

The Evolution of SASE

How the **Enterprise Browser** is transforming
the Security Landscape

Oliver Kaiser | SASE Domain Consultant



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

The Browser is the Primary Hub of

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 browsers 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

Widespread Use of SaaS, Web, and GenAI

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

Employees & Third Parties Leverage Unmanaged Devices to Get Work Done

~90%

of organizations enable employees access to corporate apps with personal devices

Palo Alto Networks/Omdia

But Unsecure Devices Compromise Top Organizations

~90%

of successful ransomware compromises originate from unmanaged devices

Microsoft

But it **hasn't transformed** the way we secure our Users



Web Filtering

- Based on Reputation DBs
- Prone to Evasion Techniques
- Can't handle HTTP3 + QUIC
- Can't inspect TLS with Pinned Certificates



Data Loss Prevention

- Can't handle modern WebSocket protocols
- Lacks native integration into SaaS Applications
- Bad User Experience results in Monitor-Mode Deployments

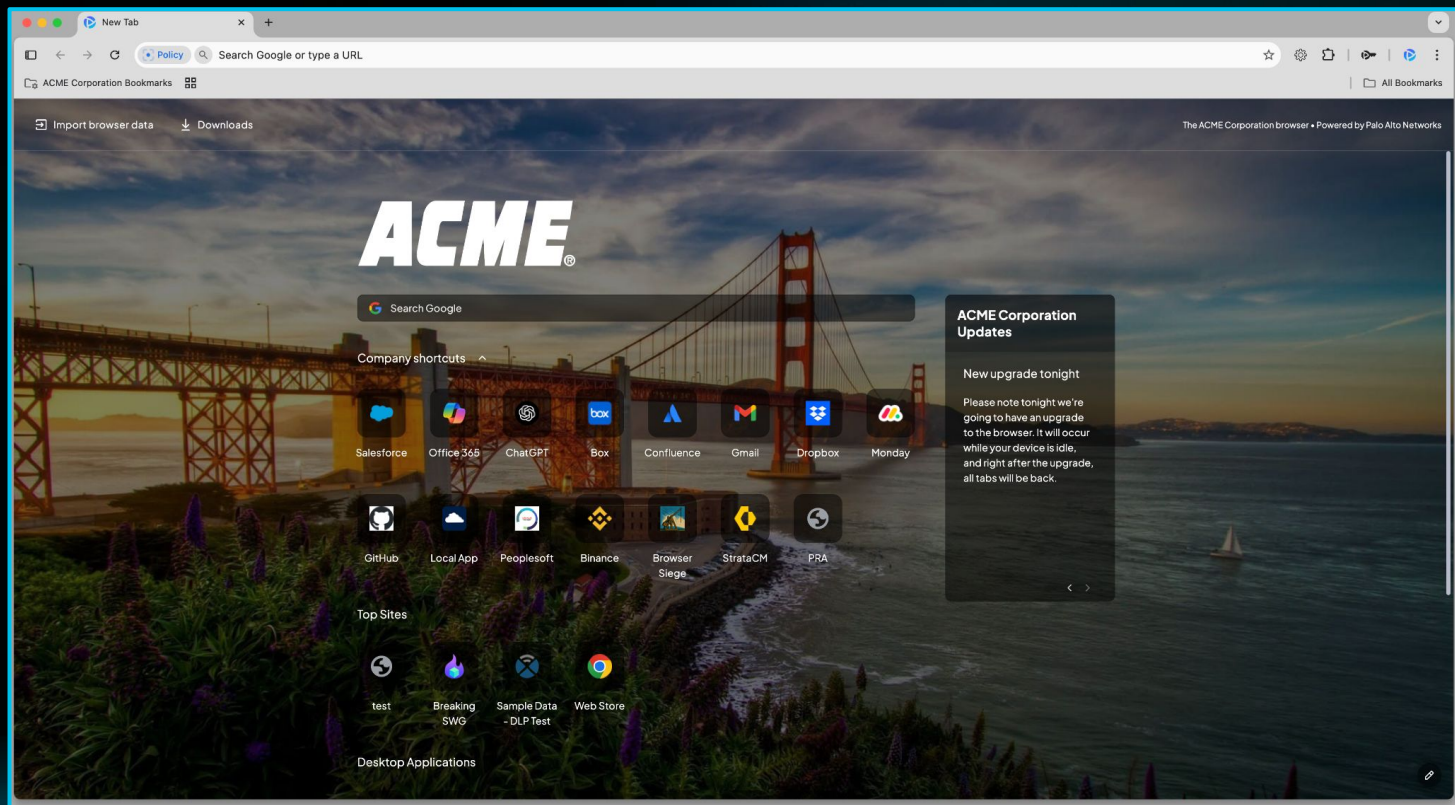


Malware Detection

- Prone to modern evasion tactics
 - HTML Embed
 - File Chunks
 - WebRTC, WebSockets, gRPC Transport
 - File Encryption

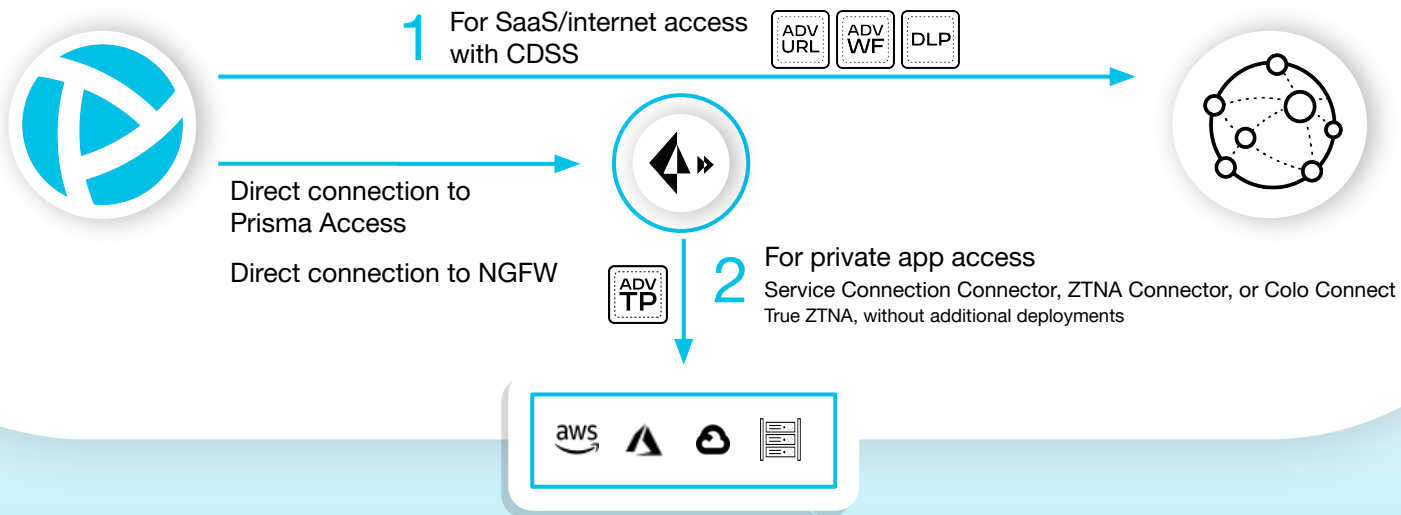
So how do we actually protect
the Modern Workplace?

Meet Prisma Browser



Prisma® Browser: **Secure Connectivity** to ALL Applications

Prisma Browser



Zero Trust with Zero Exceptions

Leveraging 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

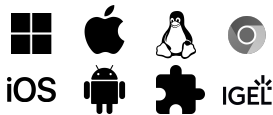
Advanced Threat Protection

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

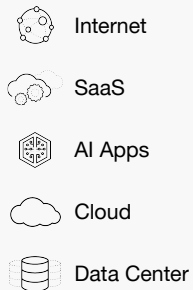
Browse Bravely with Prisma Browser

- Chromium-based, native UX
- Zero infrastructure changes
- No admin privileges required
- Unified visibility, single policy

Available on



Prisma
Browser



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



**Secure
Environment**

**Last-Mile
Data & Identity
Controls**

**User-First
Workspace**

Total Control with built-in Protection

MULTI-DIRECTIONAL PROTECTION

Protects against compromised endpoints

Hardens from tampering & Account Takeover

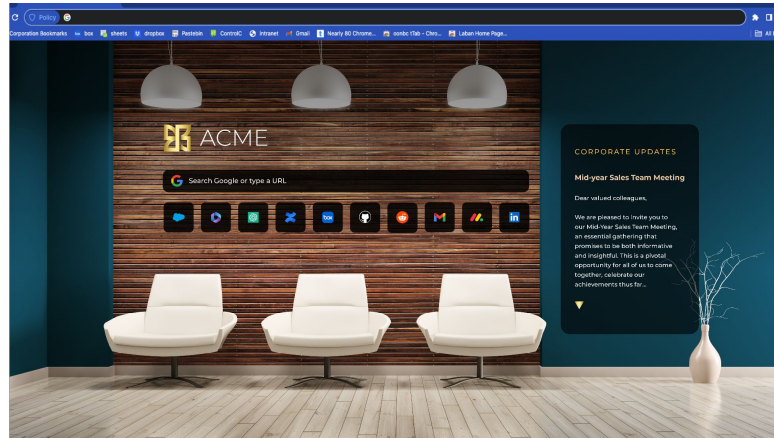
- Asset & memory protection
- Cert pinning & Integrity checks

Isolates from risky device

- Keyloggers & scrapers
- Untrusted certificates
- Public networks & MitM

Protects browser session

- Lock Screen
- Temp browser session time/data
- Max concurrent devices
- Device posture every 90 sec



Protects against web threats

Protects from malicious file download/upload

Protects from phishing

- URL reputation
- Static URL analysis
- Credential hygiene

Reduces attack surface

- Forces security patches
- Remote Browser Isolation
- Disabling browser components
- Memory protections

Defends against malicious extensions

Protect against insider risks with deep web insights for hunting and forensics

Web & user actions

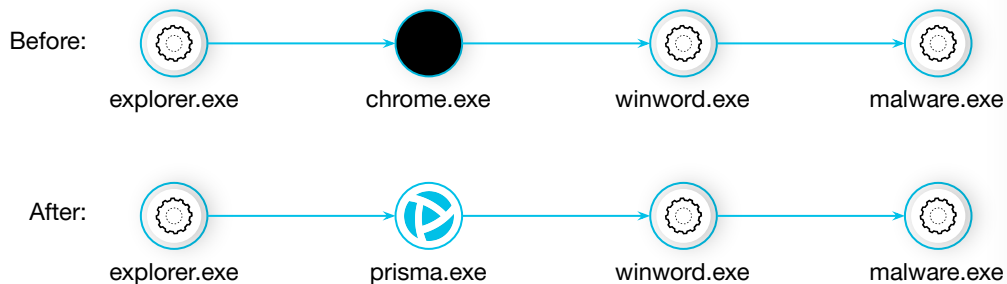
Screenshot & session recording

SaaS & Shadow IT

Browser extensions

Holistic Visibility across every digital transaction

Eliminate the browser blindspot in your
security operations



Web activities
SaaS visibility
User & data behavior
Browser extensions
Device posture (+unmanaged)
Evidence storage

Investigation Asif Amar M-MW2J6XFRHG Apr 06, 2025 16:37-17:37 Israel Session details

Search by specific data Time frame: Apr 6, 2025 0... User: asamar@paloaltonetw... Device: M-MW2J6X... Event type: A Application: A Action: A Is incident: A

Website access
Apr 6, 2025 5:00:37 PM

Access: Allowed

Metadata

Event ID	0E0V1JRSPT2HQD10Z81TTH9K86TC
Application	GitHub
User	asamar@paloaltonetworks.com
IP address	130.41.219.137
Browser version	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...
OS	macOS
MITRE	T1102
Compliance	SOC2 (CC6.2, CC6.3) PCI DSS (7.2)

URL: github.com/talon-sec/cloud-apps/pull/17685

Device: M-MW2J6XFRHG

Browser brand: Prisma Access Browser

OS version: 15.4.0

Compliance: SOC2 (CC6.2, CC6.3) PCI DSS (7.2)

Investigating Incidents across the Web like never before

Comprehensive Investigation Panel

Create a complete user journey

- Screenshots
- Event recordings
- Full session recordings
- Data snippets
- File & clipboard evidence

The screenshot displays the Investigation Panel interface. At the top, it shows the user's name (Eliazar Sikuriansky), device (M-M9WVYN220N), date (May 22, 2025), time (13:10-14:10), location (Israel), and session details. Below this is a search bar and filters for Time frame, User, Device, Event type, Application, Action, and Is incident. A bar chart at the top shows activity over time. The main area features a timeline of events, including Google Docs and YouTube access. A large screenshot shows a YouTube video player with a dark theme. Below the screenshot is a code block showing clipboard data:

```
"clipboard": {
  "data": "https://www.youtube.com/watch?v=Qcq_12JIHR8&t=61"
  "selectedElement": ""
},
```

 On the right, a 'Website access' panel for YouTube on May 22, 2025, at 1:40:54 PM, provides metadata including Event ID, Application (YouTube), User (esikuriansky@paloaltonetwork...), IP address (202.181.131.193), Browser version (137.8.0.32), and OS (OS version).



**Secure
Environment**

**Last-Mile
Data & Identity
Controls**

**User-First
Workspace**

Every Identity. Every Device. Across All Applications

ALL user & device attributes


USER / GROUP /
RISK SCORE


DEVICE POSTURE
ATTRIBUTES


NETWORK


LOCATION

ALL apps & user context


URL /
CATEGORY


SAAS APP

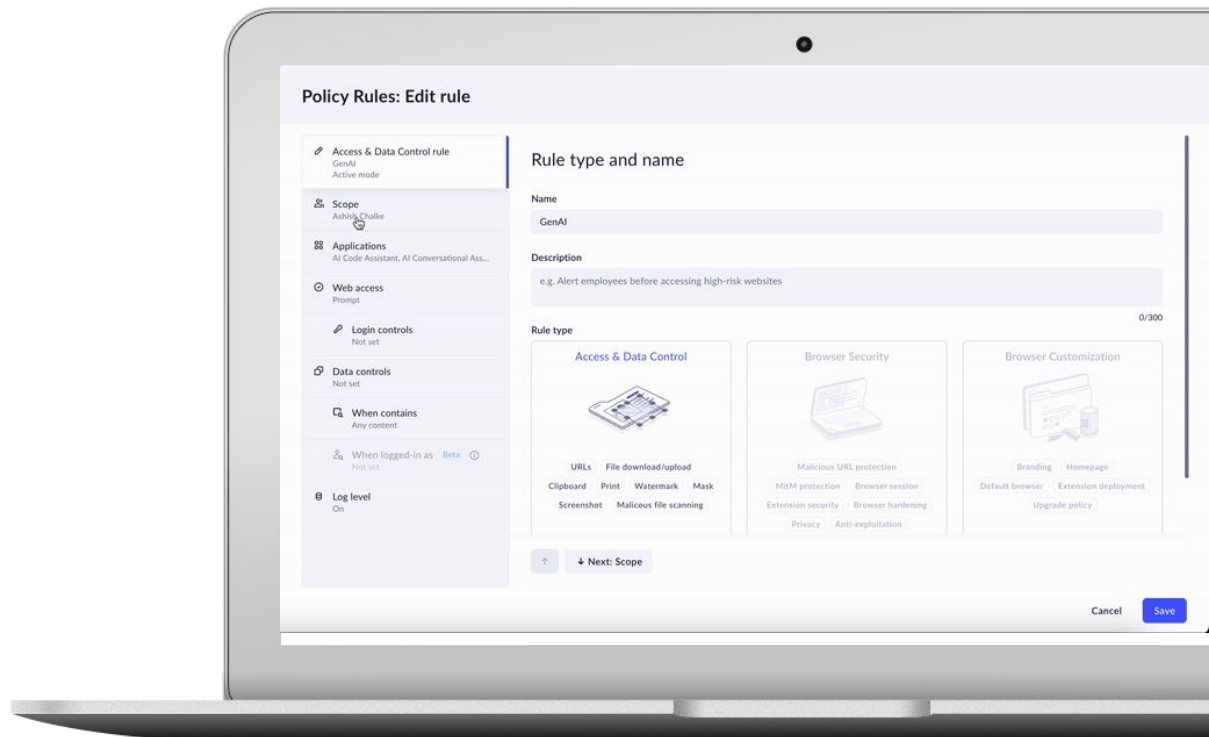

UNMANAGED
APPS


AI APPS


PRIVATE APPS


SSH/RDP


ACCOUNT TYPE &
SAAS TENANT



Take Full Control of Content

ALL actions & last mile, agnostically


Files

 File upload / download

Last-mile

 Copy / paste


 Print

 Screenshot / Screenshare


Web-specific


 Web login

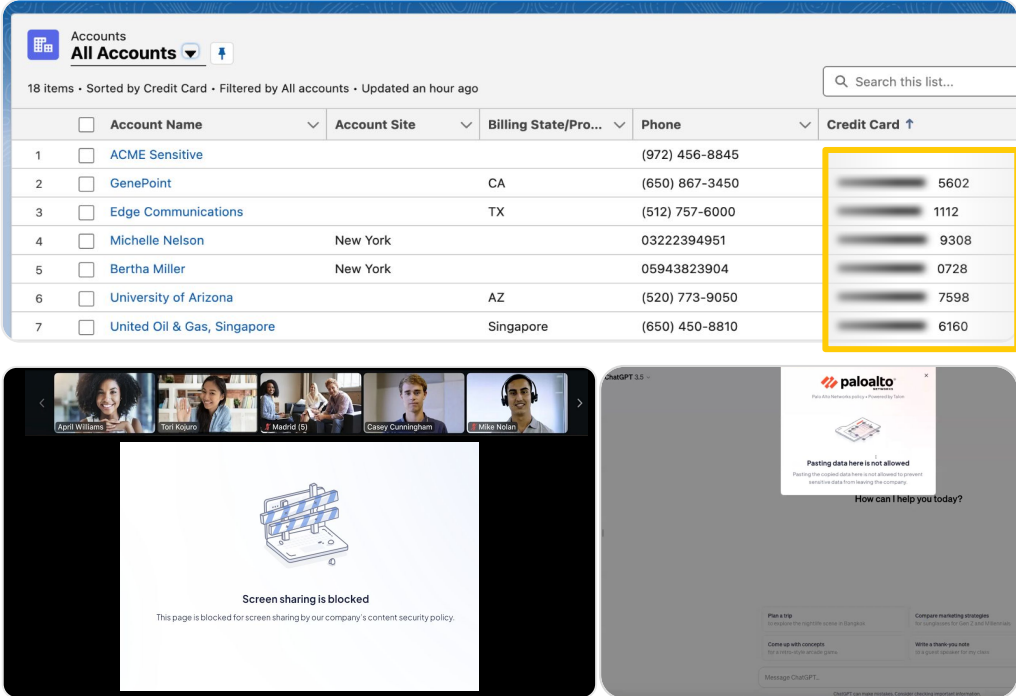
 Prompt control on GenAI

 Typing & read-only

 Masking

 Camera / Microphone

 Watermarks



The screenshot displays a web application interface with two main sections. The top section is titled "Accounts" and shows a table of 18 items, sorted by Credit Card. The table has columns for Account Name, Account Site, Billing State/Pro..., Phone, and Credit Card. The Credit Card column is highlighted with a yellow box, showing masked values and their corresponding numbers (e.g., 5602, 1112, 9308, 0728, 7598, 6160). The bottom section shows a meeting view with a video conference grid at the top and a large central area displaying a "Screen sharing is blocked" message. To the right of the meeting view, there is a "palto" logo and a message about pasting data, along with a "How can I help you today?" prompt and a "ChatGPT 3.5" interface.

	Account Name	Account Site	Billing State/Pro...	Phone	Credit Card ↑
1	ACME Sensitive			(972) 456-8845	5602
2	GenePoint		CA	(650) 867-3450	1112
3	Edge Communications		TX	(512) 757-6000	9308
4	Michelle Nelson	New York		03222394951	0728
5	Bertha Miller	New York		05943823904	7598
6	University of Arizona		AZ	(520) 773-9050	6160
7	United Oil & Gas, Singapore		Singapore	(650) 450-8810	

Holistic Access Control for Private and Public Apps

WITH leading data classification engines, **WITH** inline MFA & JIT on **ALL** controls



Data classification engines

- **One-stop shop** with shared classification library across all PANW products
- **>1K** built-in data classifiers, **80%** higher data classification with ML classifiers and 10x fewer false positives
- OCR, EDM & IDM
- **22** predefined regulations & compliance profiles (e.g., HIPAA, PII, GDPR, PCI)



Inline MFA & JIT on all web actions

- Step-up MFA with a variety of factors (including passkeys)
- End-user coaching and customized messages
- Proceed anyway with a reason
- Admin approval workflows

Prisma[®] Browser: **Unique Capabilities**



**Secure
Environment**

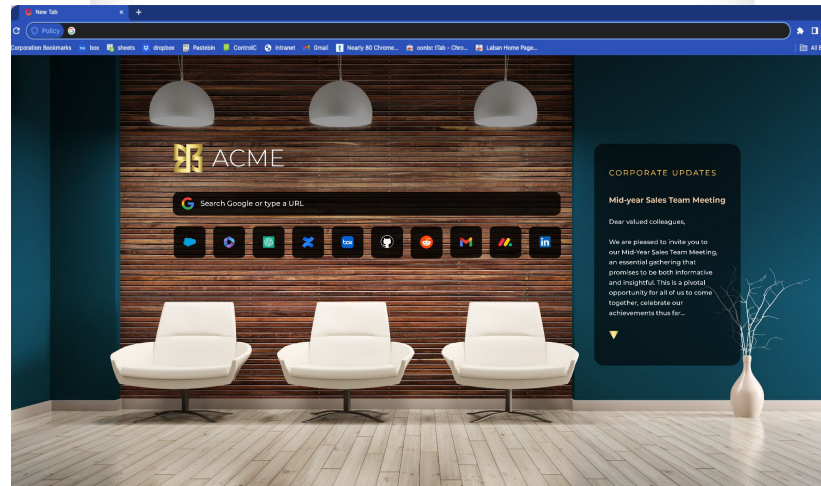
**Last-Mile
Data & Identity
Controls**

**User-First
Workspace**

Removing Friction and Enhancing User Experience

ENABLE USERS TO...

- Access all work apps as the primary work interface: Web, SaaS, GenAI, private, remote protocols, desktop apps, legacy web apps (IE)
- Onboard in minutes, with no admin privileges
- Experience maximum uptime with NO single point of failure



EMPOWER USERS TO...

- Login to apps immediately with an integrated password manager
- Quickly access company shortcuts via customized homepage and sidebar
- Preserve privacy with separate browser for personal and corporate use
- Quickly resolve issues with ADEM, remote troubleshooting and live session streaming

Taking Full Control of Credentials

Protect Credentials with the Power of an Integrated Password Manager



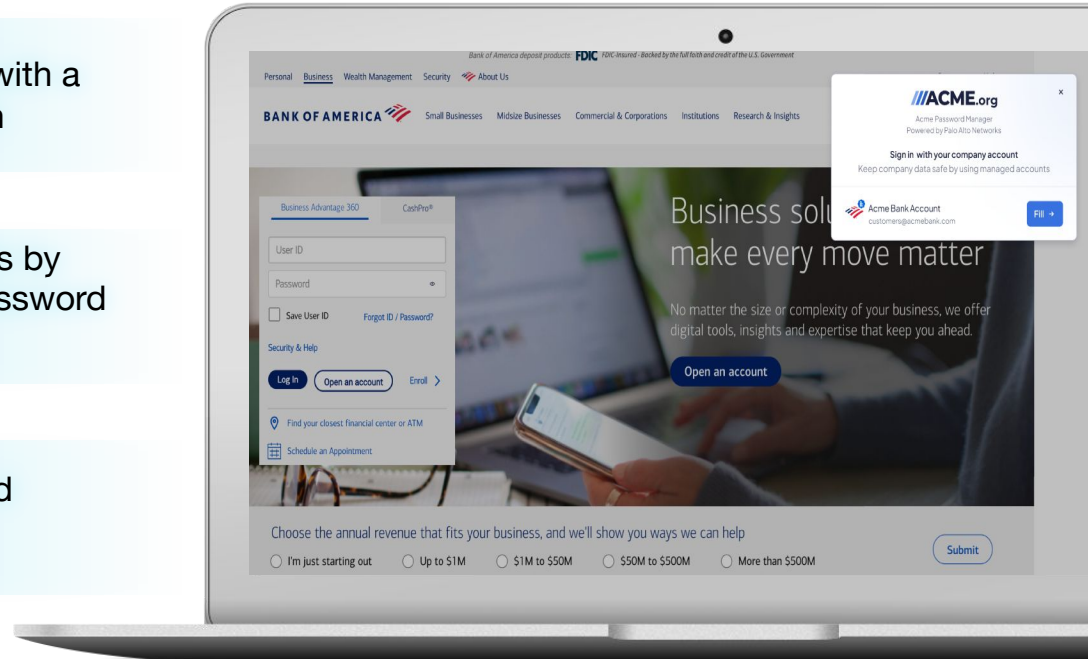
Keep credentials out of user hands with a zero-knowledge password approach



Simplify operations and reduce costs by eliminating the need for separate password tools



Speed up onboarding with auto-filled password access at first login



Simplifying Live Support

Quickly resolve issues with **remote admin operations**



Live session streaming to share the user's tab, browser, or full desktop in live



Admin troubleshooting to inspect device health, collect logs, and remediate



Autonomous Digital Experience Management with real-user metrics (RUM) for quick resolution of website issues

The screenshot displays the Prisma Access Browser interface. The main section is titled "Device health" and shows details for a device named "Yonatan-Lap". The device is online and running Windows 11 Pro (Build 26000.4652). The interface is divided into several sections:

- Device details:** Hostname: Yonatan-Lap, User: yonatang@everest.co, Status: Online.
- Metadata:** Device type: Laptop, Model: 21HE52HKO, OS platform: Windows, OS version: Windows 11 Pro (Build 26000.4652), Serial number: PF4FTK64, Device management: Unmanaged, Browser version: 118.5.5.1.58, Engine version: 1.2632.0, Session ID: 0d58497-d7c6-4450-be0f-58856975944c, Last policy update: Jul 14, 2025 13:13:41.
- Posture details:** Endpoint Protection: On, Active Firewall: On, File system encryption: On, Screen lock: On, Password policy: On, System integrity: Pass, Remote Desktop Connection: Fail.
- Diagnostics:** Diagnose connectivity issues to browser dependencies. A table lists services and their status:

Service	Status
Static assets service	✓
Configuration service	✓
Crash reporting	✓
Device service	✓
Identity Service	✓
Event ingestion service	✓
Malware protection	✓

On the right side, there is a "Live stream request" overlay. It features the Prisma Access Browser logo and text: "The Everest browser Powered by Palo Alto Networks". Below this, it says "Live stream request" and "Yonatan Gotlib is requesting to view a live stream session of your device. If approved, Yonatan Gotlib will be able to monitor your browsing session until terminated." At the bottom of the overlay are two buttons: "Decline request" and "Approve request".

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



Thank you

paloaltonetworks.com

