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 remote networks and mobile users in a consistent manner, wherever they are.
- Provides connectivity and security to access all your applications.
- Offers flexibility and cloud scalability to handle your changing requirements.

Protection for Your Growing Organization

Cloud and mobility are driving changes in your network and your security requirements. 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 and hurts the user experience.
- Routing branch and mobile user traffic directly to the internet without 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.

These issues drive up administrative costs and create operational challenges, and the market demands a change. In 2019, Gartner defined a new cloud-delivered architecture for networking and security called the "secure access service edge" (SASE), which converges first-generation, standalone products with a common service delivery model.

Prisma Access

Prisma™ Access is a SASE that helps organizations embrace cloud and mobility by providing networking and network security services from the cloud. With a growing number of users, branch offices, data, and services located outside the protection of traditional network security appliances, organizations need a cloud-based infrastructure that converges networking and network security capabilities. Prisma Access provides consistent security services and access to cloud applications (including public cloud, private cloud, and software as a service), delivered through a common framework for a seamless user experience.

All users, whether at corporate 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 is delivered as a cloud service from more than 100 locations in 76 countries for users and branch offices to connect, enabling connectivity and security for mobile users, branch offices, and retail locations.

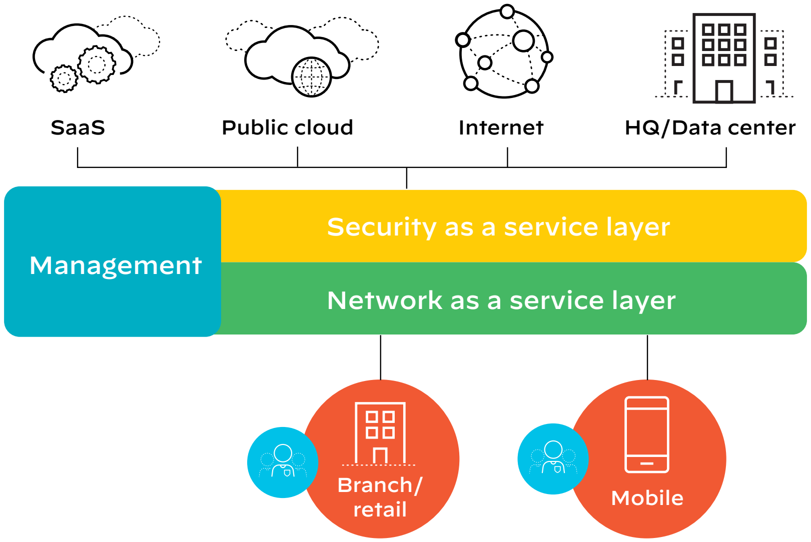

Figure 1: Prisma Access, a secure access service edge

Prisma Access
At a Glance

PRISMA™

Prisma Access for Networks

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® Instant-On Network (ION) devices, and third-party vendor products.

Prisma Access for Users

Mobile users need consistent security to access data center and cloud applications. 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 enforcement of security policy 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.

SASE Services

Prisma Access delivers both networking and security services, which include:

Networking

- **SD-WAN**—support for our NGFWs and integration with third-party SD-WAN
- **VPN**—options for connecting users and networks, including IPsec, SSL/IPsec, and clientless VPN
- **Zero Trust network access (ZTNA)**—access control and threat prevention to protect applications
- **Quality of service (QoS)**—prioritization of bandwidth for critical applications
- **Clean Pipe**—outbound internet security for managed service providers

Security

- **Firewall as a service (FWaaS)**—NGFW security for branch offices and retail locations
- **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
- **Cloud secure web gateway (SWG)**—blocking of malicious sites using static analysis and machine learning
- **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® service