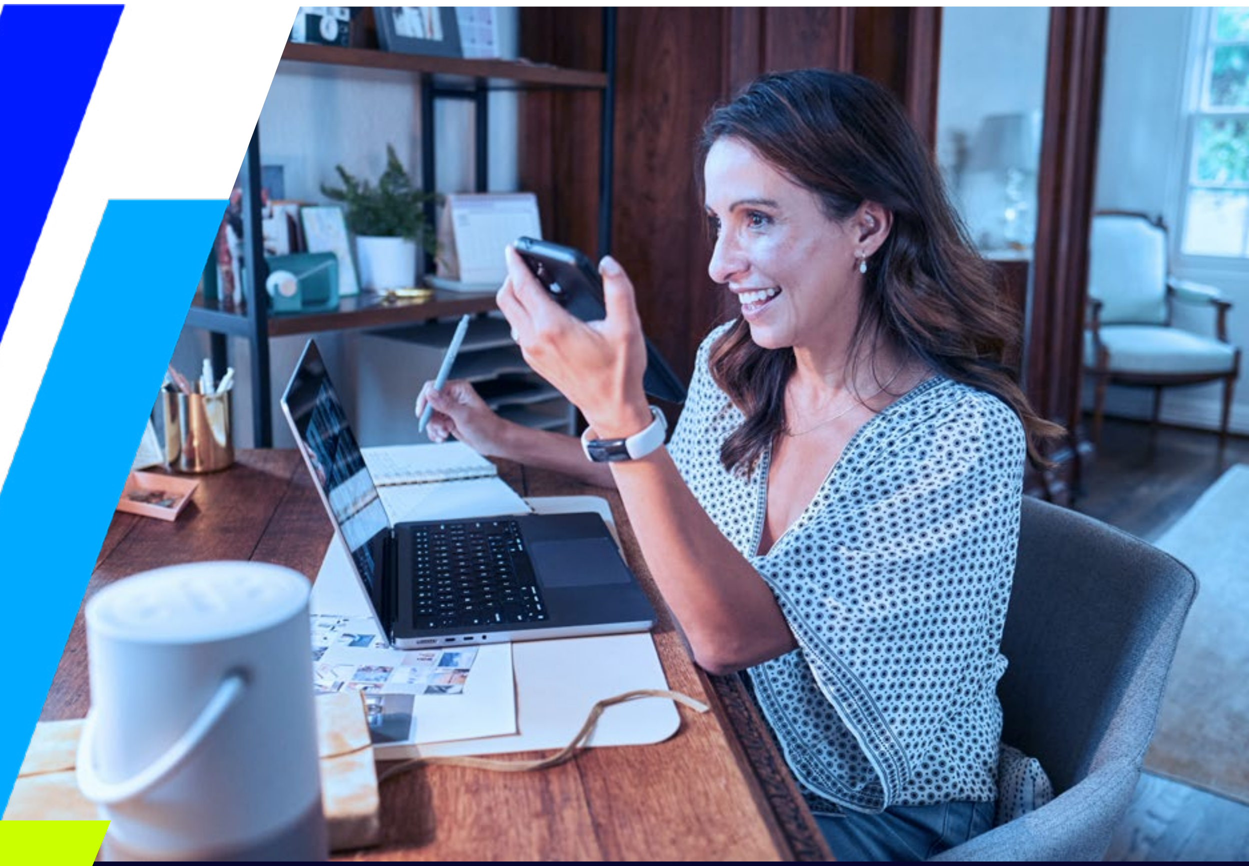

PRODUCT BRIEF

Create a Unified Approach With Prisma Access

Support Hybrid Workforce Through Identity-Based Security

The Modern Threat Landscape

With the rise of the hybrid workforce, organizations have become highly distributed, with many users working from anywhere and off of multiple devices; all while cyberattacks are increasing in frequency and their ability to evade traditional security solutions. While many organizations attempt to mitigate security risks with multiple layers of point products, this leads to gaps in security and a lack of easy visibility, while increasing network load and complexity, impacting the productivity of end users. Legacy approaches no longer meet modern business needs. It's time for a modern, unified, and cloud-first approach.

Prisma Access Creates a Unified Approach

Prisma Access remedies these pain points by providing secure connectivity and continuous verification for remote users while simultaneously empowering IT administrators, granting unparalleled visibility and control over network traffic. Serving as a virtual service edge, Prisma Access intelligently routes all users and devices to the data they need while ensuring security and high-speed network access. By using user context to verify users and enforce identity-based security, organizations can achieve zero trust access through consistently authenticating and authorizing users regardless of location. By combining the capabilities of Palo Alto Networks network-based firewalls and GlobalProtect endpoint security with network management, Prisma Access allows organizations to maximize their security investments.

Potential Benefits

- Stay ahead of current attack trends
- Create a unified approach for easy visibility and control
- Enable business growth with cloud-driven scalability
- Support hybrid workforce through identity-based security
- Manage productivity
- Maximize utilization of IT resources
- Prevent data leakage
- Ensure adherence to compliance and privacy requirements

Evolve Your Security with Prisma Access Enhancements

Palo Alto Networks has recently introduced additional features to help businesses evolve their security capabilities to reduce risk while modernizing their business operations. These new Prisma Access add-ons allow businesses to stay ahead of current attack trends and equip their IT team with the right tools to prevent attacks.

Enterprise Data Loss Prevention (DLP) is crucial for protecting sensitive information against unauthorized access, misuse, extraction, and sharing. Prisma Access Enterprise DLP uses a cloud-based service with machine learning-driven pattern recognition to identify and categorize sensitive data. Administrators can monitor and prevent uploads of sensitive data in file and non-file formats to websites and SaaS applications.

USE CASES
Intellectual property protection
Regulatory compliance
Insider threat detection
Secure collaboration
Data visibility and classification

SaaS Inline Security integrates with network security solutions to provide granular control of unsanctioned SaaS apps. By using analytics, reporting, visualization, and policy authoring, it effectively minimizes risks associated with non-compliant or risky applications. SaaS Inline discovers when employees use SaaS apps that violate compliance agreements or pose risks to the organization, enabling admins to understand and take appropriate actions. SaaS Security Inline and Enterprise DLP can be purchased as individual licenses. However, to use SaaS Security API with Prisma Access and SaaS Security Posture Management, a customer must purchase the CASB bundle.

USE CASES
Real-time traffic inspection
Data protection for SaaS applications
Policy enforcement

Next Generation Cloud Access Security Broker (CASB) assists businesses in managing productivity and collaboration applications for remote work. Unlike traditional CASB solutions, which may not provide full protection for SaaS applications, Next Generation CASB offers data protection for high volume data and SaaS security, supporting business growth with a hybrid workforce. CASB is being offered as a bundle containing all SaaS Security components and Enterprise DLP. When purchased with the initial Prisma Access license, it is activated when Prisma Access is activated.

USE CASES
Visibility into application usage
Risk assessment
Threat protection
Compliance enforcement

Autonomous Digital Experience Management (ADEM) improves network visibility using endpoint monitoring, real user monitoring, and synthetic transaction monitoring. ADEM offers native, end-to-end visibility and performance metrics for real-time application traffic, allowing organizations to quickly identify problem segments and reduce escalations. ADEM doesn't require additional appliances or agents and continuously monitors all segments from the endpoint to the remote application for mobile users utilizing GlobalProtect.

USE CASES
Network performance monitoring
Application performance management
User experience optimization

Prisma Access ZTNA Connector

The Palo Alto ZTNA (Zero Trust Network Access) application connector lets you connect Prisma Access to your organization's private apps simply and securely. ZTNA connector provides mobile users and users at branch locations access to your private app using automated secure tunnel. Because the ZTNA connector setup tunnels automatically, you do not have to manually setup IPSec tunnels and routing to the data center or headquarters locations, public cloud locations, and partner networks where your private apps are located. It also offers deep traffic inspection and threat prevention, ensuring robust application protection against potential threats.

The ZTNA Connector VMs you deploy automatically connect o the closest Prisma Access location, guaranteeing the best possible latency, in addition to scaling bandwidth access up to 1 Gbps per connector and 10 Gbps per connector group.

USE CASES	
Remote Work	Palo Alto's ZTNA application connector enables secure access to internal applications for remote workers, without exposing the entire network.
Mergers and Acquisitions	During a merger or acquisition, ZTNA can provide specific access to certain applications for the employees of the other company, without compromising network security.
Third-Party Access	ZTNA can offer controlled access to specific applications for third-party contractors, vendors, or partners, maintaining overall network security.
Micro-Segmentation	TNA aids in micro-segmenting large networks by isolating critical applications, thus limiting potential damage from a breach.
Cloud Migration	ZTNA can be deployed in the cloud during application migration, ensuring the same level of access control and security as with on-premises applications.

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.