Prisma Access
At a Glance

Digital transformation, cloud adoption, and remote work have eroded physical perimeters. Organizations need a scalable way of securing remote access for every user and branch location. Modernize your infrastructure with Prisma® Access to seamlessly extend consistent, centralized, and best-in-class security controls to every user and location.

Prisma Access Highlights

Prisma Access provides the foundation for consistent cloud-delivered security for all users and locations, delivering:

- **Protection for all application traffic:** Prisma Access provides access to all apps and secures against all threats, not just web-based apps and threats, reducing the risk of a data breach.
- **Complete best-in-class security:** Industry-leading capabilities converge into a single cloud-delivered platform, providing more security coverage than any other solution. AI- and ML-powered single-pass detection protects against previously unseen threats.
- **Exceptional user experience:** Massively scalable network connectivity offers ultra-low latency and is backed by industry-leading SLAs, ensuring the best digital experience possible for end users.

Protection for Your Growing Organization

Cloud adoption and emerging work-from-anywhere policies have rendered traditional security architectures obsolete. To date, organizations have faced numerous challenges with implementing these changes on top of existing infrastructure:

- Backhauling traffic over virtual private network (VPN) connections or multiprotocol label switching (MPLS) circuits is inefficient, scales poorly, and hurts the user experience.
- Routing branch and mobile user traffic directly to the internet without proper inspection is not safe.
- First-generation cloud-delivered security products, such as proxies, DNS filtering, and cloud access security brokers (CASB), have limited security capabilities.

Cloud-Delivered Security

Prisma Access transforms security with the industry's most complete cloud-delivered platform, allowing organizations to securely enable remote workforces and branch locations.

Prisma Access is designed from the ground up to lower the costs and complexities of securely connecting users and devices to any service required, anywhere. The cloud native architecture of Prisma Access ensures on-demand and elastic scale of comprehensive networking and security services across a global, high-performance network. Together with CloudGenix® SD-WAN, Prisma Access provides the foundational layer for a complete secure access service edge (SASE) solution that delivers networking and security with a common service delivery model.

Prisma Access fully inspects all application traffic bidirectionally—including SSL/TLS-encrypted traffic—on all ports, whether communicating with the internet, the cloud, the data center, or between branches, decreasing the likelihood of a breach by 45% according to Forrester Consulting. Additionally, Prisma Access provides more security coverage than any other solution, consolidating multiple point products into a single converged platform that includes firewall as a service, Zero Trust Network Access (ZTNA), CASB, Cloud Secure Web Gateway (SWG), VPN, and more, all managed through a single console.

Prisma Access is built upon a massively scalable network, leveraging the combined infrastructure of Amazon Web Services (AWS®) and Google Cloud, with more than 100 service access points across 76 countries and every continent. This allows Prisma Access to provide ultra-low latency, backed by industry-leading SLAs, to ensure a great digital experience for end users.

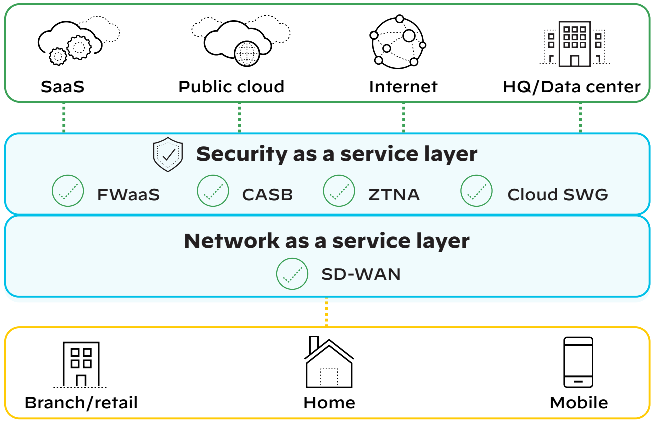

Figure 1: Prisma Access architecture

Prisma Access
At a Glance

Prisma Access for Mobile User

Mobile users need consistent security to access data centers and cloud applications. Remote access virtual private networks (VPNs) fall short because users typically connect to a gateway for access to data center applications, and then disconnect from the VPN to get better performance (but less security) when accessing cloud and internet applications.

Prisma Access brings protection closer to users so traffic doesn't have to backhaul to headquarters to reach the cloud. Prisma Access also includes native Digital Experience Monitoring (DEM) to provide network administrators with segment-wise insights across the entire service delivery path, including endpoint devices, Wi-Fi, local area networks (LANs), VPNs, internet, application performance, and Prisma Access itself. The solution monitors the conditions affecting the user experience and performs automatic remediation as needed.

Standalone VPNs and other remote access solutions also fall short by providing users access to entire LANs or applications without inspecting traffic or assessing the security posture of the connecting device. Prisma Access provides, in a client-based or clientless form, identity-based Zero Trust Network Access to the applications and services users need. The GlobalProtect™ app also lets you establish access policies based on host information profile (HIP), enabling even more granular security policies tied to device characteristics—such as operating system, patch level, and the presence of required endpoint software—when accessing sensitive applications.

Prisma Access for Network

Many branch offices and retail stores are geographically distributed and lack full-time IT staff, making deployment, management, change control, and hardware refreshes difficult.

Prisma Access can be used to connect remote networks over a standard IPsec connection—using any existing router, software-defined wide area networking (SD-WAN) edge device, or firewall that supports IPsec—to secure traffic, protect confidential information, and address data privacy needs. Prisma Access supports SD-WAN options using Palo Alto Networks Next-Generation Firewalls (NGFWs), CloudGenix SD-WAN, and third-party vendor products.

Prisma Access Service

Prisma Access delivers both networking and security services.

Networking

- **SD-WAN**—support for our NGFWs and integration with CloudGenix SD-WAN as well as third-party offerings.
- **VPN**—options for connecting users and networks, including IPsec, SSL/IPsec, and clientless VPN.
- **Explicit Proxy**—an alternative method for mobile users to connect to Prisma Access that secures internet and SaaS application traffic (HTTP/HTTPS).
- **Quality of Service (QoS)**—prioritization of bandwidth for critical applications.
- **Digital Experience Monitoring**—visibility into the entire service chain between users and applications.

Security

- **Firewall as a Service (FWaaS)**—NGFW security for branch offices and retail locations.
- **Cloud Secure Web Gateway (SWG)**—blocking of malicious sites using static analysis and machine learning.
- **Zero Trust Network Access (ZTNA)**—service- and application-specific access control.
- **DNS Security**—advanced analytics and machine learning to stop threats in DNS traffic.
- **Threat Prevention**—blocking of exploits, malware, and command-and-control (C2) traffic using threat intelligence. AI/ML-powered scanning protects against previously unseen threats.
- **Data Loss Prevention (DLP)**—prevention of data breaches, along with enhancements to data privacy and compliance.
- **Cloud Access Security Broker (CASB)**—governance and data classification to stop threats with inline and API-based security.
- **Sandboxing**—zero-day threat prevention with the industry-leading WildFire® malware prevention service.
- **IoT Security**—protection for every device on your network, delivering ML-powered visibility, prevention, and enforcement in a single platform.