# Browse Bravely with Prisma Access Browser

Pintér András

# A Web-First World has Transformed the Way We Work

## The Browser is the Primary Hub of Productivity

**85%-100%**

**of a worker's day is spent in the browser.**

Palo Alto Networks/Omdia Forrester

### But Browsers are Vulnerable

**95%**

**of organizations reported a security incident originating in the browser.**

Palo Alto Networks/Omdia

**328**

**vulnerabilities were found in the browser in 2024.**

CVE Details

## Widespread Use of SaaS, Web, & GenAI apps via the Browser

**~10,000**

**SaaS and web apps used in large organizations today, on average.**

Palo Alto Networks

### But Organizations Lack Visibility & Control in SaaS, Web, & GenAI Apps

**65%**

**of organizations have limited to no control into what data is shared in AI tools.**

Palo Alto Networks/Omdia

## Employees & Third Parties Leverage Unmanaged Devices to Get Work Done

**~90%**

**of organizations enable employees access to corporate applications with personal devices.**

Palo Alto Networks/Omdia

### But Unsecure Devices Compromise Top Organizations

**~90%**

**of successful ransomware compromises originate from unmanaged devices.**

Microsoft

# Meet Prisma Access Browser

- Any user
- Any device
- Any location
- Any application

# Unleash the Power of the Browser to Securely Enable . . .

## Independent Workers

- M&As
- Call Centers
- Frontline and Field Workers
- Lower Cost of Shipping Laptops
- Reduce VDI

## BYOD

- Workforce Agility
- Device Freedom
- Enable Mobile

## Previously Unimagined Use Cases on Any Device

- Support Undecryptable Traffic
  *(e.g., QUIC, Microsoft 365 SLA, and more)*
- Last-Mile Data Protection
- Enable GenAI
- Business Continuity Plan
- Secure Privileged Users
- Insider Threats and Browser Hunting
- Forensics and Compliance
- Access to Non-Managed Accounts
  *(e.g., Virtual Deal Room, Financial Services)*

# This is Why Prisma Access Browser is Unique

- Chromium-based
- Native UX
- No admin privileges required
- Unified visibility, single policy

Available on

iOS


**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.

Gartner

# Prisma® Access Browser Unique Capabilities

## Palo Alto Networks Precision AI®

### Malware Analysis

#### Advanced WildFire®

- Industry's largest cloud-based malware prevention engine.
- Analyzes **>28B** unique files per year, detects **>99%** of known and unknown malware.

### Web Security

#### AI-Powered URL Filtering

- Industry's biggest AI-powered threat intel DB.
- Most advanced phishing protection engines block **>41B** malicious URLs a year.

### Threat Protection

#### Advanced Threat Protection

- Real-time defense against the most advanced evasive threats.
- Deep learning models trained on millions of data points provide **90%** prevention of injection attacks.

# The Depth and Breadth of Prisma Access Browser

| Secure Environment | | Last-Mile Data and Identity Controls | | User-First Workspace | |
|---|---|---|---|---|---|
| Device isolation | Advanced URL filtering | >1K data classifiers | Watermarks | Private app access | |
| Keylogger protection | Multilayered anti-phishing | ML, OCR, EDM, IDM | Screenshot/Sharing control | SSH/RDP support | |
| Screen scrapers protection | Advanced malware prevention | Regulation profiles | Camera/Mic control | Sync across devices | Quick offboarding |
| Trusted certificate store | Advanced threat protection | Directional-based DLP | Login restrictions | App acceleration | User privacy |
| Network security and isolation | Extension visibility and protection | Any control on any app | Tenant restriction | Extension management | Productivity suite |
| Device posture | Audit trails | File protection | Password manager | Automated DEM | Integrated apps |
| Browser hardening | User timeline | Clipboard control | Step-up MFA | Enterprise branding | Deploy in minutes |
| Anti-tampering | Session recording | Typing guard | Passkeys | Internet Explorer mode | Zero infra changes |
| Attack surface reduction | Threat hunting and forensics | Data masking | Admin approval | Secure AI assistant | |
| Browser isolation | Shadow IT | Printing control | Just-in-time | SSO integration | |

**Cross-platform integrations: SIEM | SOAR | IdP | ZTNA | EDR | Threat intel | Asset management**

# Thank You

paloaltonetworks.com