10 Tenets for an Effective SASE Solution

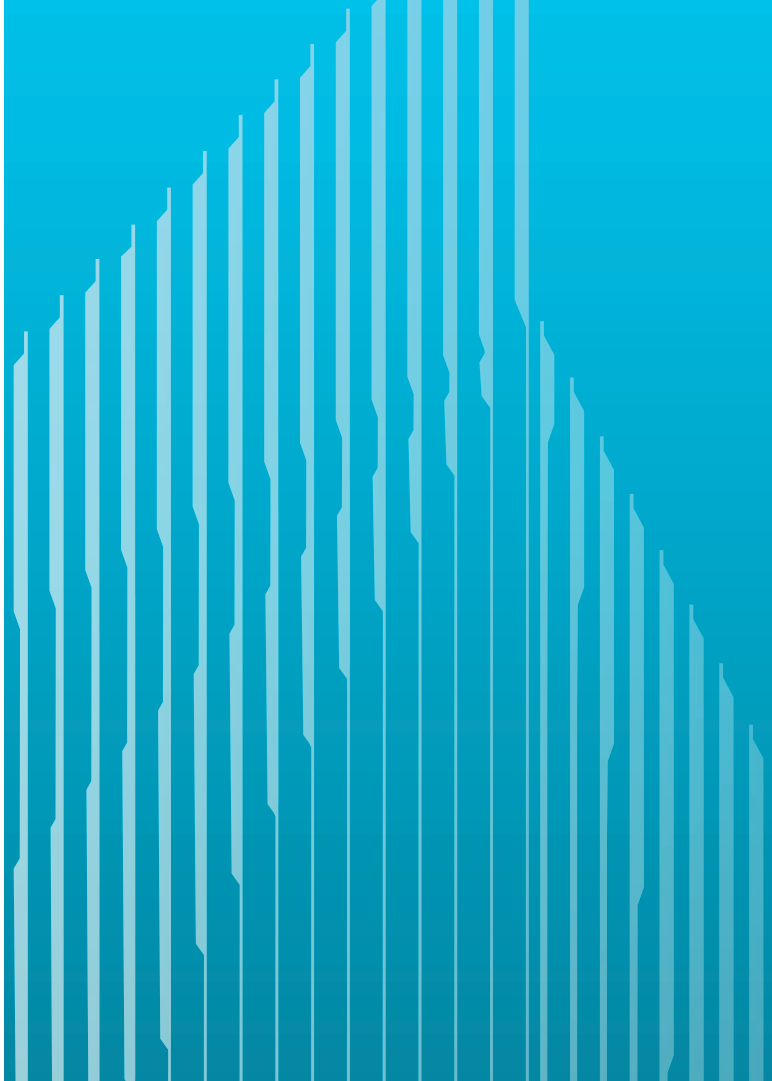

Table of Contents

Introduction

Secure access service edge (SASE) has become critical for digital transformation as organizations expand hybrid work models and the use of cloud services. Coined by Gartner in 2019 and pronounced "sassy," SASE helps organizations streamline secure deployments of cloud and mobility architectures by providing network and network security services from a common cloud-delivered architecture.

The rapid pace of SASE adoption is driven by a need to reduce complexity by consolidating networking, private application access, and internet and SaaS security under a unified platform. The SASE approach has been proven to be the most effective and efficient way to streamline and optimize security and operational outcomes. However, a SASE solution must provide consistent security services and access to all types of cloud applications (e.g., public cloud, private cloud, and SaaS) delivered through a common framework.

> **Gartner defines SASE as networking and network security converged in the cloud and delivered as a service, such as SD-WAN, secure web gateway (SWG), cloud access security broker (CASB), network firewalling, and Zero Trust Network Access (ZTNA), as a massively distributed cloud service.[1]**

Read this e-book to understand how a SASE solution addresses the limitations of disparate standalone products. Learn about the 10 fundamental principles and elements of a SASE solution and how they optimize security and overall operations while reducing complexity.

1. Andrew Lerner, et al., *Magic Quadrant for Single-Vendor SASE*, Gartner, August 16, 2023.

Tenet 1: Software-Defined Wide Area Network (SD-WAN)

What Isn't Working

Enterprises have traditionally implemented rigid and complex systems with multiple point solutions that constantly need hardware appliances updated and offer limited direct-to-app access. These legacy systems also often lack comprehensive visibility into application traffic and activities, especially IoT. This makes it especially difficult to deliver improved performance, simplify operations, and detect and protect users, apps, and devices from advanced threats.

The SASE Way

SASE offers an integrated approach that spans all users, applications, and connected devices to deliver exceptional user experience, operational simplicity, and superior security outcomes. For instance, native integration between SD-WAN and cloud security services allows direct-to-app access for all applications securely including SaaS and internet apps, resulting in improved performance compared to data center backhauled access. SASE secures all applications, users, and devices with Zero Trust to ensure that continuous trust verification and inspection are implemented and extend to IoT devices at remote locations without needing additional point products.

Key Takeaways

Protecting IoT devices should start with the SASE solution's capability to discover IoT devices continuously. Tightly integrating security services with SD-WAN, SASE increases visibility into IoT traffic patterns and enables effective security enforcement that takes into account device classification and vulnerabilities. This comprehensive approach also provides the tools needed to proactively protect networks from potential threats in the rapidly evolving IoT landscape.

> **"By 2026, 60% of new SD-WAN purchases will be part of a single-vendor secure access service edge (SASE) offering, up from 15% in 2023."[2]**
>
> – Gartner

2. Jonathan Forest et al., *Magic Quadrant for SD-WAN*, Gartner, September 27, 2023.

Tenet 2: Secure Web Gateway (SWG)

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're on-site at work or remote. What's more, in today's hybrid world, SWG security only looks at web-based traffic and protocols, completely ignoring nonweb 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 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 nonweb 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, standalone SWG to a more secure SASE architecture.

> **"A SASE solution moves SWG into the cloud, providing protection in the cloud through a unified platform for complete visibility and control over the entire network."[3]**
>
> – SASE for Dummies

3. Lawrence Miller, *Secure Access Service Edge (SASE) For Dummies 2nd Special Edition*, Palo Alto Networks, April 19, 2022.

Tenet 3: Cloud Access Security Broker (CASB)

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're 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 a comprehensive cloud-delivered enterprise DLP that utilizes ML for more accurate detection and real-time protection of sensitive data across the entire enterprise.

> **"By combining CASB and SASE, organizations can create a robust security posture that covers cloud applications, remote access, and network infrastructure. This combined approach offers enhanced visibility, control, and threat protection, contributing to a more resilient defense against evolving cyber threats."[4]**
>
> – Security Affairs

4. Pierluigi Paganini, "CYBERSECURITY: CASB VS SASE," Security Affairs, August 20, 2023.

Tenet 4: Firewall as a Service (FWaaS)

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.

> **Over the next 18 to 36 months for typical enterprise SASE adoption, enterprises should, "Eliminate physical firewalls where possible, and use FWaaS for branch office protection, ideally for inbound and outbound traffic."[5]**
>
> – Gartner

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's important to ensure your SASE solution doesn't 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.

5. John Watts, Andrew Lerner, and Neil MacDonald, *2024 Strategic Roadmap for SASE Convergence*, Gartner, December 15, 2023.

Tenet 5: Zero Trust Network Access (ZTNA)

What Isn't Working

Zero Trust Network Access (ZTNA) has been used to reduce security risks associated with hybrid work as well as combat the increasing sophistication and volume of threats designed to take advantage of this massively expanded attack surface. However, current ZTNA 1.0 solutions have significant limitations.

ZTNA 1.0 solutions violate the principle of least privilege, which inhibits threat detection and protection efforts. These solutions also assume all allowed traffic is free from malware and other threats or vulnerabilities and are unable to detect or prevent threats (e.g., malware or lateral movement across connections). This, combined with the lack of integration of threat prevention solutions, means that it takes far too long to identify and respond to threats.

The SASE Way

SASE builds on ZTNA 2.0 principles and applies them across all the other services, including threat prevention tools. It starts with enforcement of the principle of least privilege and closing other ZTNA 1.0 gaps by adding continuous trust verification and security inspections to prevent all threats, including zero-day threats. Machine learning capabilities are also included in SASE, allowing the mitigation of unknown threats in near-real time and extending visibility and security to all devices, including never-seen-before IoT devices.

Key Takeaways

Combining SASE and ZTNA 2.0 provides a single solution to consistently apply and enforce security policies across their entire network and optimize threat prevention. A SASE solution should incorporate ZTNA 2.0 continuous threat assessment and trust validation to protect applications as well as apply other security services for the consistent enforcement of threat prevention policies. It should also incorporate threat prevention tools into its framework to enable quick reaction and remediation when threats are detected. Inline machine learning should also be used to prevent unknown file- and web-based threats instantly.

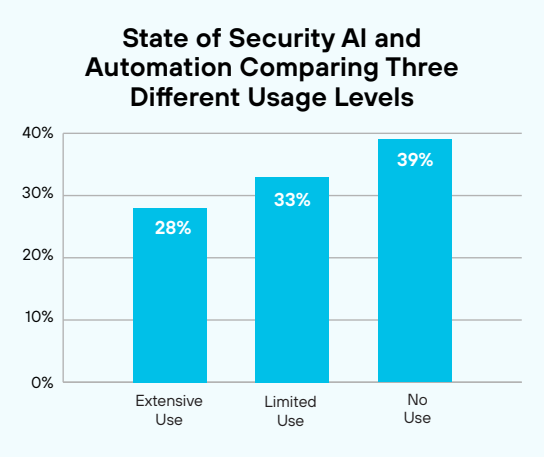

Figure 1: Percentage of organizations per usage levels[6]

6. *Cost of a Data Breach Report 2023*, IBM, July 2023

Tenet 6: Data Security

What Isn't Working

Despite advancements in data loss prevention (DLP) solutions, organizations continue to face persistent challenges with data security to safeguard sensitive information. While the adoption of SaaS, GenAI, and cloud applications (e.g., Gmail, Slack, ChatGPT, Salesforce, Zoom, etc.) may help drive business growth, they also introduce unique challenges. Some of these challenges include limited visibility into data flows across complex environments and interconnected SaaS apps, alert fatigue from legacy DLP products, and inadequate coverage and lack of granular controls—especially on unmanaged devices, leaving organizations at heightened risk.

The SASE Way

The SASE approach to DLP will provide the most comprehensive AI-powered data security for today's modern digital workforce. As part of a unified solution, organizations can proactively identify and prevent data loss across the entire data ecosystem, including SaaS apps, email, GenAI apps, and even the unmanaged devices via the browser. A unified SASE solution also allows the same DLP policies to be consistently applied to sensitive data at rest, in motion, and in use, regardless of its location. When delivered under a single SASE architecture, DLP isn't a standalone point product, but a comprehensive data security solution that helps protect sensitive data from every control point without getting in the way of users.

Key Takeaways

SASE gives organizations the visibility and control needed to safeguard sensitive information with end-to-end data security across complex environments. When deployed as part of a SASE architecture, DLP can protect data from unauthorized access and exfiltration, as well as ensure compliance with regulatory entities. Look for a SASE solution that has DLP embedded as a cloud-delivered service to proactively identify, monitor, and protect sensitive data everywhere—across networks, clouds, SaaS, email, and even browsers.

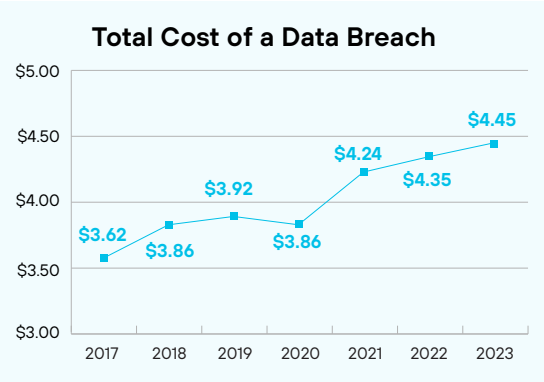

Figure 2: Measured in USD millions[7]

7. *Cost of a Data Breach Report 2023*, IBM, July 2023

Tenet 7: Enterprise Browser

What Isn't Working

The hybrid workforce's reliance on unmanaged devices presents a significant security risk, especially when accessing corporate SaaS and sensitive applications. Although cloud-based security offerings have emerged, many are only providing inconsistent and incomplete protections, as well as delivering poor performance and user experiences. These leave web apps exposed and accessible from unsecured devices, creating unacceptable security gaps.

> "75% of organizations report they experienced at least one cyberattack caused by an unmanaged device."[8]
>
> – ESG

The SASE Way

The hybrid workforce and direct-to-app architectures need a unified SASE solution to replace legacy security architectures that have become obsolete. SASE enterprise browser solutions protect hybrid workforces with the superior security of ZTNA 2.0, while providing exceptional user experiences with a simple, unified security platform. They address the emerging security demands of modern organizations accessing sensitive corporate data via web and private applications on vulnerable consumer browsers. A unified SASE solution with an integrated enterprise browser provides IT and security teams with comprehensive visibility and control over web applications and user actions.

Key Takeaways

A SASE enterprise browser solution creates a secure workspace, protecting sensitive corporate data across SaaS, web, and private applications. It leverages cloud-delivered security services, browser-based data protection, and advanced security features embedded in the browser to efficiently reduce the attack surface. With a unified management console for managed and unmanaged devices, SASE with enterprise browsers secure any device in today's hybrid workforce.

8. Gabe Knuth and Dave Gruber, *Managing the Endpoint Vulnerability Gap*, ESG, February 2023.

Tenet 8: App Acceleration

What Isn't Working

Slow app performance frustrates users and negatively impacts the productivity of today's geographically distributed workforces. Traditional approaches to address application performance typically involve accelerating WAN traffic, caching static content, or increasing geographic point-of-presence (PoP) footprints. Unfortunately, none of these approaches effectively improve application performance because they don't account for the primary causes of performance issues in modern apps and distributed workforces—poor network connectivity, cloud app architecture, and cloud processing latency. This has become more of an issue as distributed workforces demand consistent high-performance experiences for every app from anywhere.

The SASE Way

SASE app acceleration is designed to improve app performance for distributed workforces with a platform that understands how employees interact with SaaS and other cloud-based applications. It leverages that information to increase the responsiveness of cloud applications by proactively computing dynamic content on behalf of the user to dramatically reduce cloud latency. In addition, app acceleration boosts throughput for all TCP traffic to overcome adverse network conditions for mobile workforces accessing their apps over wireless connections.

Key Takeaways

With SASE app acceleration, enterprises can address the need for faster application performance to achieve consistent experiences everywhere while meeting even the most stringent security requirements. This SASE solution enables digital and cloud-first organizations to achieve high-performing, low-latency access to applications faster than accessing applications directly through the internet with robust security powered by AI and ML.

> **"Secure access service edge (SASE) frameworks enable a unified approach to connectivity and security for a hybrid workforce and decentralized deployment of devices, branches, and enterprise applications and services."[9]**
>
> –Gartner

9. John Watts, Andrew Lerner, and Neil MacDonald, *2024 Strategic Roadmap for SASE Convergence*, Gartner, December 15, 2023.

Tenet 9: Autonomous Digital Experience Monitoring (ADEM)

What Isn't Working

User experience is critical for employee satisfaction and productivity, especially as more employees work remotely. However, end-user experiences are often inconsistent and unpredictable due to the complexity of modern applications and networks. Legacy approaches weren't designed for cloud-centric hybrid workforces and are often unable to isolate the root causes of issues. This leaves IT teams to manage and troubleshoot larger and more complex environments with limited resources, which are commonly deployed to address issues with manual and labor-intensive troubleshooting sessions. This results in extended downtime and lost productivity.

The SASE Way

Encompassed with SASE, ADEM provides end-to-end visibility and insights to create a seamless digital user experience. It empowers IT operations teams to increase productivity and deliver an exceptional application experience for remote workers with holistic observability and built-in AIOps, capabilities to automate complex IT operations, and a shorter mean time to resolution (MTTR). As part of a SASE solution, ADEM also delivers segment-wise insights across the entire service delivery path to enable real and synthetic traffic analysis that allows IT teams to proactively drive the remediation of digital experience problems.

Key Takeaways

A SASE solution should incorporate ADEM to ensure comprehensive visibility, faster remediation, and detailed performance insights into endpoint devices, Wi-Fi, network paths, and applications. With a SASE solution that includes ADEM capabilities, user experiences can be optimized to support remote users and IT teams, driving productivity, expediting troubleshooting, and reducing interruptions.

> **"The productivity that users can achieve, even remotely; not having to worry about integration with other systems; and the level of security we achieve—none of that is possible without SASE."[10]**
>
> – Forrester Consulting

10. *The Total Economic Impact™ Of Palo Alto Networks Prisma SASE*, Forrester Consulting, December 2023.

Tenet 10: Network Security Platform

What Isn't Working

Embracing digital transformation is imperative but brings significant security risks. However, adding more security tools isn't a viable solution. In fact, it makes it impossible to have a holistic view of complex networks and endpoints, leaving environments even more vulnerable due to visibility gaps.

Point solutions and multiple management consoles for every new use case cause complexity, siloed views, and error-prone manual interventions (e.g., attempts to optimize performance or apply security policies). Security teams struggle to keep up despite working longer hours and being constantly on edge, which leads to burnout and mistakes that compromise security.

The SASE Way

SASE converges security with networking into a single cloud-delivered platform. It consolidates multiple point products, including ZTNA 2.0, Cloud SWG, Next-Generation CASB, FWaaS, SD-WAN, ADEM, and enterprise browser into a single integrated service that reduces network and security complexity while increasing organizational agility. A key attribute to look for is AI. The best SASE solutions facilitate digital transformation with a Zero Trust, AI-driven approach that detects and prevents sophisticated attacks and automates manual security operations.

Key Takeaways

A SASE solution should provide a unified security stack delivered as one platform that provides a consistent user experience across services and devices while reducing management complexity. Management across network environments is key to eliminating operational inefficiencies. With hybrid cloud strategies and flexible work-from-anywhere models becoming the norm, SASE provides centralized visibility across all users and locations within a single-pane-of-glass dashboard to help teams efficiently identify networking issues and prioritize response actions.

> **"We are seeing increased interest in single-vendor SASE from organizations that want to simplify their branch technology stacks. It is particularly compelling for organizations making SD-WAN investments and extending the project to include firewalling, remote access, and other security capabilities."[11]**
>
> – Gartner

11. Andrew Lerner, et al., *Magic Quadrant for Single-Vendor SASE*, Gartner, August 16, 2023

How Palo Alto Networks Can Help

Palo Alto Networks offers the industry's most complete SASE solution with AI-powered Prisma® SASE. Prisma SASE streamlines secure access by connecting all users and locations with all apps from a single solution. It consolidates multiple point products, including ZTNA 2.0, Cloud SWG, CASB, FWaaS, enterprise browser, and SD-WAN, into one integrated service, reducing network and security complexity while increasing organizational agility.

The superior security of ZTNA 2.0 protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach. AI-powered Prisma SASE is built in the cloud to secure at cloud scale while delivering exceptional user experiences. A truly cloud-native architecture provides uncompromised performance backed by leading SLAs, while the industry's only SASE-native ADEM helps ensure an exceptional experience for your end users. Organizations can embrace their hybrid workforces, knowing they can provide broad security and connectivity for their remote users and branch locations.

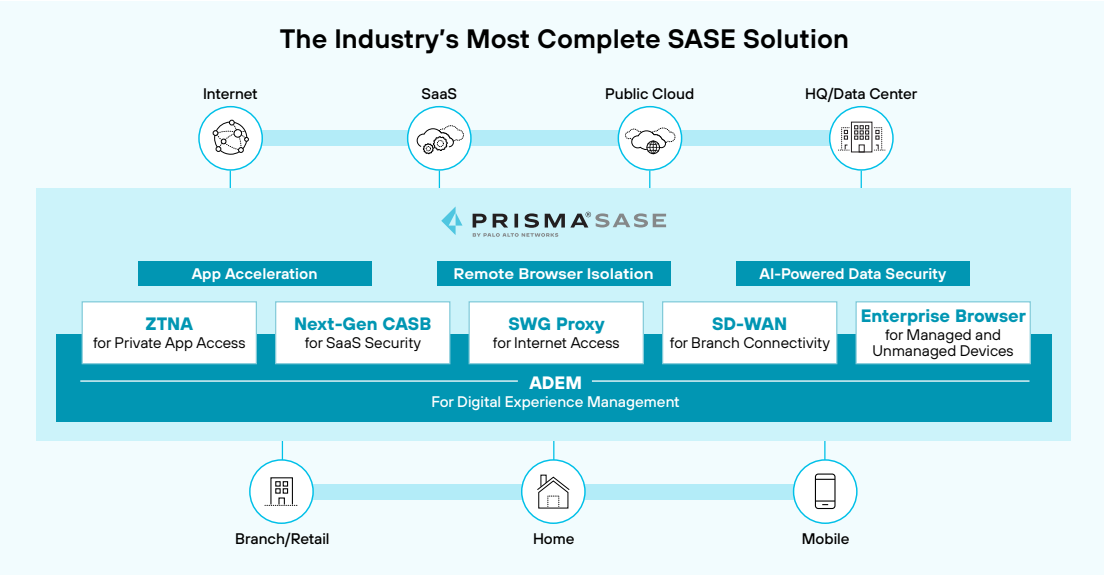

Figure 3: Prisma SASE

Conclusion

As hybrid work continues for organizations and cloud adoption grows, we encourage you to consider a unified, 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 integrated product. It offers:

- **Zero Trust security:** Prisma SASE consistently secures all apps used by your hybrid workforce, regardless of whether users are at home, on the go, or in the office. Protect all application traffic with best-in-class capabilities while securing access and data to dramatically reduce the risk of a data breach.
- **Exceptional network:** Prisma SASE, with natively integrated Prisma SD-WAN, delivers an exceptional user experience while securing your network holistically (including IoT), and automates complex IT operations.
- **AI-powered operations:** Prisma SASE is built in the cloud to secure at scale while delivering exceptional user experiences. A truly cloud-native architecture provides uncompromised performance backed by leading SLAs. The industry's only SASE-native Autonomous Digital Experience Management (ADEM) helps ensure an exceptional experience for your end users.

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

prisma_eb_10-tenets-for-an-effective-sase-solution_042424