Prisma Browser: Secure Work on Any Device

The Browser Is Where Modern Work Happens

The browser has become the new operating system for enterprises, where work, data, and AI converge. Workers spend 85% of their day in the browser, with users accessing a growing number of SaaS, web, and GenAI applications.[1] While working in the browser contributes to increased productivity, the downside is that it has become the entry point of attacks. Among organizations, 95% report experiencing a security incident that originated from the browser.[2]

In parallel, the rapid rise of GenAI tools, agentic browsers, and AI-built apps is accelerating security risk and widening blind spots. As many as 65% of organizations report that they can't see what data is shared to GenAI tools.[3] As with many AI-based solutions today, AI browsers also come with their own associated risks.

The browser has also increased enterprise work on unmanaged devices, with 90% of organizations enabling some level of access from an unmanaged device.[4] Unmanaged devices, however, are responsible for over 90% of successful ransomware attacks.[5]

1–4. *The State of Workforce Security: Key Insights for IT and Security Leaders*, an Omdia report commissioned by Palo Alto Networks, January 2025.
5. *Microsoft Digital Defense Report 2024*, October 2024.

Prisma Browser for the Agentic AI Era

Prisma® Browser™ provides the industry's most secure 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, GenAI, and private applications on any device. Available as a browser, an extension for consumer browsers, and a mobile app, it provides secure access from any location in minutes.

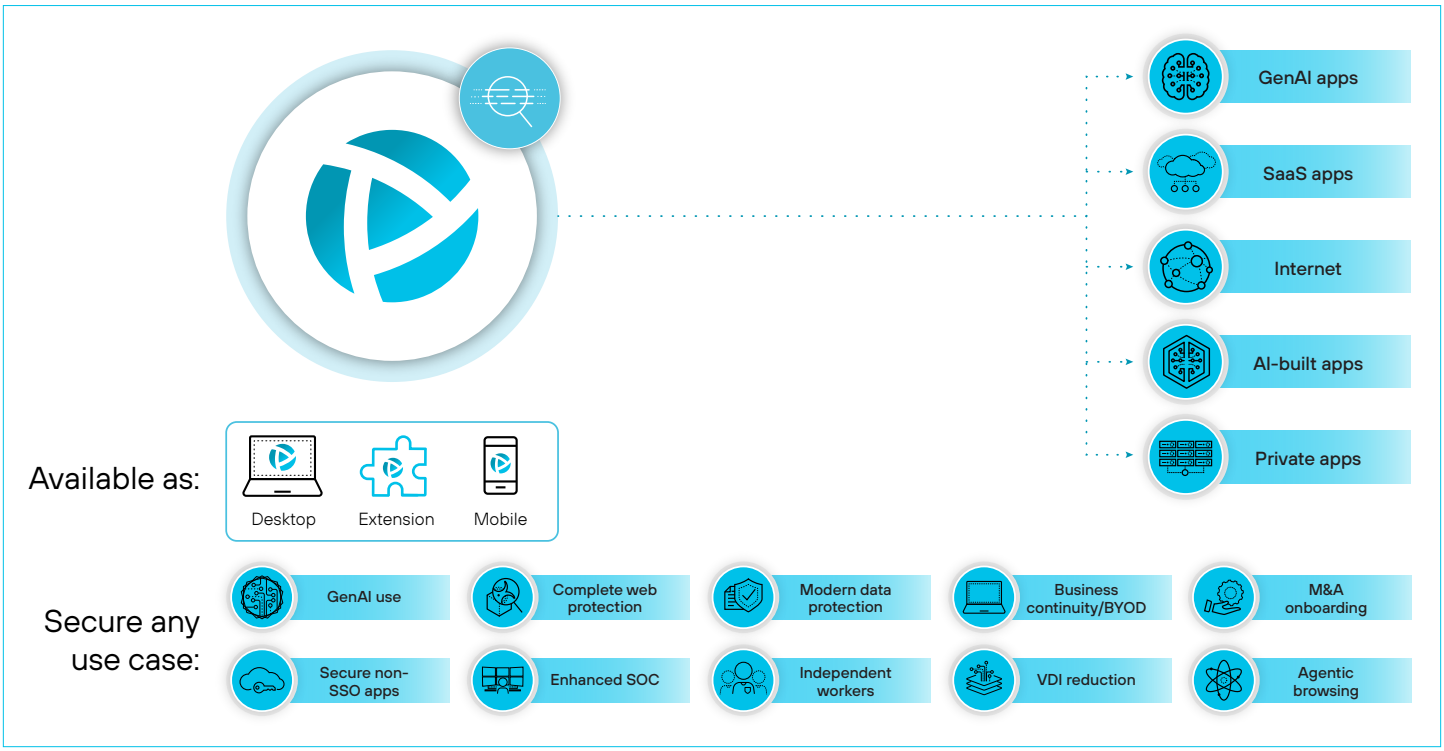

Figure 1. The Prisma Browser platform

Fight AI-Driven Attacks with AI

Prisma Browser uses our AI-powered security engines to secure all traffic, including encrypted traffic, and stop the most advanced threats:

- **Advanced URL Filtering and Advanced WildFire®:** Safeguard from AI-generated phishing and malware with the security engine that analyzes 3.8 billion new URLs and 77 million files daily.
- **Advanced web protection:** Continuously scan webpages in real time at all stages of loading to detect attacks that bypass legacy security tools and AI-driven spear phishing.
- **Advanced extension security:** Identify and block risky extensions with continuous monitoring for suspicious behavior.

Complete Zero Trust Coverage

Boost worker productivity without sacrificing sensitive data. Enforce data security policies in all AI-built, GenAI, private, SaaS, and web applications:

- **Get full visibility and granular control on user activity:** See all user activity and actions on any app. Control actions like copy and paste, printing, screenshotting, file movements, and camera and microphone controls.

- **Accurately identify data with a leading enterprise DLP engine:** Leverage built-in Enterprise DLP with over 1,000 built-in data classifiers and LLMs for 10x fewer false positives.
- **Secure the use of AI tools and agents:** Safely enable GenAI tools and agentic workflows with full visibility and last-mile data protection. Prevent data exposure, stop prompt injection attacks, and filter inappropriate prompts from users.

Secure the Workspace on Any Device

Ensure that the browser-based workspace is secure on any device or endpoint, regardless of whether they are managed or unmanaged:

- **Isolate work from risky endpoints:** Protect the browser from keyloggers and screen scrapers on the device itself.
- **Harden the browser from tampering:** An additional encryption layer safeguards browser assets on the device, and browser controls protect the integrity of runtime operations.
- **Containing data within the workspace:** Ensure data is contained within the secure browser and not exfiltrated, especially during user offboarding.

Deliver a Familiar User Experience in Minutes

Greet users on any device with a familiar browser experience and zero learning curve:

- **Secure access to private apps and resources from unmanaged devices:** Connect to private apps directly through the browser or Palo Alto Networks product portfolio (NGFW or SASE) without changes to the network architecture.
- **Save on costs compared to VDI and shipping laptops:** Save up to 85% in TCO compared to shipping laptops and up to 79% compared to VDI.
- **Provide an effortless login experience:** Using the integrated password manager for immediate, one-click login to required apps for all users while keeping passwords safe.

Secure Modern Work with Prisma Browser

Transform the browser into your main line of defense while keeping the enterprise agile. Prisma Browser safely enables many critical use cases while delivering a seamless user experience.

See how you can browse bravely—and securely—with Prisma Browser. To learn more, visit the Prisma Browser webpage.

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at 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-browser_052826