paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

The 10 Tenets of an Effective SASE Solution

Table of Contents

Introduction

The COVID-19 pandemic has forever shifted the way businesses operate. With skyrocketing remote workforces and their need to access business services, applications, and data from their homes, organizations scrambled to transform their networks and provide uninterrupted connectivity while maintaining security.

Prior to the pandemic, organizations were already facing the challenges that legacy technologies presented, dramatically limiting their ability to manage constantly evolving traffic types and security threats. Organizations were forced to adopt multiple point products to address changing business requirements, such as firewalls, secure web gateways (SWGs), cloud access security broker (CASB) solutions, and software-defined wide area networking (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 2018. 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—public cloud, private cloud, and software as a service (SaaS)—delivered through a common framework.

By removing multiple point products and adopting a single cloud-delivered SASE solution, organizations can reduce complexity; rapidly deploy and scale out remote workers and branch locations; and enforce consistent security no matter where users are, all while saving significant technical, human, and financial resources.

This e-book will help you to understand the 10 tenets of an effective SASE.

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 multiprotocol label switching (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 their return on investment (ROI).

KEY TAKEAWAY

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 unified communications as a service (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 60% of software-defined, wide-area network (SD-WAN) customers will have implemented a secure access service edge (SASE) architecture, compared with about 35% in 2020."

2020 Gartner Magic Quadrant for WAN Edge Infrastructure

Tenet 2: Zero Trust Network Access

WHAT ISN'T WORKING

Companies still lack the necessary security protections and policies 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 prior to 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. Identifying users, devices, and applications no matter where they are connecting from simplifies policy creation and management. SASE removes the complexity of connecting to a gateway by incorporating the networking services into a single unified cloud framework.

KEY TAKEAWAY

A SASE solution should incorporate 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 and of themselves, are useful for establishing who a user is, but other security controls are necessary to ensure that user's behaviors and actions are not harmful to the organization. It is also necessary to extend the same controls across access to all applications.

> **"Many companies are not regulating which apps their employees are using—only 62% have banned the installation of unapproved apps within their AUP."**
>
> ***Verizon Mobile Security Index 2020 Report***

Tenet 3: Cloud Access Security Broker

WHAT ISN'T WORKING

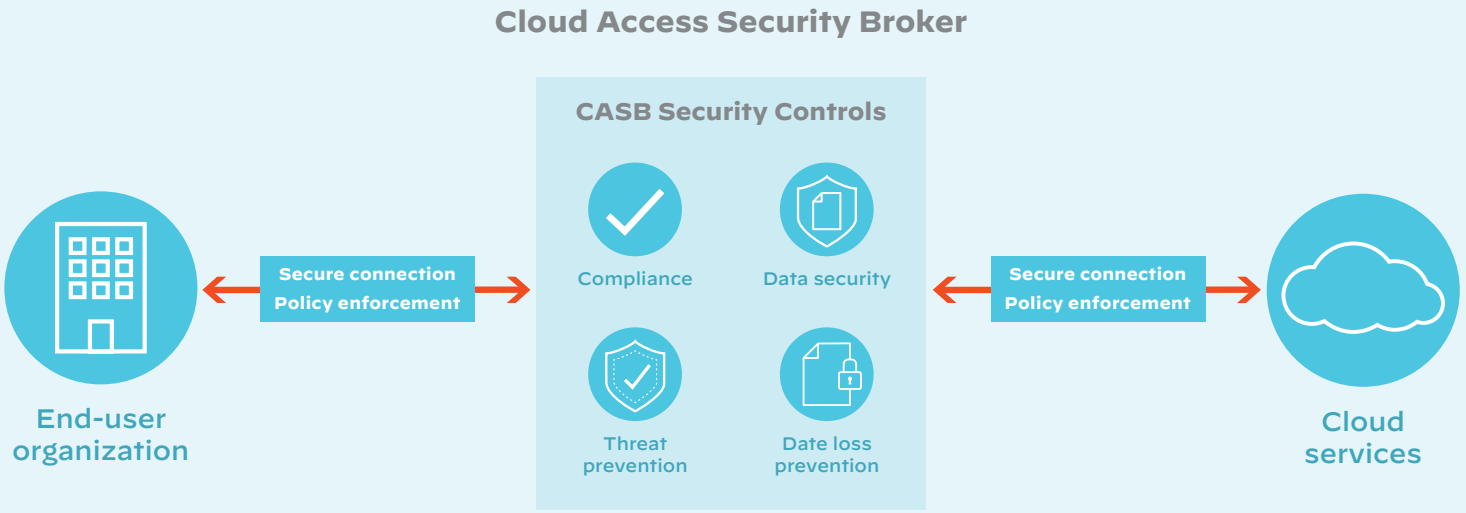
Many organizations depend on cloud access security brokers (CASBs) to provide visibility into where their data resides (e.g., SaaS apps), enforce company policies for user access, and protect their data from hackers. CASBs are cloud-based security policy enforcement points that provide a gateway for both your SaaS provider and employees.

THE SASE WAY

CASB is another security service that a SASE solution should absorb, creating a single platform for stakeholders to manage security controls for all application types. A SASE solution helps you understand which SaaS apps are being used and where data is going, no matter where users are located.

KEY TAKEAWAY

Your SASE solution should incorporate 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 combine inline and API-based security as well as contextual controls. This is also called a multi-mode CASB.



Tenet 4: Firewall as a Service

WHAT ISN'T WORKING

Physical or virtual firewalls are required anywhere applications or users exist, whether that is headquarters, branch offices, data centers, or the cloud. With the explosion of remote users and apps everywhere, organizations are struggling 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 TAKEAWAY

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 as well as 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 5% in 2020."

2020 Gartner Magic Quadrant for Network Firewalls

Tenet 5: Secure Web Gateway

WHAT ISN'T WORKING

Organizations rely on secure web gateway (SWG) 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 on-site at work or remote.

THE SASE WAY

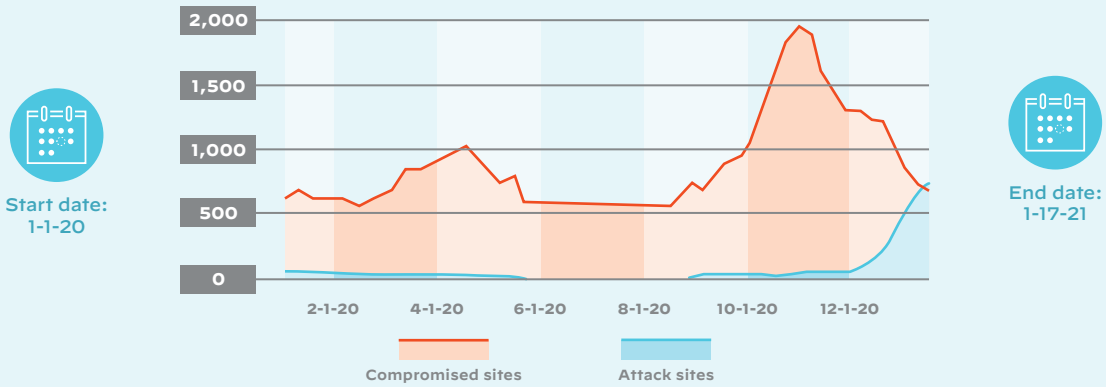
SWG is just one of the many security services that a SASE solution must provide. A cloud SWG provided by a SASE platform enables complete visibility and control over the entire network, regardless of where a user may be located, to ensure the secure use of cloud-based apps and other web services. As organizations grow and add more and more remote users, the SASE cloud SWG will automatically scale to support the organizational growth.

KEY TAKEAWAY

A SASE solution includes the same security services as a traditional SWG, allowing organizations to control access to the web and enforce security policies that protect users from hostile websites or inappropriate content. Combined with DNS security and an explicit proxy, SWG provides a simple onboarding mechanism for organizations to transition to a SASE architecture.

Google Transparency Report: Sites Hosting Malware from January 2020-January 2021

https://transparencyreport.google.com/safe-browsing/overview?hl=en



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 network and device side of things, often requiring manual and labor-intensive troubleshooting sessions to solve any remediation issues.

THE SASE WAY

Autonomous digital experience monitoring (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 the ability to drive autonomous remediation of digital experience problems as they occur.

KEY TAKEAWAY

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, automated 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, according to Gartner."

2020 Gartner Market Guide for Digital Experience Monitoring

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 they often take 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 TAKEAWAY

Stopping exploits and malware by using the latest threat 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.

Why Threat Detection and Response Is More Difficult Today

ESG Master Survey Results: The Threat Detection and Response Landscape

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 IT teams limited visibility into what they are accessing. Costly IoT security sensors and appliances offer a partial solution but create operational inefficiencies and headaches.

THE SASE WAY

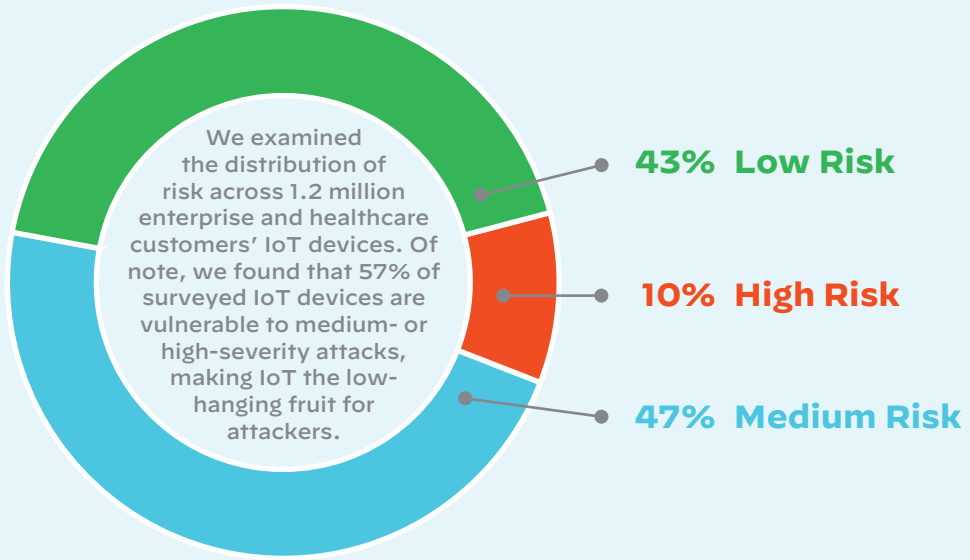
With SASE, IoT security should be integrated into the platform to secure remote branches, sites, and workers from the cloud. By utilizing the cloud, SASE is able to accurately detect devices for full visibility and enforce policies to ensure security across the network, eliminating the need for additional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

KEY TAKEAWAY

Organizations are adopting IoT devices as older technology transforms into future tech, such as smart thermostats and smart lighting systems. It is no longer just smartphones, smartwatches, and laptops that need to be protected when on the corporate network. A SASE solution should incorporate machine learning and AI, allowing organizations greater autonomy to quickly identify and remediate threats.

"57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT the low-hanging fruit for attackers."

2020 Unit 42 IoT Threat Report, Palo Alto Networks



Tenet 9: Data Loss Prevention

WHAT ISN'T WORKING

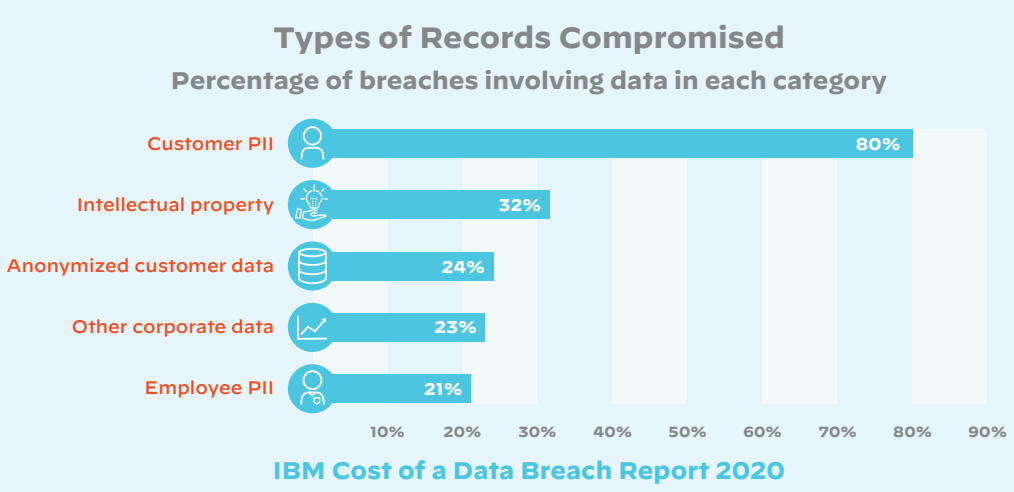
Data loss prevention (DLP) tools protect sensitive data and ensure it is not lost, stolen, or misused. DLP is a composite solution that monitors data within the environments where it is deployed (e.g., networks, endpoints, clouds) and through their egress points. It also alerts key stakeholders when policies are violated. Due to compliance requirements such as HIPAA, PCI DSS, and GDPR, 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 standalone 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 TAKEAWAY

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.



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 TAKEAWAY

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.

"Security and risk management leaders should reduce complexity by moving to one vendor for SWG, CASB, DNS, ZTNA, and remote browser isolation capabilities."

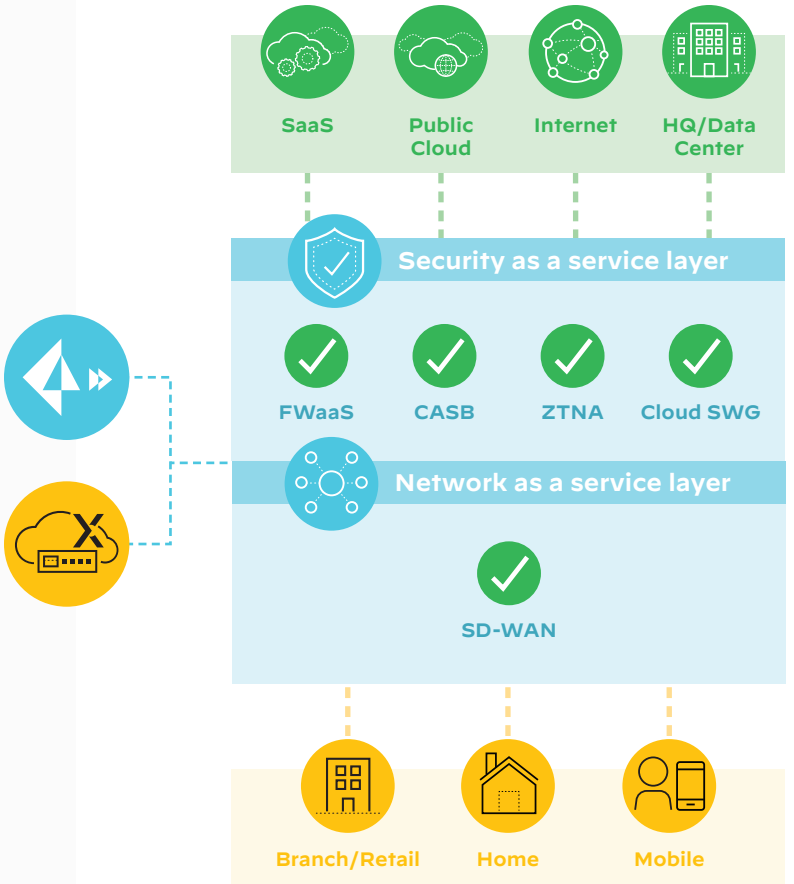
Gartner 2019 The Future of Network Security Is in the Cloud

How Palo Alto Networks Can Help

Palo Alto Networks offers the industry's most comprehensive SASE solution through its Prisma® Access and CloudGenix® SD-WAN products. Prisma Access provides cloud-delivered security to prevent cyberattacks and consistently protects all traffic, on all ports, and from all applications. CloudGenix SD-WAN is 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.

By deeply integrating Prisma Access with CloudGenix SD-WAN, 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 Access uses a common cloud-based infrastructure that delivers multiple types of security services and, together with CloudGenix SD-WAN, 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.

Prisma Access & CloudGenix SD-WAN: The Industry's Most Comprehensive SASE



Conclusion

As remote 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. The top three strategic benefits your business will realize from secure access service edge are:

1

SIMPLIFIED MANAGEMENT AND OPERATIONS

- Converge networking and network security capabilities into a single cloud-delivered service, managed from a single console.
- Automate deployment for branch locations and ongoing management.
- Use machine learning and data science methodologies to simplify network operations and reduce network trouble tickets.

2

INFINITE SCALE AND PERFORMANCE

- Leverage cloud native architecture that supports elastic scale on a global, high-performance network of 100+ locations.
- Deliver branch services from the cloud, simplifying WAN management and providing an ROI of up to 243%.
- Enrich visibility, policy, and path decisions with Layer 7 application-defined intelligence.

3

EXCEPTIONAL USER EXPERIENCE

- Ensure consistent security and compliance, no matter where users are.
- Deliver on SLAs for all apps, including cloud, SaaS, and UCaaS.

In short, a successful SASE solution offers a holistic view of your entire network while providing superior protection and performance from a single, unified, cloud-delivered platform.

Learn more about Palo Alto Networks SASE products: Prisma Access • CloudGenix SD-WAN

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