Menlo Security

PALO ALTO NETWORKS AND MENLO SECURITY

SOLUTION BRIEF

OVERVIEW

Challenges

Today, a user's device can be infected by malware simply by navigating to a compromised website or by inadvertently downloading a "weaponized" document. Any website can potentially serve malware—even those considered "safe," such as respected news and popular entertainment sites. Security professionals are locked in a cat-and-mouse struggle with smart, motivated, well-financed attackers, driving the need for tightly integrated best-of-breed security solutions.

Highlights

As a NextWave Technology Partner, Menlo Security integrates with the Palo Alto Networks® (PAN) WildFire® malware analysis solution. Palo Alto Networks customers can also steer web traffic through the Menlo Security Isolation Platform (MSIP) directly from their PAN next-generation firewalls, eliminating the need to manage a traditional proxy configuration.

- With the Palo Alto Networks WildFire integration, dangerous executable and document files passing through the MSIP can be submitted to the WildFire API for analysis.
- With the Palo Alto Networks transparent proxy integration, joint customers can steer web traffic through the Menlo Security Isolation Platform directly from their PAN next-generation firewalls, eliminating the need to configure device proxy settings—saving time, effort, and potential points of failure.

Menlo Security Isolation Platform

The cloud-based Menlo Security Isolation Platform (MSIP) eliminates the possibility of malware reaching user devices via compromised or malicious websites, emails, or documents. With Menlo Security, the user's web session and all active content—such as JavaScript and Flash—whether good or bad, is fully executed and contained in the Isolation Platform. Only safe, malware-free rendering information is delivered to the user's endpoint with a completely native user experience. No active content—especially any potential malware—leaves the platform.

Palo Alto Networks WildFire

Palo Alto Networks WildFire cloud-based threat analysis service is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware. The cloud-based service employs a unique multipronged approach combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.

SOLUTION

The Integration Solution

This integration provides Menlo Security customers with superior levels of detection-based security in the event they need to download an original file from the web. This solution offers:

- **Dynamic analysis:** Observes files as they detonate in a custom-built, evasion-resistant virtual environment, enabling detection of zero-day malware and exploits by using hundreds of behavioral characteristics.
- **Static analysis:** Provides highly effective detection of malware and exploits that attempt to evade dynamic analysis, and instantly identifies variants of existing malware.
- **Machine learning:** Extracts thousands of unique features from each file, training a predictive machine learning classifier to identify new malware and exploits not possible with static or dynamic analysis alone.
- **Bare metal analysis:** Automatically sends evasive threats to a real hardware environment for detonation, entirely removing an adversary's ability to deploy anti-VM analysis techniques.

Use Case #1

Challenge

Users contracting malware from compromised and malicious websites.

Solution

Menlo Security isolates web transactions in the cloud, accessing the web on the behalf of users, executing their sessions and requests while removing the threat of malware that might be lurking in the websites they access. Users see, and their devices and web browsers receive, only 100 percent safe, rendered information. Organizations can deploy the Menlo Security Isolation Platform as a transparent proxy, using their Palo Alto Networks next-generation firewall to steer web traffic through the Isolation Platform, eliminating the need to configure device proxy settings.

Benefit

Users are free to use the web to perform their jobs, without risk of malware infection.

Use Case #2

Challenge

Users are at risk from weaponized documents and files they find on the web.

Solution

Menlo Security Document Isolation renders the most common document types—including PDF, Word, Excel, and PowerPoint—in its cloud environment, eliminating malware before it can ever reach your users' devices. Users see—and their devices and browsers receive—only malware-free, rendered documents that look and behave like the originals. If you decide to allow specific users to download original documents, MSIP can be integrated with the WildFire cloud-based threat analysis service so only malware-free documents can be downloaded, even if they're password protected.

Benefit

Users can freely access the web and online documents without fear of malware infection.

Conclusion

In today's world, security threats lurk around nearly every corner of and website on the web. It takes multiple, advanced, world-class security solutions—working together and sharing information—to ensure user, device, and organizational security, and to protect against malware, such as ransomware, and phishing attacks.

The integration of Menlo Security Isolation Platform and Palo Alto Networks WildFire and next-generation firewalls addresses this need and enhances web and cybersecurity.

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Menlo Security's cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions, and backed by General Catalyst, Sutter Hill Ventures, Engineering Capital, Osage University Partners, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Palo Alto, California.

2300 Geng Rd., Ste. 200

Palo Alto, CA 94303

Tel: 650 614 1705

info@menlosecurity.com

menlosecurity.com