Prisma Browser

October 2025

Table of Contents

1. Welcome to a New Era of Work, from Any Device, Anywhere

As organizations transition to hybrid work models and embrace cloud-based operations, the modern web browser is fast becoming the primary workspace. It facilitates online communication and provides unparalleled productivity. Unfortunately, security infrastructures haven't evolved as fast as they should, making these browsers prone to attacks.

Despite approximately 85–100% of the workday taking place in web browsers, many enterprises lack security robust enough to respond to threats. In fact, in a joint Palo Alto Networks and Omdia survey, a staggering 95% of respondents reported experiencing browser-based attacks in the past 12 months, including account takeovers and malicious extensions. The concern becomes even more alarming when you consider that businesses already operate hundreds of web and SaaS applications, with organizations anticipating a 50% surge in application use over the next 24 months.[1]

This influx of vulnerable browsers and applications can have severe consequences for enterprises, including data breaches, financial losses, and reputational damage. For instance, account takeovers can result in unauthorized access to sensitive information, allowing attackers to steal data or disrupt operations. Malicious browser extensions can introduce malware, exfiltrate data, or provide a backdoor for further attacks. Data breaches can even lead to regulatory penalties, loss of customer trust, and significant financial costs associated with remediation and recovery efforts.

In addition to the security gaps, existing security tools create friction for users in their day-to-day workflows, which can result in decreased employee performance, general dissatisfaction, and churn of top talent. Nearly three-quarters (74%) of users will bypass security tools that get in the way of a business objective.[2] Virtual desktop infrastructures (VDI) are great examples of a traditional yet challenging approach to securing work. With the costs of VDIs reaching new peaks and the increasing complexity to implement and maintain them, IT and security teams are looking for alternatives.

Offering a new, frictionless approach to security in the browser, Prisma® Browser transforms the browser into an organization's first line of defense. Prisma Browser enables enterprise-grade security for any user, using any device, accessing any web application from anywhere in the world.

Built from the ground up to facilitate productivity and deliver a delightful user experience, Prisma Browser enables users to work confidently. It gives them the ability to onboard and offboard in minutes, and enjoy a customized workspace with zero learning curve.

2. Turn Your Browser into the First Line of Defense and Workplace of Choice

Prisma Browser is a secure browser. It's a comprehensive, secure workspace for work across your enterprise. It runs on a variety of endpoints (Windows, macOS, Android, and iOS), and it's managed by Strata™ Cloud Manager—a cloud backend and web-based management console. Prisma Browser communicates with Strata Cloud Manager to receive policy and software updates and send events.

Prisma Browser secures all websites, SaaS applications, private applications, and remote connections with the market's first secure browser natively integrated with SASE. Prisma Browser hardens the browser against malware and web-based attacks and provides deep visibility and control to prevent intentional or accidental data leakage. Deployed in minutes, Prisma Browser delivers up to 80% TCO savings compared to alternative solutions while delivering delightful end-user experiences and privacy.

[1] All statistics in this paragraph are from *The State of Workforce Security: Key Insights for IT and Security Leaders* report, based on a study conducted by Omdia for Palo Alto Networks, published March 4, 2025.

[2] "Gartner Identifies Four Myths Obscuring Cybersecurity's Full Value," Gartner, June 5, 2023.

2.1. Prisma Browser

Prisma Browser is founded on the Chromium open-source project behind popular browsers, such as Google Chrome and Microsoft Edge. This provides multiple benefits:

- Prisma Browser provides a native user experience with no learning curve for users who are already familiar with Chrome and Edge.
- Prisma Access uses the Chromium rendering engine so websites and web apps have the same look and feel as they do on other browsers such as Chrome and Edge.
- Prisma Browser supports all Chrome extensions out of the box.
- As one of the most significant open-source projects, it's continuously patched and matched with the ever-evolving web.

Prisma Browser provides comprehensive onboarding, with a customized welcome wizard for users to familiarize themselves with the browser's capabilities. Users can import everything from their existing browser—bookmarks, passwords, history, cookies, extensions, and accompanying settings.

Prisma Browser can be installed via deployment emails, self-service, or by using third-party software distribution tools. Admin permissions for installation and ongoing use aren't required.

Prisma Browser can be a fully customized and branded organizational browser based on its look and feel. You can customize the browser and icon with your organization's name, logo, and brand colors, as well as modify the homepage and its background. In addition, you can communicate with your users directly via the browser.

Prisma Browser also preserves user privacy. With local inspection in the browser, network decryption is no longer required. Because it's dedicated for work-related web browsing (and potentially separated from a user's personal browser), you're able to monitor all work-related activities without impacting the user's privacy.

Prisma Browser communicates with Strata Cloud Manager to receive policy and software updates and send events. It additionally provides the capabilities described in the sections that follow.

2.1.1. Secure Environment

Advanced security mechanisms are built into the browser to protect against compromised endpoints, web-based attacks, and malicious extensions. In addition, Prisma Browser collects insights to enable threat hunting and forensics.

2.1.1.1. Compromised Endpoint Protection

Prisma Browser isolates the workspace from the device, enabling users to safely work on compromised endpoints.

2.1.1.1.1. Hardens from Tampering and Account Takeover

- **Asset and memory protection:** To protect against infostealers and screen scrapers, Prisma Browser adds an additional layer of encryption to the browser assets on the disk and in the memory. Infostealers and screen scrapers interact with browsers to steal access tokens, cookies, credentials, credit cards, and other information to create user profiles.
- **Tampering protection:** Prisma Browser protects against tampering by bad actors, insiders, and sophisticated users, with multiple browser hardening, integrity checks, and certificate pinning.

2.1.1.1.2. Isolates from Untrusted Devices

- **Keyloggers and scrapers:** Prisma Browser protects against keyloggers and screen scrapers already installed on the device from stealing information inserted into the browser. This information includes credentials, MFA tokens, and other sensitive and proprietary information.
- **Meddler-in-the-middle (MitM) attacks:** Prisma Browser applies multiple security mechanisms to protect against network MitM: trusting specific TLS CAs, preventing users from ignoring SSL errors, applying DNS-over-HTTPS settings, and more.

2.1.1.1.3. Browser Session Protection

- **Lock screen:** Prisma Browser can be configured to lock when left idle, or when launched.
- **Temporary browser session:** A Prisma Browser session can be limited to a maximum preconfigured duration so users will be logged out after a specific time.
- **Flush browser data:** Prisma Browser data can be cleared at a preconfigured period, when left idle, or when launched.
- **Number of concurrent devices:** Prisma Browser can be restricted to a maximum number of concurrent devices.

2.1.1.1.4. Sign-In Browser Policy

- **Device posture assessment:** Prisma Browser assesses the device posture every 90 seconds to ensure the browser is running in a secure environment. If the device posture is noncompliant, access to the browser will be restricted until the device posture is compliant.

2.1.1.2. Web Protection

Built-in security services, browser isolation, and protection from malicious extensions.

2.1.1.2.1. Malware Protection

- **Advanced WildFire®:** Using Palo Alto Networks Advanced WildFire file scanning engine that analyzes 35 million files daily, Prisma Browser prevents malicious file downloads to protect the endpoint and blocks malicious file uploads to enterprise applications to prevent potential lateral movement of threats.
- **Third-party integrations:** Prisma Browser can also integrate with your preferred endpoint platform protection (EPP) or content disarm and reconstruction (CDR) engine of choice.

2.1.1.2.2. Advanced Phishing Protection

- **Advanced URL Filtering:** Using Advanced URL Filtering that analyzes 3.8 billion new URLs daily, Prisma Browser prevents harm from malicious websites based on URL reputation, URL analysis, and web content analysis.
- **Untrusted websites:** Prisma Browser can trigger the opening of high-risk websites in Prisma Access Remote Browser Isolation (RBI [see next section]) or deem the website read-only to reduce the attack surface.
- **Credential hygiene:** Block access to nonenterprise applications from Prisma Browser.

2.1.1.2.3. Remote Browser Isolation and Attack Surface Reduction

- **RBI:** Dynamically trigger RBI for high-risk websites.
- **Attack surface reduction:** Chromium is a common attack surface and serves as a

target for multiple attacks. Prisma Browser can be tuned to reduce the attack surface dramatically by disabling multiple vulnerable browser components: JavaScript JIT, WebRTC, and more than 13 additional components.

- **Memory protection:** Prisma Browser enables vulnerability mitigation engines, including Control Flow Guard, Control-Flow Enforcement Technology, and Arbitrary Code Guard.

2.1.1.2.4. Malicious Extension Protection

- **Extension allowlist/blocklist:** Allow approved extensions and block unapproved extensions.
- **Extension permission control:** Allow extensions that don't request sensitive permissions, like access to redirect traffic through proxies.
- **Extension web manipulation protection:** Prevent extensions from manipulating enterprise website content that can reduce the attack surface.
- **Extension access token protection:** Prevent extensions from accessing cookies and authorization data sent by the browser over web requests.
- **Extension risk scores:** Monitor extensions deployed across the organization, their risk scores, metadata, popularity, and more.

2.1.1.2.5. Safe Search

Prisma Browser allows filtering out inappropriate content from search results across Google, Bing, DuckDuckGo, and YouTube.

2.1.1.2.6. Browser Patching

Prisma Browser keeps track of Chromium security patches regularly with immediate updates. Admin can define the patch management lifecycle, perform a gradual rollout, manage end-of-life cycles, leverage long-term support (LTS) versions, and perform browser version rollbacks.

2.1.1.3. Web Insights

Security insights for analytics and compliance, event investigation and forensics, and threat hunting.

2.1.1.3.1. Audit Trails and User Journey

- **Collect audit trails across any web action:** Web navigation, login successful or fail, file download or upload, clipboard events, print, file open or decrypt, screenshot, typing, DevTools use, extension activities, attack surface reduction, and more.
- **Event enrichment:** Enriched events with event metadata, like URL query parameters, file hash, path, URL source/destination, and more.
- **Anonymize data trails:** Redact user-related identifications to keep users' privacy with no personal data collection.

2.1.1.3.2. Investigation

Prisma Browser enables security teams and incident response personnel to conduct detailed investigations of browser activities with unprecedented clarity and efficiency, providing a complete story of user journeys and incident origins.

2.1.1.3.3. Visual Evidence

- **Screenshot:** Capture the screen of the active tab once the user performs an action.
- **Event recording:** Capture the full recording of user actions in web applications before and after the user action for forensic investigations and compliance.

2.1.1.3.4. Copilot

Allow quick engagements in free-form conversations with a Strata Copilot™ agent to get quick answers on events, users, and devices; also, create visualizations and understand product capabilities.

2.1.1.3.5. Users and Devices

- **Users:** Monitor user actions across the organization and the user device.
- **Devices:** Monitor devices used by Prisma Browser, device metadata, active and past posture status, installed extensions, and more.

2.1.1.3.6. Apps

- **Enterprise app monitoring:** Monitor sanctioned applications as well as their user usage, access, data violations, and file bandwidth size.
- **Uncover shadow IT:** Monitor use of unsanctioned applications and users using them in a violated way.

2.1.1.3.7. Extensions

Uncover extensions used in Prisma Browser, and learn about their installation source, risk score, risk likelihood, download statistics, permissions used, and more.

2.1.2. Last-Mile Data and Identity Controls

An easy-to-use policy engine to define access, data, and identity policies at scale. With only three rule types, customers find it 50% faster to implement and scale across the organization than competitive solutions.

2.1.2.1. Zero Trust Policy Context

Extend zero trust context across all users, devices, networks, locations, and content attributes in all SaaS and web apps.

2.1.2.1.1. User Context

- **User:** Select specific users, local, or SSO.
- **User groups:** Select groups of users, either locally configured or managed by SSO over SCIM integration.
- **Network:** Select devices based on their IP address.
- **Location:** Select the geo-location of the device based on OS device location detection or GeoIP.

2.1.2.1.2. Device Posture Context

- **Device properties:** Set policies for devices based on their type, manufacturer, or model.
- **Device management:** Set policies for devices based on their serial number, installed client certificate, domain-joined Active Directory, or mobile device management (MDM).
- **OS information:** Set policies for devices based on their OS version, screen lock status, OS password policy, file existence, registry keys set, processes running in the background, OS boot mode, system integrity status, or remote session connected.
- **Third-party signals:** Set policies for devices based on their disk encryption status, EPP software status, or CrowdStrike Zero Trust Assessment Score.

- **Browser information:** Set policies for devices based on whether the browser is running with administrative privileges, the browser version, or OS location permission was given to Prisma Browser, to enable more accurate device location policies.
- **Continuous authorization:** Check device posture every 90 seconds.

2.1.2.1.3. App Context

- **URL:** Select specific or broad URL configurations.
- **Application:** Select a predefined or custom application.
- **Category:** Select the category or the assigned risk level associated with the URLs.
- **Account types:** Select the type of account logged in to the website.
- **SaaS tenant:** Select the tenant used in the SaaS app.

2.1.2.1.4. Directional Context

Apply a modern approach for data protection by only enabling file transfers and copy/paste between trusted application groups. For example, define Google Workspace and Salesforce as enterprise apps, and create a rule that all files downloaded from these sites can be uploaded to these sites. Another example is to block file transfers from a business Gmail account to a personal Gmail account.

2.1.2.1.5. Content Context

- Prisma Browser uses Palo Alto Networks Enterprise DLP, with 80% higher data classification with ML-based detection.
- Over 1,000 built-in data classifiers.
- OCR, EDM, and IDM engines.
- Ten predefined regulations and compliance profiles (e.g., HIPAA, PII, GDPR, and PCI).
- Content context can be applied to multiple data protection controls, including files, copy/paste, print, screen capture, typing, and masking.

2.1.2.2. Last-Mile Data Controls

Set last-mile data controls according to the settings outlined in Section 2.1.2 and in your company policy.

2.1.2.2.1. Web Access

Allow or block access to specific websites, applications, or categories.

2.1.2.2.2. Web Login

Allow or block login to specific websites, applications, or categories based on a user's email domain. For example, you could allow a user to log in to Dropbox only with their enterprise login credentials per company policy. If they try to log in using their personal account credentials, Prisma Browser prevents access. You can also block login to unknown and untrusted websites to defend against phishing attacks.

2.1.2.2.3. File Download/Upload

Prisma Browser lets you prevent users from downloading or uploading files, with granularity per file type, file size, file hashes, or based on Microsoft Information Protection (MIP) labels.

2.1.2.2.4. Copy/Paste

Prisma Browser lets you suppress cut, copy, paste, and drag-and-drop functions to prevent data exfiltration between websites or outside the browser.

2.1.2.2.5. Print

Prisma Browser lets you prevent users from printing webpages or files from the browser, or from using specific printers such as home printers.

2.1.2.2.6. Screenshot/Share

Prisma Browser lets you block screen captures, video recording, or screen-sharing of webpages and files.

2.1.2.2.7. Typing

Prisma Browser lets you prevent users from typing sensitive information to unsanctioned applications, like organizational secrets into ChatGPT.

2.1.2.2.8. Masking

Prisma Browser enables you to automatically mask and unmask sensitive text in webpages based on policy.

2.1.2.2.9. Watermarks

Prisma Browser lets you add watermarks to webpages to deter users from sharing screenshots and defend against data theft and copyright infringements. This helps prevent scenarios where users might take pictures of screens and then improperly use or sell the information. You can adjust the watermark's opacity, rotation, density, logo color, other settings, and more.

2.1.2.2.10. Camera/Microphone

Prisma Browser allows you to suppress camera and microphone functions in web applications.

2.1.2.3. Identity Controls

Set identity controls on any access and data browser action.

2.1.2.3.1. Password Manager

Use the Prisma Browser native password manager to secure access to web and SaaS apps with passwords saved securely within the browser.

2.1.2.3.2. Inline MFA

- Require MFA on any action users can perform in the browser, including file download/upload, clipboard, print, etc.
- Use a variety of factors, including pincode and passkeys.

2.1.2.3.3. Inline JIT

- Apply end-user coaching with customized messages on any action users perform in the browser, including web access, login, file download/upload, print, masking, screenshot, and more.
- Apply "proceed anyway with a reason" to require users to justify their need to perform any action they perform in the browser.
- Apply admin approval controls to require users to justify their needs and for an admin to approve any action users perform in the browser—either once or for a limited time.

2.1.2.3.4. Account Protection

- Enforce access with Prisma Browser to non-SSO apps to extend its visibility, identity security, and data controls across unmanaged apps.

2.1.3. User-First Workspace

Make the browser the primary interface for work by safely enabling any work app, keeping users productive and delighted.

2.1.3.1. Enhance User Productivity

Enable users to access any work app in a seamless manner and to use the browser as they're used to.

2.1.3.1.1. Access Web

Built on Chromium, Prisma Browser provides a familiar user experience with no learning curve. Built on Chrome's rendering engine, Prisma Browser guarantees that any website running on Chrome will perform the same way.

2.1.3.1.2. Access Private Apps

Enable users to access private applications published behind Prisma Access or other ZTNA tools directly from the browser, with no additional tools required, with the same audit trails, threat protection, and data security applied.

2.1.3.1.3. Access Remote Protocols

Enable users to connect over SSH, RDP, and VNC protocols directly from the browser. Users and admins benefit from a comprehensive work environment across all work apps, with the same audit trails, threat protection, and data security applied.

2.1.3.1.4. Access Desktop Apps

Enable users to connect to remote desktop apps published over VDI/DaaS environments directly from the browser. Users and admins benefit from a comprehensive work environment across all work apps, with the same audit trails, threat protection, and data security applied.

2.1.3.1.5. Extension Support

Prisma Browser supports all Chrome extensions out of the box.

2.1.3.1.6. Live Session Streaming

Prisma Browser allows users to enable administrators to see a specific tab, the full browser, or the full desktop live—right from Strata Cloud Manager to help troubleshoot issues or monitor their actions in case they access sensitive locations.

2.1.3.1.7. Onboard and Offboard in Minutes, with No Admin Privileges

- **No admin permissions:** A simple installation just like Chrome, with no admin permissions—making it the perfect solution for unmanaged devices.
- **Onboarding wizard:** An intuitive customized wizard introduces users to Prisma Browser and its capabilities.
- **Continue to work where you left off:** Users can easily onboard to Prisma Browser by importing bookmarks, history, saved passwords, cookies, authentication tokens, extensions, tabs, tab groups, and previous settings from any browser.
- **SSO integration:** Leverage an existing identity provider (IdP) or Active Directory Federation Service (ADFS) for login to the browser.
- **Microsoft local domain account integration:** The browser automatically authenticates and logs in by using the user's existing logged-in status from the operating system.
- **Profile sync:** Users can sync data between Prisma Browser instances—either between work/home computers or endpoint/mobile devices.

2.1.3.1.8. Maximum Uptime with No Single Point of Failure

Prisma Browser delivers threat and data protection locally in the browser—no need for rerouting traffic—making it provide the maximum uptime with no single point of failure.

2.1.3.1.9. Offline Support

Prisma Browser maintains operation even without an active internet connection, thus guaranteeing uninterrupted functionality during offline periods.

2.1.3.1.10. Browser Customization

- **Browser settings:** Apply the same browser settings managed in previous browsers, such as incognito, saving passwords or autofill, a homepage button, and pop-ups.
- **Homepage customization:** Set homepage shortcuts to allow easy access to all work apps, customize the background, and publish messages to your users.
- **Branding:** Incorporate your company name, logo, brand colors, and browser icon to make Prisma Browser yours.
- **Extension management:** Remotely install specific extensions across your enterprise.
- **Localization:** Use the browser in your preferred language and choose from over 50 languages.

2.1.3.1.11. Internet Explorer Mode

Allow legacy websites to be open in Internet Explorer mode with no further browsers or plugins.

2.1.3.2. Make Users Choose Prisma Browser

Inspire users to choose Prisma Browser as their default browser.

2.1.3.2.1. Autonomous Digital Experience

Reduces downtime and preempts and resolves application performance issues before the user experiences them to increase productivity and deliver better user experiences.

2.1.3.2.2. Preserve User Privacy

- **No decryption:** Inspecting data in the browser eliminates the need for organizations to decrypt traffic and violate user privacy.
- **Work-related only:** Users can separate personal and business browsing. Enterprise apps are accessible only from Prisma Browser and can be fully monitored, while personal apps are accessible from the personal browser.
- **Web tracking protection:** Apply multiple techniques protecting web tracking to improve user privacy.

2.1.3.2.3. Enterprise Password Manager

Users can leverage an embedded enterprise password manager to save passwords, apply passwords in websites, import from other browsers or other password managers, and generate strong passwords. It can also keep passwords synced across devices where Prisma Browser is installed and unlock passwords using the selected Prisma Browser MFA technique.

2.1.3.2.4. Sidebar

Users can select which apps appear in the sidebar, present or hide it easily, and use apps in the sidebar to quickly go to the active tab, reducing the number of tabs opened.

2.2. Prisma Browser Extension

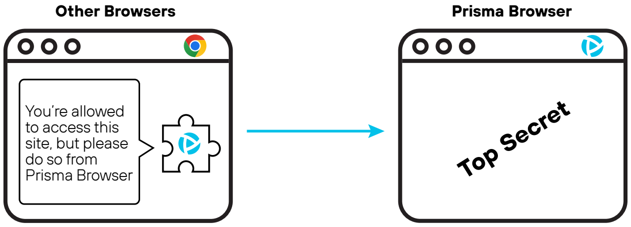
While transitioning to Prisma Browser across the organization, IT and security teams can adopt a hybrid security strategy with Prisma Browser Extension (PBX).

Employees can continue to work with their existing browsers, including Chrome running on Chrome-OS devices, while the admin and security teams can benefit from increased visibility and governance across all browsers used in the organization. PBX monitors browsing activity on consumer browsers, mitigates risks associated with shadow IT, and offers real-time protection against phishing attacks. It provides centralized visibility and control, enabling IT teams to enforce security policies consistently.

While the extension enhances consumer browser security, it wasn't designed as a standalone solution. PBX is a crucial part of the phased rollout of the full Prisma Browser, which should ultimately serve as the foundation of an organization's browser security strategy. The extension enables organizations to gain immediate visibility into browsing activities on all devices, while preparing for a smooth transition to the comprehensive protection the full secure browser offers.

Working together, Prisma Browser and its extension boost the security posture of organizations using consumer browsers, while ensuring comprehensive protection of sensitive data in predefined applications. Users accessing sensitive applications from their consumer browser will be automatically redirected to Prisma Browser. This seamless transition, the Browser Bump, allows organizations to benefit from Prisma Browser's comprehensive security features in their critical applications without disrupting workflows.

For quicker onboarding and insights into previous activity, PBX can be installed in history collection mode, gathering up to 30 days of events, such as web access and file downloads, and displaying this information in the admin console.


Other Browsers
You're allowed to access this site, but please do so from Prisma Browser
Prisma Browser
Top Secret

Prisma Browser Extension Enforcement

1. PBX is installed on consumer browsers.
2. According to policy, and to prevent insecure access from consumer browser, PBX forces the user to use Prisma Browser by bumping the site they're trying to access directly to PB.

Figure 1. PBX seamlessly redirects the web session to Prisma Browser for predefined applications

PBX provides the capabilities that follow.

2.2.1. Secure Environment

PBX enhances the security of consumer browsers.

2.2.1.1. Compromised Endpoint Protection

2.2.1.1.1. Hardens Against Account Takeover Attacks

- **Asset and memory protection:** To protect against infostealers, PBX can add an additional layer of encryption to the cookies on the disk and in the memory.

2.2.1.2. Web Protection

2.2.1.2.1. Advanced Phishing Protection

- **Advanced URL Filtering:** Using Advanced URL Filtering that analyzes 3.8 billion new URLs daily, PBX prevents harm from malicious websites based on URL reputation, URL analysis, and web content analysis.

2.2.1.2.2. Malicious Extension Protection

- **Extension allowlist/blocklist:** Allow only approved extensions and block unapproved extensions.
- **Extension permission control:** Allow only extensions that don't request sensitive permissions, like access to redirect traffic through proxies.
- **Extension risk scores:** Monitor extensions deployed across the organization, their risk scores, metadata, popularity, and more.

2.2.1.2.3. Safe Search

PBX allows users to filter out inappropriate content from search results across Google, Bing, DuckDuckGo, and YouTube.

2.2.1.3. Web Insights

Security insights for analytics and compliance, event investigation and forensics, and threat hunting—over activities in consumer browsers.

2.2.1.3.1. Audit Trails and User Journey

- **Collect audit trails across any web action:** Web navigation, login successful or fail, file download or upload, clipboard events, DevTools use, extension activities, and more.
- **Event enrichment:** Enriched events with event metadata, like file hash, path, and URL source/destination.
- **Anonymize data trails:** Redact user-related identifications to keep users' privacy with no personal data collection.

2.2.1.3.2. Copilot

Enable free-form conversations with the Strata Cloud Manager Copilot agent to get quick answers on events, users, and devices; create visualizations; and understand product capabilities.

2.2.1.3.3. Users and Devices

- **Users:** Monitor user browser actions across consumer browsers across the organization and the user device.
- **Devices:** Monitor devices used by PBX, device metadata, installed extensions, and more. On ChromeOS, also monitor by hostname, serial number, MAC address, and local IP address.

2.2.1.3.4. Apps

- **Enterprise app monitoring:** Monitor sanctioned applications as well as their user usage, access, data violations, and file bandwidth size.
- **Uncover shadow IT:** Monitor the use of unsanctioned applications.

2.2.1.3.5. Extensions

Uncover extensions used in consumer browsers, and learn about their installation source, risk score, risk likelihood, download statistics, permissions used, and more.

2.2.2. Last-Mile Data and Identity Controls

An easy-to-use policy engine to define access, data, and identity policies at scale on consumer browsers.

2.2.2.1. Zero Trust Policy Context

2.2.2.1.1. User Context

- **User:** Select specific users, local, or SSO.
- **User groups:** Select groups of users, either locally configured or managed by SSO over SCIM integration.
- **Network:** Select devices based on their IP address.
- **Location:** Select the geo-location of the device.

2.2.2.1.2. Device Posture Context

- **OS information:** Set policies for devices based on their OS type.
- **Browser information:** Set policies based on the browser type used and their minimum version.
- **Continuous authorization:** Check device posture every 90 seconds.

2.2.2.1.3. App Context

- **URL:** Select specific or broad URL configurations.
- **Application:** Select a predefined or custom application.
- **Category:** Select the category or assigned risk level that's associated with the URLs.

2.2.2.2. Last-Mile Data Controls

Set last-mile data controls according to the settings outlined in Section 2.2.2 and in your company policy.

2.2.2.2.1. Web Access

Allow or block access to specific websites, applications, or categories.

2.2.2.2.2. File Download/Upload

Prevent users from downloading or uploading files, with granularity per file type or file size.

2.2.2.3. Identity Controls

2.2.2.3.1. Inline JIT

- Apply end-user coaching with customized messages on actions users perform in the browser.
- Apply "proceed anyway with a reason" to require users to justify their need to perform the action.
- Apply admin approval controls requiring users to give admins a justification for their action before the activity is approved and enabled—whether once or for a limited time.

2.2.3. User-First Workspace

Make it simple to adopt, and ease the transition to Prisma Browser.

2.2.3.1. Enhanced User Productivity

2.2.3.1.1. Browser Bump

Seamlessly bump predefined critical web applications accessed in the consumer browser to Prisma Browser to gain its full security and productivity features without disrupting workflows.

2.2.3.1.2. Log In to PBX

- **Auto login:** No user action is required to log in. The extension logs in automatically.
- **Force login:** In scenarios where autologin cannot be accomplished, the user can be restricted from using a standard browser until manual login.

2.2.3.1.3. Browser Customization

- **Branding:** Incorporate your company name, logo, and brand colors to make PBX yours.
- **Extension management:** Remotely install specific extensions across your enterprise.

2.3. Prisma Browser Mobile

Prisma Browser creates a secure, nonintrusive workspace on iOS, iPad, and Android devices, enabling employees to work safely without compromising privacy or productivity. Organizations should secure public internet, private apps, and select SaaS apps, as well as enforce device posture checks, leverage Cloud-Delivered Security Services (CDSS) capabilities, and integrate seamlessly with IdPs. This way, they can prevent phishing attempts and protect sensitive data, while empowering a flexible, mobile workforce.

2.3.1. Secure Environment

Advanced security mechanisms are built into the browser to protect against compromised mobile devices and web-based attacks. In addition, Prisma Browser Mobile collects insights to enable threat hunting and forensics.

2.3.1.1. Compromised Endpoint Protection

2.3.1.1.1. Hardens from Tampering

Prisma Browser Mobile protects against tampering by bad actors, insiders, and sophisticated users, with multiple browser hardening integrity checks and certificate pinning.

2.3.1.1.2. Isolates from Untrusted Devices

Prisma Browser Mobile applies a security mechanism to protect against network MitM attacks by trusting specific TLS CAs or preventing users from ignoring SSL errors.

2.3.1.1.3. Browser Session Protection

- **Lock screen:** Prisma Browser Mobile can be configured to lock when left idle or when launched.
- **Flush browser data:** The data for Prisma Browser Mobile can be cleared regularly according to a preconfigured period, when left idle or when launched.

2.3.1.1.4. Sign-In Browser Policy

- **Device posture assessment:** Prisma Browser Mobile assesses the device posture every 90 seconds to ensure the browser is running in a secure environment. If the device posture is noncompliant, access to the browser will be restricted until the device posture is compliant.

2.3.1.2. Web Protection

2.3.1.2.1. Advanced Phishing Protection

Using Advanced URL Filtering that analyzes 3.8 billion new URLs daily, Prisma Browser Mobile prevents harm from malicious websites based on URL reputation, URL analysis, and web content analysis.

2.3.1.2.2. Safe Search

Prisma Browser Mobile allows the filtering out of inappropriate content from search results across Google, Bing, DuckDuckGo, and YouTube.

2.3.1.2.3. Browser Patching

Prisma Browser Mobile keeps track of browser security patches regularly with immediate updates. Admin can require users to upgrade their mobile browser via the App Store or Google Play.

2.3.1.3. Web Insights

2.3.1.3.1. Audit Trails and User Journey

- **Collect audit trails across any web action:** Web navigation, login successful/fail, file download/upload, clipboard events.
- **Event enrichment:** Enriched events with event metadata, like URL source/destination.
- **Anonymize data trails:** Redact user-related identification to keep users' privacy with no personal data collection.

2.3.1.3.2. Copilot

Enable free-form conversations with the Strata Cloud Manager Copilot agent to get quick answers on events, users, and devices; create visualizations, and understand product capabilities.

2.3.1.3.3. Users and Devices

- **Users:** Monitor user actions across the organization and the user device.
- **Devices:** Monitor devices used by Prisma Browser Mobile, device metadata, active and past posture status, and more.

2.3.1.3.4. Apps

- **Enterprise app monitoring:** Monitor sanctioned applications as well as their user access and data violations.
- **Uncover shadow IT:** Monitor use of unsanctioned applications and users using them in a violated way.

2.3.2. Last-Mile Data and Identity Controls

An easy-to-use policy engine to define access, data, and identity policies at scale on mobile.

2.3.2.1. Zero Trust Policy Context

2.3.2.1.1. User Context

- **User:** Select specific users, local, or SSO.
- **User groups:** Select groups of users, either locally configured or managed by SSO over SCIM integration.
- **Network:** Select devices based on their IP address.
- **Location:** Select the geo-location of the device.

2.3.2.1.2. Device Posture Context

- **Device properties:** Set policies for devices based on their type or manufacturer.
- **OS information:** Set policies for devices based on their OS version, screen lock status, root/jailbreak status, or app integrity store verification.
- **Continuous authorization:** Check device posture every 90 seconds.

2.3.2.1.3. App Context

- **URL:** Select specific or broad URL configurations.
- **Application:** Select a predefined or custom application.
- **Category:** Select the category or the assigned risk level associated with the URLs.

2.3.2.2. Last-Mile Data Controls

2.3.2.2.1. Web Access

Allow or block access to specific websites, applications, or categories.

2.3.2.2.2. File Download/Upload

Prisma Browser Mobile lets you prevent users from downloading or uploading files, with granularity per file type or file size.

2.3.2.2.3. Copy/Paste

Prisma Browser Mobile lets you suppress cut, copy, and paste functions to prevent data exfiltration between websites or outside the browser.

2.3.2.2.4. Print

Prisma Browser Mobile lets you prevent users from printing webpages or files from the browser, or from using specific printers such as home printers.

2.3.2.2.5. Watermark

Prisma Browser Mobile lets you add a watermark to webpages to deter users from sharing screenshots, and to defend against data theft and copyright infringements. This helps prevent scenarios where users might take pictures of screens and then improperly use or sell the information.

2.3.2.2.6. Screenshot/Share

Prisma Browser Mobile lets you block screen captures, video recording, or screen-sharing of webpages and files.

2.3.2.3. Identity Controls

2.3.2.3.1. Password Manager

Use Prisma Browser Mobile’s native password manager to secure access to web and SaaS apps with passwords saved securely within the browser.

2.3.2.3.2. Inline JIT

- Apply end-user coaching with customized messages on any action users perform in the browser.
- Apply “proceed anyway with a reason” to require users to justify their need to perform the action.

2.3.3. User-First Workspace

Make the mobile browser the primary, secure interface for work.

2.3.3.1. Enhanced User Productivity

2.3.3.1.1. Access Web

Users enjoy a familiar browsing experience with no learning curve.

2.3.3.1.2. Access Private Apps

Enable users to access private applications published behind Prisma Access directly from the browser, with no additional tools required, using the same audit trails, threat protection, and data security applied.

2.3.3.1.3. Onboard and Offboard in Minutes, with No Admin Privileges

- **No admin permissions or device profile:** Simple installation, with no admin permissions or device profiles—making it the perfect solution for unmanaged devices.
- **SSO integration:** Leverage existing IdP for log in to the browser.
- **Profile sync:** Users can sync data between Prisma Browser instances—either between work/home computers or endpoint/mobile devices.

2.3.3.1.4. Browser Customization

- **Browser settings:** Apply browser settings, including incognito, saving passwords, homepage button, and pop-ups.
- **Launch app control:** Set specific SaaS apps to be launched in the native mobile app.
- **Desktop mode:** Set specific websites or applications to be rendered in desktop mode instead of mobile mode.
- **Homepage customization:** Set homepage shortcuts to allow easy access to all work apps, and customize the background.
- **Branding:** Incorporate your company name, logo, brand colors, and browser icon to make Prisma Browser Mobile yours.
- **Custom notice:** Set a notice that's presented to users when launching Prisma Browser Mobile.

2.3.3.1.5. Default Browser for Microsoft Intune Managed Apps

Prisma Browser Mobile can be designated as the default for Microsoft Intune managed apps, securely opening links and protecting users from malicious websites.

3. Deployment Alternatives

A core value of Prisma Browser is its simple deployment, which can be achieved in any of the following ways:

- **Distribution tools**: Remotely and automatically deploy Prisma Browser on managed devices using third-party software distribution tools such as Microsoft Configuration Manager (ConfigMgr), Microsoft Group Policy Object (GPO), unified endpoint management (UEM), and MDM tools.
- **SSO integration**: Add a link to download Prisma Browser from the SSO login page. Users can install it in self-service mode, with no admin privileges required.
- **Deployment emails**: Send invitation emails to users of your choice. They can start using Prisma Browser right after a simple, standard installation, with no admin permissions required.
- **Hybrid transition with PBX**: While transitioning to Prisma Browser across the organization, IT and security teams can adopt a hybrid security strategy with PBX. The extension enables organizations to gain immediate visibility into browsing activities on all devices while preparing for a smooth transition to the comprehensive protection the full secure browser offers.

We deliver all Prisma Browser features with no latency and zero infrastructure changes. There's no need to redirect traffic or deal with complex SSL stripping operations.

4. Enforcement Alternatives

You can enforce Prisma Browser in multiple ways over your enterprise as the single access method or the main browser.

4.1. IdP Authorization (Conditional Access) Enforcement

This method of enforcement is the most common form of enforcement among Prisma Browser customers.

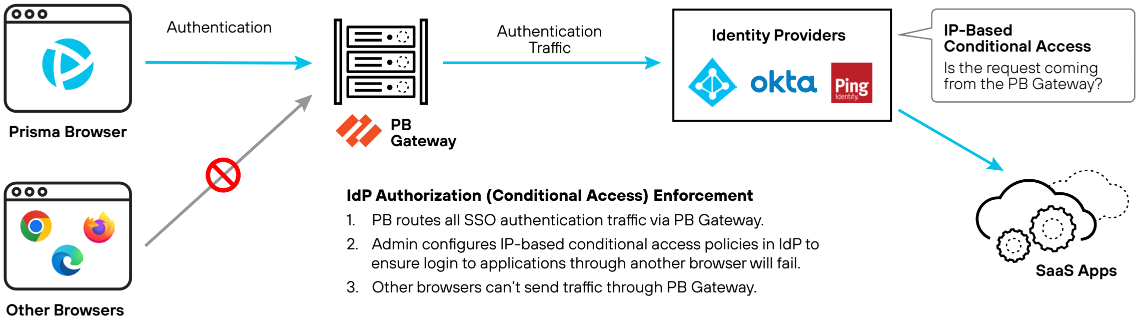
You can enforce Prisma Browser with IP-based conditional access policies according to the IdP. With this method, specific users (or all users) can be required to use Prisma Browser to access specific SSO applications (or all SSO applications).

To enable IP-based enforcement, Prisma Browser routes all SSO authentication traffic through the Prisma Browser Gateway (PB Gateway). Other browsers and users will be blocked from sending traffic through the PB Gateway and therefore also blocked from accessing the SSO applications.

Your organization is provided with unique, dedicated IP addresses.

Supported IdPs include:

- Microsoft Entra ID
- Okta
- PingID
- OneLogin
- VMware Workspace ONE Access
- Google Workspace
- Additional IdPs can be supported upon demand



IdP Authorization (Conditional Access) Enforcement

1. PB routes all SSO authentication traffic via PB Gateway.
2. Admin configures IP-based conditional access policies in IdP to ensure login to applications through another browser will fail.
3. Other browsers can't send traffic through PB Gateway.

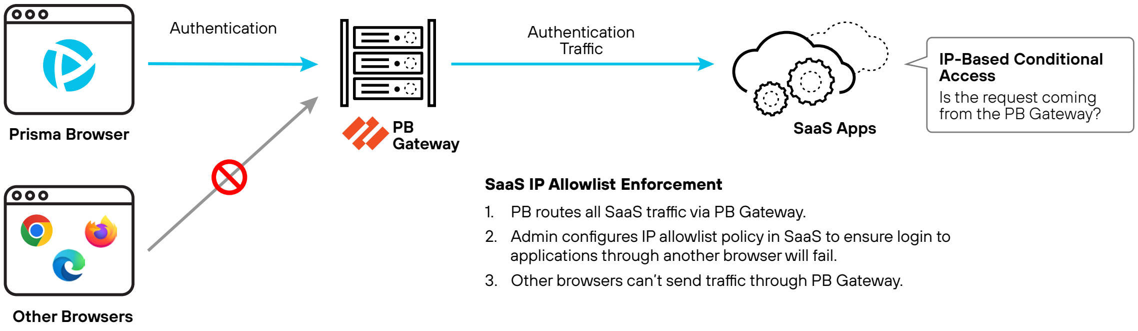
Figure 2. Enforcing IP-based IdP conditional access to business applications via PB Gateway

4.2. SaaS IP Allowlist Enforcement

You can enforce Prisma Browser by using IP-based IP allowlist policies.

To enable IP-based enforcement, Prisma Browser routes all SaaS traffic through the PB Gateway. Other browsers and users will be blocked from sending traffic through the PB Gateway and therefore also blocked from accessing the SaaS applications.

Customers are provided with unique, dedicated IP addresses.



SaaS IP Allowlist Enforcement

1. PB routes all SaaS traffic via PB Gateway.
2. Admin configures IP allowlist policy in SaaS to ensure login to applications through another browser will fail.
3. Other browsers can't send traffic through PB Gateway.

Figure 3. Enforcing IP-based IdP conditional access to business applications via PB Gateway

4.3. Client Certificate Enforcement

Each Prisma Browser cloud tenant has a unique preconfigured certificate authority that can generate client certificates. A unique client certificate is generated for each Prisma Browser session and is saved in the TPM/KeyChain so other browsers can't access it.

This client certificate, accessible only by Prisma Browser, can be used for enforcement.

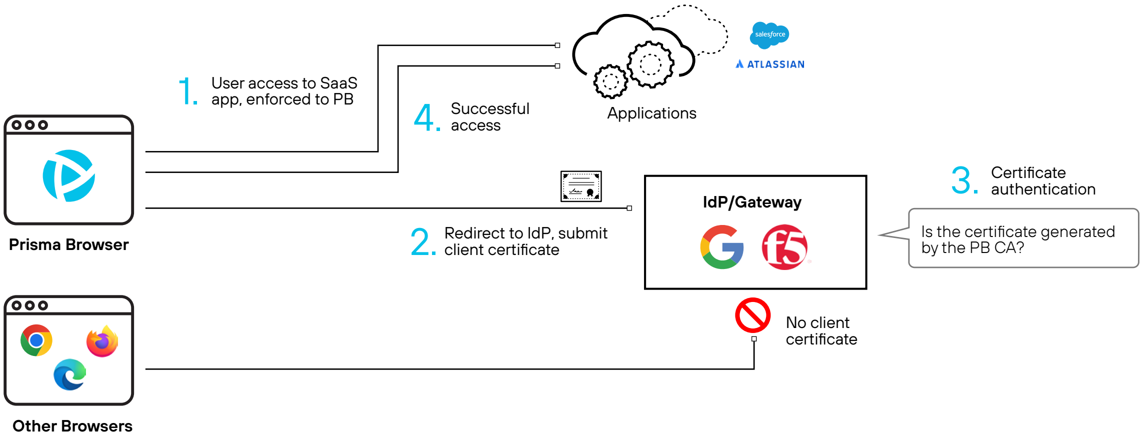

1. User access to SaaS app, enforced to PB
4. Successful access
Applications
salesforce
ATLASSIAN
Prisma Browser
2. Redirect to IdP, submit client certificate
IdP/Gateway
3. Certificate authentication
Is the certificate generated by the PB CA?
No client certificate
Other Browsers

Figure 4. Enforcing certificate-based access to business applications

4.4. Network Gateway Enforcement

The existing enterprise firewall or network gateway can be used to inspect and block traffic from browsers other than Prisma Browser. The network gateway can differentiate between Prisma Browser and Prisma Browser Mobile and other browsers in multiple ways, such as a unique User-Agent, HTTP header, or the destination IP by routing all traffic via explicit proxy.

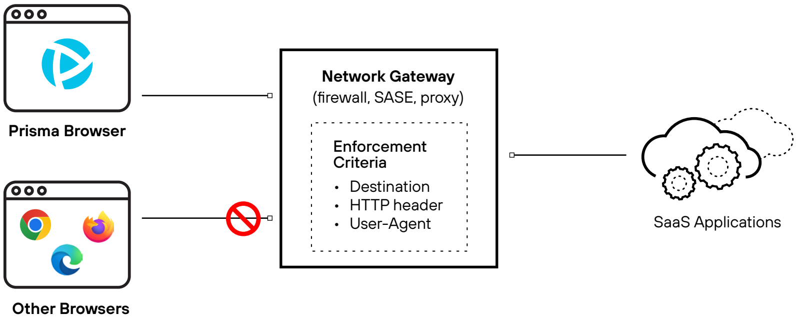
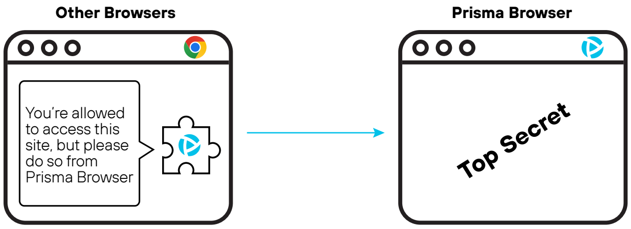


Figure 5. Network gateway or enterprise firewall only allows traffic from Prisma Browser to access the network

4.5. Prisma Browser Extension Enforcement

As organizations slowly roll out Prisma Browser in a staged approach across the organization, the PBX can serve as an ideal temporary enforcement solution. Organizations rely on PBX to enforce a web session redirect to Prisma Browser for predefined sites according to policy.

PBX can be installed on any Chromium browser to enhance the security and visibility of user actions in other browsers, while seamlessly redirecting user sessions to Prisma Browser for predefined critical applications. The transition is virtually transparent to the user.


Other Browsers
Prisma Browser
You're allowed to access this site, but please do so from Prisma Browser
Top Secret

Prisma Browser Extension Enforcement

1. PBX is installed on consumer browsers.
2. According to policy, and to prevent insecure access from consumer browser, PBX forces the user to use Prisma Browser by bumping the site they're trying to access directly to PB.

Figure 6. PBX automatically redirects web sessions to Prisma Browser

4.6. Single Browser Enforcement

Enforcing Prisma Browser as the sole browser in the organization and blocking other consumer browsers from managed devices can be implemented in a variety of ways:

- Block common browser executables from opening based on process name or certificate signature, using MDM or EPP/EDR tools.
- Block traffic from browser executables, using EPP/host firewall.
- Schedule a script that uninstalls other browsers and prevents reinstallation, using MDM/GPO.
- Apply URL blocklist on other browser policy to block all or some sites, using MDM/GPO.

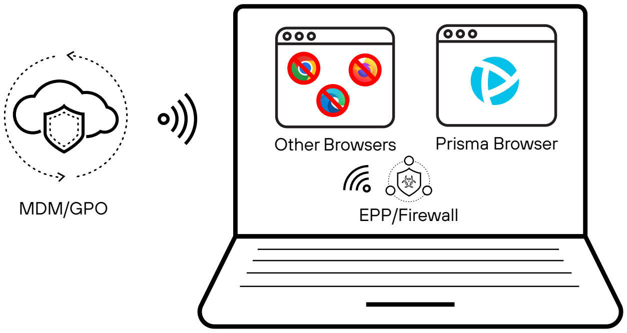


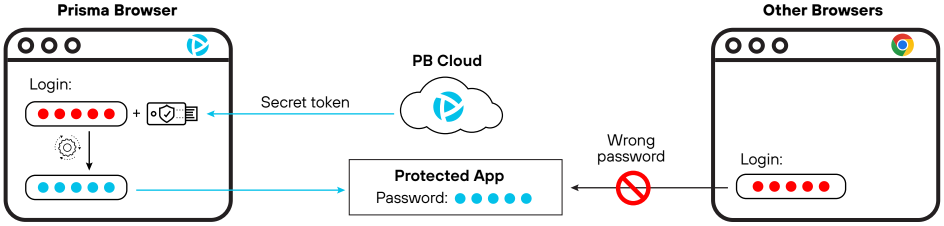
Figure 7. Endpoint tools block other consumer browsers to allow only Prisma Browser

4.7. Unknown Password Enforcement

Almost all organizations have critical data stored in accounts that are neither managed by their IT teams or integrated with IdPs using SSO. For example, bank accounts, insurance or financial services, virtual deal rooms, and more. These accounts present a major risk to the organization as IT and security teams have no control over their security.

Prisma Browser brings robust last-mile controls to these unmanaged applications by ensuring access is only enabled through the browser. Enforcement of these applications is performed via a patent-pending Account Protection feature. The feature adds a secret element to every user password stored in Prisma Browser. This prohibits access to the account from any other browser and by any other user.

Users can only log into the application in Prisma Browser using their original password. Note that the original password is not stored in Prisma Browser so without the original password, access to the application isn't possible.



Account Protection Ensuring Access to Non-SSO Applications Is Only Possible from Prisma Browser

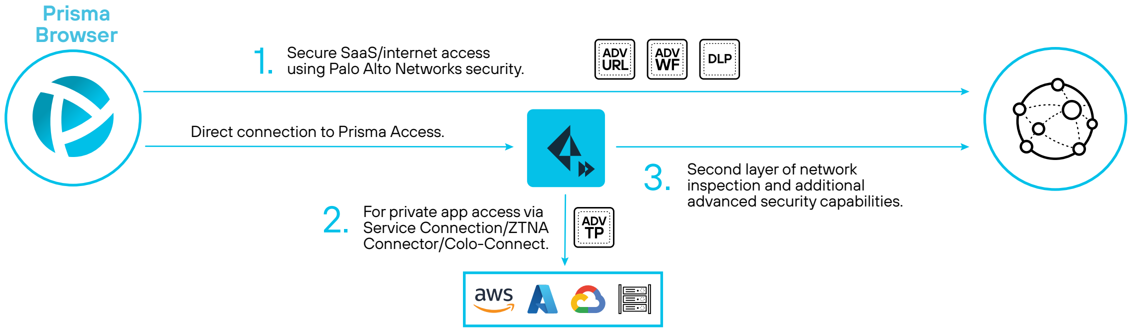
1. Users are required to set/reset their password through the secure browser once.
2. The secure browser uses a unique token to create a new password using a proprietary algorithm.
3. Resultant password is used as the actual user password in the application.
4. The user can only log in to the application from the secure browser.

NOTE: We don't store the user's actual password to the application.

Figure 8. Protecting company data in non-SSO applications with Account Protection

5. Private App Access with Prisma Access

Prisma Browser offers secure direct access to web and SaaS apps—with Palo Alto Networks CDSS, delivered directly from the browser. To access private apps, Prisma Browser integrates with Prisma Access, which provides access and robust security for internal applications.



Prisma Browser
1. Secure SaaS/internet access using Palo Alto Networks security.
ADV URL
ADV WF
DLP
Direct connection to Prisma Access.
3. Second layer of network inspection and additional advanced security capabilities.
2. For private app access via Service Connection/ZTNA Connector/Colo-Connect.
ADV TP
aws

Figure 9. Prisma Browser connectivity methods to web, SaaS, and private apps

5.1. Accessing Prisma Access from a Remote Location

To enforce access to private apps via Prisma Browser, the browser connects to Prisma Access through an explicit proxy via a dedicated port (443) to an HTTPS proxy. Mutual authentication is established via a JWT token and is only minted for Prisma Browser. As shown in figure 7, access from alternative browsers is blocked. This proxy encrypts the CONNECT phase (unlike a normal proxy that performs CONNECT in an unencrypted way).

Alternative browsers can access the explicit proxy via port 8080 without strict authorization. This port doesn't enable access to private apps.

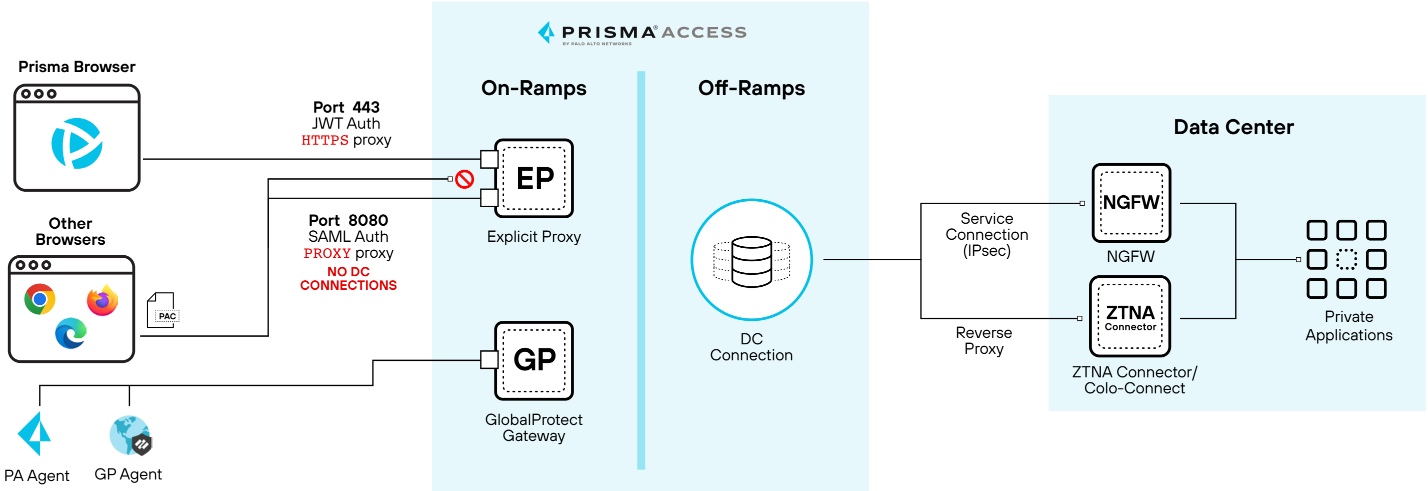


Figure 10. Prisma Browser connects to Prisma Access through an explicit proxy

5.2. Accessing Prisma Access from the Office or with GlobalProtect or Prisma Access Agent

When a user is located in the office behind a remote network (RN), or is connected to GlobalProtect® or Prisma Access Agent, Prisma Browser automatically detects the branch network or the agent tunnel. It then routes traffic via the existing routing instead of the explicit proxy.

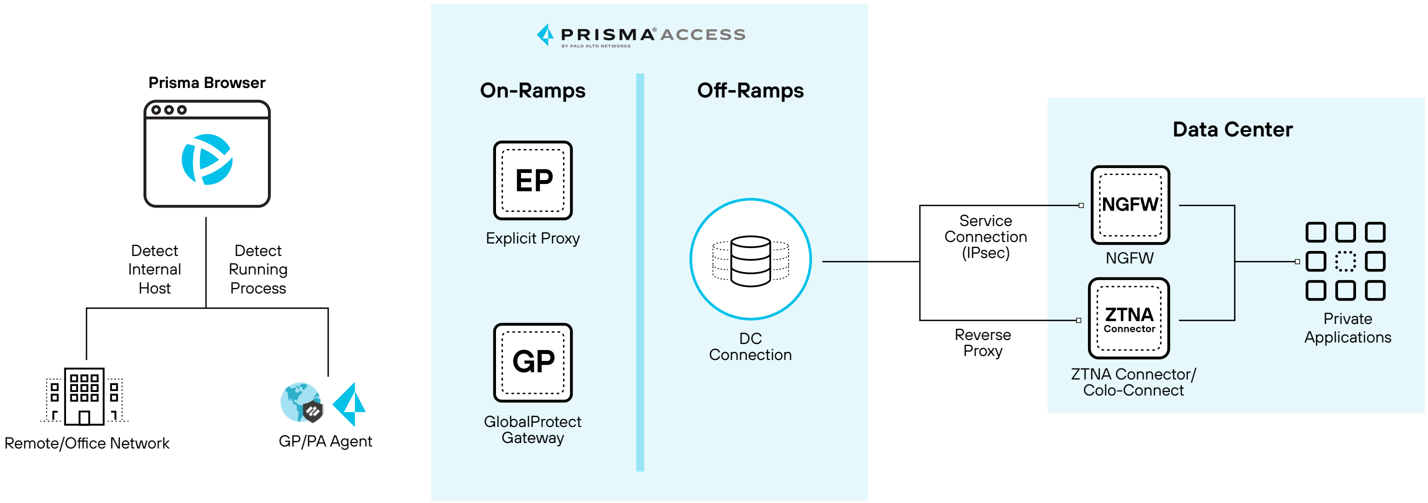


Figure 11. Optimized network routing

6. System Requirements

Windows	
Operating System	Windows 10 64-bit Windows 11 64-bit
CPU	64-bit
No admin permissions required.	
macOS	
Operating System	macOS 11 Big Sur macOS 12 Monterey macOS 13 Ventura macOS 14 Sonoma
CPU	Intel x86 Apple M1 and above
No admin permissions required.	
Linux	
Operating System	Ubuntu 24.04.2 LTS and above Fedora 41 and above IGEL OS 12 and above
CPU	64-bit
No admin permissions required.	
Android	
Operating System	Android 11 and above
iOS	
Operating System	iOS 17 and above
Prisma Browser Extension	
Web Browsers	Chrome version 127 and above Edge version 127 and above Brave version 1.71.114 and above Arc version 1.63.0 and above

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

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