SASE

AVANT 6-12 Report

September 2021

Complimentary report provided by:

DMGI INNOVATION | AVANT

Complimentary Report Courtesy of

DMGI INNOVATION

We are excited to provide you with a complimentary copy of the AVANT Research & Analytics 6-12 Report. As your Trusted Advisor, we aim to empower you with the information and resources you need to support your company's digital transformation.

There has never been a faster rate of change in IT, and the pace is accelerating every year. This 6-12 Report arms you with the most relevant information and insights necessary to assist you in evaluating your communications needs over the next six to twelve months.

We look forward to supporting your IT needs and business outcomes to help you differentiate and stay ahead of your competition in this fast-paced and ever-changing world.

TRUSTED ADVISOR™
POWERED BY AVANT

Copyright © 2020 AVANT Communications, Inc.

AVANT Research & Analytics: The 6-12 Report

Each “6-12 Report” is developed by AVANT Research & Analytics with the assistance of technical teams within AVANT. These market research reports are backed by a wealth of data secured by AVANT in our normal course of business, our own primary research of end-customers, and other reputable industry sources.

6-12: CCaaS | 6-12: UCaaS | 6-12: Security | 6-12: SD-WAN | State of Disruption Report

Our reports focus on today’s most disruptive technologies, those where the pace of change is rapid. Companies or technologies which – only a few years ago – may have been unknown, are now highly viable solutions that resolve the business needs that led to their creation. They have disrupted the IT landscape, a market already well known for its accelerating pace of change and innovation.

Every AVANT 6-12 Report gives enterprise technology leaders a contemporary and relevant overview of the featured subject suitable to making a purchase/non-purchase decision over the next six to 12 months. We select each topic based on the potential competitive advantages companies can realize if they adopt a given solution, depending on their particular industry, market space, or company size.

All currency values in this report are expressed in U.S. dollars.

Copyright © 2021 AVANT Communications, Inc.

AVANT enables Trusted Advisors (agents, managed service providers, consultants, and specialized channel partners) to assist with the technology decision-making process through our specialization in disruptive technologies and solutions. We accomplish this with our:

- Engineering Team of consummate professionals who study the ins-and-outs of the latest IT products from the perspective of what best meets the needs of end users.

- AVANT Assessment Data collected during thousands of customer assessments and decisions.

- Primary Research collected by surveying customers and Trusted Advisors to inform our decision-making process.

- AVANT PATHFINDER: an IT decision making tool and repository of AVANT's market intelligence, empowering comparative searches and intelligent queries.

- AVANT analysts who conduct original research and analyze data for in-depth insight focused on, about and for Trusted Advisors, end-customers, and the surrounding ecosystem.

We also collect content in conjunction with the Trusted Advisor community, through initial assessment data and various market research tools, including surveys, interviews, focus groups, and external reports.

Copyright © 2021 AVANT Communications, Inc.

Key Takeaways

- SASE combines network security functions (such as SWG, CASB, FWaaS, RBI, and ZTNA), with WAN capabilities.

- "SASE is about building that next generation network for application delivery, which means it needs to mitigate risk, reduce costs, or increase productivity and profits." Matt Douglas, CBTS

- Interpretations of what constitutes SASE vary. Vendors will most likely draw those definitions based on the security and networking segments from which they enter the SASE landscape.

- The SASE market will grow at a compound annual growth rate of 116%, CAGR, attaining a market value of $5.1 billion by 2024. – Dell'Oro Group

- In a recent survey of Trusted Advisors conducted by AVANT Research & Analytics, 85% of the respondents were familiar with SASE, and 35% have one or more engagements under way. In 67% of the responses, enhanced security was the customers' most prominent objective.

- According to the survey by AVANT Research & Analytics, more than 90% of customers intend to adopt SASE on an incremental basis, as opposed to using a single engagement approach.

- According to the same survey by AVANT Research & Analytics, 76% of customers turn to Trusted Advisors to provide educational assistance for SASE.

> "SASE is a journey; not a destination."
> - Rich Korn, Masergy

Copyright © 2021 AVANT Communications, Inc.

SASE: The Landscape

Secure Access Service Edge (better known as “SASE,” and pronounced “sassy”) is widely viewed as a critical foundation to providing security in the rapidly expanding environment of cloud computing. Advocates will note that SASE is also an important path towards improving application performance, but AVANT Research & Analytics has learned that the security component is pre-eminent. More than two-thirds of the respondents in our survey point to security as the main benefit of SASE.

The reasoning is compelling.

What once was a relatively straightforward equation of building a virtual moat around the network perimeter has become infinitely more complicated, given that the notion of the network perimeter, itself, has become obsolete in a borderless cloud-based environment in which almost anything can be delivered “as a service.”

While this phenomenon had been gaining momentum for several years, the Covid-19 pandemic further accelerated the trend as work from home was no longer the exception but became the fundamental means of conducting business. Numerous studies show that many employees have a strong preference for a work-from-home paradigm, and some are even quitting their current jobs in favor of employers willing to accommodate that preference. Amidst a veritable Rubik’s Cube of locations and conditions, effective security becomes more important and more challenging than ever.

SASE is a security model, typically cloud-based, which bundles software-defined networking with network security functions, all of which are delivered by a single provider using multiple points-of-presence (POPs) to maintain high performance on a global basis.

SASE combines critical network security functions, such as CASB, RBI, SWG, and ZTNA, with WAN capabilities (e.g. SD-WAN) to deliver secure services and applications at reliable performance levels. Each of these technologies will be defined and further explored below.

As is common with most new(ish) technology concepts, SASE definitions can vary widely as vendors and service providers strive to advance public perceptions that best match their own product/service lines and, by extension, their respective installed bases.

Copyright © 2021 AVANT Communications, Inc.

"The goal of SASE is two-fold. Number One: improving application performance; Number Two, improving security. Everything else is marketing," said Rich Korn, security product specialist at Masergy, a software defined networking services company based in Plano, Texas. "There is so much marketing out there, it is impossible for the customer to truly understand what their options are. And that's why they need the Trusted Advisor. In looking at SASE as a framework, the customers' questions are, what do I need from a connectivity standpoint, on a site-by-site basis, and what do I need from a security standpoint on a site-by-site basis, taking into consideration each site's application performance requirements, security requirements, redundancy requirements, and budgetary requirements. These will vary from site to site, depending on the circumstances."

The transition to SASE is widely recommended to be done on an incremental basis, as opposed to all at once, with buy-in secured from multiple teams within the customer organization. By introducing new technologies consecutively, as opposed to concurrently, any glitches are generally easier to identify, locate, and resolve.

"It's a different kind of platform that moves away from the current paradigm of appliance-rendered capabilities for networking and security," said Mark Peay, channel director at Cato Networks, an Israeli SASE company that converges SD-WAN and network security into a cloud-native service. "Technology needs to be looked at more holistically; to center the enterprise network around the user and identity, as opposed to the data center."

About the Analyst

Ken Presti develops the strategic framework and manages the process of leveraging AVANT's internal data and external data to drive high-value market research designed to help consultants, agents, channel partners, and other members of the Trusted Advisor community more effectively help their business customers understand and evaluate Information Technologies (IT).

Presti brings a wealth of experience in market research, survey development, focus group moderation, interviewing, and content development for the technology industry. His primary area of expertise focuses on go-to-market and channel strategies spanning networking, cloud, security, and telecom.

A former Research Director of IDC's Network Channels & Alliances service, he has served as a Trusted Advisor to several key networking vendors and service providers. Presti also has led his own market research and channel advisory firm, Presti Research & Consulting, and has worked with other prominent channel consultancies. Presti specializes in combining empirical data and his experience partnering with industry leaders to fully illustrate technology trends, business model evolution, likely outcomes, and strategies for success.

Copyright © 2021 AVANT Communications, Inc.

Your SASE Data Points

SASE is, in effect a convergence of several networking and security functions into a unified, cloud-native solution designed to enhance application performance and defense against intruders, malware, and other threats. The Dell'Oro Group, a prominent, California-based market research firm, expects the SASE market will grow at a compound annual growth rate of 116%, attaining a market value of $5.1 billion by 2024. Other projections range upwards to $5.4 billion.

Looking at the component parts of SASE, researcher MarketsandMarkets says the global SD-WAN market is likely to grow from

$1.9 billion in 2020 to $8.4 billion by 2025

The firm expects the global Secure Web Gateway (SWG) market to grow from

$4.6 billion in 2019 to $10.9 billion by 2024

The cloud access security brokers market size is estimated to grow from

$3.34 Billion in 2015 to $7.51 billion by 2020

MarketsandMarkets also projects the global Zero Trust security market size to grow from

$19.6 billion in 2020 to $51.6 billion by 2026

Meanwhile, Firewall as a service, which the firm measured at

$0.56 billion in 2017 is expected to reach $1.70 Billion by 2022.

Copyright © 2021 AVANT Communications, Inc.

Furthermore, in a public blog post by a prominent analyst, Gartner, Inc. has predicted that 30% of enterprises will adopt SWG, CASB, ZTNA and branch office firewall as a service (FWaaS) capabilities from the same vendor by 2024, up from less than 5% in 2020. The firm further predicts that by 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020.

In a recent survey of Trusted Advisors conducted by AVANT Research & Analytics, 85% of the respondents were familiar with SASE, and 35% have one or more engagements under way. In 67% of the responses, enhanced security was the customers' most prominent objective, as shown in the table below.

67% Enhanced Security

14% Simplified Management

9% Cost Savings

7% Operational Efficiency

2% Enhanced Application Performance

Copyright © 2021 AVANT Communications, Inc.

As is frequently recommended, most customers intend to adopt SASE on an incremental basis, as opposed to using a single engagement approach, as shown below.

46% Incremental Migration Planned

44% Likely to be Incremental Migrations

5% Not Likely to be Incremental Migrations

5% No Incremental Migration Planned

Throughout the process, Trusted Advisors will likely factor heavily in SASE migrations, particularly, but not limited to, education for end customers.

Top Reasons to Engage Trusted Advisors in SASE Decisions

76% Education

9% Product/Solution Selection

7% Integration with Legacy Systems

5% Developing Migration Strategy

2% Coordinating Buy-in within Customer Organization

Copyright © 2021 AVANT Communications, Inc.

Business Drivers

The move towards SASE is driven by nothing less than the preservation of the company. If that sounds like hyperbole, consider the effects of a successful ransomware attack that has locked down your data. Will you pay, or will you not pay? Do you have insurance, and does that insurance have the caveats necessary to enable the company to deny your claim? Can you restore from backups, or did the attackers gain control of those, too?

"It's never happened to us before" is the common response of the unprepared, who often use this fact as a reason to refrain from investing in security. Yet once an attack has been unleashed, this reasoning is rarely seen as satisfactory.

On a more benign front, SASE customers also want solid performance from their applications delivered anywhere in the world through reliable connectivity and efficient, policy-based management of an integrated cloud service that addresses both networking and security functions. This can also offload IT teams from menial tasks associated with updates, some aspects of routine maintenance, and the general administration of an on-premises network.

"You can no longer have a rational conversation about security without including the network, and you can no longer have a rational discussion about the network without including security," said Rich Korn of Masergy. "They are much too tightly integrated. The end customer needs to look for someone who can combine those and add a consultative approach. Everyone wins when the partner, the customer, and the technical resources are all on the same page and targeting the desired outcome."

In addition, the integration of the network and security silos, combined with the consolidation of point products can favorably impact the expense line.

Copyright © 2021 AVANT Communications, Inc.

> SASE is about building that next generation network for application delivery, which means it needs to mitigate risk, reduce costs, or increase productivity and profits
>
> -Matt Douglas
>
> Senior Director of Solution Engineering CBTS

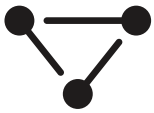
"Compliance is another driver," added Michael McKinnon, senior vice president of Solutions & Engineering at Globalgig, a network services company based in San Antonio, Texas. "It's much easier to check for compliance when you're able to offload your security to central location that can be scanned. The ability to leverage Zero Trust networking is another driver. That basically ties into remote branches and remote users. Trying to develop a Zero Trust network means that if this device is connecting to my network, it's already authorized. The policies are already applied as soon as it hits the network. This is beneficial to customers because, in the traditional scenario, when a device is going onto that network, you have to go in and program that device to meet customer needs. But in this case, all that happens dynamically."

Copyright © 2021 AVANT Communications, Inc.

Technology

As described earlier, the mission of SASE is to deliver effective and secure customer outcomes. With that in mind, any effective SASE solution must include the ability to reliably authenticate users, generally in conjunction with multi-factor authentication (MFA).

Here are a few technologies that frequently come into play when building a strategy for SASE migration:



SD-WAN stands for software-defined wide area network. It provides a flexible, more redundant network that is less complex to manage than a legacy network design.

SD-WAN is transport-agnostic, which means that it can unify different types of connectivity into one cohesive WAN. It also boasts dynamic path selection meaning that it can assess the performance of the available network paths, including packet loss, latency, jitter, and congestion, and select the best available path for the circumstances.

SD-WAN leverages all available circuits, as opposed to requiring rarely used backup networks. By leveraging multiple circuits, SD-WAN provides better performance than any one circuit could on its own, allowing businesses to leverage cost-effective Internet circuits to increase efficiency. Doing so often means moving away from legacy hub-and-spoke designs and avoiding network backhaul.

"SD-WAN is compatible, but SASE is not a replacement for it," said Globalgig's Michael McKinnon. "SASE is about security and remote access. SD-WAN is more about application routing, policy routing, determining the best path for performance, and failover management."

Copyright © 2021 AVANT Communications, Inc.

Technology [cont.]

Zero Trust Network Access (ZTNA)

Whereas many of the component technologies associated with SASE are well known to most IT decision-makers, Zero Trust Network Access stands among the more recent concepts, although these frameworks are not necessarily embedded in every SASE solution.

With ZTNA, every resource is considered to be already compromised, and every individual is considered to be a malicious intruder, until proven otherwise. Users and machines are granted access to specific resources only when necessary and after identities are verified. ZTNA also isolates on the targeted application as opposed to providing access to servers in general, thereby making it more difficult for intruders to move laterally through the network, as is typically the case when Virtual Private Networks (VPN) are in use.

As an example, a user would need permission to access specific files or folders required to do work as opposed to having access to the entire file server. It also uses security tools, such as multifactor authentication, to validate who has access to what information. Not only are users required to prove their identities, but devices are also strategically validated to work with other specific devices.

Copyright © 2021 AVANT Communications, Inc.

> ZTNA is completely in its infancy," said Matt Douglas of CBTS. "ZTNA also forces IT shops to take a close look at how they support work-from-home application access. It's a completely different model.

"There were people saying a few years ago that the VPN client is dead, and that you have to go to ZTNA," Douglas continued. "But that's not what we're seeing in the marketplace. One of the main features that customers want in the new SASE platform is a VPN client. If they're moving away from the data center, they need cloud security, they're going to move to SD-WAN with a lot of Internet connectivity, they've got to figure out how they're going to get their work from home people reliably back, and they are not prepared to make a massive shift to ZTNA. They just want a VPN client that's part of their work from home and SD-WAN fabric. I think you're going to see providers having both a ZTNA option and a VPN option because there are going to be use cases for both of them."

Masergy's Rich Korn agreed. "VPN in the standard sense provides access to an environment," he said. "ZTNA, as opposed to giving access to an environment, gives access only to a specific application. Think of it as a much more focused version of a VPN. It's still a virtual private tunnel, but it goes to a specific application as opposed to an environment, in which case you can then move laterally. You can't move laterally with ZTNA. They are two different methodologies to achieve the same goal of accessing corporate data.

"ZTNA can be great in a SASE context, but not as a standalone component," Korn continued. "You still need to have defense-in-depth with access controls, policy controls, and behavioral monitoring and control. You have to have all three."

Traffic must also be prioritized so that latency-sensitive applications, like Voice over IP (VoIP) and Virtual Desktop Infrastructure (VDI) can take priority over traffic that is less dependent on speed.

The move to ZTNA is seen as a major undertaking that is not to be taken lightly, especially within environments where IT teams are running at full throttle. It can also be a challenge to integrate SASE in organizations where the security team and networking team are siloed and not able to work closely together.

Copyright © 2021 AVANT Communications, Inc.

Firewall as a service (FWaaS) refers to the cloud-based, subscription-based delivery of capabilities commonly associated with firewall hardware. These capabilities include access controls, advanced threat prevention, intrusion prevention systems (IPS), DNS security, packet filtering, network monitoring, deep packet inspection, and Internet Protocol security (IPsec), typically managed from a single pane of glass.

"The firewall inspects inbound outbound traffic, whereas a secure web gateway is for the Internet and is literally a proxy, so if anything bad is happening, it's happening in the gateway before it gets to you," said Niko O'Hara, senior director of Engineering at AVANT. "SWG is an additional layer of internet security on top of having a firewall."

Cloud Access Service Broker (CASB)

Cloud access security broker, referred to as "CASB," is software that allows businesses to safely use the cloud by monitoring user activity and enforcing security policies between users and cloud applications. It is a type of Identity and Access Management technique that is used to regulate who or what can view and use resources in a computing environment. Specific data loss prevention policies can enable the detection of sensitive data in the network and stop that data from being transferred.

This capability has become increasingly important as "shadow IT' and the work-from-anywhere" models have gained momentum.

Secure Web Gateway (SWG)

A secure web gateway, (SWG), enforces policies, supports regulatory compliance, and blocks unwanted and harmful traffic from entering a company's network. This is accomplished through a combination of malicious website detection (URL filtering), application controls, malware blocking (malicious code detection), and intrusion detection and prevention.

Remote Browser Isolation (RBI)

Remote Browser Isolation is a technology that enables the user to access websites or applications over a separate server that then sends an image of that web page to the user's computer without actually accessing the resource from the user's machine. "You're looking at an image instead of being on the website, itself, with a local browser," said AVANT's Niko O'Hara.

Copyright © 2021 AVANT Communications, Inc.

Order of Adoption

Since SASE is something that is generally best implemented over an extended period of time, the order of adoption for the various SASE-related technologies deserves particular consideration.

Start with a thorough review of your circumstances, and then build a strategy based on a three- to five-year time horizon leveraging a cross-functional team representing security, networking, compliance, Finance, IT management, and, of course, your Trusted Advisor. The discussions should begin with preferred business outcomes and then drive downward into more specific details to support users, applications, and remote locations leveraging the cloud and wide area networks. To the extent that non-cloud related assets continue to be in use, consider a cloud migration at the soonest practical time. Perhaps your list of vendors can be consolidated in order to reduce complexity and costs. These are just a few of the variables worthy of consideration. As the migration continues over time, conduct ongoing audits to ensure that the desired effects are being achieved.

"SASE is a journey; not a destination," said Masergy's Rich Korn. "Understand what you need to do and then prioritize and proceed accordingly."

"For some people, SASE will look like it's just too much, which is one of the reasons you might want to migrate over a period of time," said Bill Franklin, senior director of Cloud Engineering at AVANT. "Bring in service providers to run a health or gap assessment and look at it from a posture perspective. Detail your network, operations, and the security side, which will include SASE components like secure web gateway and identity access management. At this point we just want a lay of the land to help us understand the gaps and establish priorities."

"The choice of what to prioritize always begins with the question of what's not working well," said Cato's Mark Peay. "What do people complain about? What's keeping people from being optimally productive? What causes end customers pain? Those are the places you want to start. You can even use hybrid strategies to resolve pain points without having to re-invent the wheel. That's how cloud-based services get peppered in and layered."

Copyright © 2021 AVANT Communications, Inc.

"Start by understanding the network itself and identifying any issues, and cleaning those up, agreed Globalgig's McKinnon. "Regardless of which technologies you'd like to add, if you have underlying issues, they're not magically going to be fixed. So, I would apply SASE after I deal with the network architecture issues. The only exception would be if you had some kind of compliance requirement that needed to be addressed immediately. I don't see any problem with deploying SASE ahead of that. But typically, if you apply SASE while you have an underlying network issue, you're only complicating matters because now you have multiple new components and you have to determine what's causing the problem."

Once priorities are established, the methodology for migration pretty much writes itself.

Another complicating factor may be a managerial reluctance to take a stand in favor of SASE migration or, at the other end of the spectrum, a situation in which you have "too many cooks in the kitchen." In the first case, the CIO or other executives may need to clearly articulate the direction and assign team members to take direct action. In other situations, networking people, security staff, and others may begin jockeying for budgetary position, in which case the resulting strategy may become less coherent. In extreme cases, you may see multiple tools serving the same function because a clear strategy was not in place.

"The network and security teams sometimes don't like each other," added AVANT's Bill Franklin. "Some teams have been stepping on each other's toes for years, in which case you need to start at a place where both sides can agree."

"Some individuals may be more cloud-focused than others who are more appliance-based – which means you may be displacing vendors with whom they've been working for a long time, and that could cause friction."

In such cases it's not just a technical decision; it's a political decision as well.

Copyright © 2021 AVANT Communications, Inc.

Choosing Your Solution

In addition to SD-WAN, ZTNA, CASB, SWG, RBI, and FWaaS, there is a number of other capabilities that should also be considered when choosing your SASE path. These would include DNS protection, sandboxing, and API/application protection. Your Trusted Advisor will be instrumental in helping you to assess the full range of options, including what should be done, and in what order they should be executed.

As you map out your journey, it might become clear that you need fewer technology vendors than you have in the past. If such a move is feasible, this can potentially reduce costs and almost always results in streamlined management procedures and improved visibility into the functions of the network and its security components.

In some cases, you can go from 10 vendors to perhaps two or three. Getting down to a single vendor is often impossible given that there are very few vendors, if any, that will be able to meet every requirement.

You may have different options from different vendors that can be bundled together by the same SASE provider. These decisions should be prominent in your solution selection process, and your Trusted Advisor can be instrumental in helping you to make the right choices.

"If you buy an SD-WAN product from one company and then a next generation firewall and secure web gateway from another, and CASB from someone else, it creates a hodge-podge of vendors that you have to manage," said Peay of Cato. "In some cases, it also drags down performance for the user. Large enterprises often have fiefdoms in which they use certain products because they like them, but we end up with a hodge-podge. It helps to work with the C-suite as much as possible."

Copyright © 2021 AVANT Communications, Inc.

"One theory is that one provider builds everything together with the idea that this will be easier," said Rich Korn of Masergy. "The other option is best-of-breed. You want the simplest design that does not degrade your application performance and your security requirements."

"Our position favors 'best of breed,' but you'd better have a managed services overlay," countered Matt Douglas. "So, our approach to date has been using best of breed but delivering it in a bundled fashion, out of the same project management teams, the same support teams, the same deployment teams. You've got to deliver a best-of-breed solution that feels like a bundle and can be supported like a bundle."

Meanwhile, bear in mind that, for the foreseeable future, interpretations of what constitutes SASE will likely be widely variable. Vendors will most likely draw those definitions based on the security and networking segments from which they enter the SASE landscape. For example, some are more focused on cloud-native offerings while others are more driven by appliances in the customer premises. Such variations in approach are common to new technologies, but it also requires end customers to be diligent in developing a vision for their desired end state. Doing so will go a long way towards ensuring that expenditures are properly aligned.

"You'll also want to understand the ecosystems," added McKinnon. "As you consider different options, it's important to know exactly what the product offerings are. Some have acquired companies and have not fully integrated it, whereas others have done a really good job of this."

Top Questions to Ask Your Trusted Advisor

- How should we design a SASE roadmap?
- How does SASE work, compared to my current technology?
- Will SASE replace MPLS, VPNs, SD-WAN, or similar technologies?
- Help me quantify the business value.
- How can SASE reduce my need for security-related apps and MSP services?
- How will SASE impact the ability of apps and services to work together?
- How difficult is implementation and use?
- How do the vendors compare against one another?
- How much training will be needed, and for whom?
- What feedback are you getting from earlier customers?

Copyright © 2021 AVANT Communications, Inc.

Key Roles

SASE involves companies serving in a variety of roles that represent different portions of the value proposition. The general categories listed below are not mutually exclusive, as different companies may have or merge diverse models. Here are the general categories:

Product Vendor

These companies develop software, hardware, platforms, and solutions. You will likely find some products are more effective than others, and some will work together in the same environment better than others. When they don't interoperate well, they might cancel out one another's benefits or cause systems to work more slowly, due to the different products' poor interaction. Vendors often rely upon Trusted Advisors, managed service providers (MSPs), and indirect channel partners to bring their products to market, though some also may sell directly to the client. From the customer standpoint, direct sales efforts are led by people with quotas and allegiance to one vendor. Thus, the product they offer may or may not be the best fit for your circumstances.

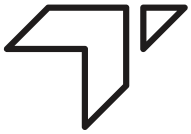
Managed Service Provider (MSP)

MSPs use vendor products, sometimes with a portfolio of vendors to choose from, to deliver a solution. They are not product developers, although some combine different products into a bundled offer – perhaps with an additional homegrown service or software that differentiates them from their competition. MSPs often optimize a given solution to your needs and function in a mode very similar to consultants (see below). In most cases, the buyer will have certain options available but cannot make detailed requirements on which vendors and solutions. This limitation is typically balanced by enhanced simplicity. Carriers can provide managed security services working with an MSP model. In most cases, carrier-based offerings are made in conjunction with other offered services.

Copyright © 2021 AVANT Communications, Inc.

Consultant/Agent/Reseller

This segment typically does not have an internally developed product or technology. Instead, these organizations function as independent entities that help you sort through available options based on your company's needs, budgets, and legacy infrastructure. They do the legwork, understanding each potential solution's differentiators, as well as those of the vendors that provide them. Aside from helping with the pre-sales phase of the engagement, they deploy, optimize, deliver support and training, and help with other facets of technology.



Trusted Advisor

A Trusted Advisor is a technology company that translates the offerings of technology vendors and service providers into integrated solutions that further customers' interests, typically by reducing costs or boosting productivity. They often are called "agents," "resellers," integrators," or "managed service providers," each of which has its own business-model variation. Trusted Advisors are third parties; they are neither owned by a vendor nor part of an internal IT department. They advise clients and make recommendations that customers then use in their decision making.

Copyright © 2021 AVANT Communications, Inc.

Trusted Advisors understand products and their key differentiators. However, their knowledge of technology must interweave with their knowledge of business functions in order to devise technology-based solutions that successfully resolve business problems. Their strategies are, therefore, highly consultative, and Trusted Advisors seek an ongoing and direct line of sight into each customer's needs.

They typically have a technology or vertical specialty that spans multiple technologies, although most will offer an array of services in allied sectors, either directly or via partners. How those specialties align, combined with the resources and footprint of the company, generally determines the portion of the market they serve, ranging from small business to large enterprise.

Trusted Advisors specializing in the technology-of-interest are generally the first step enterprise decision makers take in their acquisition process.

Copyright © 2021 AVANT Communications, Inc.

Action Items

"ZTNA can be great in a SASE context, but not as a standalone component. "You still need to have defense-in-depth with access controls, policy controls, and behavioral monitoring and control. You have to have all three." Rich Korn, Masergy

"The choice of what to prioritize always begins with the question of what's not working well. What do people complain about? What's keeping people from being optimally productive? What causes end customers pain? Those are the places you want to start." Mark Peay, Cato

In addition to SD-WAN, ZTNA, CASB, SWG, and FWaaS, there is a number of other capabilities that should also be considered, including DNS protection, Remote browser isolation, sandboxing, and API/application protection. Your Trusted Advisor will be instrumental in helping you to assess the full range of options.

Start with a thorough review of your circumstances, and then build a strategy based on a three- to five-year time horizon leveraging a cross-functional team representing security, networking, compliance, Finance, IT management, and, of course, your Trusted Advisor.

Copyright © 2021 AVANT Communications, Inc.

SASE Vendors

The Major Players in the SASE Market include:

- Akamai
- Broadcom
- Cato Networks
- CBTS
- Check Point Software Technologies
- Cisco
- Citrix
- Cloudflare
- Forcepoint
- Fortinet
- Globalgig
- Masergy
- McAfee
- Netskope
- Open Systems
- Palo Alto Networks
- Versa
- VMware
- Zscaler

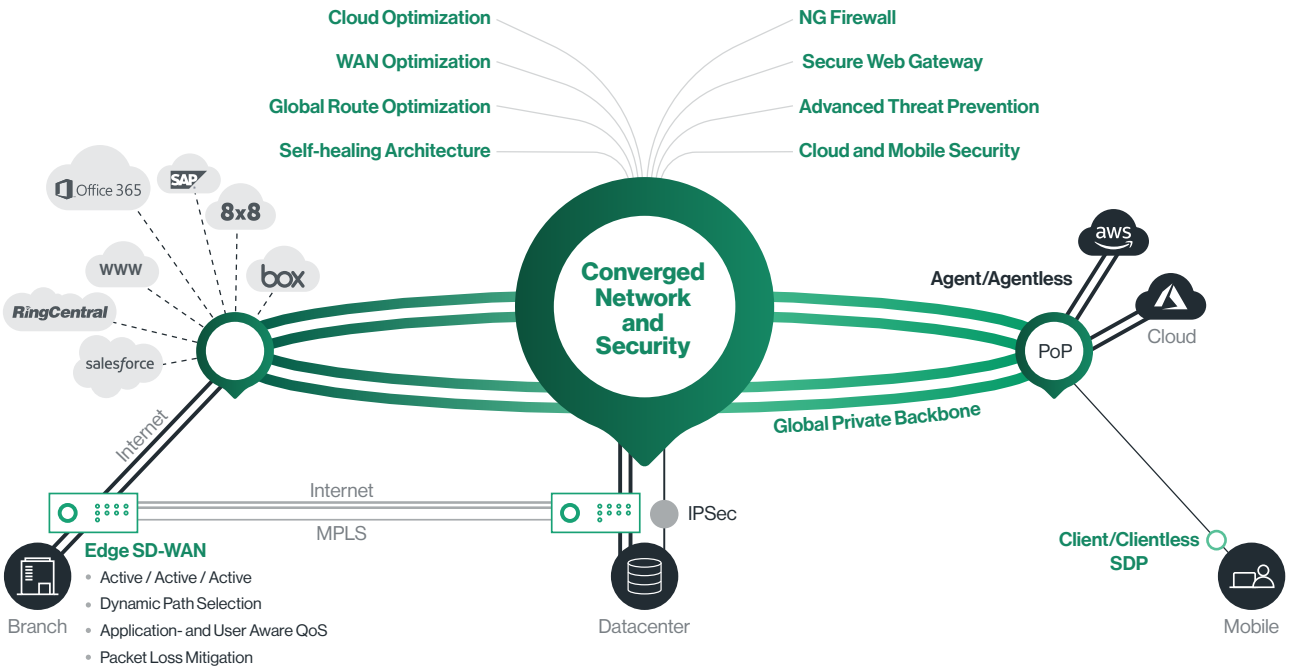
Copyright © 2021 AVANT Communications, Inc.

Cato Networks

The World's First SASE Platform

Global, SD-WAN, Security, Cloud , Mobility. **Converged.**

Cato provides a global, converged SD-WAN and network security cloud service. Cato enables you to move away from legacy MPLS, a bundle of security point solutions, and expensive managed services, to a simple, agile, and affordable network. Self-service or a managed service is up to you.



Aligned with the principles set by Gartner's Secure Access Service Edge (SASE) framework, Cato's global, cloud-native, and software-defined architecture enables you to optimize the user experience, protect users against emerging threats, and embrace new business opportunities – everywhere. With Cato, your network, and your business, are ready for whatever's next.

Tech Shorthand

Cloud Access Security Broker (CASB) is software that allows businesses to safely use the cloud by monitoring user activity and enforcing security policies between users and cloud applications. It is a type of Identity and Access Management technique that is used to regulate who or what can view and use resources in a computing environment. Specific data loss prevention policies can enable the detection of sensitive data in the network and stop that data from being transferred.

Firewall as a Service (FWaaS): Firewall as a service refers to the cloud-based, subscription-based delivery of capabilities commonly associated with firewall hardware. These capabilities include access controls, advanced threat prevention, intrusion prevention systems (IPS) DNS security, packet filtering, network monitoring, deep packet inspection, and Internet Protocol security (IPsec), typically managed from a single pane of glass.

Remote Browser Isolation (RBI): Remote Browser Isolation is a technology that enables the user to access websites or applications over a separate server that then sends an image of that web page to the user's computer without actually accessing the resource from the user's machine.

SD-WAN: A Software-defined wide area network provides a flexible, more redundant network that is less complex to manage than a legacy network design. It is transport-agnostic, which means that it can unify different types of connectivity into one cohesive WAN. It also boasts dynamic path selection meaning that it can assess the performance of the available network paths, including packet loss, latency, jitter, and congestion, and select the best available path for the circumstances.

Secure Web Gateway (SWG): A secure web gateway enforces policies, supports regulatory compliance, and blocks unwanted and harmful traffic from entering a company's network. This is accomplished through a combination of malicious website detection (URL filtering), application controls, malware blocking (malicious code detection), and intrusion detection and prevention.

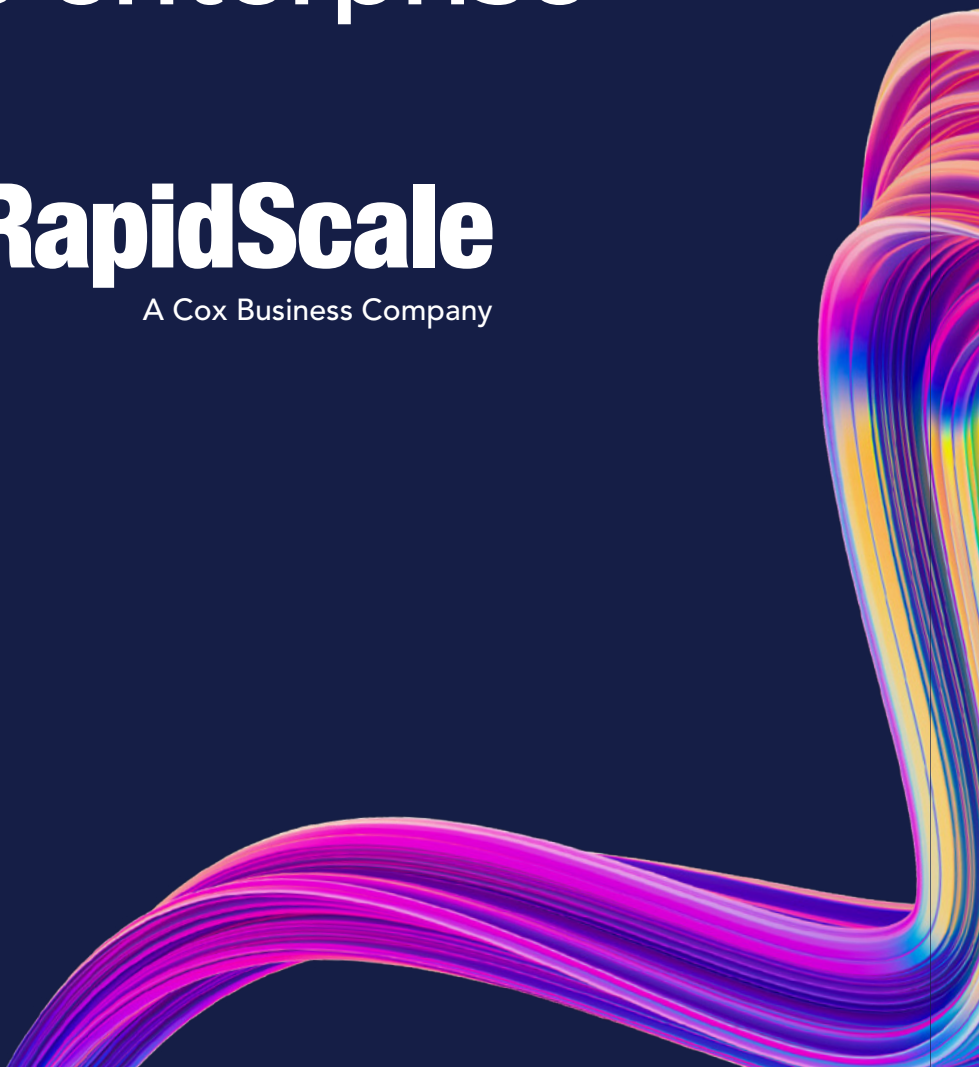
Zero Trust Network Access (ZTNA): With Zero Trust Access, every resource is already compromised, and every individual is considered to be a malicious intruder until proven otherwise. Users and machines are granted access to specific resources only when necessary and after identities are verified. ZTA also isolates on the targeted application as opposed to providing access to servers in general, thereby making it more difficult for intruders to move laterally through the network, as is typically the case when Virtual Private Networks (VPN) are in use.

Copyright © 2021 AVANT Communications, Inc.

Flexible enough for the SMB and powerful enough for the enterprise

RapidScale

A Cox Business Company



Increase IT productivity, improve security and empower remote workforces with managed cloud solutions.

Learn more at rapidscale.net

Acknowledgements

Our Partners:

Matt Douglas, CBTS; Rich Korn, Masergy; Michael McKinnon, Globalgig; Mark Peay, Cato

The Avant Team:

Erin Christianson, Joe Colletti, Joan Courtney, Alex Danyluk, Jennifer Gallego, Jesse Garing, Lindsay Giersch, Jen Greco, Isaiah Hogberg, Tony Ikpi, Jace Inman, Brooke Kennedy, Prerna Khandelwal, Ian Kieninger, Drew Lydecker, Jaime Matoba, Shane McNamara, Rob Merhej, Juan Ochoa, John Paullin, Bana Qashu, Rick Reed, Scott Sawyer, JP Tucker, Lily Weibel, Brent Wilford

Technical Advisors:

Bill Franklin, Niko O'Hara

Lead Analyst

Ken Presti

Public Relations

Walker Sands

Copyright © 2021 AVANT Communications, Inc.

SASE

AVANT 6-12 Report

Copyright © 2021 AVANT Communications