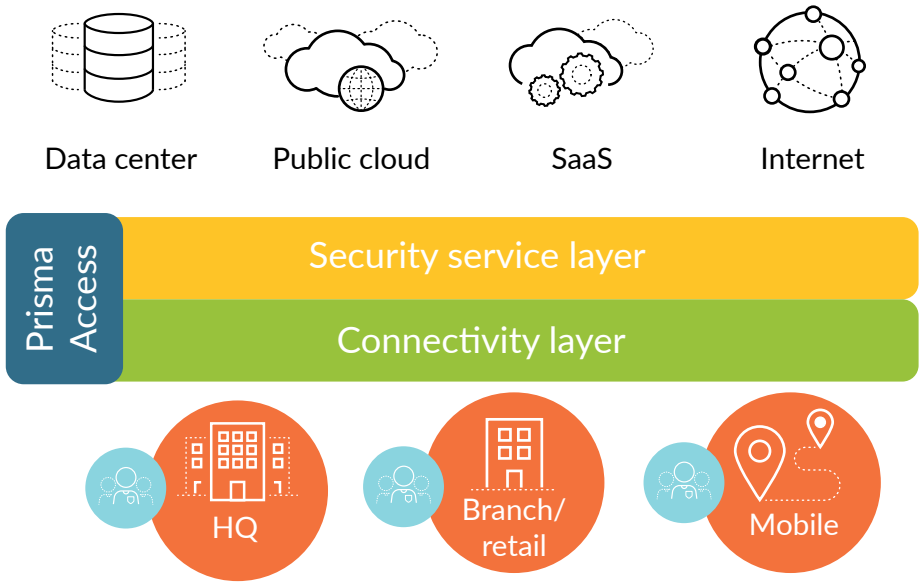
PRISMA ACCESS
BY PALO ALTO NETWORKS

Prisma Access: At a Glance

Global expansion, mobile workforces, and cloud computing are shifting the location of your applications, data, and users. These changes introduce new opportunities, but they also create new vectors for cybersecurity risk.



Prisma Access Highlights

- Protects your applications, remote networks, and mobile users in a consistent manner, wherever they are.
- Provides networking and security to connect and protect access to all your applications.
- Flexible and cloud-scalable to handle your changing requirements.

Protection for Your Growing Organization

Your security policies should be consistent wherever your users are, whether at headquarters, branch offices, or on the go. The same goes for your applications, whether in your data center or the cloud. However, maintaining consistent security at different locations is difficult, especially with the limitations of most networking and security technologies:

- Backhauling over a virtual private network (VPN) or multiprotocol label switching (MPLS) network to HQ and hairpinning to the cloud is inefficient and hurts the user experience.
- Routing branch and mobile user traffic directly to the internet without inspection is bad for visibility and security.
- First-generation cloud-delivered security, such as proxies, DNS filtering, and cloud access security broker proxies, has limited security capabilities.
- Using multiple point products drives up administrative costs and create operational challenges.

Prisma Access

Prisma™ Access (formerly GlobalProtect™ cloud service) helps your organization deliver consistent security to your remote networks and mobile users. It's a generational step forward in cloud security, using a cloud-delivered architecture to connect all users to all applications.

All your users, whether at your headquarters, branch offices, or on the road, connect to Prisma Access to safely use cloud and data center applications as well as the internet. Prisma Access consistently inspects all traffic across all ports and provides bidirectional networking to enable branch-to-branch as well as branch-to-HQ traffic.

Prisma Access delivers protection at scale with global coverage so you don't have to worry about things like sizing and deploying hardware firewalls at your branches, or building out and managing appliances in collocation facilities.

Prisma Access uses Cortex™ Data Lake for centralized analysis, reporting, and forensics.

PRISMA ACCESS
BY PALO ALTO NETWORKS

Prisma Access for Networks

Many branch offices and stores are geographically spread out and lack full-time IT staff, which makes deploying, managing, and upgrading security hardware logistically challenging.

You can use Prisma Access to connect your remote networks over a standard IPsec connection (using any existing router, SD-WAN edge device, or firewall that supports IPsec) to secure traffic, protect confidential information, and address data privacy compliance requirements.

Prisma Access implements a full-mesh VPN within the security overlay, eliminating the complexity and headaches normally associated with branch-to-branch networking.

Prisma Access for Users

Mobile users need consistent security to access data center and cloud applications as well. Remote access VPN falls 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 your users so traffic doesn't have to backhaul to headquarters to reach the cloud. It works together with the GlobalProtect app on a user's smartphone, tablet, or laptop. The app automatically establishes an IPsec/SSL VPN tunnel to Prisma Access for the full protection of the Security Operating Platform® without the backhaul to headquarters. With Prisma Access, all users have secure, fast access to all applications in the cloud, on the internet, or in your data center.

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.

Large populations of users may need to change locations from time to time, as conferences, weather, and natural disasters can strain local infrastructure. Prisma Access monitors conditions and automatically scales to add capacity in regions that need it.

Comprehensive Prevention Built In

Prisma Access centralizes the delivery and enforcement of key security services to stop a cyberattack:

- **Threat Prevention** stops exploits from reaching vulnerable endpoints and workloads, disrupts command-and-control traffic, and enforces IPS protections across all ports and protocols.
- **Malware Prevention** blocks the delivery of malicious payloads carrying known/unknown malware and ransomware, based on the latest Unit 42 threat intelligence, third-party threat feeds, and automated updates from Palo Alto Networks WildFire® service.
- **URL Filtering** blocks access to inappropriate or malicious websites and prevents credential theft by blocking attempts to submit corporate credentials to unknown websites.
- **DNS Security** identifies infected hosts attempting to establish contact with an attacker by sinkholing DNS queries to hostile domains.
- **User and entity behavior analytics (UEBA)** uses Cortex to track down attackers operating from within your organization.
- **App visibility** lets you maintain total oversight of all applications, across all ports and protocols. You can enforce policies to allow access to sanctioned applications based on User-ID™ technology and HIP, allow tolerated applications with threat inspection, and block unsanctioned applications.

Licensing Options

You can license **Prisma Access for networks** based on the total bandwidth used across all sites, and divide the bandwidth pool into the amounts each location needs (minimum bandwidth pool 200 Mbps).

You can license **Prisma Access for users** based on the total number of users, with tiers from 200 users up to 100,000+ users. Prisma Access for users requires the GlobalProtect app. Supported endpoints include Microsoft Windows®, Apple macOS® and iOS, Android®, Google Chrome® OS, and Linux.