rigorous 99.999% service availability SLAs. Delivering low latency and predictable performance globally via 65+ geographically distributed PoPs interconnected by multiple Tier-1 carriers, Cato SASE Cloud optimizes on-premises and cloud connectivity, enables secure branch access, and offers client and clientless access options for remote users.

At-a-Glance: Cato SASE Cloud

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
-	-	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Secure branch, cloud, and mobile access		MPLS to SD-WAN migration	
Eliminate security appliances with FWaaS		Optimize cloud access	
Pricing Model			
Pricing is based on an OPEX, per-Mbps and per-user subscription model			

A single product sold as-a-service, Cato SASE Cloud encompasses a global private backbone, edge appliances connecting physical locations to the cloud, built-in security-as-a-service, mobility solutions, and self-service management applications for configuration and analytics. Cloud data centers are connected to the Cato SASE Cloud via an IPSEC tunnel or Cato vSocket, while private clouds are connected with either a Cato Socket Edge SD-WAN device or IPSEC tunnel from existing appliances.

Multi-tenant, scalable, and ubiquitous, the backbone's cloud-native software provides full encryption,

self-healing capabilities, and dynamic path selection while implementing the inspection and enforcement functions needed by Cato's security services. Global routing and WAN optimization utilize advanced congestion management algorithms for maximizing end-to-end throughput. Favoring performance over cost, Cato's proprietary routing algorithms—using a single-pass traffic processing engine designed and built from the ground up—factor in latency, packet loss, and jitter to select the optimal route for each network packet.

Cato's Security as a Service includes an application-aware, next-generation firewall (NGFW), IPS, advanced anti-malware, a SWG with URL filtering, and Managed Threat Detection and Response (MDR). Available on every Cato PoP, Advanced Threat Prevention System—a collection of network security and related defenses—examines fixed and mobile network traffic flows, providing complete visibility while detecting and blocking vulnerability exploits.

Since 2015, Cato Cloud claims to have onboarded over 900 enterprises in more than 100 countries, connecting nearly 11,000 datacenters (physical and cloud), offices, and branches encompassing some 250,000 remote software-defined perimeter (SDP) and zero-trust users.

Strengths: Customers with a global footprint can leverage Cato's global private backbone to replace international MPLS services to reduce cost, meet service levels, improve performance, and deliver security everywhere. Based on existing case studies, customers have increased network availability, capacity, performance, and security with the same network spend.

Challenges: A relatively new entrant, Cato SASE Cloud's feature set and capabilities are not yet as granular or as robust as other enterprise solutions on the market. While small to mid-size cloud-based companies will find it to be a good fit, larger enterprises with a mix of on-premises and cloud applications and services may want to wait for the advanced CASB, DLP, and RBI features currently in development.

Cisco (Cisco SD-WAN, Cisco Umbrella & Cisco Secure Access by Duo)

The largest SD-WAN solution provider in the world with over 30,000 customers, Cisco's SSA strategy combines networking with a broad set of security functions in the cloud and end-to-end observability, allowing customers to expand their existing on-premises and cloud capabilities. Incorporating Cisco SD-WAN, Cisco Umbrella, and Cisco Secure Access by Duo (also referred to simply as Duo) via a single intuitive dashboard, Cisco shifts security to the edge, enforcing policies consistently across all environments, applications, and devices.

At-a-Glance: Cisco SD-WAN, Cisco Umbrella, and Cisco Secure Access by Duo

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Mobile connectivity		Branch Internet services	
Legacy DNS replacement		Regulatory compliance assurance	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

As the name suggests, Cisco Umbrella unifies multiple security capabilities within a single cloud-delivered service, reducing the time, money, and resources previously required to deploy, configure, manage, and protect distributed locations, devices, and users. Providing global coverage via Cisco SD-WAN—a cloud-delivered, global overlay fabric centralizing network analytics, management, and policies—and over 1,000 of the world's top internet service providers (ISPs), content delivery networks (CDNs), and SaaS platforms, Cisco offers a predictable user experience underpinned by consistent, end-to-end on-premises and cloud security.

Cisco Umbrella incorporates integrated DNS-layer security, cloud application security broker (CASB) functionality, a cloud-delivered firewall (CDFW), a full proxy SWG, and threat intelligence. The CDFW monitors Layer 3, 4, and 7 activity, blocking unwanted traffic using IP, port, and protocol rules, and utilizes signature detection to recognize applications before taking appropriate action. Duo (acquired by Cisco in 2018) provides controls to verify user identity and device health, establish trust, enforce policies, and ensure continuous visibility to reduce the risk of data breaches and meet compliance standards.

Leveraging threat intelligence from Cisco Talos, one of the largest commercial threat intelligence teams globally, Cisco Umbrella utilizes advanced statistical and machine learning models to identify new attacks, accelerate threat investigations, and reduce remediation times, automating responses across multiple security products.

Strengths: Offering one-click integration and automated deployment options, Cisco simplifies purchasing with a single Cisco SD-WAN and Umbrella package, quickly connecting hundreds of locations via a consolidated, cloud-based dashboard with simplified management and consistent policy control.

Challenges: With Cisco Umbrella "unifying"—or bundling—security products and packaging them as an easy-to-use, single cloud service in keeping with market trends, some are not as tightly integrated as customers may wish. As "open" network and security vendors accelerate innovation in this space, Cisco users may find themselves locked into different code bases and an aging product portfolio.

Citrix (Citrix SD-WAN, Citrix SIA, and Citrix SWA)

With products used by over 100 million users in more than 400,000 organizations, Citrix is an established player in the security and user experience market. Delivering a unified approach integrating cloud-delivered security and networking services, Citrix offers a consistent set of secure access services protecting enterprise infrastructure from external threats. The solution also blocks exfiltration of confidential corporate data from both internal and SaaS apps. Citrix's approach targets the replacement of traditional, multi-vendor, and hardware-based solutions—including VPNs, firewalls, and secure web gateways—with a unified, single-vendor solution.

At-a-Glance: Citrix SD-WAN, Citrix SIA and Citrix SWA

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
-	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Secure internet access for remote users		Consistent security policy and enforcement	
VPN-less access to internal applications		Automatic scaling of security services	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model. Citrix SD-WAN includes a CAPEX component.			

The Citrix SSA offering leverages and enhances the Citrix Workspace solution and incorporates Citrix Secure Internet Access (SIA), Citrix Secure Workspace Access (SWA), Citrix SD-WAN, and Citrix Analytics for Security. Citrix SIA provides comprehensive cloud security (SWG, FW, DLP, CASB, malware protection, and sandbox), while Citrix SWA offers zero-trust network access via a cloud-delivered architecture. Citrix also integrates with third-party identity and authentication vendors and SIEM providers.

Through enablement of compliance with local and global regulations, Citrix's multi-tenant, "instance-based" architecture offers complete data segregation and sovereignty, along with IP addresses that are retained and can be extended into the cloud for upstream integration with SaaS providers as required by law. Direct Internet Access (DIA) provides secure access without backhauling traffic to an on-premises data center. There is no hardware to deploy, no software updates or patches required, and an inherent, built-in ability to scale.

Managed from the same unified Citrix Cloud management console as Citrix's security offerings, Citrix SD-WAN offers deep integration with Citrix SIA, automating the setup of resilient tunnels to Citrix SIA points of presence. The convergence of networking and security simplifies the onboarding of new locations and mitigates the risk of network or infrastructure unpredictability interfering with the user experience.

Strengths: Leveraging its longstanding reputation as a leading digital workspace provider, Citrix offers

converged networking and security services that allow vendor consolidation. Delivered via a "thin branch, heavy cloud" architecture, Citrix provides fast, secure access to the internet, SaaS apps, and Citrix Workspace with DIA connections.

Challenges: While Citrix unifies numerous networking and security products under a common cloud console, integrating them to create a seamless administrator experience with a bundled acquisition model is an ongoing process. Moreover, while some organizations may appreciate a one-stop-shop for all their security needs, others may prefer to choose point products offering advanced AI and machine learning features and capabilities.

Cloudflare (Cloudflare One)

Founded initially as a reverse proxy company in 2009, Cloudflare launched Cloudflare One in 2020 as a comprehensive, cloud-based network-as-a-service (NaaS) solution securely connecting remote users, offices, and data centers to each other and to the resources they need. Built on Cloudflare's edge network, Cloudflare One replaces MPLS links and SD-WAN deployments with a single network comprising global, cloud-based zero-trust security, performance, and control via a single user interface. Providing consistent, standardized services, Cloudflare gateways are available in more than 200 cities, spanning over 100 countries, and interconnecting over 9,500 networks globally.

At-a-Glance: Cloudflare One

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Remote branch, employee, and third-party connectivity		Zero-trust security	
Unified visibility of on-premises and SaaS applications		Network obscurity	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Delivering security at the edge with single-pass inspection and single-pane management, Cloudflare One offers secure remote access, secure SaaS access or CASB, secure web gateway (including recursive DNS, HTTPS proxy, remote browser isolation, and a connectivity client for major OSes), DDoS protection (including FWaaS for Layer 3 and 4 networks), and traffic acceleration.

According to the company, Cloudflare's Anycast network is one of the largest and most interconnected, boasting PoPs less than 100 milliseconds from 99% of the internet-connected population in the developed world—with a 100% global uptime SLA. Cloudflare One uses a serverless computing platform deployed at the edge, enabling the rapid delivery of new innovations to improve performance, enhance security, and increase reliability. Intelligent routing accelerates customers' traffic from any user to any resource, while policy changes and threat intelligence updates are

propagated from users to every PoP worldwide within 500 milliseconds.

Cloudflare One provides onramps to connect users, devices, or locations to Cloudflare's edge (agents for endpoints and IP transit or interconnects for networks). At the same time, filters shield networks from attacks (Magic Transit), inspect and isolate traffic for threats (Gateway), and apply least-privilege rules to data and applications (Access). In March 2021, Cloudflare announced partnerships with Aruba, Infovista, and VMware, simplifying WAN, SD-WAN, and private interconnect connectivity to Cloudflare's global network. The company also expanded its Cloudflare Network Interconnect Partners program, adding 70 new colocation facilities to reduce cross-connect lead times.

Strengths: With every Cloudflare data center running every security service, Cloudflare One enables customers to enforce zero-trust security policies at the edge. It rationalizes complicated deployments and improves security, performance, and cost efficiency across users, offices, and data centers for on-premises applications, SaaS applications, and internet connections.

Challenges: Despite boasting an impressive array of capabilities and partners, Cloudflare lacks the visibility of some of its larger competitors. In addition, though Cloudflare has an ambitious roadmap for rolling out new features in 2021 to meet customer demand, we expect some of these to slip into 2022 or beyond, given the sheer volume of new features and functions.

Dispersive (Dispersive™ Virtual Network (DVN))

Founded in 2010, Dispersive provides programmable networking for mission-critical solutions. Inspired by battlefield-proven wireless radio techniques, the Dispersive™ Virtualized Network (DVN) offers a radically different software approach for delivering new levels of security, reliability, and performance across networks, providing a foundation for innovation and transformation across industry verticals. Supporting cellular, landline, satellite, and WiFi connections, Dispersive's programmable networking allows enterprises and partners to securely connect digital businesses, products, and technologies end-to-end across any network infrastructure with 99.999% reliability, including over the public internet.

At-a-Glance: Dispersive™ Virtual Network (DVN)

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Multi-tenant secure network communications		Secure transportation networks	
Fast, private, ultra-secure ad-hoc networks		Secure distributed energy renewable (DER) grids	
Pricing Model			
Pricing is based on an OPEX, per-service subscription model			

A software-defined overlay network guaranteeing packet delivery with an improved service experience, DVN intercepts packet data on edge devices, splitting session-level IP traffic into multiple independent and individually encrypted packet streams, then transfers each stream using a different path across the internet. The authenticated destination reassembles the split packet, with missing packets re-requested to ensure packet delivery.

With built-in acceleration offering up to a 10x performance improvement over SD-WAN and VPN-based solutions, DVN monitors every connection and adapts to changing conditions, including BGP, DoS, DDoS, and man-in-the-middle attacks. If traffic congestion or an attack anomaly is detected, DVN dynamically deflects packets away from degrading paths or threats in real-time, thereby maintaining QoS levels by reducing overall latency and packet loss.

A subscription-based product functioning as a platform, Dispersive offers DVN-as-a-Service on its hosted cloud and partners with providers deploying the service on their own hosted cloud architecture. Red team tested—simulating a realistic cyberattack employing recently used methods and techniques for real-world attacks against businesses—and field-proven under military-grade attacks, DVN has established a reputation for resilience and network reliability within the United States Federal Government.

Strengths: Easy to provision and administer, ad hoc networks can be deployed in a fraction of the time compared to most other solutions. Supporting autonomous networking, blockchain, and IoT, DVN increases performance and detects and defends against security attacks with a self-healing, resilient network.

Challenges: Initially targeting government and military sectors, Dispersive lacks buyer awareness in the enterprise space. As a network-focused company, it needs to forge strong partnerships with security partners to fill gaps in its portfolio, while simultaneously expanding its capabilities in the areas of containerization and IoT support.

Fortinet (FortiSASE)

Founded in 2000, Fortinet offers a comprehensive product portfolio supporting hardware, software, virtual machines, containers, and cloud-based deployment options. The Fortinet Security Fabric is a broad, integrated, and automated platform encompassing over 30 orchestrated products spanning five key areas: zero-trust access, security-driven networking, dynamic cloud security, AI-driven security operations, and its alliance ecosystem. In July 2020, Fortinet acquired OPAQ Networks in a bid to form a best-in-class cloud security platform combining OPAQ's patented zero-trust network solution with Fortinet's on-premises or data center Fortinet Security Fabric to create FortiSASE.

At-a-Glance: FortiSASE

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Remote branch, employee, and third-party connectivity		Cloud enablement and migration	
Appliance elimination and cost reduction		MPLS and SD-WAN alternative	
Pricing Model			
Pricing is based on an OPEX, per-device subscription model			

Intuitive to deploy and manage, FortiSASE provides a single, integrated system delivering consistent security and user experience across all edges. Powered by FortiOS, FortiSASE provides next-generation firewall and SD-WAN capabilities, CASB, multi-cloud workload protection, advanced endpoint identity and multifactor authentication, browser isolation, web security, sandboxing, and web application firewall capabilities. FortiSASE SIA offers up-to-date real-time protection to terminate client traffic, scan traffic for known and unknown threats, and enforce corporate security policies for users anywhere.

Highly scalable and elastic, FortiSASE is delivered in two primary form factors: FortiSASE SIA and FortiSASE Thin Edge. Incorporating FWaaS, IPS, DLP, DNS, SWG, and sandboxing, FortiSASE SIA delivers high-performance, always-on threat protection through the cloud to remote off-network users via a FortiClient Agent. Mitigating the risk of unprotected corporate-managed devices, FortiClient detects when the user is outside of the enterprise network, rerouting traffic through the FortiSASE SIA for off-net service via tunneling to ensure the enforcement of security policies. FortiSASE Thin Edge provides the same high-performance, always-on, cloud-delivered threat protection as FortiSASE SIA, but to thin edge users via a FortiExtender appliance.

FortiSASE leverages AI-enabled FortiGuard and FortiSandbox Cloud capabilities to protect against unknown attacks, using dynamic analysis to identify threats and create new signatures to block future attacks for automated mitigation.

Strengths: Regardless of a user's location, FortiSASE enforces unified firewall, networking, and security policies at all network edges by extending on-premises policies to remote users and their devices. The solution supports managed security services provider (MSSP) multi-tenancy deployment with delegated access for end-customers while providing centralized visibility and management.

Challenges: Navigating Fortinet's comprehensive portfolio of over 30 solutions—each providing different capabilities and supporting different deployment models—can be challenging. Fortinet currently lacks a cloud-hosted SSA offering. And while pricing varies according to each company's needs, prospective clients should be aware that Fortinet's portfolio targets large enterprises handling sensitive data, and is priced accordingly.

Masergy

Operating a software-defined cloud and network platform supporting over 1,400 enterprise clients in more than 100 countries, Masergy offers a full stack of secure business networking and communications solutions. Unlike many other SD-WAN providers, however, Masergy partners with best-of-breed vendors, integrating security with Masergy's Secure Edge Network—a private, high-performance, and globally available software-defined network—as tightly as those providers will legally allow to provide a comprehensive, end-to-end SSA solution.

At-a-Glance: Masergy

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
			X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Remote branch, employee, and third-party connectivity		Cloud enablement and migration	
Appliance elimination and cost reduction		MPLS and SD-WAN alternative	
Pricing Model			
Pricing is based on an OPEX, per-service subscription model			

A pioneer in the enterprise networking and cybersecurity industries with over twenty years in innovation around software-defined networks, Masergy owns multiple patents for machine-learning behavioral analysis on wide-area networks. Masergy's Secure Edge Network is dynamic and programmable, allowing the company to add new features based on customer performance requirements and business objectives. Having recorded less than five minutes of downtime per year for over 15 consecutive years, Masergy offers industry-leading 100% site-level and cloud app availability SLAs for SD-WAN deployments configured for high availability.

Rather than just reselling add-on security products to customers, Masergy integrates best-of-breed technologies from vendors recognized as industry leaders in their respective areas, including Bitglass (CASB), Fortinet (SD-WAN, SWG, ZTNA), and Sentinel One (EDR). This approach results in a hybrid of cloud-native (delivered via over 50 secure Masergy PoPs strategically located near major population centers) and on-prem SSA deployments working seamlessly together to provide a unified, fully-managed service on a global scale. Turnkey managed detection and response services include 24/7 continuous monitoring from three global security operations centers (SOCs). Masergy believes this approach offers customers optimal network performance combined with the protection they need irrespective of location.

Providing a new, vendor-agnostic approach to threat detection and response, Masergy is in the process of leveraging its best-of-breed cybersecurity partnerships to launch a unified detection and response (UDR) platform, combining multiple XDR-style systems into a single unified service. Applying the company's embedded real-time analytics and AI-enhanced automation to proactively identify

sophisticated threats, Masergy UDR will offer full visibility into traffic moving across networks, clouds, and endpoints—from a single unified portal.

Strengths: Unlike other managed services providers offering a range of point security solutions, Masergy leverages its networking strengths to give enterprises a flexible and pragmatic approach to SSA on a global scale with multiple deployment options—in the cloud, on-premises, or both. By integrating multiple security technologies into a single unified service, Masergy offers customers a flexible, high-performance, and secure solution meeting specific business needs.

Challenges: Despite having integrated high-performance networking and best-of-breed security into a unified, highly available platform spanning cloud and on-premises, Masergy has not yet productized it as an end-to-end service for customers.

Netskope (Netskope Security Cloud)

Founded in 2012 by security and networking architects and engineers from Cisco, Juniper Networks, Palo Alto Networks, and VMware, Netskope claims to be the most well-connected network for cloud-native data security. Powered by data centers in over 40 different regions— and burst capacity to 130 data centers if needed—with new data centers being added monthly, NewEdge is a carrier-grade, private cloud network reserved exclusively for Netskope customers. Running on top of it, Netskope Security Cloud provides complete visibility and real-time data and threat protection across cloud services, private apps, and websites, irrespective of location or device.

At-a-Glance: Netskope Security Cloud

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
		X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X			
Primary Use Cases			
Mitigate risk and data loss in the cloud		Simplify security architectures	
Secure unmanaged, business-led cloud services		Govern on-premises, mobile, and remote cloud users	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Netskope claims to be the only vendor combining a world-leading CASB, next-generation SWG capabilities, cloud-based security posture management, zero-trust network access, and advanced machine learning to detect unauthorized data exfiltration and advanced threat protection.

Using patented technology called Netskope Cloud XD™, the Netskope Security Cloud converges network-as-a-service with security-as-a-service to eliminate blind spots with a granular, data-centric approach enabling fine-grain control of IaaS and SaaS cloud services and websites. With full control from within Netskope Security Cloud, Cloud XD takes into account content and context to increase

detection efficiency and accuracy, providing 360° data protection using a combination of big data analytics and advanced data loss prevention (DLP) capabilities.

The Netskope Security Cloud runs on NewEdge, which deploys full compute at every service point for real-time, inline traffic processing, eliminating performance trade-offs. With zero reliance on public cloud infrastructure or virtual points of presence (vPoPs), NewEdge can achieve sustained, single-digit millisecond latency. The platform offers direct peering with cloud, SaaS, and web providers—including Apple, Amazon, Google, Microsoft, Rakuten, Salesforce, and Tencent—in every location to deliver a secure, high-performance application experience.

Strengths: With over 80 patents, numerous awards, and more than 25% of the Fortune 100 as customers, Netskope is well-established as a leading cloud security provider. Converging networking and security within a single architecture and single console, the Netskope Security Cloud offers advanced, fully cloud-native, real-time data policy enforcement with cloud performance and scale.

Challenges: Netskope continues to expand its security capabilities through "silent" acquisitions, but lacks some features available in best-of-breed point solutions. While those acquisitions will benefit customers in the long run, in the interim, customers can expect to see some disconnect between different products, including the need to install agents on users' devices to achieve maximum value.

Palo Alto Networks (Prisma Access, Prisma SD-WAN, and Cortex XDR)

With over 80,000 customers in more than 150 countries, Palo Alto Networks has been an established player in the market since 2015. Built on a massively scalable, ultra-low latency network backed by industry-leading SLAs, Prisma Access consolidates best-of-breed security capabilities—including CASB, FWaaS, SWG, ZTNA, and other functions—all managed through a single console. With Prisma SD-WAN and Cortex XDR, Prisma Access provides the foundational layer for a complete SSA solution delivering converged networking and security via a shared service delivery model.

At-a-Glance: Prisma Access, Prisma SD-WAN, and Cortex XDR

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Secure remote workforces		Secure branch and SD-WAN	
Mergers and acquisitions			
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Providing the foundation for consistent cloud-delivered security, Prisma Access is built from the ground up on a massively scalable network leveraging the combined infrastructures of AWS and GCP, with over 100 service access points across 76 countries. This combination enables Prisma Access to provide ultra-low latency backed by industry-leading SLAs to ensure a great digital experience for end users. Consolidating more point products into a single converged cloud-delivered platform than any competing solution, Prisma Access provides a consistent global services edge delivering comprehensive security coverage.

Formerly known as CloudGenix, Prisma SD-WAN leverages machine learning and automation to simplify network and security management, combining deep application visibility with Layer 7 intelligence for network policy creation and traffic engineering. Facilitating application-defined policies improves the end-user experience and enables the secure, cloud-delivered branch.

Detecting risks with AI-driven analytics to reveal the root cause, Cortex XDR—combined with Palo Alto Network's Managed Threat Hunting service—accelerates threat detection and response and provides round-the-clock protection and industry-leading coverage of MITRE ATT&CK® techniques.

Strengths: Palo Alto Networks provides consistent cloud-delivered security for remote users. Accessed via a single console, it adds simple and intuitive workflows to streamline configuration, automated continuous configuration assessments, and security recommendations based on best practices. It also offers comprehensive visibility into all users, applications, and threats to improve security posture and reduce risk.

Challenges: The incumbent in many enterprise and mid-market accounts, Palo Alto Networks is aggressively moving to the cloud by acquiring the necessary building blocks and investing in integration with security vendors so customers don't have to rip and replace when deploying SSA. However, due to the size and scope of its portfolio, we anticipate the company's ability to to deliver a fully-integrated SSA platform will lag compared to other vendors with more SaaS experience.

Symantec (Symantec Integrated Cyber Defense)

Acquired by Broadcom in 2019, Symantec's enterprise security product portfolio is recognized as an industry leader in all the primary security categories. Comprising multiple security solutions, Symantec Integrated Cyber Defense (ICD) delivers integrated endpoint, identity, information, and network security across on-premises and cloud infrastructures, providing comprehensive threat protection and compliance for corporate assets.

At-a-Glance: Symantec Integrated Cyber Defense

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Move security to the cloud		Secure BYOD/unmanaged device access	
Support a mobile workforce		Report on compliance and privacy policies	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Utilizing a platform approach, user traffic is steered to ICD from Symantec's endpoint and forward proxy footprint to its closest cloud point-of-presence, where key security capabilities are applied. With core security services residing within ICD, the Symantec Web Security Service (WSS) delivers a broad set of advanced capabilities—including anti-virus scanning, data loss prevention (DLP), email security, sandboxing, an SWG, software-defined perimeter, and web isolation—and makes them available from the cloud.

WSS runs on a high-performance, fully redundant cloud-native infrastructure spanning more than 40 regions globally. While utilizing private networks in some markets, most of Symantec's infrastructure has been migrated recently to Google Cloud to take advantage of its global, edge-optimized private network backbone, enhancing the speed and scalability of Symantec's service delivery. Symantec is expanding the multi-tenant Google Cloud infrastructure with AWS, for countries where AWS has a local presence, to meet regulatory data governance requirements. The self-healing, software-defined infrastructure provides increased availability compared to previous generations of cloud infrastructure relying on physical network appliances to scale.

Symantec also provides customer access to its Global Intelligence Network (GIN)—one of the world's largest civilian threat collection networks—via embedded integration with Symantec Endpoint Security Complete. A comprehensive endpoint security solution delivering protection, detection, and response, SES Complete stops endpoints from being compromised with superior next-gen protection technologies spanning the attack chain. Sophisticated attack analytics and proactive attack surface reduction technologies provide a strong defense against hard-to-detect threats, blocking full-blown breaches before exfiltration can occur and resolving persistent threats in real-time.

Strengths: With a broad set of critical capabilities fully integrated and supported by a single vendor, Symantec lets enterprises reduce operational complexity and optimize the effectiveness of their investments with a range of integrated solutions seamlessly sharing threat intelligence, management consoles, policies, and agents. In addition, Symantec offers single purchase transactions comprising multiple capabilities and deployment models.

Challenges: While the move to Google CloudGCP has enhanced Symantec's capabilities, the

acquisition by Broadcom appears to have created a certain amount of disruption. Some product development slowed and channel partners and customers experienced issues with service and support. While we expect these issues to resolve in the near future, potential customers should seek clarification on product roadmaps and SLA commitments. In addition, though strong on the security front, Symantec currently lacks the strategic SD-WAN partnerships required to provide a converged solution.

Tempered (Airwall™)

Founded in 2012, Tempered takes a radically different approach to security by addressing one of the root causes of internet attacks—the visibility of network devices to bad actors. Securing every endpoint in your network—from local data centers to global infrastructure—Tempered's Airwall™ makes everything on the network invisible to protect against cyber attacks. Using gatekeepers—known as Airwall Gateways—in front of any IP-connected device protects critical physical infrastructure while still allowing secure global connectivity and mobility. Requiring no change to the underlying network, Airwall is a comprehensive solution extending to cloud, virtual, and physical environments.

At-a-Glance: Airwall™

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
		X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Remote branch, employee, and third-party connectivity		Microsegmentation	
Threat remediation		Software-Defined Perimeter (SDP)	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Eliminating the need for VPN solutions, Airwall uses the Host Identity Protocol (HIP)—an open standards-based network security protocol—to create a secure overlay fabric spanning existing network infrastructures. HIP-enabled private networks can generally traverse any firewall and seamlessly move among private, public, and mobile networks. First deployed within the aerospace and defense industries, HIP is a cost-effective, scalable way to mitigate threats without implementing complex security policy management.

The creation of a secure overlay network using an encrypted identifier cloaks vulnerable infrastructure, rendering it undetectable to unauthorized users and bad actors. Delivering defense-in-depth, Airwall comprises a software-defined network, a software-defined perimeter, microsegmentation at every endpoint, multi-factor authentication (MFA), and zero-trust access. While Airwall is generally deployed as a software solution, an easy-to-deploy hardware gateway is available if required.

Airwall includes an intuitive centralized graphical management console, enabling user devices to be added or removed from a trusted list with just a few clicks. Modern policy objects enable real-world management of user groups and network assets. A full API allows network security teams to fully automate all aspects of network configuration and user provisioning and includes a fully auditable configuration history.

To provide a more secure, rapid response approach against industrial-grade network attacks, a partnership with Nozomi Networks integrates Nozomi's network visibility, threat detection, and incident response system with Airwall's policy enforcement and centralized, software-defined, perimeter management console.

Strengths: Building secure connections directly between two communicating systems whenever possible, Airwall's HIP-based solution reduces the attack surface and ensures protection by cloaking vulnerable infrastructure. An easy-to-use GUI makes Airwall easy to set up and manage.

Challenges: Since traffic is sent over end-to-end encrypted HIP tunnels, commercially available traffic analysis solutions are "blind" in a Tempered environment. Tempered is investing in providing increased visibility within Airwall, and is working to integrate Airwall with third-party solutions to provide additional network traffic insights and control. Potential customers should explore with Tempered its existing solutions and options for secure monitoring and analysis, which might not be adequate to meet their needs.

Versa Networks (Versa SASE)

Founded in 2012, Versa claims to be the only vendor delivering a fully integrated, converged SSA solution deployed either on-premises or in the cloud—or as a hybrid combination of both—in a single software stack (VOS™) built on a single-pass parallel processing architecture. A converged, integrated, and scalable solution, Versa SASE offers best-of-breed security, advanced networking, industry-leading SD-WAN, true multi-tenancy, and advanced analytics. Available on-premises, cloud-delivered, or hosted by Versa-powered service providers, it simplifies and streamlines the management of networking and security policies and services.

At-a-Glance: Versa SASE

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Secure branch, employee, and third-party connectivity		Consistent on-premises and cloud policy management	
Appliance elimination and cost reduction		Lean IT	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Running on on-premises appliances or in the cloud—using distributed Versa Cloud Gateways running in 90 regions—Versa SASE leverages the single-pass parallel processing architecture found in the Versa Operating System (VOS™). A multi-service, multi-tenant software solution built on cloud principles, VOS provides automation, programmability, and segmentation at scale. Touching each packet only once for both networking and security, VOS's unique architecture increases performance and mitigates security vulnerabilities and exposure. Versa SASE takes advantage of the Versa Traffic Engineered Protocol to steer traffic between Versa Cloud Gateways across the private backbone, eliminating jitter, reducing latency, and minimizing packet loss.

Comprising a comprehensive set of services in a single solution, Versa SASE includes a CASB, NGFWaaS, SD-WAN, SWG, ZTNA, user and entity behavior analytics (UEBA), and other functions such as analytics, automation, and multi-tenancy to allow granular roles and segmentation.

Providing a subset of Versa SASE's cloud-native services, Versa Titan addresses the needs of smaller lean IT organizations lacking in-house security or network-focused architects, engineers, and technicians.

Strengths: Built from the ground up, Versa SASE delivers increased security and consistent security policies across branches, remote offices, and individual users, eliminating security gaps and vulnerabilities introduced when connecting multiple security solutions. Customers deploying Versa SASE also report significant increases in business and application performance for multi-cloud and on-premises deployments.

Challenges: While boasting a competitive offering, numerous awards, a healthy roadmap, and over 5,000 SD-WAN customers, Versa Networks still lacks end-user awareness in the SSA space. And despite Versa's "one architecture fits all" philosophy, Versa SASE lacks the flexibility and many of the granular controls available in other vendor solutions.

VMware (VMware SASE Platform™)

An established player in the networking and security space, VMware's cloud-native VMware SASE Platform combines CASB, SD-WAN gateways, SWG, ZTNA, and NGFWaaS functionality. Leveraging a software-defined architecture with a single pane of glass for management, reporting, troubleshooting, and visibility, these networking and security services can be delivered in an intrinsic or sequenced manner to branch edges, campuses, mobile users, and IoT devices.

At-a-Glance: VMware SASE Platform

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Provide a consistent, cloud-like user experience		Improve visibility into user/application activity	
Define granular policies for specific users/applications		Ensure secure access to public and private clouds	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

With varying degrees of integration, all components comprising the VMware SASE Platform and endpoint security are from VMware's portfolio, including Carbon Black, Workspace ONE, VMware SD-WAN, VMware Secure Access, and NSX Cloud Firewall. Running natively inside the VMware SASE PoPs, the VMware Cloud Web Security component is an OEM product from Menlo Security. Taking a comprehensive architectural approach to security, the platform includes defense, starting with managing endpoints with Workspace ONE, hardening and behavioral prevention of endpoints with Carbon Black, built-in stateful firewall at the edge, various services for cloud security, and workload protection for the data center.

Following VMware's Intrinsic Security strategy, VMware SD-WAN leverages infrastructure and control points across apps, clouds, and devices—combined with threat intelligence—enabling customers to shift quickly from a reactive posture to a position of strength. Serving as an onramp to SaaS and other cloud services, VMware's approach to SD-WAN includes over 150 PoPs hosted by VMware or service provider partners worldwide, providing less than 10ms latency from 80% of the world's population and less than 5ms from all major cloud providers. This footprint gives VMware a global presence for launching new networking and security services and integrating them with best-of-breed security partners.

Available as a web-based user interface, VMware SASE Orchestrator provides centralized, enterprise-wide installation, configuration, and real-time monitoring of VMware SASE Platform services and is responsible for orchestrating the data flow throughout the cloud network. Orchestrator provides a simple, one-click setup for connecting VMware PoPs to third-party cloud security services.

Strengths: Encompassing several solutions, the VMware SASE Platform converges networking and security delivered as a cloud-hosted service. It enables reliable, secure, and efficient access to any on-premises, SaaS, or virtual application by users located anywhere in the world while protecting users and infrastructure against internal and external threats.

Challenges: VMware is in the process of filling gaps in its portfolio, investing in areas such as DNS security and FWaaS. However, integrating them at a deeper level will take time. Despite the widespread adoption of VMware products, customers should recognize the VMware SASE Platform

for precisely what it claims to be—a SASE platform—and not yet a fully integrated SSA solution.

Zscaler (Zscaler Private Access and Zscaler Internet Access)

Founded in 2008 and boasting an impressive list of Fortune 2000 customers, Zscaler promotes a "best-of-breed platform" over best-of-breed point products. Its flagship services, Zscaler Private Access (ZPA) and Zscaler Internet Access (ZIA), combine to create fast, secure connections between users and applications, irrespective of device, location, or network. Used in over 185 countries, Zscaler operates the world's largest cloud security platform, blocking over 100 million threats every day as customer traffic traverses 150 data centers across six continents.

At-a-Glance: Zscaler ZPA and ZIA

Target Market			
Cloud Service Providers (CSPs)	Network Service Providers (NSPs)	Managed Service Providers (MSPs)	Enterprises (Large, Medium, Small)
X	X	X	X
Deployment Model			
Private Cloud	Public Cloud	Multi-Cloud	Hybrid Cloud
X	X	X	X
Primary Use Cases			
Provide a consistent, cloud-like user experience		Improve visibility into user/application activity	
Define granular policies for specific users/applications		Ensure secure access to public and private clouds	
Pricing Model			
Pricing is based on an OPEX, per-user subscription model			

Built from the ground up for performance and scalability, Zscaler services are 100% cloud-delivered, offering an enhanced user experience by peering with hundreds of partners in major internet exchanges worldwide. Comprising four comprehensive solutions delivered via a cloud-based, zero-trust exchange, Zscaler claims to simplify IT by consolidating functionality and eliminating point products. Two of those solutions—ZPA and ZIA—combine to make up Zscaler's SSA solution.

Leveraging a distributed architecture to provide fast, secure access to private applications, ZPA runs as a cloud service on-premises or in the public cloud. The service provides application access based on context and uses inside-out connections to make applications invisible to unauthorized users. As the internet becomes the enterprise's new transport network, microsegmentation connects users to specific apps, limiting lateral movement.

A secure internet onramp and web gateway, ZIA is delivered as a service from the cloud compromising Cloud Firewall, Cloud IPS, Cloud Sandbox, Cloud DLP, CASB, and Cloud Browser Isolation. Whether connecting via a router tunnel to the closest Zscaler data center (for offices) or forwarding traffic via the lightweight Zscaler Client Connector (for mobile users), users enjoy the same protection. Sitting between your users and the internet, ZIA provides full inline content inspection across multiple security techniques, including SSL. ZIA uses basic Layer 3 and Layer 4 firewall policies by default, but customers can upgrade to a NGFW for Layer 7 application control, advanced DNS, user and group policies, and full logging.

Strengths: The Zscaler “best-of-breed platform” architecture helps accelerate cloud adoption by removing network and security friction through the consolidation and simplification of IT services. Peering at the edge with leading application and service providers, Zscaler optimizes traffic routing to provide a frictionless and transparent experience for users across all locations.

Challenges: Despite boasting an extensive global network, not every service runs on every server and data center in Zscaler’s network. As Zscaler increases market share in the converged networking and security sector, it is being targeted aggressively by competitors offering best-of-breed replacement point products based on price or differentiating features.

6. Analyst's Take

As distributed enterprise and remote work become the norm, seamless, secure access to cloud-delivered services irrespective of location and device is essential. While incumbent vendors are repositioning legacy products as SSA platforms or engaging in acquisitions and strategic alliances to fill the gaps in their portfolios, new entrants are emerging with innovative approaches in an increasingly competitive market. We expect that trend to continue throughout 2021 and 2022.

As the naming of their solutions indicate, many vendors are piggybacking on the hype surrounding SASE. Others are focusing on building out ZTNA solutions. While both models have merit, we believe a more comprehensive approach is needed. Encompassing SASE, ZTNA, XDR, and NTDR, SSA shifts the focus of security consumption from the data center or edge to ubiquitous users, apps and devices everywhere.

Moreover, despite some analysts recommending that enterprises and organizations look to a single vendor for network and security convergence, we recommend that decision-makers develop one or more strategic partnerships based on the specific needs of their business. Some have already invested heavily in "best-of-breed platform" vendors—including Cisco, Citrix, Palo Alto Networks, Symantec, VMware, and Zscaler—who are evolving or repositioning their offerings in line with market expectations. At the same time, these incumbents are in the crosshairs of some of the emerging players in the space—such as Cato Networks, Cloudflare, and Versa Networks—that claim significant benefits in terms of cost savings and speed.

Customers should be aware that, in some cases, incumbent vendors lack distributed PoPs and may not be in a position currently to provide cloud-based delivery of converged networking and security services. Due diligence is required, and decision-makers should take the time to explore new, cost-effective approaches, including secure overlay networks from vendors—such as Ananda, Dispersive, Tempered, and Zscaler—to meet the needs of specific use cases.

In addition, customers need to consider the approach that best meets the needs of their business based on features, functions, and the availability of in-house expertise:

- An end-to-end SSA platform from a single vendor
- Multiple, best-of-breed point products integrated and delivered by a single provider
- Multiple, best-of-breed point products deployed and managed in-house

As you explore SSA, we recommend using this report to evaluate your current and future needs based on these different approaches before creating a shortlist of vendors supporting your target market, deployment model, and use case.

7 About Chris Grundemann

Chris Grundemann is a passionate, creative technologist and a strong believer in technology's power to aid in the betterment of humankind. He is currently expressing that passion by helping technology businesses grow and by helping any business grow with technology.

Chris has well over a decade of experience as both a network engineer and solution architect designing, building, securing, and operating large IP, Ethernet, and Wireless Ethernet networks. He has direct experience with service provider and enterprise environments, design and implementation projects, for-profit and not-for-profit organizations, big picture strategic thinking and detailed tactical execution, and standards and public policy development bodies. Chris frequently works with C-level executives and senior engineering staff at internet and cloud service providers, media and entertainment companies, financials, healthcare providers, retail businesses, and technology start-ups.

Chris holds eight patents in network technology and is the author of two books, an IETF RFC, a personal weblog, and a multitude of industry papers, articles, and posts. In addition to being the lead research analyst for all networking and security topics at GigaOm, he is the co-host of Utilizing AI, the Enterprise AI podcast. He is also a cofounder and Vice President of IX-Denver and Chair of the Open-IX Marketing committee. Chris has given presentations in 34 countries on 5 continents and is often sought out to speak at conferences, NOGs, and NOFs the world over.

Currently based in West Texas, Chris can be reached via Twitter.

8 About Ivan McPhee

Formerly an enterprise architect and management consultant focused on accelerating time-to-value by implementing emerging technologies and cost optimization strategies, Ivan has over 20 years' experience working with some of the world's leading Fortune 500 high-tech companies crafting strategy, positioning, messaging, and premium content. His client list includes 3D Systems, Accenture, Aruba, AWS, Bespin Global, Capgemini, CSC, Citrix, DXC Technology, Fujitsu, HP, HPE, Infosys, Innso, Intel, Intelligent Waves, Kalray, Microsoft, Oracle, Palette Software, Red Hat, Region Authority Corp, SafetyCulture, SAP, SentinelOne, SUSE, TE Connectivity, and VMware.

An avid researcher with a wide breadth of international expertise and experience, Ivan works closely with technology startups and enterprises across the world to help transform and position great ideas to drive engagement and increase revenue.

9. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

10. Copyright