Prisma Access Browser

The Uncomfortable Truth About Enterprise Security

In today's digital era, the primary security challenge is no longer within the corporate network itself, but the unmanaged devices used by the hybrid workforce. These devices, whether they belong to contractors or are part of an employee's BYOD policy, pose a significant risk when accessing corporate SaaS and sensitive, business-critical applications. In fact, 80% of data breaches occur from web applications and email,[1] which are primarily accessed via vulnerable, consumer web browsers, and a vast majority of organizations say more than half of remote workers access corporate apps via unmanaged devices.[2]

Traditional solutions to this challenge, like shipping managed laptops and large VDI deployments, are costly to implement, difficult to manage, and often provide poor user experience to workers. The cyberthreats many organizations face require a solution capable of securing the modern, dispersed workforce without hindering productivity.

What if a security solution enabled your business, instead of restricting it?

Introducing Prisma Access Browser

Palo Alto Networks provides the industry's only SASE solution with a natively integrated enterprise browser to create a secure workspace on managed and unmanaged devices. For the first time, users can enjoy consistent, frictionless Zero Trust access to SaaS and private applications on any device.

Prisma® Access Browser secures both managed and unmanaged devices, addressing the evolving security demands of modern organizations and their hybrid workforces. By extending SASE's protective reach to any device in minutes, Prisma Access Browser safeguards business applications and data against a spectrum of threats.

Unparalleled, Frictionless Security

Be agile: Secure any device in minutes with Prisma SASE, the only SASE solution with an integrated Enterprise Browser. This capability ensures comprehensive protection for business apps and data across any device.

Be confident: Protect with confidence using Prisma SASE, the only platform integrating AI to thwart threats on the fly, across browsers and apps. It effectively detects over 1.5 million unique attacks daily, providing a level of security unmatched by any other solution.

Be efficient: Experience unmatched efficiency with Prisma SASE, the only platform offering unified management for all devices. Simplify operations, reduce overhead, and automate IT tasks, securing your digital environment end to end.

1. *2023 Data Breach Investigations Report*, Verizon, June 6, 2023.
2. "Market Sentiment Survey: Network security concerns and requirements in the face of durable work-from-home realities" (unpublished study), ESG, August 2022.

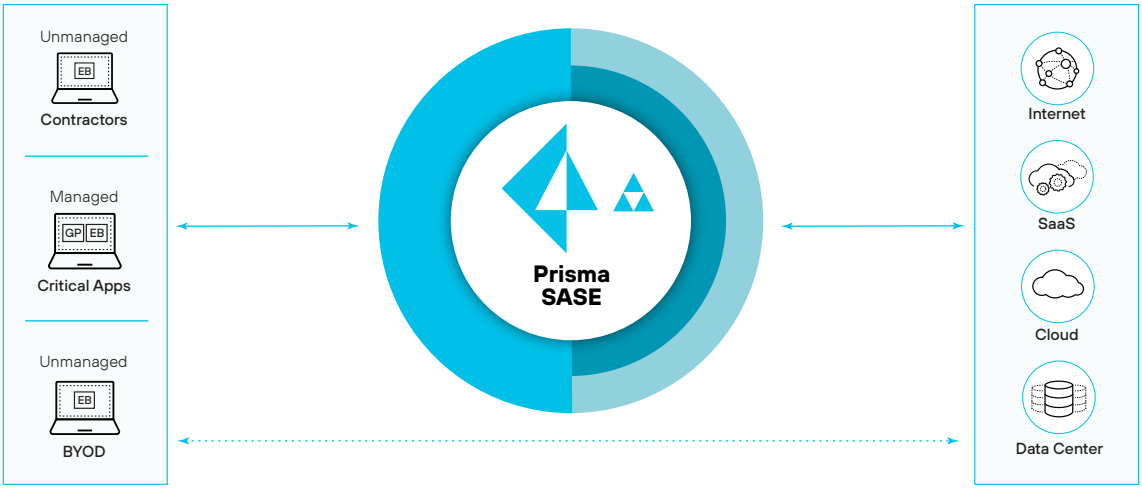

Figure 1: SASE extends to all devices with Prisma Access Browser

Use Cases

Prisma Access Browser supports a wide range of scenarios, including:

Securing third-party and contractor access: Prisma Access Browser delivers enterprise-grade security to contractors, delivering organizational control and visibility over external interactions with applications and data. Extending SASE's comprehensive security controls to unmanaged devices via the browser not only ensures compliance with corporate security policies but also reduces the cost and complexity of deploying traditional solutions. This approach provides robust protection for sensitive data and resources, enabling seamless collaboration with external partners while maintaining stringent security standards.

Enabling employee BYOD: With Prisma Access Browser, employees can effortlessly access corporate applications from personal devices without exposing their organization to risk. By harnessing the power of SASE, it ensures every personal device operates within a secure, compliant framework, enabling the flexibility of BYOD but with uncompromised security. This innovative approach eliminates the need for traditional device management solutions, striking an ideal balance between user freedom and device choice without compromising organizational security.

Providing secure access to critical web apps: In a landscape where sensitive web applications are central to business operations, Prisma Access Browser shields sensitive applications from web-based and internal attacks, and compromised endpoints across all devices. By embedding SASE's robust security features directly into the browsing experience, it empowers organizations to achieve operational excellence and maintain high productivity, confidently protecting their data on critical applications on all devices.

Key Benefits[3]

- **85% savings vs. shipping laptops**: Achieve significant cost reductions by eliminating the need to ship corporate laptops to remote workers and contractors, opting instead for the secure, cost-effective capabilities of Prisma Access Browser.

3. Based on internal analysis with independent third-party review. For the customer deck with calculations and use cases, please contact a Palo Alto Networks sales rep.

- **79% TCO savings vs. VDI**: Experience a dramatic decrease in total cost of ownership when compared to traditional VDI solutions, thanks to Prisma Access Browser's efficient, cloud-native architecture and operational simplicity.
- **Up to 100% of devices secured**: Remove gaps in security programs by ensuring comprehensive coverage across all devices, managed and unmanaged. Prisma Access Browser extends robust security measures to every endpoint, safeguarding corporate data regardless of the device's origin or user's location.

> "By 2030, enterprise browsers will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience."[4]
>
> – Gartner

Enhanced Security Features of Prisma Access Browser

Extend Zero Trust to the Browser

Prisma Access Browser incorporates Zero Trust Network Access, transforming traditional security by assuming no inherent trust in users or devices. These ZTNA 2.0 capabilities enable granular, identity-based access control directly within the browser, enhancing security and minimizing exposure to threats.

Table 1: Zero Trust—Prisma Access Browser vs. Consumer Browsers

Consumer Browser	Prisma Access Browser
No device posture control, risking access by compromised devices to sensitive information.	Enforces rigorous device posture checks before granting access, utilizing Continuous Trust Verification and security inspections to ensure compliance and mitigate risks.
Fails to confirm user identity for actions, increasing the vulnerability to identity-based attacks.	Integrates just-in-time MFA, providing an extra layer of security for ultrasensitive actions.

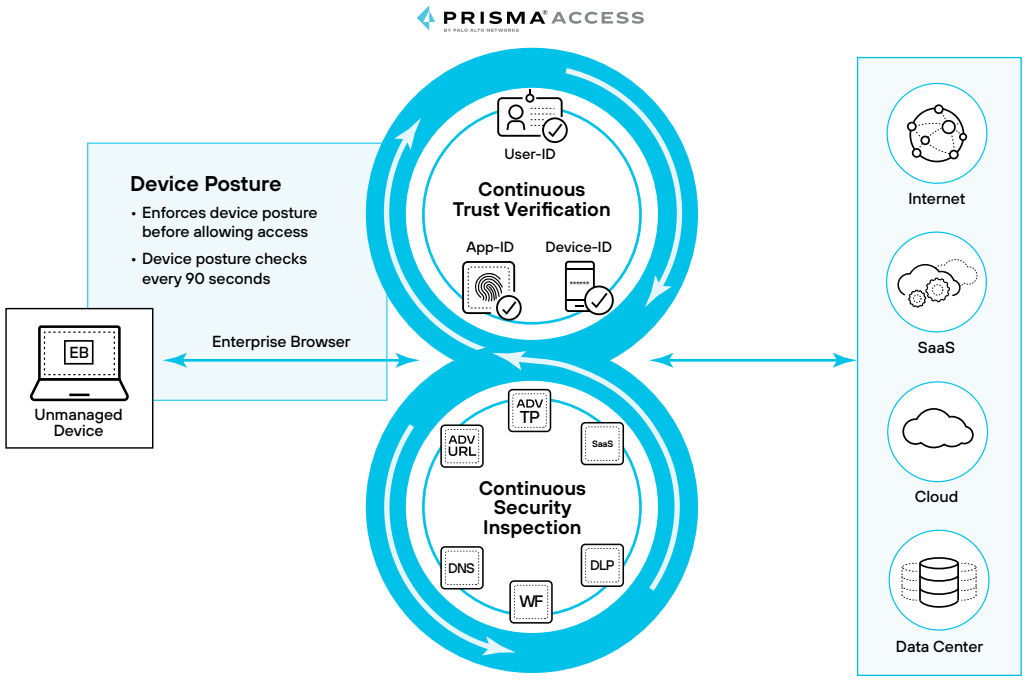

Figure 2: Prisma Access Browser enables Continuous Trust Verification and Security Inspection for unmanaged devices

4. Dan Ayoub et al., *Emerging Tech: Security—The Future of Enterprise Browsers*, Gartner, April 14, 2023.

Prisma Access Browser uses Prisma Access Continuous Trust Verification to provide fine-grained, least-privileged access, and deep and ongoing security inspection, and Prisma Access Continuous Security Inspection to provide a full spectrum of security services, including Advanced Threat Prevention, Advanced URL Filtering, DNS Security, sandboxing, and more.

Create a Secure Workspace on Any Device

Prisma Access Browser creates a secure environment for web browsing by safeguarding browser assets, runtime, and surface area against vulnerabilities and attacks. This comprehensive protection ensures that all online activities and data within the browser are insulated from web-based threats and threats from compromised endpoints.

Table 2: Secure Workspace—Prisma Access Browser vs. Consumer Browsers

Consumer Browser	Prisma Access Browser
Browser Assets	
Not all browser assets are encrypted, and those that are can be easily bypassed.	An additional encryption layer protects all browser assets with a trusted encryption chain that's independent of the operating system.
Threat actors can spoof the operating system to de-encrypt browser assets.	Implements security measures specifically designed to counteract spoofing attempts, preventing unauthorized access to encrypted browser assets.
Browser Runtime	
Lacks protection from endpoint malware targeting the browser.	Built-in keylogger protection and defense against screen scrapers.
Unable to mitigate risk from insiders tampering with the browser memory.	Implements controls to protect browser memory from tampering, ensuring the integrity of runtime operations.
Overreliance on the endpoint certificate store, exposing the browser to potential certificate-based attacks.	Enhances security by protecting against manipulation of device certificates, reducing reliance on the endpoint's certificate store.
Browser Surface Area	
Components are prone to vulnerabilities.	Allows disabling or controlling of vulnerable browser components on untrusted websites, mitigating exposure to common vulnerabilities.
Includes only minimal security controls against malicious extensions.	Provides full control over installed extensions and their permissions, ensuring that extensions that could access sensitive information are strictly managed and controlled.

Protect Sensitive Data Directly Where It's Accessed

Prisma Access Browser integrates browser-based Data Loss Prevention to safeguard sensitive information within the browsing environment. This feature proactively prevents the unauthorized sharing, transfer, or leakage of sensitive data, aligning with compliance requirements and corporate data policies.

Table 3: Data Protection—Prisma Access Browser vs. Consumer Browsers

Consumer Browser	Prisma Access Browser
No capability to mask sensitive data.	Masks sensitive data dynamically, based on content and context, ensuring that confidential information remains protected.
Vulnerable to data exfiltration through screenshots, sharing, copy/paste, and printing.	Blocks screenshotting, sharing via collaboration tools, copy/paste, and printing with configurable company watermarks on sensitive screens to prevent unauthorized capture.
Minimal control over file movements, leading to potential unauthorized data transfers.	Manages file transfers with encryption for downloads from corporate apps and blocks uploads to personal drives. Additionally, restricts file download/upload based on content and source, ensuring files move only within approved channels.

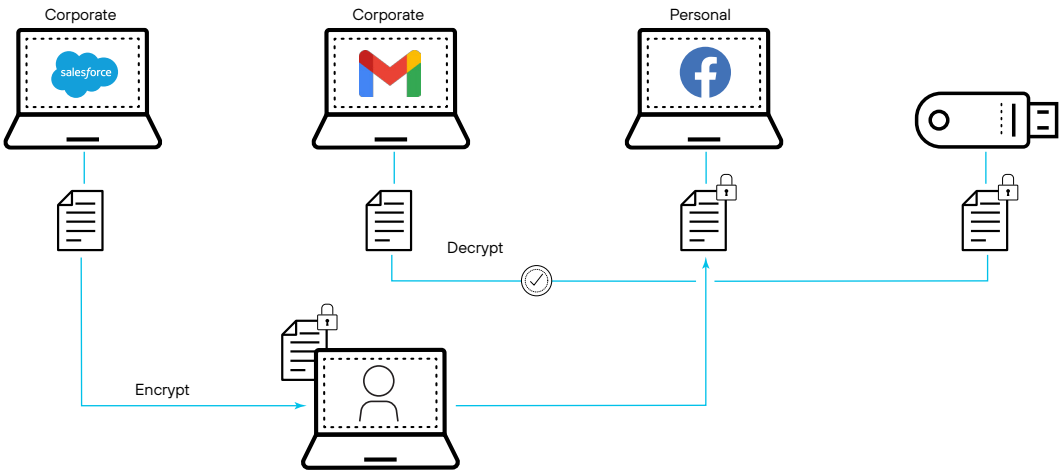

Figure 3: Protect sensitive data with file access based on user, application, and destination

Prisma Access Browser enables granular encryption and file access based on user, application, and file type, making it easy to secure sensitive data and minimize the risk of unauthorized access and data leakage.

Special Offers for Prisma Access Browser

For existing Prisma Access Enterprise Mobile User customers as of January 31, 2024, upgrade to the enterprise browser for free with the purchase of Professional Services for deployment. This upgrade is available until your next contract renewal or July 31, 2025, whichever comes first.

Additionally, take advantage of our exclusive bundle: two for the price of one with Autonomous Digital Experience Management (ADEM) and Prisma Access Browser, ensuring comprehensive protection for all account users. This special offer for new and existing Prisma Access customers requires the purchase of Professional Services prior to deployment.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice. For more information, visit www.paloaltonetworks.com.

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

prisma_sb_prisma-access-browser_073024