Secure Your BYOD Program with Prisma Access Browser

Bring Your Own Device Brings Risk

In today's digital-first workplace, enterprises increasingly embrace bring-your-own-device (BYOD) policies to boost flexibility, employee satisfaction, and responsiveness to rapid market changes. In fact, a significant portion of the global workforce now uses personal devices for professional tasks. However, that introduces potential vulnerabilities into the corporate IT ecosystem, increasing operational risk.

Moreover, the adoption of enterprise SaaS and web-based applications has expanded the scope of application delivery infrastructure. This significantly alters user behavior and expands the organization's attack surface. Studies show that a majority of successful ransomware attacks and data breaches originate from unmanaged devices.[1] Eighty percent of these breaches occur through web applications and email, accessed predominantly via web browsers.[2] Traditional security solutions like VDI and DaaS often fall short due to their complexity, cost, and inability to deliver a seamless user experience. Unfortunately, this sometimes drives users to seek workarounds that further expose the organization to risk.

That's why it's critical to adopt a more secure, cost-effective, and user-friendly approach to securing BYOD programs. Organizations need an advanced, strategic solution that delivers these benefits seamlessly, without any compromise.

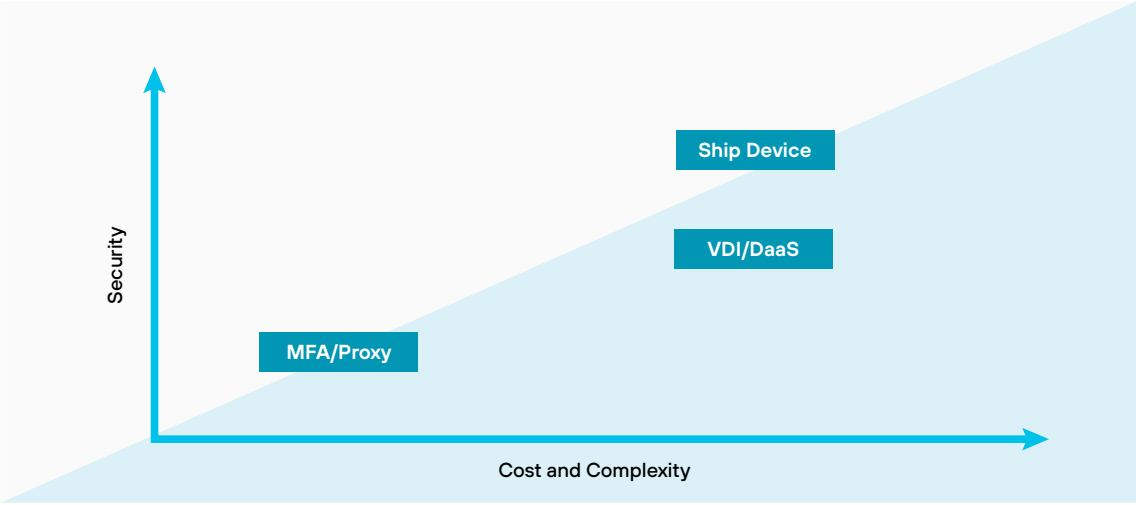

Figure 1: Traditional solutions become more costly and complex the more they secure unmanaged devices

Empowering BYOD 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 for employees' personal 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 personal devices used by employees. This extends SASE's protective reach to unmanaged devices in minutes, safeguarding applications and data against a spectrum of threats. It essentially addresses the evolving business landscape of modern organizations.

1. *Microsoft Digital Defense Report*, Microsoft, October 2023.
2. *2023 Data Breach Investigations Report*, Verizon, June 6, 2023.

Central to the design is the ability to deploy granular security policies tailored to specific job functions. This means employees using their own devices for work gain necessary access to perform their roles effectively, yet securely. Granular, browser-based controls ensure comprehensive and consolidated security is maintained without compromising the productivity or user experience of BYOD employees.

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 your employees' personal devices in minutes.

Be confident: The AI-powered Prisma SASE platform effectively stops threats on the fly from the app to the browser. Detecting over 1.5 million unique attacks daily, it has a level of security unmatched by any other solution.

Be efficient: Prisma SASE unifies visibility across managed and unmanaged devices for comprehensive oversight. It simplifies operations, reduces overhead, and automates IT tasks, securing your digital environment end to end.

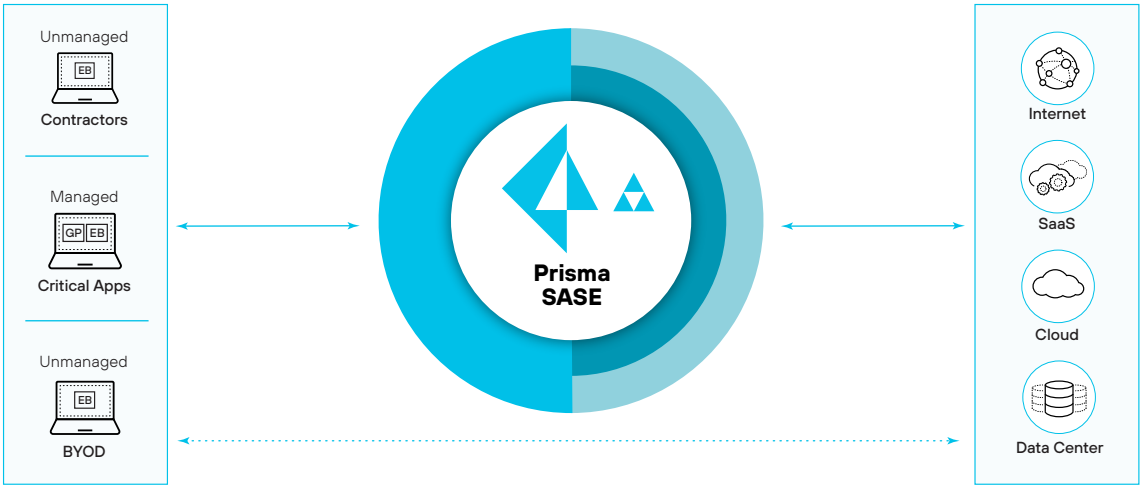

Figure 2: SASE extends to all devices with Prisma Access Browser

Key Benefits[3]

- **85% savings vs. shipping laptops**: Achieve significant cost reductions by eliminating the need to ship corporate laptops. Employees can instead use personal devices with 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. This is enabled by Prisma Access Browser's efficient, cloud-native architecture and operational simplicity.
- **Up to 100% of devices secured**: Remove gaps in security with comprehensive coverage across all devices, from managed to unmanaged. Prisma Access Browser extends robust security to every endpoint, safeguarding data regardless of the device or user location.

3. 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, transforming traditional security by assuming no inherent trust in users or devices. 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—Consumer Browser vs. Prisma Access Browser

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. Utilizes continuous trust verification and security inspections to ensure compliance and risk mitigation.
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.

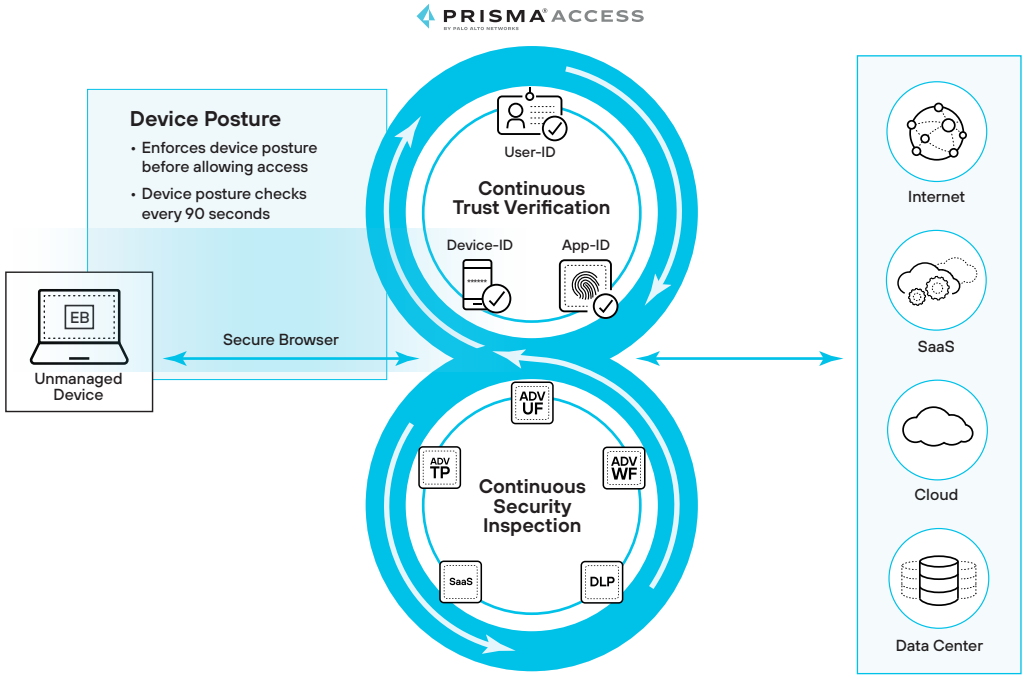

Figure 3: Prisma Access Browser enables continuous trust verification and continuous security inspection for unmanaged devices

Prisma Access Browser uses continuous trust verification to provide fine-grained, least-privileged access. Continuous security inspection provides 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 attacks. This comprehensive protection ensures that all online activities and data within the browser are insulated from threats, including those on compromised endpoints.

Table 2: Secure Workspace—Consumer Browser vs. Prisma Access Browser	
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 such as JavaScript, JIT, and WebRTC 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 and overly permissive extensions.	Provides deep oversight on both installing extensions and managing their access rights, protecting sensitive information effectively.

Protect Sensitive Data Directly in the Browser

Prisma Access Browser enhances BYOD security with integrated browser-based DLP. This approach blocks the unauthorized dissemination, transfer, or exposure of critical information, fully aligning with both compliance mandates and internal data policies. Since IT departments may not have the same level of control over personal devices as they do over company-issued equipment, it's crucial to fortify your defenses against data exfiltration risks—accidental or deliberate.

Table 3: Data Protection—Consumer Browser vs. Prisma Access Browser	
Consumer Browser	**Prisma Access Browser**
No capability to mask sensitive data.	Masks sensitive data dynamically, based on content and context. This ensures that sensitive information remains protected.
Vulnerable to data exfiltration through screenshots, sharing, copy/paste, and printing.	Enhances data security by preventing unauthorized screen captures and blocking screenshotting, copy/paste, and printing. Additionally, applies configurable company watermarks on sensitive screens deterring capture through collaboration tools.
Minimal control over file movements, leading to potential unauthorized data transfers.	Manages file transfers, encrypting downloads from corporate apps and blocking uploads to personal drives. Restricts file download/upload within approved channels based on content and source.

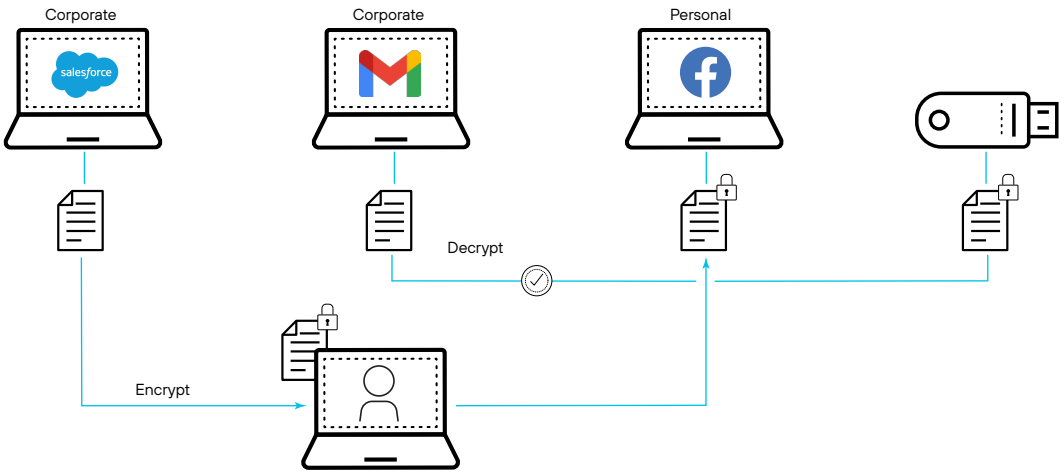

Figure 4: Protect sensitive data with file access based on user, application, and destination

Prisma Access Browser enables granular encryption and file access based on user, application, and file type. This makes it easy to secure sensitive data and minimize the risk of unauthorized access and data leakage.

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 em-powers 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 cdw.com/paloaltonetworks.

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_secure-your-byod-program-with-prisma-access-browser_010925