LEARNING MADE EASY

Prisma Access Browser: The Secure Browser for the Modern Enterprise

for dummies®
A Wiley Brand

Palo Alto Networks Edition

The browser is where work happens. It's the primary hub of productivity for the modern workforce. In fact, according to a study conducted by Palo Alto Networks in collaboration with market research firm Omdia, more than 85 percent of a worker's day is spent in the browser accessing business-critical software as a service (SaaS) and web applications — such as Google Workspace, Microsoft 365, Salesforce, and others — as well as sensitive information.

But browsers are also vulnerable. The same Palo Alto Networks/Omdia study found that 95 percent of organizations reported a security incident originating in the browser. According to the Verizon *2024 Data Breach Investigations Report* (DBIR), 80 percent of data breaches occur from web applications and email, which are primarily accessed via vulnerable traditional browsers such as Google Chrome, Microsoft Edge, and Mozilla Firefox.

In this brief, we'll explore the need for secure browsers to support common business use cases, and explain how Palo Alto Networks Prisma Access Browser helps modern enterprises address evolving requirements around securing the future of work in the new browser-based world.

What Is a Secure Browser?

A secure browser is the next evolution of the enterprise browser. Unlike traditional browsers, which individual

users manage, enterprise browsers are centrally managed by the organization. Enterprise browsers are typically used to securely access business-critical SaaS, private, web, and generative artificial intelligence (GenAI) applications from unmanaged or personal devices that are used by remote/hybrid workers, contractors, and third-party workers.

However, although enterprise browsers are more secure than traditional browsers, they may not be adequate in securing browser-based workspaces against artificial intelligence (AI)–powered phishing attacks and advanced malware. Some enterprise browser solutions use commodity-grade security solutions that rely on outdated malware detection technology. They also often lack access to vast threat intelligence, making it difficult for them to detect new and evolving cyber threats.

REMEMBER

Secure browsers provide all the features of an enterprise browser and additional security capabilities including full visibility into user actions, granular identity and access controls, blocking unsafe activity, requiring additional authentication, and last-mile AI-powered data loss prevention (DLP).

Secure browsers also have advanced AI-powered security capabilities to protect the browser-based workspace against sophisticated phishing and malware threats.

Exploring Key Business Use Cases

A secure browser is the gateway to corporate resources for independent workers, like contractors and third parties, as well as employees who perform work on their personal devices (that is, "bring your own device," or BYOD). A secure browser also supports a variety of previously unimagined new and evolving use cases, such as securing encrypted traffic without requiring decryption, and enabling business continuity in times of IT outage.

Empowering independent workers

Secure browsers deliver enterprise-grade security to the browser-based workspace for independent workers such as hybrid and remote employees, frontline and field workers, and contractors and other third parties. Secure browsers extend organizational control and visibility over interactions with business-critical applications and data. Extending the comprehensive security controls of a secure access

service edge (SASE) to unmanaged devices via the browser ensures compliance with corporate security policies, protects sensitive data from leakage, and reduces the cost and complexity of deploying alternative solutions, such as virtual desktop infrastructure (VDI) and physical laptops.

SASE is a cloud-native architecture that unifies software-defined wide-area networking (SD-WAN) with security functions like secure web gateway (SWG), cloud access security broker (CASB), firewall as a service (FWaaS), and Zero Trust network access (ZTNA) into one cloud-delivered service.

Securing BYOD

With a secure browser, employees can effortlessly access corporate applications from personal devices — wherever and whenever they need to get work done — without exposing their organization to risk. By harnessing the power of SASE, secure browsers ensure that 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 or user privacy.

Enabling cutting-edge use cases on any device

Secure browsers address a variety of previously unimagined use cases that were difficult or impossible to achieve with existing tools, including:

- **Securing encrypted traffic:** Secure encrypted traffic, such as QUIC protocol and Microsoft 365 service-level agreement (SLA) data, without the need for decryption.
- **Implementing last-mile data controls:** Enable last-mile granular content and context-based data control policies to protect data against leakage through the browser, enabling you to control user actions such as clipboard, screen sharing, printing, and downloading.
- **Safely enabling the use of GenAI tools:** Provide IT and security teams with deep visibility and tight user control over all GenAI applications, enabling the safe use of GenAI tools across the organization.

- **Securing privileged users:** Securely manage privileged remote access through secure browsers. Ensure that remote sessions are isolated from endpoint-based threats, implement granular access and identity controls, and centralize management and monitoring.
- **Stopping insider threats:** Prevent both accidental and intentional data loss by users without hindering productivity with highly granular last-mile data protection based on content and context and data sharing restrictions with complete audit trails.

Introducing Prisma Access Browser

Prisma Access Browser is the world's only SASE-native secure browser (see Figure 1). It protects work on any device, for any user, in any location, and in any application in minutes.

Powered by Palo Alto Networks Precision AI, which detects and blocks up to 8.95 million new attacks daily, Prisma Access Browser protects against advanced web-based threats, malicious extensions, and compromised devices. It extends Zero Trust principles and last-mile data controls to the browser, with

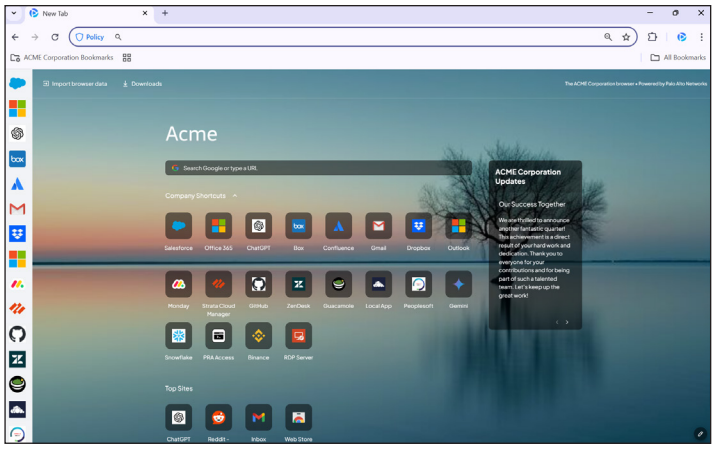

Figure 1: Based on Chromium, Prisma Access Browser looks and feels like a traditional browser.

more than 1,000 built-in data classifiers to protect sensitive information, and leverages AI-driven data classification to provide 20x more accuracy than traditional DLP solutions.

Key security capabilities and features in Prisma Access Browser include the following:

- **Advanced malware detection and prevention:** Integration with the entire Palo Alto Networks platform amplifies the security capabilities of Prisma Access Browser. Powered by Palo Alto Networks Precision AI, Advanced WildFire — the industry's largest cloud-based malware prevention engine — analyzes more than 77 million new files and prevents up to 450,000 new and unique malicious files every day. Advanced Threat Prevention offers real-time defense

against sophisticated threats, with deep learning models preventing 90 percent of injection attacks.

- **AI-powered anti-phishing protection:** Phishing remains one of the most significant threats today, as attackers leverage AI to craft increasingly convincing emails and websites to deceive employees into revealing sensitive information or installing malware. Prisma Access Browser leverages Advanced URL Filtering, which uses Precision AI to analyze 3.8 billion new URLs everyday. It can identify new and unique malicious URLs that traditional URL filtering solutions may miss.
- **Robust enterprise DLP:** Prisma Access Browser mitigates data loss with a robust feature set. Security teams gain granular insights into user interactions with corporate resources, allowing for real-time monitoring and response to potential threats. They can see all user and device attributes, including user/group, device posture, network, and location. This visibility enables organizations to implement stringent data protection measures and control access to sensitive information based on user roles, contexts, and behaviors. It helps prevent unauthorized data access and exfiltration, ensuring that only authorized personnel can perform high-risk actions. The secure browser has Palo Alto Networks Enterprise DLP built into it, which includes more than 1,000 built-in data classifiers and advanced machine learning (ML)/natural language processing (NLP), as well as optical character recognition (OCR), exact data matching (EDM), and indexed data matching (IDM) capabilities. This ensures Prisma Access Browser delivers strong content-based protection.

The future of work is here, and it's browser-based. As organizations continue to embrace hybrid work models, the need for secure, efficient, and user-friendly tools will become even more critical. Prisma Access Browser not only meets these needs but also anticipates the future challenges of a dynamic and ever-changing work environment. By providing unparalleled security and a seamless user experience, it ensures that businesses can stay productive and secure, no matter where or how their employees work.

TIP

Learn more about Prisma Access Browser and how it provides consistent visibility, control, and security for SaaS and web applications on any device at: www.paloaltonetworks.com/sase/prisma-access-browser.

See how Prisma Access Browser can help you browse bravely. Schedule a personalized demo. https://start.paloaltonetworks.com/prisma-access-browser-demo

paloalto® NETWORKS

 ISBN: 9781394302024