Prisma SASE

Power the Future of Work with the Industry's Most Comprehensive SASE Solution

The rise of the hybrid workforce, cloud applications, and data sprawl have fundamentally broken the traditional perimeter security model. Organizations today struggle with a complex stack of point products—VPNs, proxies, SD-WAN, and firewalls—that create security gaps, introduce operational friction, and degrade user experience. To help them overcome these challenges, they need a cloud-native, scalable, and resilient security fabric.

Power the future of work with AI-powered Prisma® SASE, the industry's most comprehensive SASE solution that protects all your users, apps, data, and devices to deliver best-in-class security, exceptional user experiences, and resilient, simplified operations. From your hybrid workforce to your zero trust branch, drive transformation with confidence on a resilient, multicloud architecture.

Key Drivers for SASE Adoption

Three fundamental shifts are driving the need for network transformation in the enterprise:

- **Supporting the hybrid workforce** has become the new normal. 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, which is why enterprises adopt a multicloud strategy.
- **The branch is back**, paving the way to accelerated branch transformation initiatives that support a hybrid workforce and the rapid evolution of applications moving toward the cloud. Many employees prefer hybrid work and significant adoption of collaboration tools like UCaaS for productivity. For this reason, branch transformation is well underway and fueling the migration to a single-vendor SASE solution.

Mix-and-Match SASE Solution Challenges

Organizations transitioning to a SASE architecture have two options: multivendor or mix-and-match SASE or a unified, single-vendor approach. Taking a multivendor approach to SASE results in the following challenges:

- **Compromised security posture** with disparate policies and manual processes.
- **Loss of SD-WAN functionality** with legacy solutions that lack application awareness, direct-to-app connectivity, and end-to-end performance visibility, resulting in operational complexity and adverse effects on security.
- **Increased cost and complexity** resulting from procuring, deploying, and managing multiple solutions.
- **Siloed processes and limited visibility and collaboration** across security and networking teams.

Why Single-Vendor SASE Is the Right Approach

As SASE adoption continues to accelerate with the adoption of hybrid work and cloud at scale, organizations need to think about the right approach that will allow them to scale their security and networking infrastructure effectively over time.

Organizations need an integrated platform approach to SASE, like Prisma SASE, which offers:

- Better security outcomes with unified policy and context sharing.
- Reduced operational complexity through unified management.
- The ability to leverage AI and ML with a unified data lake.

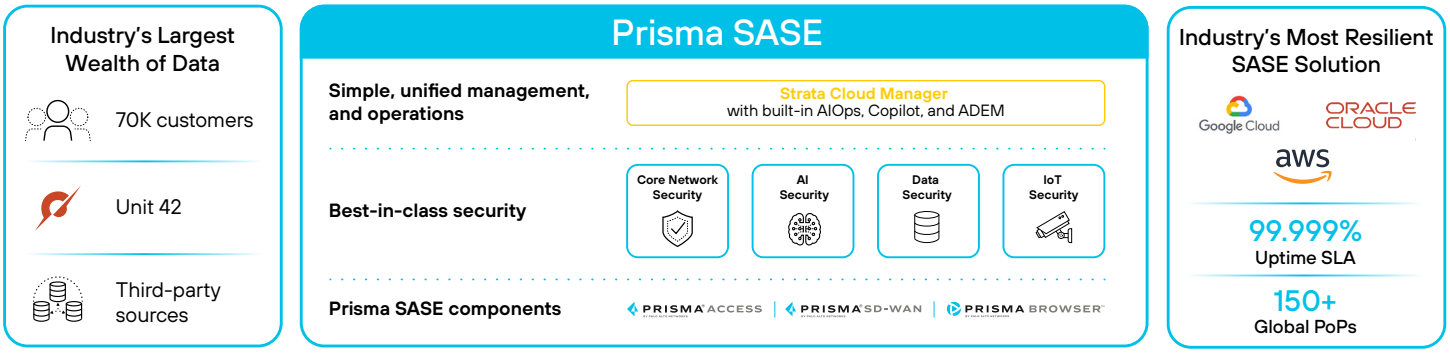

Figure 1. Prisma SASE architecture

Prisma SASE eliminates the limitations of mix-and-match SASE and uniquely delivers best-in-class security, exceptional user experience, and resilient, streamlined operations:

- Prisma SASE offers **unified management and operations** with Strata™ Cloud Manager, enabling administrators to manage Prisma Access, Prisma SD-WAN, Prisma Browser™, and Autonomous Digital Experience Management (ADEM) from one interface.
- Prisma Access provides **secure, reliable access for all users, data, applications, and devices** regardless of location, ensuring true zero trust by using Precision AI® to stop the most sophisticated threats.
- Prisma SD-WAN provides **seamless connectivity and tight integration with Prisma Access**, empowering organizations with the most advanced Layer 7 application-aware SD-WAN fabric.
- Prisma SASE enables **digital experience management for Prisma Access and Prisma SD-WAN** to deliver always-on visibility for applications, users, and devices.
- Maintain a **consistent security framework using App-ID™, Device-ID, and User-ID™**, resulting in security policy enforcement across the fabric.
- **Extend zero trust security with the enterprise-grade Prisma Browser**, which provides deep visibility and granular policy control for all devices and governs data movement within the browser.

Table 1. Prisma SASE Features

Feature	Description
App-ID	Continuously classifies all applications regardless of the port, SSL/TLS encryption, or technique an attacker uses to evade detection. Unlike legacy solutions that depend on Layers 3 and 4 as the first layers of control before application classification is applied, Prisma Access applies App-ID along with other Layer 7 controls, such as User-ID.
User-ID	Integrates with a wide range of user identity repositories so your policies follow your users and groups regardless of their location. User repositories include wireless LAN controllers, VPNs, directory servers, browser-based authentication portals, proxies, and more.
Device-ID	Allows policies to be created that follow a device no matter where it's connected in the network. Enforcement based on device attributes, such as operating system version, enables security teams to control the attack surface more strictly. Device-ID logging provides additional visibility as well as context. When combined with App-ID and User-ID, it allows for deep insights into behavior on the network.
SSL Decryption	Inspects and applies policy to SSL/TLS-encrypted traffic, both inbound and outbound, including traffic that uses HTTP/2. For privacy and regulatory compliance, you can enable or disable decryption flexibly based on the URL, source, destination, user, user group, and port.
Dynamic User Group Monitoring	Provides dynamic security actions based on user behavior to restrict suspicious or malicious users. Allows you to define Dynamic User Groups in Prisma Access to take time-bound security actions without waiting for changes to be applied to user directories.
GlobalProtect®	Provides secure, identity-based connectivity to Prisma Access and on-premises gateways. It uses host information profile (HIP) checks to verify device health and posture before granting access to sensitive resources.
Prisma Agent	A cloud-optimized, high-performance agent that provides always-on zero trust connectivity. It features built-in antitampering, integrated Endpoint DLP, and advanced traffic steering for a seamless user experience.

Table 1. Prisma SASE Features (continued)	
Feature	**Description**
Explicit Proxy Onboarding	Allows customers to choose proxy mode. This explicit proxy option is an alternate way for users, servers, and VDIs to connect to Prisma Access and secure their internet and SaaS application traffic (HTTP/HTTPS). GlobalProtect or Prisma Agent in proxy mode and PAC files are supported for browser configuration.
PAN-OS® Policy Optimizer	Provides a simple workflow to migrate your legacy port-based rulebase to an App-ID rulebase. It reduces your attack surface and increases the efficacy of your security policies.
Remote Browser Isolation	Provides the ability to isolate internet web traffic (either select or all) that is unknown, deemed risky, or suspicious for managed and unmanaged devices. It supports integration with third-party RBI clouds through CloudBlades.
Reporting	Includes, as a standard, a detailed, customizable SaaS application usage report that provides insight into all SaaS traffic—sanctioned and unsanctioned—on your network. You can also create custom reports based on your needs and easily schedule, download, and share them with others in your organization.
User Authentication	Supports all existing PAN-OS authentication methods, including Kerberos, RADIUS, SAML, LDAP, client certificates, and a local user database. Once GlobalProtect authenticates the user, it immediately provides Prisma Access with user-to-IP address mapping for use by User-ID technology.
Advanced Threat Prevention	Analyzes up to 673 million new sessions daily and proactively blocks 28.2 billion threats in real time, including zero-day exploits, malware, C2 traffic, and evasive techniques. Advanced Threat Prevention delivers cutting-edge security at an unmatched scale.
Advanced WildFire®	Proactively stops up to 450,000 new threats every day with the industry's most powerful malware prevention engines. Advanced WildFire identifies and blocks zero-day malware, ransomware, remote access Trojans (RATs), weaponized documents, and other evasive attack techniques before they can impact your organization.
Advanced DNS Security	Delivers real-time protection that instantly blocks sophisticated DNS request and response-based threats, including DNS hijacking, domain generation algorithms, DNS tunneling, and C2 callbacks. It analyzes over 1.1 billion new domains daily and identifies up to 7.7 million newly malicious domains, preventing more than 2 billion threats inline. This powerful first line of defense stops threats at the DNS layer, whether they originate inside or outside the network.
Advanced DNS Security Resolver	A cloud-delivered, AI-powered DNS resolution service that provides real-time protection against DNS-based threats—including C2, tunneling, and hijacking—across any hybrid or multivendor environment without requiring infrastructure changes.
Advanced URL Filtering	Safeguards web access by blocking up to 151 million threats inline every day while analyzing 3.8 billion new URLs daily. Advanced URL Filtering protects against phishing, malware, ransomware, C2 communications, and sophisticated web-based attacks, ensuring a secure and seamless browsing experience.
Data Loss Prevention (DLP)	Network DLP, E-DLP, and Email DLP enable the prevention of data breaches, along with enhancements to data privacy and compliance. By delivering consistent policies across all distributed control points from a single cloud-delivered DLP engine, the solution enables a unified approach at egress points, the edge, and in the cloud.
Device Security	Secures your blind spots and protects every connected device unique to your vertical with our zero trust solution for IoT devices, discovering managed and unmanaged devices.
Autonomous Digital Experience Management	Natively integrated with Prisma SASE, ADEM transforms IT operations leveraging AI to enhance productivity and user experience. Its unified observability and built-in AIOps automate complex tasks, enabling faster issue resolution, improved efficiency, and reduced downtime. Further ensuring exceptional user experience, ADEM combines synthetic monitoring with browser-based RUM into a single dashboard to deliver precise root cause analysis, helping IT teams quickly address application performance issues.
Private App Security	Provides AI-powered, SASE-native protection for distributed private applications and microservices. It offers deep visibility into unprotected apps and APIs, using self-learning security to automatically recommend policies and block zero-day attacks in real time.
Host Information Profile	Checks the endpoint to get an inventory of how it's configured and builds a HIP. Prisma Access uses the HIP to enforce application policies that only permit access when the endpoint is properly configured and secured.
Device Quarantine	Blocks compromised devices from accessing privileged data. You can add compromised devices manually or automatically to a quarantine list and block users from logging into the network from those devices using GlobalProtect. Also, you can restrict access to applications from these compromised devices.
Quality of Service (QoS)	Enables you to dependably run high-priority applications and traffic under limited network capacity. QoS prioritizes business-critical traffic or traffic that requires low latency, such as VoIP or videoconferencing. You can also reserve a minimum amount of bandwidth for business-critical applications.

Table 1. Prisma SASE Features (continued)	
Feature	**Description**
IPv6 Internal Traffic	Secures all internal IPv6 traffic between endpoints and private applications. It's supported for mobile users, GlobalProtect, remote networks, and service connections.
Site-to-Site IPsec VPN	Supports site-to-site tunnels over IPv4 and IKEv1/IKEv2 to ensure compatibility. For multiple connection sites, ECMP routing can provide additional redundancy and cost efficiency by balancing sessions over available internet connections.
Logging	Shows overall traffic, application, user, threat, URL, and data filter logging to facilitate organization of data via the cloud-based Strata Logging Service.
Traffic Replication	Enables forensic analysis, threat hunting, breach impact analysis, and application troubleshooting across the entire SSE or SASE architecture. This capability would otherwise be impossible to accomplish without a copy of the network traffic from all remote users. This feature also aids in meeting regulatory requirements.
User and Entity Behavior Analytics (UEBA)	Enables tools and methods that proactively detect and mitigate security risks by using insights, such as unusual patterns and behaviors based on Prisma Access network traffic logs to provide faster incident response while improving overall network security.
Policy Automation	Enables you to use information from third-party sources to drive security policy updates dynamically through a combination of Dynamic Address Groups (DAGs) and the XML API.
Private App Connections	Enables you to connect Prisma Access to your organization's private apps and internal resources securely. Connection options include: • Zero Trust Network Access (ZTNA) Connector to connect mobile users and users at branch locations to your private apps using an automated secure tunnel. • Colo-Connect for high-bandwidth, low-latency connections into colo-based dedicated or partner interconnects. • Service Connections for connecting mobile users and users on remote networks to private apps and resources, and for enabling mobile users and remote networks to communicate with each other.
ZTNA Connector	Enables you to connect to your organization's private apps simply and securely. It provides mobile users and users at branch locations access to your private apps using an automated secure tunnel, eliminating the requirement of setting up IPsec tunnels and routing definitions to access the private apps. ZTNA Connector does not require any routing from the customer infrastructure and can provide access to applications that use overlapped IP addresses in your networks.
Service Connection	Provides secure, high-bandwidth connectivity between Prisma Access and on-premises data centers or headquarters. It enables mobile users and remote sites to access internal applications (e.g., Active Directory) and facilitates peer-to-peer communication across the organization.
Colo-Connect	Provides high-speed, non-IPsec private connectivity with up to 100 Gbps throughput per region. Designed for data centers and high-bandwidth workloads, it offers ultralow latency and direct interconnects while ensuring full security inspection for massive traffic volumes.
App Acceleration	Dynamically adapts to first-mile connectivity conditions for hybrid workers to boost connection performance without requiring changes to applications or the infrastructure. Leverages an intelligent "app-aware" edge platform to proactively prepare dynamic content for users, boosting the responsiveness of cloud applications up to 5x faster than direct to the internet.
Dynamic Privileged Access	Enables granular segmentation of users and networks, facilitating secure access to resources while strictly adhering to zero trust principles. It ensures that users have access only to the resources relevant to their projects, mitigating the risk of unauthorized access. Via administrative controls, Dynamic Privileged Access enables administrators to assign projects to individuals based on their country or geographic region, enabling seamless, secure connectivity.
End-User Coaching	Improves productivity, reduces help desk tickets, and enhances security experiences with just-in-time notifications for end users when access restrictions occur.
Secure Agentless Access	Enables clientless access to nonweb apps (e.g., RDP or SSH) via any web browser so you can easily onboard third parties or contractors with unmanaged devices.

For more details, see the following datasheets:

- Prisma Access
- Prisma SD-WAN Instant-On Network Device Specifications
- Prisma Browser
- Strata Cloud Manager

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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

prisma_ds_prisma-sase_041326