Menlo Security

NEXT-GENERATION SECURE WEB GATEWAY USING REMOTE BROWSER

ELIMINATE MALWARE AND BREACHES

Virtually any website, link or web advertisement can be used to deliver malware today, launching an attack on a user's endpoint device that quickly spreads throughout your organization, infecting any device it can reach. The answer? **Menlo Security's Next-Generation Secure Web Gateway.**

Today's Threat Landscape

1. Safe, legitimate websites can be hijacked to deliver malware via drive-by download or watering hole attacks
2. Known URLs can appear to be trustworthy, but are really spoofed or use homographic attacks, infecting a user with malware
3. Users are asked to download documents from the web to collaborate and are unknowingly downloading malware

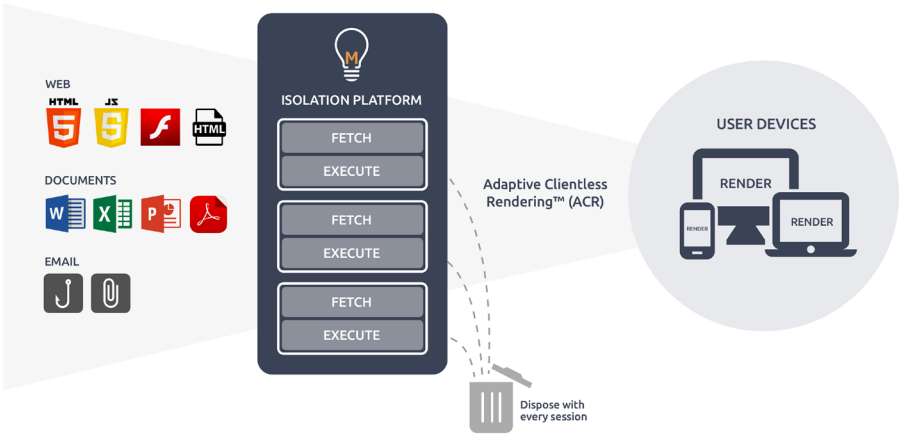
SOLUTION

Protect with Next-Generation Secure Web Gateway

We don't determine what websites are infected with malware, rather we just assume that all web content is risky (zero trust approach to security) and hosts potentially malicious content and isolate all web traffic. We don't block or allow traffic based on coarse categorization and analysis, customers should employ an isolate or block policy.

Menlo Security enables this approach by intercepting all web traffic in its cloud isolation platform, preventing malicious content from ever reaching endpoints where it can do real damage. With Menlo, web content is fetched and executed in the Menlo Security Isolation Platform (MSIP) cloud instead of on users' browsers.

Menlo uses ACR (Adaptive Client rendering) to efficiently deliver only safe and authorized content to the end users browser with minimal impact on user experience, privacy or productivity. Nor is there special client software or plug-ins to deploy and install. This restores 100 percent confidence in security posture for security teams and worry-free and productive browsing experience for end users.



PROBLEM

Detect and Respond is Ineffective and Inefficient

Traditional legacy security solutions and conventional threat prevention products that rely upon a detect and respond approach have failed to keep up with the evolving nature of sophisticated malware attacks.

Malware developers have proven they can circumvent existing technologies designed to detect their patterns and activity, allowing them to determine if it has been detected or sandboxed and evade detection before it can be captured for analysis.

An inability to detect attacks causes malware prevention responsibilities to fall to the individual or user--untrained and unaware, prone to the susceptibility of human nature. Additionally, zero-day or unknown attacks for which signatures have not been established will easily penetrate existing defenses.

Anti-Malware Protection Key Features and Benefits

100% Protection from Malicious Web Sites

Web Isolation

- Eliminates false positives that block legitimate content and generate alerts
- Eliminates false negatives that allow malware to reach a user's endpoint device
- Eliminates the need to detect "good" vs "bad" while eliminating phishing, malware, ransomware and zero-day threats.

Stateless Sessions hosted in the Cloud

- Disposable Virtual Containers (DVC) are disposed after every browsing session while user cookies are stored for seamless browsing experience, it eliminates any chance for malware to escape and infect a user's endpoint device by sending only clean content to the endpoint

Dynamic or Active content Isolation

- Neutralization of "command-and-control" (C&C) communications because dynamic content – that can be infected with malware is removed from web pages and documents and executed within the isolation platform

Isolation from Adobe Flash

- Allows users access to Flash-produced content, without risk of infection

Isolates cascading style sheets (CSS)

- Protects the user and their endpoint device from malware hidden within cascading style sheets (CSS)
- Eliminates the threat of malware concealed in web page images and fonts, protecting the user and their endpoint device

Disarms Weaponized Documents

Document isolation

- Eliminates any user risk from weaponized documents, such as Adobe Acrobat, and Microsoft Office and Office 365 (Microsoft Word, Excel and PowerPoint) documents

Optional "safe" or original downloads

- "Safe" downloads remove and execute any dynamic content, such as JavaScript, within the isolation platform, ensuring safe documents in Adobe Acrobat
- Original downloads may be required, and are offered as an authorized option, on a per user basis

HTTPS Traffic isolation / Protection

- Isolates and protect against encrypted web sessions using HTTPS traffic to camouflage malware and bypass existing security solutions

HTTPS Document rendering

- Protects the user and their endpoint device from encrypted documents harboring malware

Flexibility of deployment options

The Menlo Security Next-Gen Secure Web Gateway can be deployed in a variety of different customer environments.

Cloud Service

Deploying Menlo Security as a cloud service reduces infrastructure management requirements and ensures service availability and platform upgrades.

MSIP is hosted on an industry leading public cloud, high-availability platform with a global footprint, geo-redundancy and "least latency" based routing.

A web-based administration console provides granular control over configuration features, security policies and access rule settings. Traffic analysis, reporting and logs are available through the administration portal as well and can also be downloaded via an API.

Enable protection no matter where you do business

Menlo Security's Global Elastic Cloud provides high-availability, auto-scaling and bandwidth management that is completely transparent to the user with fixed pricing irrespective of bandwidth or CPU utilization.

Rather than let the platform's performance be tied to a Service Level Agreement (SLA) from a public cloud provider, Menlo measures the platform's reliability and uptime against those of Cloud Service Providers. With more than 20 ISO27001 and SOC2-certified data centers worldwide, Menlo achieves 99.995% global availability with transparent and automatic failover between data centers--making it possible to fully protect your users no matter where they do business around the world.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents and email.

Menlo Security's cloud-based and on-premise Isolation platform scales to provide comprehensive web, email and document protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience.

Menlo Security is trusted by major global businesses, governments and verticals, including Fortune 500 companies and financial services institutions, and backed by leading venture capital firms and banks.

Menlo Security is headquartered in Palo Alto, California.

To learn more, visit **menlosecurity.com** or contact **sales@menlosecurity.com**