Prisma Access Browser: An Integral Part of SASE

More Work in the Browser Means More Risk for Organizations

The way we work has changed. The way we access corporate resources in the cloud via a rising number of SaaS and web applications, chat with coworkers via instant messaging, and use AI to write emails has become reality in this new work paradigm. The devices we depend on to get work done have expanded from laptops in the office to smartphones on the go.

The modern workforce has changed. With staff augmentation, third-party business partners, consultants, and outsourcing, the word "colleague" has taken on a whole new meaning in the modern workforce. The boundaries of the modern workspace are infinite.

With all this change, security needs to change—it has to. Policies and controls that were once simple to implement and enforce in a centralized office environment have now expanded to the farthest reaches of the globe. New workers across different locations, with any number of devices, require the same level of protection and attention as their colleagues in the central office, with standardized, easy-to-configure security that doesn't get in their way. Otherwise, workers—remote or not—will bypass these security controls to keep productive.

In this environment, extended hybrid work models and AI assistance are now crucial to productivity in the workplace. The modern workforce relies on an array of SaaS apps and devices to maintain its business cadence. And the place this work is getting done? That's changed, too. Now, work happens in the browser—almost exclusively.

Palo Alto Networks recent research reveals that employees spend over 85% of their workday in web browsers.[1] The browser has a central role in everyone's day to day. However, this also makes the browser a prime target for cyberattacks, with nearly 95% of surveyed organizations reporting browser-based threats across all devices.[2] Why so high? Because traditionally, the web browser has been a blind spot for security solutions and the teams that use them.

It's been difficult to keep up, to say the least.

Figure 1: Workers spend the vast majority of their time in a web browser, which is risky

To combat this growing vulnerability, Palo Alto Networks introduced Prisma® Access Browser as a core element of SASE. This secure browser unlocks the full potential of SASE, providing comprehensive security to any device within minutes. The first and only secure browser natively integrated into the SASE framework, it empowers organizations to safeguard their workforce against threats while ensuring secure access to essential web applications and compliance with multiple privacy and data regulations, all with minimal user friction.

1. *Optimizing Security for Modern Workforces*, Palo Alto Networks and Omdia, January 2025.
2. Ibid.

The Evolution of Secure Access

Legacy security solutions worked for the era from which they came, but they can no longer deliver the protection needed for today's workforce. Increasing reliance on unmanaged devices, cloud-based infrastructures, and new network protocols stretch these old-school solutions thin. As a result, gaps in security and poor user experiences persist, leaving organizations vulnerable and less productive.

Traditional security implementations fell short in providing comprehensive coverage against browser-based threats, leaving organizations exposed to attacks from cloud-native applications and extensions. As the browser becomes the primary workspace, it has also become a lucrative target for adversaries aiming to breach sensitive corporate networks. This shift necessitates a new approach that integrates SASE principles directly into the browsing environment.

As more work is conducted within web browsers and reliance on SaaS applications increases, it's crucial to close the gaps in outdated SASE approaches. Complete SASE solutions must extend to the browser to ensure secure, policy-enforced access, and last-mile data controls for modern workforces using SaaS and unmanaged devices. Without full visibility and control over user interactions within web and cloud applications, organizations face increased risks of data exposure and compliance issues. As businesses shift to cloud environments and hybrid work, extending SASE to cover all browser-based activities is essential for comprehensive security and reducing vulnerabilities across user actions. Extending SASE to the browser adds an additional layer in a multilayered, multidimensional security strategy—network, endpoint, and browser—ensuring powerful protection.

Enabling the Modern Workforce with a New SASE

The need for a complete SASE solution has never been more apparent: one that's built with the current work environment top of mind; a global, flexible, and dispersed solution tailored to the needs of the workers of today, not yesterday; and, most importantly, a solution that provides visibility, security, and control where work is done—in the 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, ongoing, frictionless Zero Trust access to SaaS and private applications on any device, and admins can have control where the users and data meet. Now, the same security policies and experience can extend to any worker, anywhere.

Central to the solution's design is the browser's ability to deploy granular security policies tailored to specific job functions. Workers receive access only to the data and applications necessary for their roles, with sensitive information masked and nonessential apps and websites blocked. This least-privileged access policy helps ensure robust security without impacting job performance for any worker.

Key Features of Prisma Access Browser

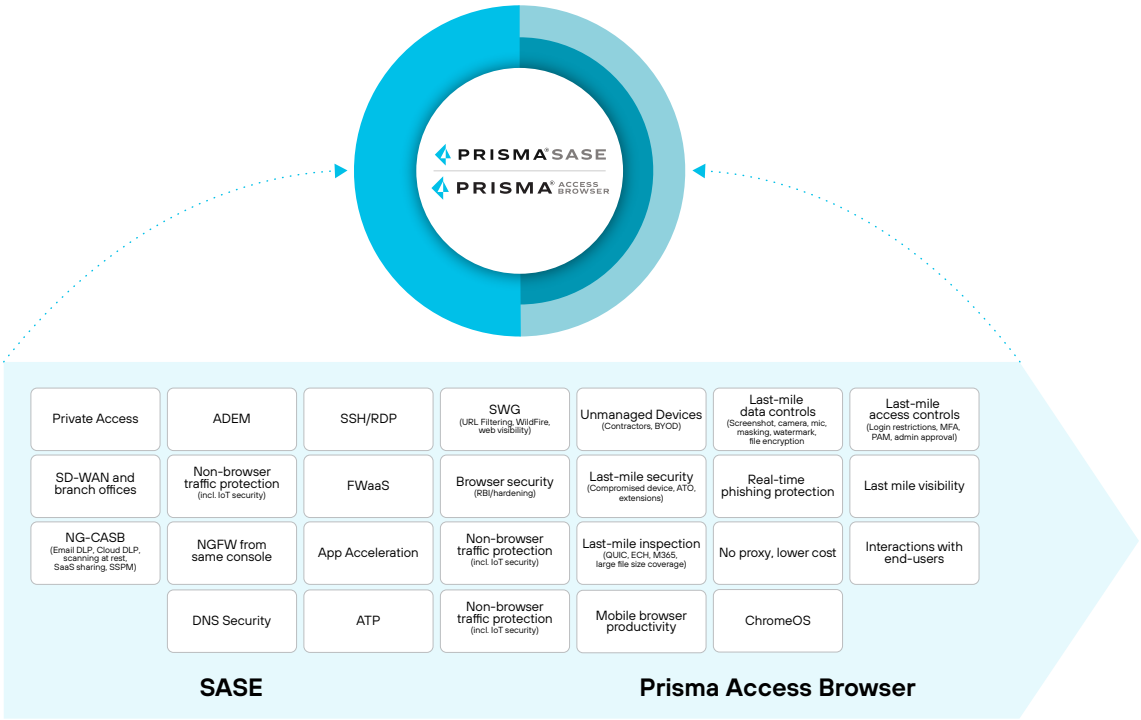

Figure 2: Prisma Access Browser extends SASE and expands security through the browser to provide unparalleled protection

Multidirectional Security on Any Device

Protect Against Compromised Endpoints

Prisma® Access Browser provides enhanced security for both managed and unmanaged devices, creating a secure workspace on any device, whether it's a company device or a personal smartphone, tablet, or laptop. This allows users to work securely from any location, without compromising the integrity of the corporate network. The browser isolates enterprise applications from potential threats posed by untrusted endpoints, reducing the risk of data breaches and malware infiltration.

On managed devices, vulnerabilities can still arise from outdated software, user error, or sophisticated phishing attacks. Phishing remains one of the most significant threats, as attackers craft convincing emails and websites to deceive employees into revealing sensitive information or installing malware. With phishing techniques becoming increasingly sophisticated, it's crucial to have comprehensive protection. Prisma Access Browser combats these threats by embedding advanced security features directly into the browser. It provides automated web monitoring and threat detection, ensuring prompt identification and blocking of phishing attempts and other threats.

Protect Against Threats

Prisma Access Browser adds an additional layer of encryption at the browser layer, protecting against keyloggers, screen scrapers, untrusted certificates, and threats from public networks. By reducing the attack surface through the disabling of sensitive browser components and defending against malicious extensions, the browser ensures that work remains protected at all times. Prisma Access Browser's proactive security measures, such as checking device posture every 90 seconds and collecting web insights for threat-hunting and forensics, further enhance security.

Integration with the entire SASE suite amplifies the security capabilities of Prisma Access Browser. Powered by Palo Alto Networks Precision AI™, Advanced WildFire®—the industry's largest cloud-based malware prevention engine—analyzes over 77 million new files and prevents up to 450,000 new and unique malicious files every day. AI-powered URL Filtering leverages the industry's largest pure-play AI-powered threat intelligence database to block 151 million malicious URLs every day. Advanced Threat Prevention offers real-time defense against sophisticated threats, with deep learning models preventing 90% of injection attacks.

For organizations, enabling secure work on any device is crucial in today's work environment. This flexibility boosts worker productivity and satisfaction by allowing them to use their preferred devices while mitigating security risks associated with unmanaged endpoints. By providing comprehensive protection across all devices, organizations can maintain a strong security posture, reduce the risk of data loss, and ensure compliance with regulatory requirements.

Boost Visibility and Control Across SaaS and Web Apps

Prisma Access Browser enhances visibility and control over all user activities within SaaS and web applications, extending context-based Zero Trust policies to every action performed in every app. This ensures consistent application and enforcement of data, identity, and privileged access controls across the board. By broadening Zero Trust to cover all user and device attributes, all web applications, and all actions and last-mile controls, organizations can maintain comprehensive oversight and protect against accidental and intentional data leakage.

With leading data classification engines, multifactor authentication (MFA), and just-in-time (JIT) permissions on all controls, it provides unparalleled security coverage. Whether accidental or intentional, data leakage can lead to far-reaching consequences. In fact, 55% of organizations say that they've experienced accidental data leakage in the last 12 months.[3]

Prisma Access Browser mitigates data loss with a robust feature set. Security teams gain granular insights into user interactions with corporate resources, allowing for real-time monitoring and response to potential threats. They can see all user and device attributes, including user/group, device posture, network, and location. This visibility enables organizations to implement stringent data protection measures and control access to sensitive information based on user roles, contexts, and behaviors. It helps prevent unauthorized data access and exfiltration, ensuring that only authorized personnel can perform high-risk actions.

Enhanced visibility and control are essential for maintaining a secure and compliant environment, particularly when dealing with sensitive data and critical applications. Prisma Access Browser allows organizations to log, monitor, and control all web and SaaS traffic without the need for decryption. Prisma Access Browser also enables organizations to set controls for file upload/download, copy/paste, text typing, text masking, printing, screenshotting/sharing, and camera/microphone use. By integrating with Palo Alto Networks DLP, which includes over 1,000 built-in data classifiers and advanced ML/NLP as well as OCR, EDM, and IDM capabilities, the browser ensures strong content-based protection. Additionally, it supports 22 predefined regulations and compliance profiles, including as HIPAA, PII, GDPR, and PCI.

3. *The State of Workforce Security: Key Insights for IT and Security Leaders,* Palo Alto Networks and Omdia, February 2025.

By applying last-mile data, identity, and access controls across all applications, organizations can ensure consistent enforcement of their security policies, regardless of the user's location or device. Step-up MFA and JIT permissions, including passkeys and admin approval processes, add extra layers of security, particularly for securing privileged users.

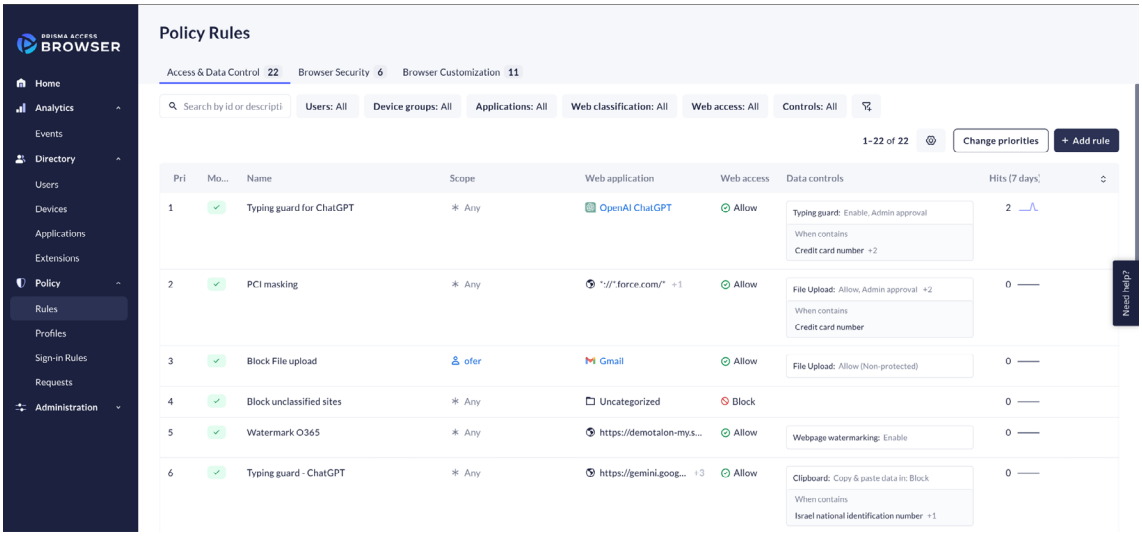

Figure 3: Ultraconfigurable rules cover all user and device attributes across all apps

Provide a Delightful User Experience

Prisma Access Browser is designed to deliver an exceptional user experience, characterized by maximum uptime and significantly improved performance. Its fully distributed infrastructure ensures reliability and speed, providing users with a seamless and productive browsing experience. Access to all work applications—from public and SaaS apps to private and SSH/RDP applications—is available directly from the browser. By minimizing security measures that typically hinder productivity, Prisma Access Browser helps ensure users maintain compliance without the need to bypass protocols. Furthermore, with the increasing demand for GenAI applications, the browser supports secure and efficient access to these advanced tools, enabling enhanced productivity without compromising security.

Users benefit from faster access to applications, with performance improvements up to five times greater than traditional solutions. This enhanced performance translates to increased productivity, as employees can accomplish tasks more quickly and efficiently. The browser proactively prefetches the most relevant content, ensuring fast and smooth interactions. Additionally, the streamlined onboarding and offboarding process, which can be completed in minutes without requiring any infrastructure changes, reduces the total cost of ownership by approximately 80% compared to shipping laptops, further simplifying IT operations.

Providing a delightful user experience is critical for user adoption and satisfaction. When employees have a fast and reliable browsing experience, they're more likely to embrace the security measures in place rather than seek workarounds. This not only enhances overall productivity but also ensures adherence to security policies. Prisma Access Browser's ability to maintain maximum uptime with no single point of failure further enhances user confidence and satisfaction.

Reduced IT costs and simplified device management mean the organization can allocate more resources to other strategic initiatives, driving overall business growth and efficiency. The browser allows for easy policy definition and scaling across the organization. Autonomous Digital Experience Management (ADEM) preempts and resolves application performance issues, showing device performance, network performance, Wi-Fi issues, and more.

As part of ADEM, Real User Monitoring (RUM) helps to ensure uninterrupted productivity on the browser with additional performance insights like page-load and rendering times. Integration with AI Access Security™ enables safe AI adoption for employees, providing full real-time visibility of AI usage, through viewing which AI apps are used and by whom, and comprehensive data protection by scanning shared data, secrets, and IP. Access control at the fingertips allows blocking of unsanctioned apps, application of InfoSec policies, and protection of data, ensuring a secure and delightful user experience.

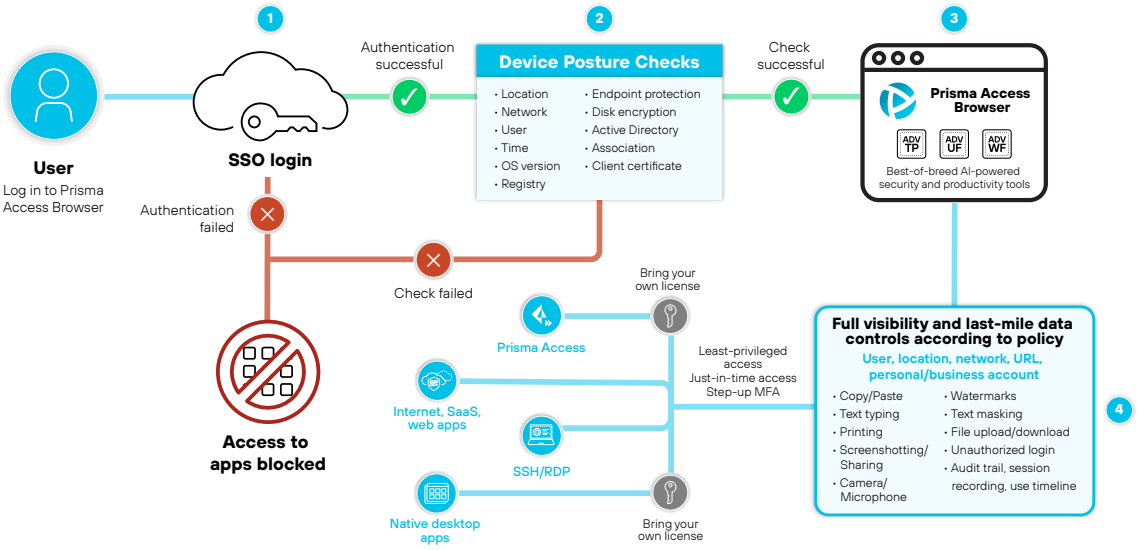

Figure 4: Example of how a user accesses their work with Prisma Access Browser

Prisma Access Browser Real-World Use Cases

Independent Workers

Prisma Access Browser is designed to provide secure, efficient access for third parties and contractors, enabling them to connect to SaaS and private applications from any device within minutes. This capability is crucial for various scenarios, including mergers and acquisitions, call centers, and frontline and field workers. Unlike traditional solutions that require administrative privileges, Prisma Access Browser offers seamless access and security without the need for user intervention.

Mergers and Acquisitions

During mergers and acquisitions, it's vital to quickly and securely integrate disparate IT systems and resources. It's also crucial to keep employees productive during the transition to lower time-to-value, a key metric for M&A success. Prisma Access Browser facilitates these by allowing newly acquired teams to access critical applications on any device, managed or unmanaged, in minutes without compromising security. Quick secure access to corporate, SaaS, and GenAI apps through Prisma Access Browser ensures employees stay productive through the M&A process, with lower costs compared to shipping laptops and VDI. By enforcing granular security policies and leveraging advanced threat prevention, organizations can ensure that sensitive data remains protected throughout the integration.

Call Centers

Call centers often employ a mix of full-time employees, contractors, and third-party vendors who need quick and secure access to customer data and corporate applications. Prisma Access Browser provides the solution by enabling secure, context-based access from any device. This ensures that call center agents can efficiently perform their duties while maintaining compliance with data protection regulations.

Frontline and Field Workers

Frontline and field workers frequently operate in environments where traditional security measures are impractical. With Prisma Access Browser, these workers can securely access corporate applications and data from their mobile devices, ensuring they have the tools they need to perform their tasks effectively.

By offering secure access to SaaS and private applications for third parties and contractors, Prisma Access Browser helps organizations extend their security perimeter beyond traditional boundaries. This capability not only supports operational agility and flexibility but also ensures that all users, regardless of their location or device, can work securely and efficiently.

Bring Your Own Device

Prisma Access Browser empowers employees with the flexibility to use their own devices for work, providing secure access to business applications anytime, anywhere. This BYOD capability brings several key benefits, including enhanced workforce agility, device freedom, mobile enablement, lower costs, and reduced reliance on VDI.

Workforce Agility

In today's fast-paced business environment, employees need the ability to access corporate resources on the go. Prisma Access Browser enables this agility by allowing employees to securely connect to SaaS and private applications from their personal devices. Whether working from home, traveling, or in the office, employees can maintain productivity and continuity without being tethered to a specific device or location.

Device Freedom

With Prisma Access Browser, employees are no longer restricted to using company-issued devices. They can access business applications from their preferred smartphones, tablets, or laptops, providing a more personalized and convenient work experience.

Enable Mobile Devices

Mobile device enablement is critical for employees who need to access business applications outside traditional office settings. Prisma Access Browser ensures the secure integration of mobile devices into the corporate network, providing seamless access to essential tools and information. This capability is particularly valuable for field workers, sales teams, and remote employees who rely on their mobile devices to stay connected and productive.

Lower Cost of Shipping Laptops

Shipping corporate laptops to remote employees can be costly and logistically challenging. Prisma Access Browser eliminates this need by enabling secure access from any personal device a new worker may already have. This significantly reduces the costs associated with provisioning and shipping hardware, especially for larger IT integrations or temporary workers.

Prisma Access Browser's BYOD capabilities empower employees with the freedom to use their own devices, enhancing workforce agility and productivity. By providing secure, flexible access to business applications, organizations can reduce costs, streamline IT operations, and support a modern, mobile-enabled workforce.

Secure GenAI

Generative AI tools are transforming business operations, but they also introduce potential security risks. Prisma Access Browser reduces risk by providing a secure environment for using web-based GenAI tools. With the browser's last-mile DLP controls, data interactions with AI platforms within the browser are protected.

Secure Data Interactions

Workers can unintentionally upload sensitive corporate data to GenAI apps, making data protection critical. Prisma Access Browser applies last-mile data protections to block copy-paste, disable file uploads, and prevent typing sensitive information into the app. Protection of data in-use is vital when safeguarding against data leakage, which can occur if users inadvertently share sensitive information with AI systems.

Visibility and Access Control

One of the biggest challenges with using GenAI tools is gaining visibility into shadow AI and maintaining user access controls. Prisma Access Browser offers visibility into AI adoption and use, allowing IT security teams to monitor and manage interactions with platforms like ChatGPT. This visibility is crucial for safeguarding sensitive information and ensuring that workers comply with acceptable use policies. This is particularly useful when an organization allows the use of unmanaged devices.

Prisma Access Browser with AI Access Security

When Prisma Access Browser is paired with AI Access Security, a purpose-built solution for GenAI, organizations can enable safe AI adoption and use for both managed and unmanaged devices, and protect sensitive data from the client side and the network. AI Access Security enables control of sanctioned GenAI apps and provides additional protections around GenAI posture management, AI marketplaces, plugins, and more. The combined offering, as part of a comprehensive SASE solution, enables browser and device freedom while providing robust security and control.

Prisma Access Browser, as part of a holistic SASE solution, helps organizations to innovate and boost productivity while maintaining robust security controls. This balance between security and innovation is crucial as AI continues to play a larger role in business operations.

Reduce VDI

VDI solutions can be complex and expensive to maintain. By offering a browser-based solution, Prisma Access Browser reduces the reliance on VDI infrastructure while still providing a secure and controlled environment for accessing business applications. Reducing VDI deployments not only lowers operational costs but also enhances the user experience by delivering faster and more reliable access to applications.

Resource Optimization

Traditional VDI environments require significant resources to manage and operate, often resulting in high costs and complex infrastructure. Prisma Access Browser alleviates these demands by shifting routine browsing activities to the secure browser. This approach reduces the load on VDI systems, allowing for more efficient resource allocation and reduced overall infrastructure costs.

Segmented User Groups

Not all employees require full VDI access; many only need secure browsing capabilities. Prisma Access Browser allows organizations to segment their user base into browser-only and full-desktop groups, optimizing VDI deployments by providing the appropriate level of access based on user needs. This segmentation leads to cost savings and improved performance for users who don't require full desktop environments.

Cost Savings

Maintaining VDI infrastructure can be expensive, both in terms of hardware and ongoing operational costs. Prisma Access Browser offers a cost-effective alternative by enabling secure, browser-based access to business applications. This reduces the need for costly VDI deployments and lowers the total cost of ownership, all while providing a secure and controlled environment for accessing corporate resources.

By reducing the reliance on traditional VDI, Prisma Access Browser helps organizations lower costs, simplify their IT infrastructure, and improve the overall user experience. This modern approach to remote access is particularly valuable as businesses continue to adopt more flexible and scalable IT solutions.

Business Continuity

Ensuring seamless access to critical business applications during disruptions is vital for maintaining operations. Prisma Access Browser supports business continuity by enabling secure, uninterrupted access to corporate resources from any device, anywhere. With built-in data protection and real-time threat detection, it safeguards sensitive information and ensures that business activities can continue smoothly, even in the face of unforeseen events or disruptions.

Secure Access from Any Device

Enable employees to continue to work despite the disruption. An enterprise browser allows workers to securely access corporate applications from any device—even unmanaged, from anywhere in the world.

Activation in Minutes

In the event of a disruption, Prisma Access Browser can become your new, primary workspace in one click. You can easily configure which users can access the applications of your choice, ensuring device posture checks and security requirements for each activity. In the event of an outage, employees can securely access their work tools without delay.

Advanced Security

Cybercriminals often use major events like the pandemic, wars, and widespread IT outages opportunistically, exploiting the spectacle to defraud confused employees and other innocent people. Prisma Access Browser allows you to maintain business operations in a secure environment, with full visibility and control over activity in the browser. With highly granular access as well as data and identity controls, you can define the exact configuration required to maintain your business operations and gain unprecedented visibility including event logs, session recording, and more.

Frictionless Adoption for All Employees

With 85% or more of a worker's day spent in the browser, working in Prisma Access Browser feels natural. Instead of getting busy with rebooting systems and shipping laptops, your workers around the world can simply open their laptop and quickly respond to changes required in the production environment, communicate with customers and peers, access sensitive information, and operate remote machines and servers to maintain work processes, along with any other critical tasks required to keep the business running smoothly.

Secure Apps That Don't Allow Decryption

Today's enterprises rely on a large number of SaaS and web applications, many of which utilize encrypted channels to ensure operational effectiveness. Unfortunately, attackers have seized on this reliance, exploiting encrypted channels in widely trusted applications like Microsoft 365, Google Workspace, and Slack to hide malware, establish command-and-control channels, and exfiltrate sensitive data. Eight-six percent of cyberthreats are now delivered over encrypted channels,[4] so visibility into these applications is a critical component of a true Zero Trust security framework.

Unmatched Decryption with Palo Alto Networks Security Solutions

Palo Alto Networks provides industry-leading decryption across both web and nonweb traffic via our Next-Generation Firewall (NGFW) and SASE solutions. Driven by Precision AI, these solutions enable deep inspection of encrypted traffic, providing the ability to prevent both known and unknown threats while offering robust data protection through advanced DLP capabilities. However, certain types of traffic aren't decrypted due to application functionality, compliance mandates, or user experience requirements. This leaves as much as 64% of web traffic encrypted and potentially vulnerable to hidden threats.[5]

Complementing Decryption with Secure Visibility

To address the challenges of traffic that remains undecrypted, Prisma Access Browser works alongside our leading network decryption capabilities, forming a unified, multilayered approach to Zero Trust security. As the only SASE-native secure browser, Prisma Access Browser delivers visibility and control over every application accessed through the browser without the need to decrypt traffic. It also extends Zero Trust policies to all browser-based activities, tapping into the same advanced threat detection and data protection capabilities that power our broader network solutions. This approach ensures that even undecrypted traffic can be monitored and controlled, minimizing risk without impacting performance.

A Dual-Layered Approach for Comprehensive Protection

By integrating Prisma Access Browser with Palo Alto Networks network security platform, organizations gain comprehensive visibility and control over encrypted traffic across all applications and communication channels. While network security delivers unmatched decryption and threat prevention, Prisma Access Browser secures browser-based activity where decryption isn't possible. Together, they ensure that no traffic, whether decrypted or undecrypted, remains a blind spot.

This dual-layered model detects hidden threats, safeguards sensitive data, and provides seamless protection across both managed and unmanaged devices. With Prisma Access Browser, enterprises can adopt a true Zero Trust posture that covers all traffic without compromising user experience or productivity, ensuring a resilient security stance in today's complex threat landscape.

Previously Unimagined Use Cases

By integrating advanced security features directly into the browser, Prisma Access Browser unlocks a range of use cases, which are either difficult or impossible to achieve with traditional solutions. This enables organizations to quickly address new and dynamic scenarios with highly flexible data, access, and identity controls. Some of the key use cases include supporting last-mile data protection, securing privileged users, preventing insider threats, ensuring business continuity, enabling the use of GenAI tools, and managing shadow IT.

4. "86% of cyberattacks are delivered over encrypted channels," Help Net Security, December 21, 2023.
5. *The State of Workforce Security: Key Insights for IT and Security Leaders,* Palo Alto Networks and Omdia, January 2025.

Last-Mile Data Protection

The final stage of data transmission and access is where data is most vulnerable to breaches. With an average of 85% of employees' workdays spent in the browser, securing this "last mile" is critical. Prisma Access Browser provides seamless integration of security measures, such as encryption, access controls, and real-time monitoring, directly within the browser. The browser's comprehensive protection includes advanced controls like data masking, screenshot blocking, limiting sharing via collaboration tools, controlling copy/paste functions, preventing printing, and applying watermarks on sensitive screens.

Securing Privileged Users

Privileged users with elevated access rights are prime targets for cyberattacks. Prisma Access Browser enhances the security of these users through features like step-up multifactor authentication during critical workflow stages, last-mile data protections, visibility controls to ensure data integrity, device posture checks, and detailed audit trails of all activities (including session recordings). These comprehensive security measures ensure that privileged users operate within a secure and controlled environment.

Mitigating Insider Threats

Intentional and even accidental insider threats pose significant risks to corporate data security. Prisma Access Browser provides a range of controls to prevent such threats by defining which applications users can only access in the secure workspace of the browser. Organizations can isolate business workspaces from personal accounts and control the type of files workers can share or access. For instance, files downloaded from a corporate app can be encrypted and restricted from access by noncorporate SaaS applications, ensuring that sensitive data remains protected within the secure browser environment.

Access to Unmanaged Accounts

Organizations often need to provide access to accounts they don't manage, such as virtual deal rooms or financial services, which can be challenging to secure. Prisma Access Browser secures these applications with a patent-pending account protection feature. This feature adds a secret element to every user password, which is stored in Prisma Access Browser. This prohibits access to the account from any other browser and by any other user.

Shadow IT

Shadow IT, where employees use unapproved applications and devices, poses significant security risks. Prisma Access Browser provides visibility into all web-based activities, allowing organizations to monitor and manage shadow IT effectively. This comprehensive oversight helps prevent data leakage and ensures that all applications and devices used within the organization comply with security policies.

Prisma Access Browser unlocks a myriad of new use cases by providing highly flexible data, access, and identity controls directly in the browser. This not only enhances security but also boosts productivity, enabling organizations to address dynamic scenarios with confidence and agility. By closing the browser gap in enterprise security, Prisma Access Browser provides a powerful, holistic solution that addresses the complex challenges of modern enterprises.

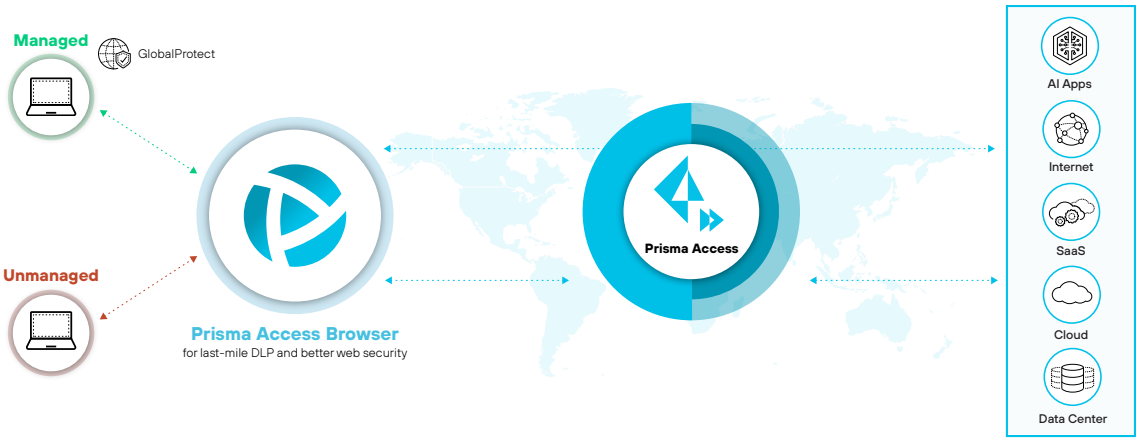

Figure 5: Prisma Access Browser unlocks the power of SASE

The Road Ahead

It's no secret that with all the changes in securing our workforces, the threats are evolving too. As we adapt to new ways of working, from leveraging cloud resources to using AI for everyday tasks, the challenges we face in maintaining security and productivity are becoming increasingly complex. Traditional security models, designed for a more static work environment, are no longer sufficient. We need solutions that are as dynamic and flexible as the modern workforce itself.

Prisma Access Browser represents a significant step forward in addressing these challenges. By extending SASE through the browser, it provides a seamless and secure user experience across all devices, managed and unmanaged, to every corner of the globe.

Looking ahead, the importance of secure browsers will only grow. Gartner predicts that "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."[6] This shift underscores the need for solutions like Prisma Access Browser that can provide comprehensive security while supporting the flexibility and agility that modern businesses demand.

The future of work is here, and it's browser-based. As organizations continue to embrace hybrid work models, the need for secure, efficient, and user-friendly tools will become even more critical. Prisma Access Browser not only meets these needs but also anticipates the future challenges of a dynamic and ever-changing work environment. By providing unparalleled security and a delightful user experience, it ensures that businesses can stay productive and secure, no matter where or how their employees work.

It's clear that our security solutions must evolve alongside our work. Prisma Access Browser makes this evolution easy, offering a powerful, integrated approach to securing the browser—where work happens. With its advanced features and seamless integration into the SASE framework, it sets a new standard for enterprise security, paving the way for a future where productivity and security go hand in hand.

6. Dan Ayoub et al, *Emerging Tech: Security — The Future of Enterprise Browsers*, Gartner, April 14, 2023.

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_wp_pab-integral-part-of-sase_020425