Prisma SASE
At a Glance

Prisma SASE Highlights

Palo Alto Networks Prisma SASE is the industry's most complete secure access service edge (SASE) solution, delivering:

- **Superior ZTNA 2.0 Security:** Consistently protect the hybrid workforce with the superior security of ZTNA 2.0.
- **Simplified Operations:** Enable IT agility with a fully converged SASE solution.
- **Exceptional User Experience:** Cloud-native architecture with integrated Autonomous Digital Experience Management (ADEM) ensures the best user experiences.

Legacy Network Architectures No Longer Work in Today's Cloud-Enabled World

Enterprises have traditionally taken a hardware-based approach to connecting their people and offices to their resources. With the increased adoption of SaaS applications and cloud resources, however, backhauling traffic to the central data centers has become inefficient, resulting in additional costs and performance issues. Additionally, inconsistent policies and capabilities depending on a user's physical location create inherent gaps in security. Finally, the backhauling of traffic to a data center for policy enforcement and inspection impacts the user experience.

The Industry's Most Complete SASE Solution

Palo Alto Networks Prisma SASE brings together best-of-breed security and next-gen SD-WAN into a cloud-delivered platform. It consolidates multiple point products, including ZTNA 2.0, Cloud SWG, CASB, FWaaS, and SD-WAN, into a single 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.

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. The industry's only SASE-native ADEM helps ensure an exceptional experience for your end users.

Prisma SASE Use Cases

Three fundamental shifts are driving the need for network transformation in the enterprise: hybrid work, cloud and digital transformation, and branch transformation:

- **The hybrid workforce** has become the new normal and a requirement for many organizations as a result of the pandemic. Research indicates that organizations expect 62% of their employees to work in a remote or hybrid manner, even after COVID-19 mandates are lifted ("2021 SASE Trends Survey," ESG, July 2021). As a result, most organizations are planning to support a model where the majority of employees can work fluidly between corporate offices, branch offices, home offices, and on the road.
- **Cloud and digital** initiatives are driving organizations to invest more in SaaS and other public cloud services. Cloud adoption enables companies to be more agile, efficient, and flexible, indicative of why 92% of all enterprises are now adopting a multicloud strategy (Flexera, 2021). SASE brings protection closer to users so traffic doesn't have to backhaul to headquarters to reach the cloud.
- **Branch transformation** is well underway, driven by new hybrid work and digital transformation initiatives. Organizations are fundamentally changing the branch—leveraging branches as collaboration hubs rather than primary places of work—while retailers are transforming the way they engage in-store with customers. This trend is fueling the demand for WAN transformation, from legacy MPLS to SD-WAN and SASE.

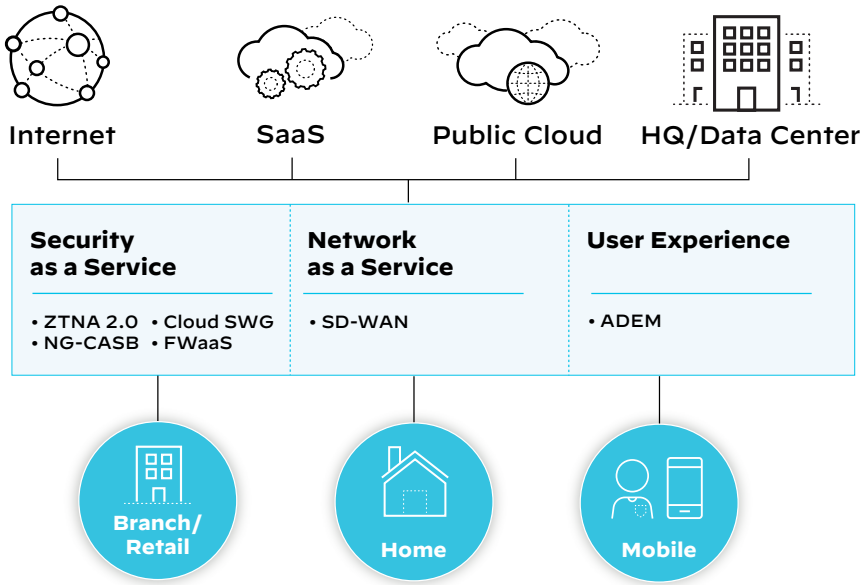

Figure 1: Prisma SASE architecture

Prisma SASE
At a Glance

Complete Digital Experience Management for SASE

The Autonomous Digital Experience Management (ADEM) add-on for Prisma SASE helps IT teams see, understand, and improve digital experiences for all their users and branch locations. ADEM delivers SASE-native visibility into digital experience, with segment-wise insights across the entire service delivery path, including intelligence gathered from endpoint devices, synthetic tests, and real user traffic. It also monitors application and endpoint performance at branch locations and natively integrates with Prisma SD-WAN for comprehensive overlay and underlay remote network performance visibility on all configured WAN paths. With ADEM, IT can solve application performance problems quickly and keep their business flowing.

Prisma SASE Features

AIOps for SASE: Powerful, natively integrated AIOps capabilities prevent outages and improve security posture with anomaly detection and forecasting, automated trouble-shooting, change management modeling, security policy analysis, and more.

Autonomous Digital Experience Management (ADEM): Provides segment-wise insights across the entire service delivery path with real and synthetic traffic analysis to drive proactive remediation of digital experience problems.

Cloud Access Security Broker: Applies governance, data classification and stops threats with both inline and API-based security for SaaS applications.

CloudBlades: Enables the seamless integration of branch services into the SASE fabric without needing to update branch appliances or controllers, thus eliminating service disruptions and complexity. This unique cloud-based API architecture automates deployments of third-party services, enabling organizations to simplify network operations and multicloud connectivity, and expedite deployments.

Cloud Secure Web Gateway: Secures web-based threats using static analysis and machine learning while simplifying the onboarding experience for customers migrating from legacy proxy-based solutions to SASE.

Explicit Proxy: Prisma SASE offers flexible connectivity options, including support for explicit proxy connection methods. With Prisma SASE explicit proxy, customers can easily migrate from legacy proxy-based solutions without the need for network architecture changes, facilitating an easy transition to a more secure solution that protects all apps, ports, and protocols.

Data Loss Prevention: Comprehensive data protection that keeps sensitive data safe by categorizing it and protecting it while in motion across remote users and remote locations.

DNS Security: Uses advanced analytics and machine learning for protection against threats in DNS traffic.

Firewall as a Service (FWaaS): Protects remote locations with Palo Alto Networks Next-Generation Firewall security, delivered as a service from the cloud.

IoT Security: Combines machine learning, risk assessment, inline prevention, policy recommendations, and automated policy enforcement to secure IoT devices without the need to deploy costly and difficult to manage sensors.

ML-Powered Security: Leverage machine learning for proactive real-time and inline zero-day protection with automated policy recommendations.

SD-WAN: Deep, seamless integration with Prisma SD-WAN, the industry's first next-generation SD-WAN that is application-defined, autonomous and cloud-delivered.

Threat Prevention: Blocks exploits, malware, and command-and-control traffic using the combined threat intelligence of the entire Palo Alto Networks ecosystem.

VPN: IPsec, SSL, and clientless VPN provide options for connecting users and networks into the secure access service edge.

Zero Trust Network Access (ZTNA) 2.0: Combines fine-grained, least-privileged access with behavior-based continuous trust verification and deep, ongoing security inspection and enterprise DLP to consistently protect all users, devices, apps, and data everywhere.

Learn More About Prisma SASE

Visit paloaltonetworks.com/sase.