Prisma Access

The hybrid workforce and direct-to-app architectures have rendered legacy security architectures obsolete while dramatically increasing our attack surface. Cloud-based security offerings have emerged, but they can offer only inconsistent and incomplete protections as well as deliver poor performance and user experiences.

Palo Alto Networks Prisma® Access protects hybrid workforces with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, Prisma Access delivers the industry's only ZTNA 2.0 solution that protects all internet, SaaS, and private application traffic with best-in-class Cloud-Delivered Security Services and data protection to effectively reduce the attack surface. With a common policy framework and single-pane-of-glass management, Prisma Access secures today's hybrid workforce without compromising performance, backed by industry-leading SLAs to ensure exceptional user experiences.

The Prisma Access Difference

Prisma Access enables organizations to securely connect all users to the internet, SaaS, and private applications they need, regardless of where they're accessing them from or which device they are using, all while significantly reducing risk. It provides a cloud-native single product to secure hybrid enterprises and workforces, is made up of best-in-class security capabilities, optimizes the user experience with dynamic scalability, and guarantees maximum end-user performance. Prisma Access makes securing today's hybrid workforces and cloud-first organizations easy by offering:

- **The superior protection of ZTNA 2.0** that combines fine-grained, least-privileged access with deep and ongoing security inspection as well as enterprise DLP to protect all users, devices, apps, and data.
- **A unified security product** with comprehensive protections converged into a single unified product, single-pane-of-glass visibility, consistent policy management, and shared data for all users and all apps.
- **The best user experiences** from a truly cloud-native architecture built to secure at cloud scale, providing uncompromised performance—all backed by leading SLAs.

Prisma Access consolidates best-in-class security in a leading cloud-native security service edge (SSE) platform. When combined with Prisma SD-WAN, businesses are able to transform their networking and security with the most complete secure access service edge (SASE) solution in the industry.

Security-as-a-Service Layer

Prisma Access includes comprehensive security capabilities consolidated into a single SSE platform that delivers ZTNA 2.0 with the best user experience on a single unified platform.

Firewall as a Service

Prisma Access provides firewall-as-a-service (FWaaS) capabilities with the full functionality of Palo Alto Networks Next-Generation Firewalls (NGFWs). This includes inbound and outbound protection, native user authentication and access control, and Layer 3–7 single-pass inspection to secure branch offices against threats.

Cloud Secure Web Gateway

Prisma Access provides cloud secure web gateway (SWG) functionality to protect users from threats when accessing the internet and SaaS applications. Flexible connectivity options include proxy auto-configuration (PAC) files, agent, agentless, and IPsec tunnel/SD-WAN. Proxy-based connectivity through the single unified GlobalProtect app enables organizations with proxy architectures to benefit from ZTNA 2.0 while even coexisting with third-party VPN agents. IT teams can operationalize next-generation internet, SaaS, and application security that meets all proxy-based routing and compliance requirements. Organizations can easily migrate from legacy on-premises web proxies or alternative cloud-based proxies with ease.

Cloud SWG is natively integrated with Next-Generation CASB and supports all the web security protections Prisma Access offers, including Advanced Threat Prevention, Advanced WildFire, Advanced URL Filtering, DNS Security, and DLP. Also, remote browser isolation (RBI) is supported via integration with the CloudBlades architecture in Prisma Access.

Zero Trust Network Access 2.0

Prisma Access ZTNA 2.0 connects all users and all apps with fine-grained access controls, providing behavior-based continuous trust verification after users connect to dramatically reduce the attack surface. It secures all apps, all the time, including premises-based, internet-based, legacy, SaaS, and modern/cloud-native apps, with deep and ongoing security inspection to ensure all traffic is secure without compromising performance or user experience. What's more, Prisma Access ZNTA 2.0 provides consistent visibility with a single DLP policy to secure both access and data across the entire enterprise.

Next-Generation Cloud Access Security Broker

Prisma Access natively provides the industry's only Next-Generation CASB that automatically keeps pace with the SaaS explosion by combining powerful SaaS Security Posture Management (SSPM) capabilities, proactive visibility, real-time data protection including hard-to-detect secrets exchanged in collaboration apps, and best-in-class security. It delivers multimode functionalities via inline and API-based security for sanctioned and unsanctioned SaaS apps to help today's cloud-first organizations:

- Detect and stop activity from compromised accounts and malicious insiders before any damage is done.
- Detect suspicious user activity that could indicate a compromised account or malicious insider.
- Go beyond standard compliance checks and get comprehensive protection from the industry's first Security Posture Policy Engine.
- Eliminate the risk of compromise and data loss due to user misconfiguration.
- Resolve critical misconfigurations with a single click, dramatically reducing remediation time.

Network-as-a-Service Layer

Prisma Access provides consistent, secure access to all applications—in the cloud, in your data center, or on the internet.

Networking for Hybrid and Mobile Users

Connect hybrid and mobile users with the GlobalProtect app, which supports user-based always-on, pre-logon always-on, and on-demand connections. Prisma Access supports split tunneling based on access route and application types, including its associated risk and bandwidth utilization.

Networking for Remote Networks

Connect branch offices to Prisma Access over a standard IPsec VPN tunnel using common IPsec-compatible devices, such as your existing branch router or software-defined wide area network (SD-WAN) appliance. You can use Border Gateway Protocol (BGP) or static routing from the branch, and you can use equal-cost multipath (ECMP) routing for faster performance and better redundancy across multiple links.

Autonomous Digital Experience Management

The Autonomous Digital Experience Management (ADEM) add-on for Prisma Access provides native end-to-end visibility for SASE. With ADEM, you gain segment-wise insights across the entire service delivery path, with real and synthetic traffic analysis that enables autonomous remediation—now including user self-service remediation with ADEM Self-Serve—of digital experience problems when they arise. The platform's built-in AI-based incident detection, diagnostics, predictive analytics, and automated workflows empower IT teams to detect and resolve complex problems before they have a widespread impact. The complimentary Prisma Access Insights lets you monitor and get on-demand visibility into the health of your Prisma Access deployment.

Centralized Management

Prisma Access supports flexible management options:

- **Prisma Access Cloud Management** streamlines Prisma Access configuration management with seamless onboarding, including secure out-of-the-box configurations built on best practices, continuous assessment of security posture, digital experience monitoring, and reporting through a unified experience delivered from the cloud.
- **Panorama network security management** centralizes policy management across all Palo Alto Networks Next-Generation Firewalls and Prisma Access. Panorama saves time and reduces complexity by managing network security through a single pane of glass.

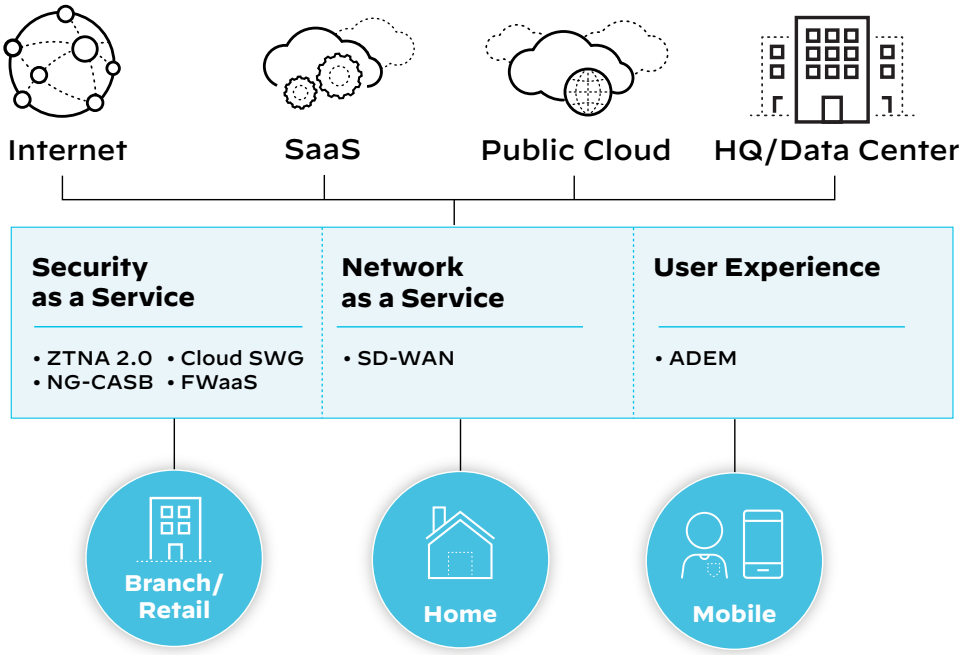

Figure 1: Prisma Access architecture

Table 1: Prisma Access Details, Features, and Specifications			
	Prisma Access for Networks	**Prisma Access for Users**	**Prisma Access for Clean Pipe**
Locations	100+ in 87 countries	• 100+ in 87 countries (GlobalProtect) • 25 locations (explicit proxy)	17 locations
Connection Type	IPsec tunnel	• GlobalProtect app IPsec/SSL/Explicit Proxy • GlobalProtect Clientless VPN • Explicit proxy	Peering via Partner Interconnect (VLAN attachment per tenant)
GlobalProtect App Platform Support	n/a	• Apple iOS • Apple macOS • Google Android • Android App for Chromebook • CentOS Linux • Red Hat Enterprise Linux • Ubuntu • Windows 10 and UWP	n/a
		IoT Platforms • Raspberry Pi OS • Windows IoT Enterprise • Ubuntu • Google Android	
Service-Level Agreements			
Uptime Availability	99.999% per calendar month		
Connectivity	99.99% per calendar month for 10 ms latency		

Table 2: Prisma Access Features	
Feature	**Description**
App-ID	Continuously classifies all applications regardless of port, SSL/TLS encryption, or technique used by an attacker 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 that your policies follow your users and groups regardless of their location. User repositories include wireless LAN controllers, VPNs, directory servers, browser-based captive portals, proxies, and more.
Device-ID*	Allows policies to be created that follow a device no matter where in the network it is connected. 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 and, combined with App-ID and User-ID, allows for deep insights into behavior on the network.
SSL Decryption	Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses HTTP/2. For privacy and regulatory compliance, you can enable or disable decryption flexibly based on URL, source, destination, user, user group, and port.
Dynamic User Group (DUG) Monitoring	Provides dynamic security actions based on user behavior to restrict suspicious or malicious users. Allows you to define DUGs in Prisma Access to take time-bound security actions without waiting for changes to be applied to user directories.
AI/ML-Based Detection	Delivers inline, signatureless attack detection and zero-day exploit prevention. Prisma Access adapts and provides instantaneous real-time protection vs. scheduled updates. It prevents up to 95% of unknown threats instantly, with less than 10-second signature delivery, resulting in a 99.5% reduction in infected systems.
IoT Security*	Combines machine learning with our leading App-ID technology and crowdsourced telemetry to profile all devices for discovery, risk assessment, vulnerability analysis, anomaly detection, and trust-based policy recommendations. It prevents known and unknown IoT, IoMT, and OT threats and delivers native enforcement with a Palo Alto Networks ML-Powered NGFW or orchestration with third parties.
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). The GlobalProtect app 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 App-ID rulebase. This reduces your attack surface and increases the efficacy of your security policies.
Remote Browser Isolation Support	Provides the ability to isolate internet web traffic (either select or all) that is unknown, deemed risky and/or suspicious for managed and unmanaged devices. 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 a user-to-IP address mapping for use by User-ID technology.
DNS Security	Applies real-time protections and inline machine learning to disrupt C2 callback and other attacks that use DNS. Natively integrated into Prisma Access, Advanced DNS Security provides automated protections, preventing attackers from bypassing security measures, and eliminates the need for independent tools or changes to DNS routing.

Table 2: Prisma Access Features (continued)	
Feature	**Description**
Advanced URL Filtering	Superior protection against web-based threats, such as phishing, malware, and C2, that combines powerful database protections with an ML-powered web security engine that categorizes and blocks new malicious URLs in real time. Industry-leading phishing protection tackles the most common causes of breaches, letting you take back control of your web traffic through fine-grained controls and policy settings that automate security actions based on users, risk ratings, and content categories.
Data Loss Prevention (DLP)*	Includes a set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing. DLP on Prisma Access enables you to enforce data security policies and prevent the loss of sensitive data across mobile users and remote networks.
Digital Experience Monitoring (DEM)*	The ADEM add-on for SASE enables organizations to get visibility into mobile user and remote network application and network performance. ADEM Observability gives you end-user monitoring of user-to-application health and performance with synthetic tests, while AI-Powered ADEM delivers comprehensive capabilities including AIOps to automate and streamline complex operations, empower IT teams to detect and resolve issues faster, boost staff efficiency, reduce costly downtime, and drive proactive IT operations.
Host Information Profile (HIP)	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 either manually or automatically add compromised devices to a quarantine list and block users from logging into the network from those devices using GlobalProtect. You can also 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.
IPv6 Internal Traffic	Secures all internal IPv6 traffic between endpoints and private applications. This is 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 Cortex Data Lake.
Traffic Replication	Enables forensic analysis, threat hunting, breach impact analysis, and application troubleshooting across the entire SSE/SASE architecture that would otherwise be impossible to accomplish without a copy of the network traffic from all remote users, and also aids in meeting regulatory requirements.
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.
Intrusion Prevention System (IPS)	Blocks vulnerability exploits, buffer overflows, and port scans. Additional capabilities, such as blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect you from attackers' evasion and obfuscation methods. Vulnerability-based signatures are continuously updated from the Advanced WildFire malware prevention service. Custom signatures can also be manually imported, including from popular formats like Snort and Suricata.

Table 2: Prisma Access Features (continued)	
Feature	**Description**
Antimalware	Uses a stream-based engine that blocks inline at very high speeds, detecting known malware as well as unknown variations of known malware families. IPS and antimalware address multiple threat vectors with one license, eliminating the need to buy and maintain separate IPS and proxy-based products from legacy security vendors.
C2 Protection	Stops malicious outbound communications stemming from malware infections, passively analyzes DNS queries, and identifies the unique patterns of botnets. This reveals infected users and prevents secondary downloads and data from leaving your organization.
Unknown Threat Detection with Advanced Analysis	Identifies unknown threats with shared data from the industry's largest enterprise malware analysis community, including threats submitted from networks, endpoints, clouds, and third-party partners. Leveraging our custom-built hypervisor with bare metal analysis, Advanced WildFire uses various complementary analysis engines that can detect sandbox-evading attacks.
Protection from Unknown Threats	Automatically generates protections across the attack lifecycle when a new threat is first discovered—blocking malicious files, access to malicious URLs, and C2 traffic—and then delivers those protections to all Advanced WildFire subscribers in seconds for most new threats.
File Behavior Analysis	Uses detailed behavior analysis to help you understand how newly discovered malware operates. Integrated logs enable you to quickly identify infected users and investigate potential breaches with detailed analysis of and visibility into unknown threat events.
Cloud-Based Prevention	Employs a unique cloud-based, modular architecture, providing automatic prevention based on global threat intelligence without the headache of having to implement and manage separate devices for web and email at every ingress/egress point in your network.
Multivector Analysis and Visibility	Combines the cloud scale of Advanced WildFire with advanced file analysis and URL crawling to deliver Multivector Recursive Analysis, a unique and comprehensive solution that prevents multistage, multihop attacks. Unlike other solutions, Advanced WildFire can follow multiple stages of attack even if execution fails in a given stage. When Advanced WildFire visits embedded links or links in emails as part of its email link analysis, it updates Advanced URL Filtering if any corresponding webpages host exploits or display phishing activity.
Comprehensive File Execution	Executes unknown files in multiple OS and application versions simultaneously to fully understand the scope of a threat. Multiversion analysis ensures Advanced WildFire analysis is thorough, unlike sandboxes that require golden images, which could deem a malicious file benign simply because the target OS or application version wasn't specified in the golden image.
Private App Connections	Enables you to connect Prisma Access to your organization's private apps and internal resources securely. Connection options include: ZTNA Connector for connecting 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, and Service Connections for connecting mobile users and users at remote networks to private apps and resources as well as enabling your mobile users and remote networks to communicate with each other.

Note: Regional differences may apply. For more details, refer to the Prisma Access Service-Level Agreement.

* Requires an add-on license.

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