Secure Your Independent Workers' Digital Workspace with Prisma Access Browser

Bridging the Security Gap for Independent Workers

Modern enterprises rely heavily on independent workers and third parties to supplement expertise, scale operations, and enhance flexibility in response to dynamic business demands. This includes outsourced workers, supply chain partners, franchisees, freelancers, and other third parties that routinely access corporate applications and systems using unmanaged endpoints. In the United States alone, almost 40% of workers identify themselves as an independent worker providing professional services to a number of industries and organizations.[1]

In addition, independent workers and third parties are accessing a wider variety of applications, specifically enterprise SaaS and web-based applications. This changing application delivery infrastructure and user behavior have opened organizations up to a far larger attack surface. More than 80–90% of successful ransomware attacks originate from unmanaged devices,[2] and 80% of data breaches are via web applications and email, which are primarily accessed from web browsers.[3]

Traditional solutions, such as virtual desktop infrastructure (VDI) and desktop as a service (DaaS), are costly and complex to maintain, they don't provide consistent, high-performance user experiences, leading to user frustration or, even worse, attempts to bypass these controls. Now is the time to embrace a simpler and more secure approach to managing independent workers and third-party access, providing a user experience that's both more productive and significantly less costly than traditional solutions.

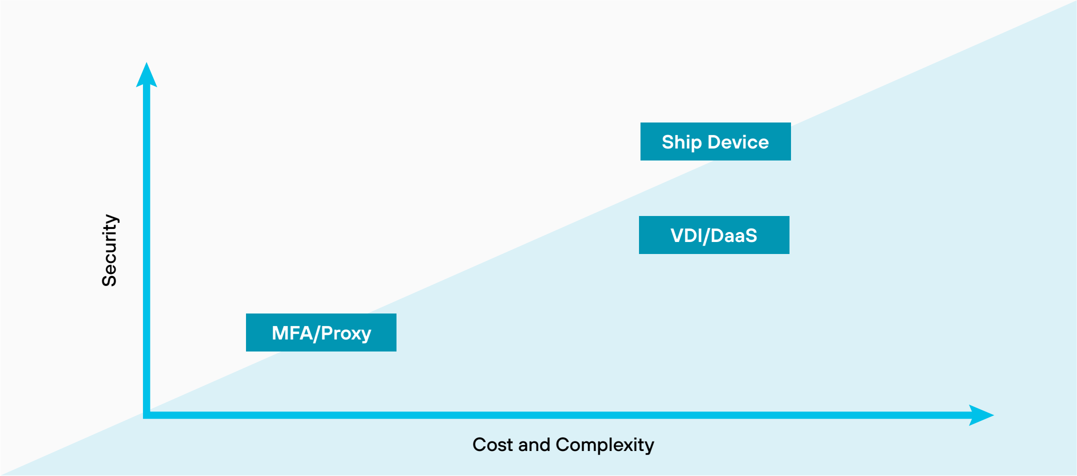

Figure 1: Traditional solutions to secure unmanaged devices become more costly and complex the more security they provide

Enabling the Modern Workforce with Prisma Access Browser

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

Prisma® Access Browser enables rapid onboarding and offboarding of independent workers to address the evolving business landscape of modern organizations. By extending SASE's protective reach to independent workers' unmanaged devices in minutes, Prisma Access Browser safeguards business applications and data against a spectrum of threats, which these workers can introduce.

[1] André Dua et al., "Freelance, side hustles, and gigs: Many more Americans have become independent workers," McKinsey & Company, August 23, 2022.

[2] *Microsoft Digital Defense Report*, Microsoft, October 2023.

[3] *2023 Data Breach Investigations Report*, Verizon, June 6, 2023.

Central to the solution's design is the browser's ability to deploy granular security policies tailored to specific job functions. Independent workers receive access only to the data and applications necessary for their roles, with sensitive information masked and nonessential apps and websites blocked, while other employees can access what they need to do their work without hindrance. This precise policy control helps ensure robust security without impacting job performance for any worker.

Unparalleled, Frictionless Security

Be agile: Secure any device in minutes with Prisma SASE, the only SASE solution with an integrated secure browser. Easily extend SASE protection to field agents, franchisees, temporary workers, and freelancers.
Be confident: Protect with confidence using the AI-powered Prisma SASE platform, thwarting 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, unifying visibility across managed and unmanaged devices for comprehensive oversight. Simplify operations, reduce overhead, and automate IT tasks, securing your digital environment end to end.

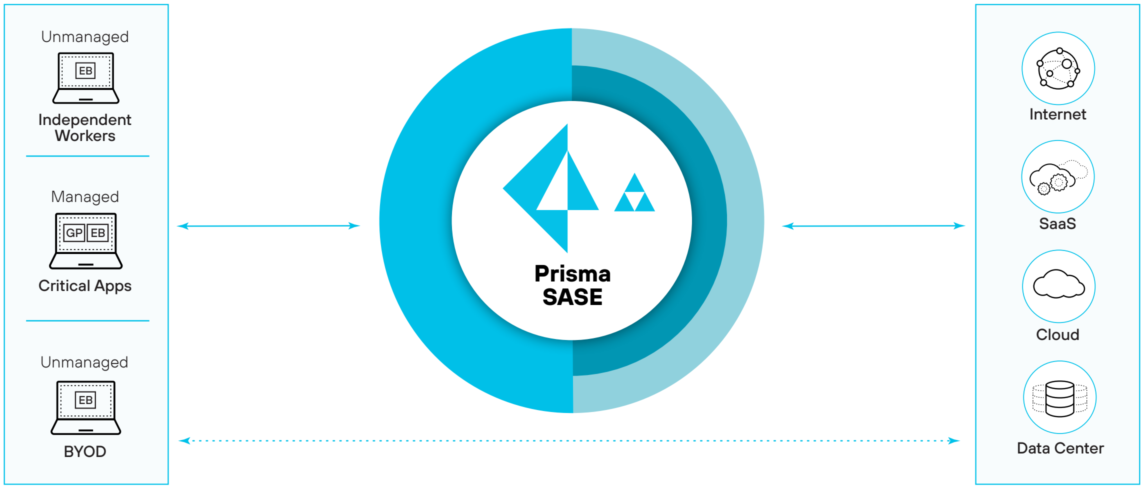

Figure 2: SASE extends to all devices with Prisma Access Browser

Key Benefits[4]

- **85% savings vs. shipping laptops:** Achieve significant cost reductions by eliminating the need to ship corporate laptops to independent workers, opting instead for the secure, cost-effective capabilities of Prisma Access Browser.
- **79% TCO savings vs. VDI/DaaS:** 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, from managed corporate devices to unmanaged independent worker devices. Prisma Access Browser extends robust security measures to every endpoint, safeguarding corporate data regardless of the device's origin or user's location.

[4] Based on internal analysis with independent third-party review.

Enhanced Security Features of Prisma Access Browser

Extend Zero Trust to the Browser

Prisma Access Browser incorporates Zero Trust Network Access (ZTNA), transforming traditional security by assuming no inherent trust in users or devices, which can be critical when working with third parties or in industries with high churn rates. 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, potentially allowing compromised devices to access sensitive information.	Enforces rigorous device posture checks before granting access, using 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.

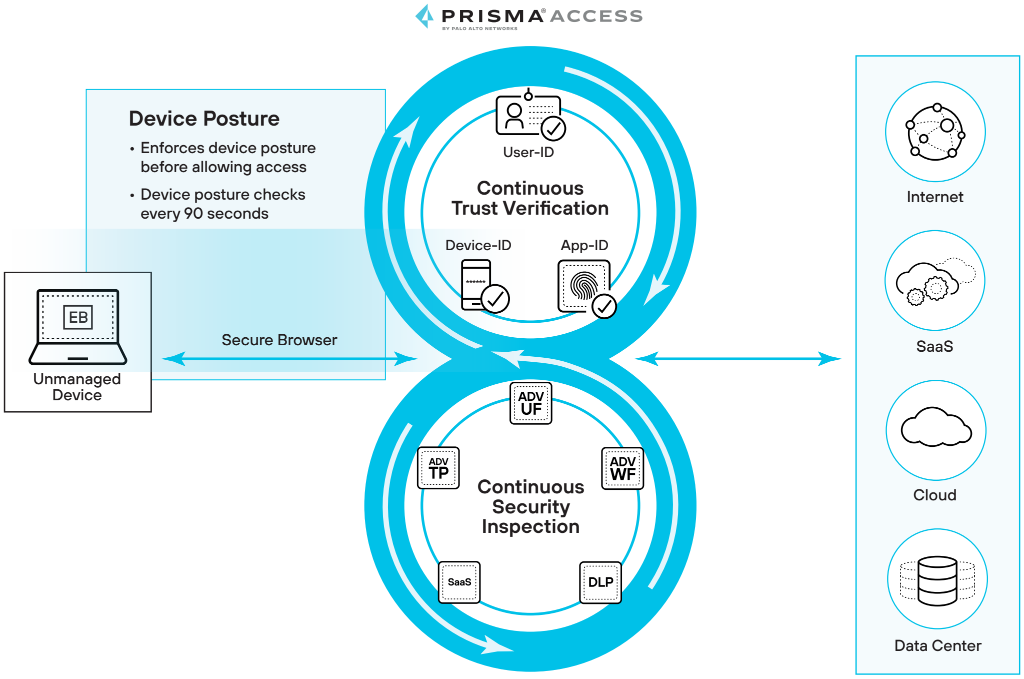

Figure 3: Prisma Access Browser enables Continuous Trust Verification and Continuous Security Inspection for unmanaged devices

Prisma Access Browser uses Continuous Trust Verification to provide fine-grained, least-privileged access. It uses Continuous Security Inspection to provide a full spectrum of security services, including Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire®, Data Loss Prevention (DLP), 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.
Over reliance 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 extension installation and installed extensions and their permissions, ensuring that extensions that could access sensitive information are strictly managed and controlled.

Protect Sensitive Data Directly in the Browser

Prisma Access Browser integrates browser-based DLP 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. Given that independent workers and third parties typically don't undergo the same rigorous onboarding checks that employees do, ensuring that your organization is protected from intentional or inadvertent data exfiltration is paramount.

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 sensitive 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. Also restricts file download/upload based on content and source, ensuring files move only within approved channels.

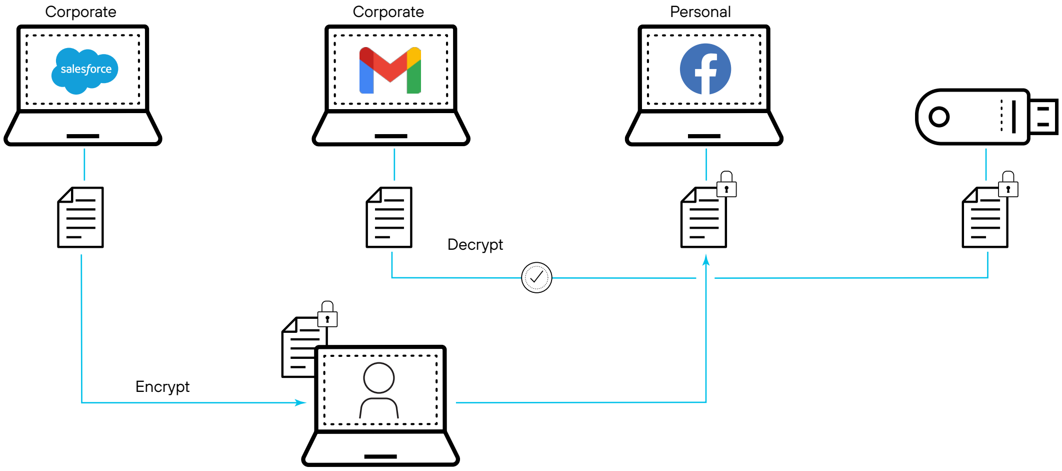

Figure 4: Protect sensitive data with file access based on user, application, and destination

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 secure browser for free with the purchase of Professional Services for deployment. Customers must purchase Professional Services before renewal or July 31, 2025, whichever comes first, to avail this offer. Customers taking advantage of this offer are entitled to use Prisma Access Browser until renewal of the Prisma Access license.

Contact the Palo Alto Networks Sales team for additional information on this offer and other exclusive offers you may qualify for.

To learn more about Prisma Access Browser, visit www.paloaltonetworks.com/sase/prisma-access-browser.

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security and security operations. Powered by Precision AI, our technologies deliver precise threat detection and swift response, minimizing false positives and enhancing security effectiveness. Our platformization approach integrates diverse security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection. From defending network perimeters to safeguarding cloud environments and ensuring rapid incident response, Palo Alto Networks empowers businesses to achieve Zero Trust security and confidently embrace digital transformation in an ever-evolving threat landscape. This unwavering commitment to security and innovation makes us the cybersecurity partner of choice. For more information, visit www.paloaltonetworks.com.

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