Menlo Security

MENLO SECURITY SOLUTION BRIEF

MENLO SECURITY NEXT-GEN SECURE WEB GATEWAY WITH WEB ISOLATION

PREVENT MALWARE FROM REACHING YOUR ENDPOINTS

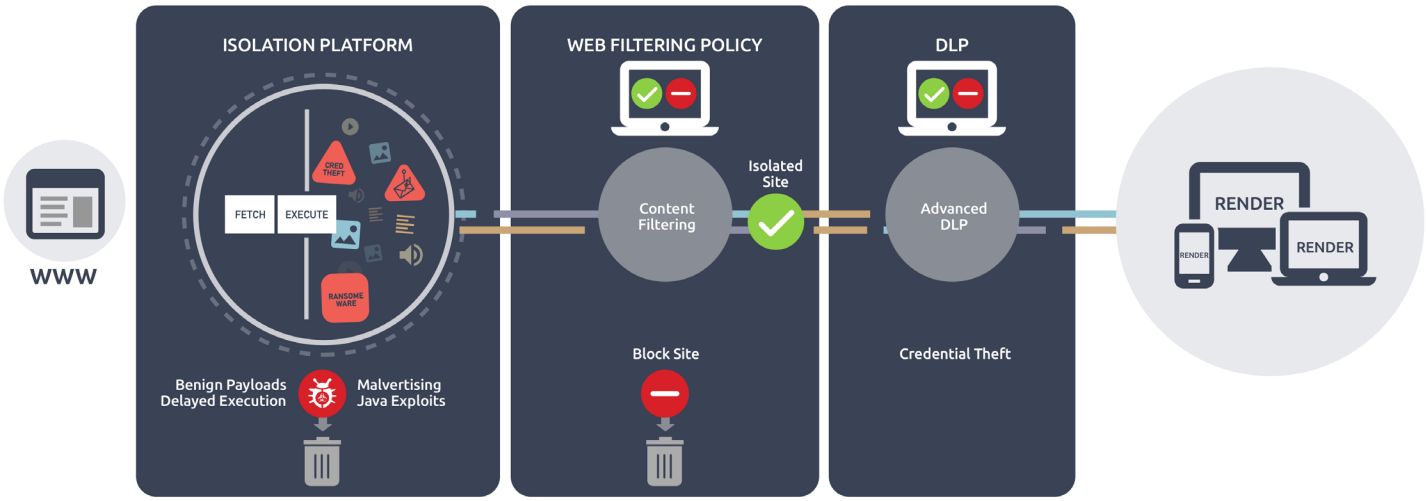
Traditional SWG Solutions are Now Outmanned

Business today is conducted largely on the internet. Users need access to web-based tools and platforms while interacting with customers and partners on social media and other collaborative sites. Unfortunately, not all websites--even seemingly legitimate and trusted sites--are safe. Malware lives surreptitiously on the web, waiting for unsuspecting users to visit a spoofed URL or a compromised site where it can download malicious code onto their devices with the ultimate goal of infiltrating the corporate network and mission-critical business systems.

Traditional Secure Web Gateway (SWG) solutions act as a filter between users and the internet, making a determination in real time about whether a site can be trusted. However, these legacy solutions fail to protect the modern workforce from increasingly sophisticated and stealthy attacks. For one, users are more spread out in remote offices, at home and on the road, making it difficult to redirect traffic to a central point for URL filtering. Secondly, today's media-rich websites are made up of dozens or even hundreds of content blocks served from third-party partners and sources, and these content blocks are constantly rotated in and out--daily, hourly, even by the minute. So, even trusted sites can harbor hidden malware--even if they have already been deemed safe by threat intelligence sources. More modern approaches such as sandboxing or deploying a traditional anti-virus engine also rely on the assumption that someone else has either identified a malicious site and threat intelligence has been updated. This, of course, takes a combination of time and luck--neither of which should be the foundation of any cybersecurity strategy.

What You Can Accomplish with Menlo Security NextGen Secure Web Gateway

1. Protect users from all malware hosted on websites and linked documents that use hijacked websites, drive-by downloads and watering holes attacks to deliver malware to endpoints.
2. Prevent users from entering credentials or exposing personally identifiable information (PII) on suspicious webforms by making risky sites read-only and limiting uploads to prevent data lost.
3. Enforce a set of rules and regulations by blocking access to inappropriate or offensive content on the web using categorization.
4. Safely and confidently allow targeted and privileged users with unrestricted access to potentially risky and uncategorized websites--without impacting productivity or risking malware attacks by implementing an "Isolate" instead of "Block" web filtering policy.
5. Granularly monitor user access to websites and documents on the Internet and provide insights into threats, vulnerabilities and web activity for improved security investigations, remediation and compliance.



MENLO SECURITY SOLUTION BRIEF

MENLO SECURITY NEXT-GEN SECURE WEB GATEWAY WITH WEB ISOLATION

PREVENT MALWARE FROM REACHING YOUR ENDPOINTS

It's Time to Upgrade to a Next-Gen SWG Solution

Next-gen SWG solutions take a different approach to web security: Web Isolation. Rather than rely on detect and respond technologies that are susceptible to increasingly-sophisticated threats and the dynamic nature of modern web pages, Menlo Security Next-Generation SWG assumes that all web content is malicious, keeping it far away from users' devices where it can do damage. All content is passed through the Menlo Security Isolation Platform (MSIP), a web-based browser where all code is fetched and executed in the cloud. Only safe content is mirrored safely to users' browsers--effectively cutting off any access to endpoint devices.

Web isolation eliminates the need to make an allow or block determination based on coarse categorization and analysis--replacing it with an isolate or block decision. For content that is allowed and therefore isolated, Menlo Adaptive Client Rendering (ACR) efficiently delivers authorized content to the end user's browser with no impact on user experience or productivity. This allows users to safely interact with websites, links and documents online without compromising security. Most importantly, users' web browsing experience is not impacted at all, giving them unrestricted yet safe and transparent access to all web content.

Comparing Menlo Next-Gen SWG to Legacy SWG

Benefit	SWG	Next Gen
Protection against Advanced Threats - Websites	Use of threat feeds sourced from various vendors on internal sources and the URL list is updated. Threat feeds include IP/URL/Domain. Assumes there is a patient zero and threat intel is updated immediately after a source has discovered it is malicious.	No threat feed required as all websites are isolated. No malicious content is fetched or executed on users' devices--effectively eliminating the possibility of any malware infection.
Protection against Advanced Threats - Files	Use a sandbox to open a file to determine if malicious activity is happening. Assumes there is a patient zero and then blocks future downloads.	All documents are isolated and rendered to end users as read-only documents. Administrators have an option to allow original documents following a sandbox check.
URL Filtering	Use a URL database that allows administrators to control access to certain sites. The database requires vendors to crawl and know every part of the internet.	Administrators simply set policies that restrict actions on websites rather than the websites themselves and renders some sites and documents in read-only mode. This opens up parts of the internet that would have been previously blocked.
Central Management and Configuration	Integration with customer directory services for user authentication and group information for granular policy setup. Can require different management consoles for remote users and offices.	In addition to auth integration, administrators use a cloud management portal to configure web control and isolation policies, ensuring that new and updated changes to policies are implemented across all devices immediately-- including remote users, branch offices and all global users.
Data Loss Prevention	Use of regex and pattern matching to determine if sensitive data is being leaked. Can be integrated with existing DLP solutions to ensure uniformity across all data channels.	Allows administrators to control data being transferred in HTTPs streams and presents user data in a consistent and simple format that any DLP can understand. HTTPS form data is intercepted, and DLP policies can be applied without requiring a break in HTTPS connection. This enhances the visibility and effectiveness of existing DLP solutions.

Menlo Security

Menlo Security's cloud-based Next-Generation 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**