The 10 Tenets of an Effective SASE Solution

paloalto® NETWORKS | PRISMA® BY PALO ALTO NETWORKS

Table of Contents

Introduction

The 2020 pandemic has forever shifted the way businesses operate. As businesses continue to reopen, hybrid workforces are now the new normal, requiring access to business services, applications, and data from any location. Organizations are still transforming their networks to provide uninterrupted connectivity while maintaining security to those working in offices, at home or on the road.

Prior to the pandemic, organizations were already facing the challenges that legacy network and network security technologies presented, dramatically limiting their ability to manage new traffic patterns and security threats. Organizations were forced to adopt multiple point products to address changing business requirements, such as firewalls, secure web gateways, cloud access security broker solutions, and SD-WAN. The pandemic exacerbated these challenges, as businesses were now forced to rapidly support global remote working while ensuring privacy and security.

The concept of a secure access service edge (SASE) came to fruition in 2019. Coined by Gartner, SASE (pronounced "sassy") is designed to help organizations embrace cloud and mobility by providing network and network security services from a common cloud-delivered architecture. A SASE solution must provide consistent security services, and access to all types of cloud applications (e.g., public cloud, private cloud, SaaS) delivered through a common framework.

Not all SASE solutions are created equal. An effective SASE solution must converge SD-WAN and security into a single, integrated offering that delivers consistent protection with a high-performance experience for all users, regardless of location.

This e-book will help you understand the 10 tenets of an effective secure access service edge.

Tenet 1: Software-Defined Wide Area Network

What Isn't Working

Companies have embraced the software-defined wide area network (SD-WAN) to connect branch offices to the corporate network and provide local internet breakout as an alternative to costly MPLS connections. Legacy SD-WAN solutions present many challenges, as they rely on taking the traditional model of packet routing and forcing it to fit the cloud-ready enterprise. In addition, these legacy solutions lack scale and require branch services, such as networking and visibility, to be bolted on, adding cost and complexity.

The SASE Way

In a SASE solution, the branch architecture is completely cloud-delivered. Organizations can enable branch services, including security and networking, to be completely delivered from the cloud, simplifying WAN management and increasing ROI.

Key Takeaways

As you look to simplify your SD-WAN solution, you should consider a solution that is cloud-delivered and autonomous—like SASE. Your SD-WAN solution should be application-defined rather than packet-based for better application visibility, enabling app SLAs that include SaaS, cloud, and UCaaS. What's more, SASE is the convergence of networking and security; thus, an effective SASE solution must offer integrated SD-WAN with consistent policies as part of a cohesive platform, versus the alternative approach of bolting on disparate products from multiple vendors.

> "By 2024, more than 70% of software-defined wide-area network (SD-WAN) customers will have implemented a secure access service edge (SASE) architecture, compared with 40% in 2021."[1]
>
> –Gartner

[1] Jonathan Forest, Naresj Singh, Andrew Lerner, Evan Zeng, *2021 Gartner Magic Quadrant for WAN Edge Infrastructure*, Gartner, September 20, 2021.

Tenet 2: Zero Trust Network Access

What Isn't Working

Companies still stuck in legacy virtual private network (VPN) architectures lack the necessary security protections and policies needed to keep their users and data safe. Zero Trust Network Access (ZTNA) requires users who want to connect to an application to first authenticate through a gateway before gaining access. This provides security administrators the ability to identify users and create policies to restrict access, minimize data loss, and quickly mitigate potential threats.

Many ZTNA products are based on software-defined perimeter (SDP) architectures, which do not provide content inspection, thus creating a discrepancy in the types of protection available for each application. In terms of consistent protection, the organization must build additional controls on top of the ZTNA model and establish inspection for all traffic across all applications.

The SASE Way

SASE builds upon the ZTNA key principles and applies them across all the other services within a SASE solution. By accurately identifying users, devices, and applications, no matter where they are connecting from, policy creation, management, and enforcement are simplified. SASE removes the complexity of connecting to a gateway by incorporating required networking and security services into a single unified cloud framework.

Key Takeaways

A SASE solution should incorporate continuous threat assessment and trust validation into ZTNA for protecting applications as well as apply other security services for the consistent enforcement of data loss prevention (DLP) and threat prevention policies. This is because access controls, in of themselves, are useful for establishing who the person is, but other security controls are necessary to ensure their behaviors and actions are not harmful to the organization. It is also necessary to extend the same controls across access to all applications.

> **"80% of new digital business applications opened up to ecosystem partners** will be accessed through zero trust network access (ZTNA), and by 2023 60% of enterprises will phase out their remote access virtual private networks (VPN) in favor of ZTNA."[2]
>
> –Gartner

[2] Steve Riley, *Gartner Market Guide for Zero Trust Network Access*, Gartner, July 30, 2020.

Tenet 3: Cloud Access Security Broker

What Isn't Working

Today's digital businesses with hybrid workforces struggle to keep up with the explosion of SaaS application usage across their organization. Their sensitive data is increasingly exposed across multiple applications while cloud-based threats continue increasing in volume and sophistication. Current CASB solutions only solve part of the problem as they fail to provide adequate visibility and control along with robust security to help organizations monitor SaaS usage, protect their sensitive data, and prevent SaaS application risks. Also, they are disjointed from the security infrastructure and are quite complex to deploy and manage.

The SASE Way

CASB is a core component of SASE, creating a single platform for administrators to manage security controls for all application types. A SASE solution with integrated CASB helps you understand which SaaS apps are being used and where sensitive data is going, no matter where users are located.

Key Takeaways

Your SASE solution should be able to automatically keep pace with the explosion of SaaS applications—including modern collaboration applications—by incorporating both inline and API-based SaaS controls for governance, access controls, and data protection. To provide superior visibility, management, security, and zero-day protection against emerging threats, SASE should also deliver comprehensive cloud-delivered enterprise DLP that utilizes ML for more accurate detection and real-time protection of sensitive data across the entire enterprise.

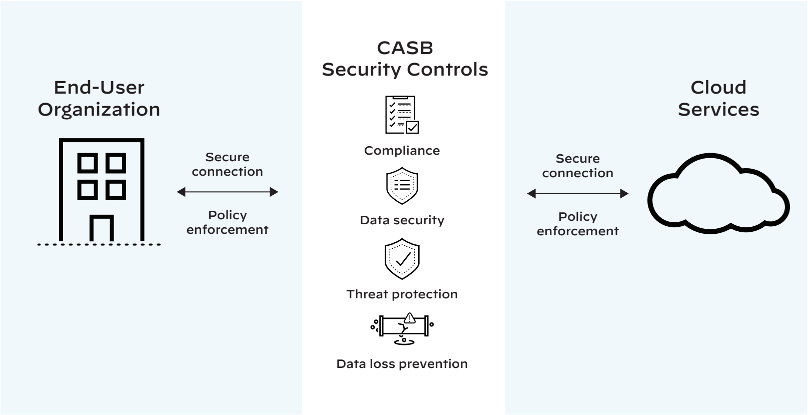


Figure 1: How CASB works

Tenet 4: Firewall as a Service

What Isn’t Working

Physical or virtual firewalls are required anywhere applications or users exist, whether headquarters, branch offices, data centers or the cloud. With the explosion of remote users and apps everywhere, organizations struggle to manage dozens to hundreds of firewalls.

Firewall as a service (FWaaS) is a deployment method for delivering firewall functionality as a cloud-based service, and good FWaaS offerings will provide the same features as a next-generation firewall.

The SASE Way

A SASE solution incorporates FWaaS into its unified platform, providing the same services as a next-generation firewall but as a cloud-delivered service. By encompassing the FWaaS service model within a SASE framework, organizations can easily manage their deployments from a single platform.

Key Takeaways

A SASE solution should enable FWaaS capabilities equivalent to the protections of a next-generation firewall by implementing network security policy in the cloud. It is important to ensure your SASE solution does not only provide basic port blocking or minimal firewall protections. You need the same features a next-generation firewall embodies and the features cloud-based security offers, such as threat prevention services and DNS security.

> “By 2025, 30% of new distributed branch office firewall deployments will switch to firewall as a service, up from less than 10% in 2021.”[3]
>
> –Gartner

[3] Rajpreet Kaur, *Magic Quadrant™ for Network Firewalls*, Gartner, December 15, 2021.

Tenet 5: Secure Web Gateway

What Isn't Working

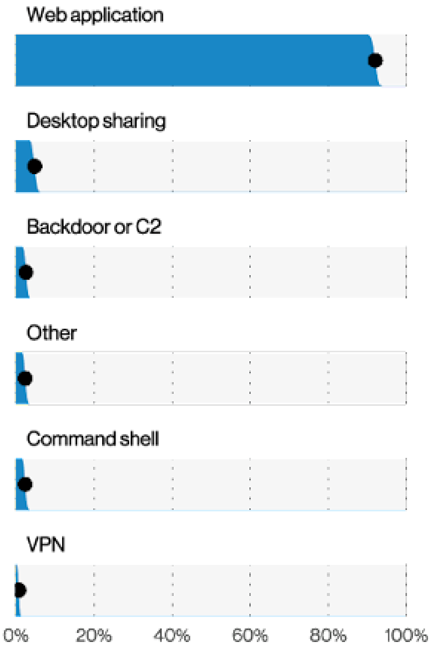
As enterprises continue to adopt hybrid cloud strategies and offer flexible work-from-anywhere options for their employees, they need a security solution that can secure all their apps. Traditionally, organizations relied on secure web gateway (SWG) products to protect users and devices from accessing malicious or inappropriate websites. SWG with DNS security can be used to block inappropriate content (e.g., pornography, gambling) or websites that businesses simply don't want users accessing while at work, such as streaming services (like Netflix). Unfortunately, SWGs are offered as separate appliances or services, resulting in users receiving inconsistent policy enforcement when they are onsite at work or remote. What's more, in today's hybrid world, SWG security only looks at web-based traffic and protocols, completely ignoring non-web traffic, applications and data, leaving organizations, their users, and data exposed.

The SASE Way

SWG is just one of the many security services that a SASE solution must provide, which also includes FWaaS, CASB and ZTNA. A SASE platform that includes SWG security should enable complete visibility and control over all traffic, regardless of where a user may be located, to ensure the secure use of cloud-based apps and other web services. As organizations grow and add more and more remote users, the SASE cloud SWG will automatically scale to support organizational growth.

Key Takeaways

A SASE solution includes the same security services as a traditional SWG as well as additional security services, allowing organizations to control access to web and non-web applications and enforce security policies that protect all ports, protocols and applications. Combined with DNS security and an explicit proxy, SWG provides a simple onboarding mechanism and a seamless method for organizations to transition from legacy, stand-alone SWG to a more secure SASE architecture.



Verizon 2021 DBIR Report

Figure 2: Top hacking vectors in breaches

Tenet 6: Digital Experience Monitoring

What Isn't Working

User experience is critical for employee satisfaction and productivity. A digital experience is now necessary as employees need to work from anywhere. IT teams struggle with visibility challenges on the application, network and device side of things like Wi-Fi, often requiring manual and labor-intensive troubleshooting sessions to solve any remediation issues.

The SASE Way

Autonomous Digital Experience Management (ADEM) provides end-to-end visibility and insights to create a seamless digital user experience. Encompassed with SASE, ADEM provides segment-wise insights across the entire service delivery path, allowing real and synthetic traffic analysis that enables organizations to proactively drive remediation of digital experience problems.

Key Takeaways

Optimizing the user experience is crucial now that employees are working from anywhere. To benefit both the user and IT teams, your SASE solution should incorporate ADEM for comprehensive visibility, faster remediation, and detailed performance insights into endpoint devices, Wi-Fi, network paths, and applications.

> "IT leaders will have to report user experience metrics for 70% of the technology undertakings their companies launch in 2025. That's up from only 15% in 2019."[4]
>
> –Gartner

[4] Federico De Silva, *Market Guide for Digital Experience Monitoring*, Gartner, October 16, 2020.

Tenet 7: Threat Prevention

What Isn't Working

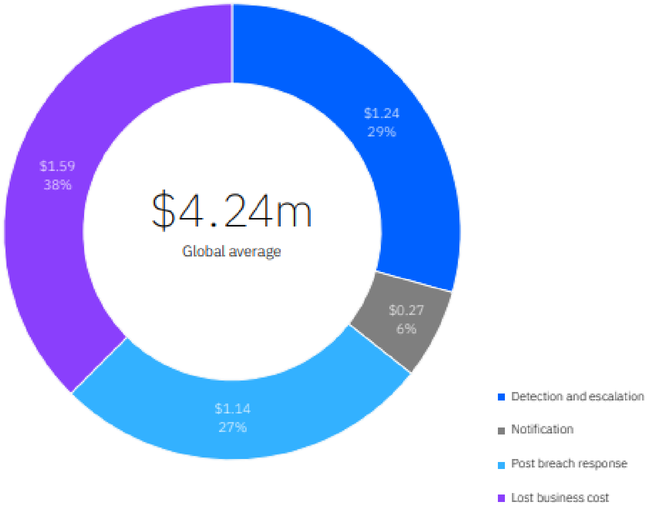
In today's world of small- to large-scale breaches, where ransomware attacks occur on a daily basis, threat prevention is key to protecting your organization's data and employees. There are various threat prevention tools out there, from anti-malware to intrusion prevention and file blocking, providing organizations ways to stop threats. However, these point products require separate solutions, making management and integration difficult and often taking too long to identify and respond to threats.

The SASE Way

Within a SASE solution, all these point products and services are now integrated within a single cloud platform. This provides simplified management and oversight of all threats and vulnerabilities across your network and cloud environments. Machine learning capabilities should be included in SASE, allowing the prevention of other unknown threats in near-real time and extending visibility and security to all devices, including never-seen-before IoT devices.

Key Takeaways

Stopping exploits and malware by using the latest threat intelligence as well as advanced machine learning and artificial intelligence is crucial to protecting your employees and data. Your SASE solution should incorporate threat prevention tools into its framework so you can react quickly and swiftly to remediate threats. Inline machine learning should also be incorporated so unknown file- and web-based threats are instantly prevented. Additionally, automated policy recommendations can save time and reduce the chance of human error.



IBM Cost of a Data Breach Report 2021

Figure 3: Average total cost of a data breach divided into four categories

Tenet 8: Internet of Things

What Isn't Working

Internet of Things (IoT) devices are often unmanaged by an organization but connected to the corporate network. This introduces security gaps, as these devices often have vulnerabilities, rely on users to install updates, and offer limited visibility to IT teams in what they are accessing. Costly IoT security sensors and appliances offer a partial solution but create operational inefficiencies and headaches.

The SASE Way

With SASE, IoT security should be integrated into the platform to secure remote branches, sites, and workers from the cloud. By utilizing the cloud, SASE is able to accurately detect devices for full visibility and enforce policies to ensure security across the network, eliminating the need for additional IoT security solutions.

Key Takeaways

Organizations are adopting IoT devices as older technology transforms into future tech, like smart thermostats and smart lighting systems. It is not just smartphones and watches as well as laptops that need to be protected when on the corporate network. A SASE solution should incorporate machine learning and AI, allowing organizations with greater autonomy to quickly identify and remediate threats.

> "From January to June of 2021, some 1.51 billion breaches of Internet of Things (IoT) devices took place, an increase from 639 million in 2020."[5]
>
> –IoT World Today

[5] Callum Cyrus, "IoT Cyberattacks Escalate in 2021, According to Kaspersky," IoT World Today, September 17, 2021.

Tenet 9: Data Loss Prevention

What Isn’t Working

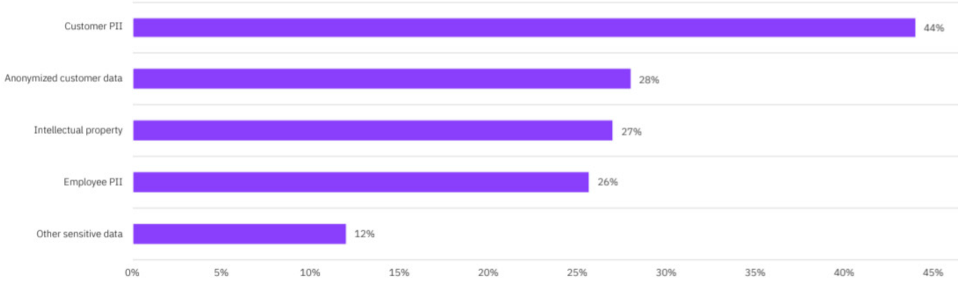
Data loss prevention (DLP) tools protect sensitive data and ensure it is not lost, stolen, or misused. DLP is a composite solution that monitors data within the environments where it is deployed (such as network, endpoints, and cloud) and through their egress points. It also alerts key stakeholders when policies are violated. Due to compliance requirements from HIPAA to PCI DSS, GDPR, etc., DLP is a crucial solution needed for data security and compliance. Legacy DLPs rely on old core technology initially designed for on-premises perimeters and subsequently extended and adapted to cloud applications. Loaded with features, disjointed policies, configurations, and workarounds, DLPs have become very complex, difficult to deploy at scale, and too expensive. Digital transformation and new data usage models demand a fresh approach to data protection.

The SASE Way

Through the SASE approach, DLP becomes one cloud-delivered solution centered around the data itself, everywhere. The same policies are consistently applied to sensitive data, at rest, in motion, and in use, regardless of its location. In the SASE architecture, DLP is not a stand-alone solution anymore but is embedded in the organization’s existing control points, thus eliminating the need to deploy and maintain multiple tools. With SASE, organizations can finally enable a comprehensive data protection solution that relies on a scalable and simple architecture while enabling effective machine learning by leveraging access to global traffic.

Key Takeaways

DLP is a necessary tool to protect sensitive data and ensure compliance throughout the organization. To this end, the SASE solution must include this core capability. With SASE, DLP is an embedded, cloud-delivered service used to accurately and consistently identify, monitor, and protect sensitive data everywhere—across networks, clouds, and users.



IBM Cost of a Data Breach Report 2021

Figure 4: Types of records compromised

Tenet 10: Platform Extensibility

What Isn't Working

Organizations are embracing the cloud, but adding and integrating multiple cloud-based services from different vendors can be complex. It is difficult to find one tool that solves every single challenge, so it is important to have solutions that can talk to each other to eliminate security gaps. Unfortunately, not many cloud solutions are designed to elegantly integrate with third-party services, and vendors often don't want to help organizations along that journey.

The SASE Way

A SASE solution should embrace the integration of third-party services and simplify the process for administrators by providing a platform that easily integrates these services. By providing a platform for integration, organizations can quickly add the services they need with the full support of their SASE provider.

Key Takeaways

With an extensible SASE solution, organizations can easily add services to the platform, addressing all possible use cases. Without the deterrent of point solutions that are not integrated with each other, organizations can increase their capabilities and functionality with their existing third-party services to satisfy their needs.

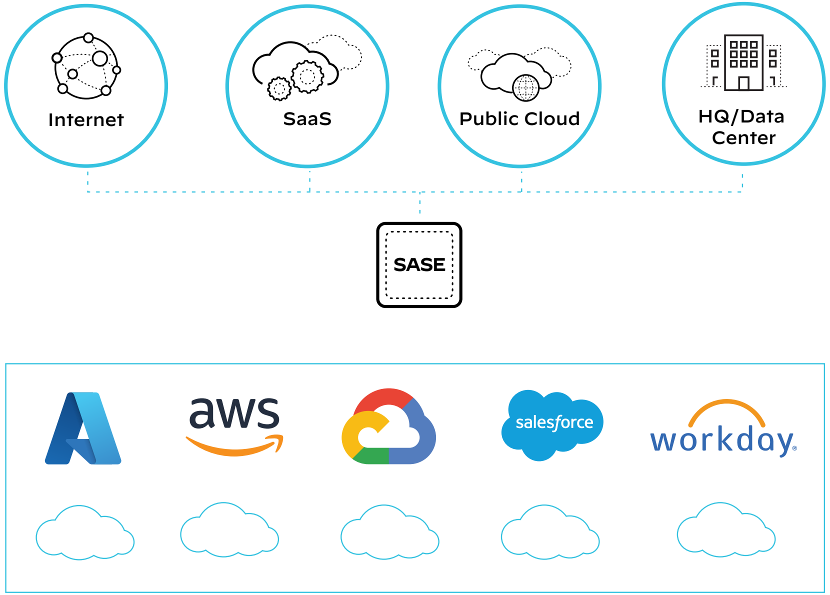


Figure 5: The SASE solution

How Palo Alto Networks Can Help

Palo Alto Networks offers the industry's most comprehensive SASE solution with Prisma® SASE. Prisma SASE combines cloud-delivered security to prevent cyberattacks and consistently protects all traffic, on all ports, and from all applications, with the industry's first Next-Generation SD-WAN solution that uses machine learning and automation to simplify both network and security operations and provide an exceptional user experience.

Organizations can embrace their remote workforces, knowing they can provide broad security and connectivity for their remote users and branch locations. Rather than creating single-purpose technology overlays that are normally associated with point products, Prisma SASE uses a common cloud-based infrastructure that delivers multiple types of security services and combines networking services to provide a complete solution. In addition, customers can benefit from comprehensive threat intelligence powered by automated threat data from Palo Alto Networks and hundreds of third-party feeds.

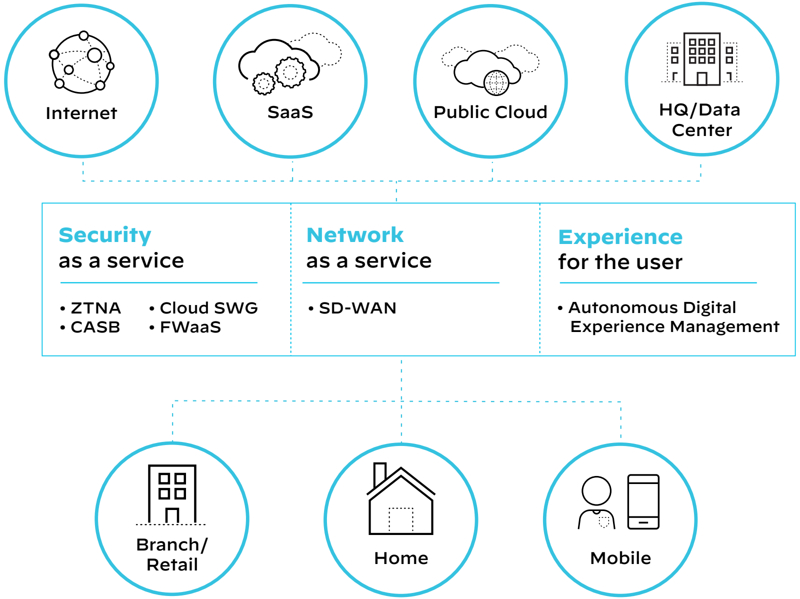


Figure 6: Prisma SASE

Conclusion

As hybrid work continues for organizations and cloud adoption grows, we encourage you to consider a comprehensive SASE solution to solve your networking and networking security needs.

Palo Alto Networks Prisma SASE is the industry's most complete SASE solution, converging network security, SD-WAN, and ADEM into a single cloud-delivered service. It offers:

1. **Convergence without compromise**
   It consolidates multiple point products, including ZTNA, Cloud SWG, CASB, FWaaS, and SD-WAN, into a single integrated service, reducing network and security complexity while increasing organizational agility.
2. **Complete, best-in-class security**
   Prisma SASE consistently secures all apps used by your hybrid workforce, regardless of whether users are remote, mobile, or working from a branch office. Our proven cloud-delivered security services leverage ML-powered threat prevention to instantly stop 95% of web-based threats inline, significantly reducing the risk of a data breach.
3. **Exceptional user experience**
   Prisma SASE includes the industry's only SASE-native ADEM that helps ensure an exceptional experience for your end users. With end-to-end visibility and insights across both mobile and branch users, guaranteed by performance SLAs that are 10X better than the closest competitors, your employees will be happier and more productive.

Learn more about Palo Alto Networks Prisma SASE.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com