Palo Alto Networks and Menlo Security

Safe Browsing and Proactive Threat Prevention

The Challenge

Now more than ever—especially with the growing adoption of mobility and cloud transformation—business is conducted on the internet. The internet is fraught with malicious content, however, from fake login portals to malware-infected websites. Unfortunately, taking a very strict approach to what users are allowed to access on the internet negatively impacts their productivity. Moreover, it strains overburdened IT support teams that are locked in a daily struggle with intelligent, motivated, and well-financed adversaries. These issues are driving the need to tightly integrate best-in-class security solutions. As cybercriminals' tools evolve to evade traditional detection technologies, enterprises need to eliminate threats earlier in the attack lifecycle while empowering their IT security teams with visibility and forensics.

Menlo Security Browser Isolation

Menlo Security Browser Isolation assumes that all web content is risky and hosts potentially malicious content. This approach eliminates the need to make an "allow or block" determination based on coarse categorization and detailed analysis. Instead, Menlo Security offers an additional option to "isolate" potentially risky or uncategorized websites. For content that is isolated, Menlo efficiently delivers only safe and malware-free content to the end user's browser with no impact on user experience or productivity, and without requiring an endpoint agent or browser plugins. All active content, such as JavaScript and Flash, whether good or bad, is fully executed and contained within the Menlo Security Isolation Core™. This eliminates the possibility of malware ever leaving the isolated web browsing session within the Isolation Core. This approach restores 100% confidence in your security posture and enables security teams to empower worry-free and productive clicking, downloading, and browsing for end users.

Palo Alto Networks Prisma Access

Palo Alto Networks Prisma® Access transforms security with the industry's most complete cloud-delivered platform, allowing organizations to enable secure remote workforces. Legacy network security products require significant manual effort to deploy, manage, and maintain; do not scale; and leave gaps in coverage that impact productivity and increase risks. Prisma Access provides more security coverage than any other solution, protecting all application traffic to reduce the risk of data breaches while providing guaranteed performance with leading service-level agreements (SLAs) to offer an exceptional end user experience.

All users, whether at corporate headquarters, branch offices, or on the road, connect to Prisma Access to safely access cloud and data center applications as well as the internet. Prisma Access consistently inspects all traffic across all ports and provides bidirectional networking to enable branch-to-branch as well as branch-to-HQ traffic.

Palo Alto Networks and Menlo Security

As a Palo Alto Networks Technology Partner, Menlo Security integrates with Prisma Access. Joint customers can selectively route web traffic through Menlo Security Browser Isolation via existing policy controls on their Prisma Access instance, ensuring a single pane of glass for policy management while leveraging the Menlo Security Browser Isolation to execute content away from users' endpoints.

Prisma Access and Menlo Security Browser Isolation work together to deliver the most proactive threat prevention available without hindering productivity applications like web browsers and email. The integrated solution:

- Eliminates all types of malware from risky and unknown/uncategorized websites.
- Neutralizes malware from weaponized documents and files.
- Complies with various mandates and regulations for air-gapping high-value users.
- Ensures user productivity that is unhindered by excessive blocking of websites.
- Reduces the influx of help desk tickets from users whose access to websites has been blocked.
- Extends the Prisma Access policy framework to include isolation in a single pane of glass.

Use Case 1: Simplify User Policy Enforcement

Challenge

The internet contains more than 4 billion websites, with millions more launched every month. Many are new and, therefore, uncategorized, while others are inaccessible because of "false positive" classification. This leaves organizations with the difficult choice to either allow or deny user access. Allowing access supports user productivity but increases cyber risk, whereas denying access limits productivity and dramatically increases help desk tickets requesting website categorizations and recategorizations.

Solution

Together, Prisma Access and Menlo Security Browser Isolation allow organizations to leverage the URL policy capabilities of Prisma Access and selectively steer specific websites—such as uncategorized websites or those that register a false positive—to Menlo Security Browser Isolation. This allows users to access such websites safely without risking the organization's security posture. Users will experience 100% native web browsing, and their web browsers will receive 100% safe visual components for local rendering.

Use Case 2: Protecting High-Risk Users and Applications

Challenge

Many organizations have a group of users that may require elevated security while accessing websites. These users may be privileged administrators, or they may have access to highly secure systems (e.g., payment systems, SWIFT interbank transfer systems) from their devices. The extra level of security may also be mandated by industry or government regulations.

Solution

All web traffic for specific users or groups of users may be directed through Menlo Security Browser Isolation via integration with Prisma Access. This ensures that any website the specified user or group accesses is executed within the cloud-based Menlo Security Browser Isolation, returning only safe and malware-free visual components to the user's device for local rendering in a web browser.

Prisma Access can integrate with Menlo Security to provide web isolation for users in two ways. The first method is via URL prepend, wherein URLs associated with a user's web traffic are prepended with safe[.]menlosecurity[.]com. The second method utilizes traffic steering policies in Prisma Access, wherein web traffic is redirected across an IPsec tunnel to Menlo Security Browser Isolation and is completely transparent to end users for a more seamless experience. End users will see no change and can browse webpages with a native experience.

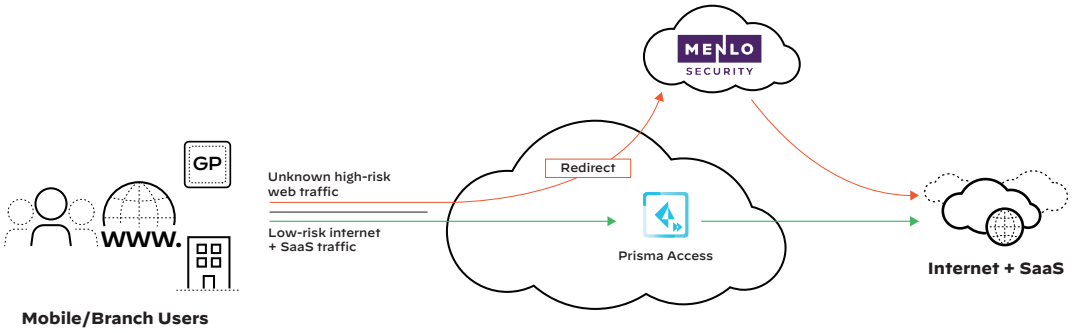

Figure 1: Forwarding of specific traffic to Menlo Security for browser isolation

About Menlo Security

Menlo Security, Inc. delivers security without compromise and helps enterprises achieve digital transformation to leverage the full benefits of the cloud. Its solutions are built on the world's first and only Isolation Core™ and delivers 100 percent protection against web and email threats. For more information, please visit www.menlosecurity.com."

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS | MENLO SECURITY

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