Menlo Security

BRIEF

Give Users Safe Access to Original Files without Putting the Organization at Risk

Menlo Security's Isolation Core™ Seamlessly Integrates with GateScanner® Content Disarm and Reconstruction (CDR) from Sasa

Benefits:

- Provides a true Zero Trust approach for file downloads
- Secures original downloaded files
- Pre-filters malicious files and uses proprietary file disarm to prevent undetectable threats

The speed of business requires fast, reliable access to mission-critical systems, files, apps, and data, but as users continue to increasingly log in from outside the corporate firewall, security becomes a major concern. Attackers have found that they can exploit embedded objects, automation macros, scripts, and other plug-ins to overwrite memory and trigger the execution of malicious content. However, detecting these attacks through sandboxing delays file access, and stripping out the malicious code affects the powerful capabilities of these apps. Either way, the native user experience suffers and productivity is impacted—especially for remote workers. True agility requires real-time access to original files without putting the organization at risk.

Detect-and-Respond Security Solutions Fail to Neutralize the Threat

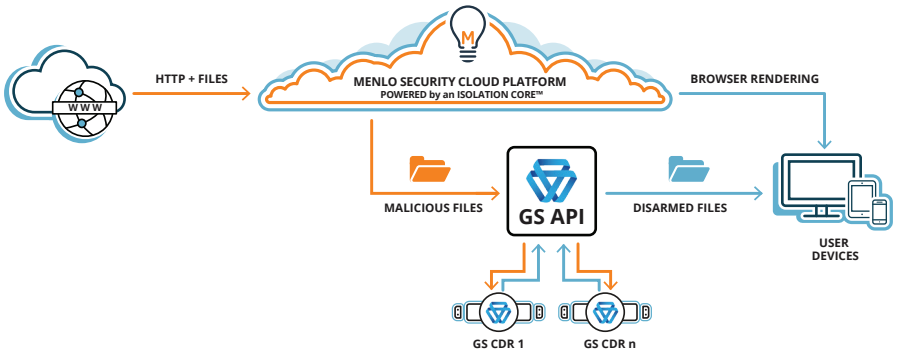
Advanced file-based attacks continually evolve and are capable of evading both static scanning and dynamic analysis technologies used by sandboxing, accounting for more than 50 percent of security incidents. Content Disarm and Reconstruction (CDR) technology closes the gap by protecting against known malware as well as exploits and weaponized content that have never been seen before.

Unlike legacy security products, the Menlo Security Global Cloud Proxy with an Isolation Core™ does not rely on a detect-and-respond approach, but rather on the assumption that all web content is risky and potentially malicious, and thus neutralizes it by isolating it in the cloud. However, there are instances when organizations need to allow user access to original content (such as PDFs, Excel files, etc.). Organizations are limited to allowing a simple sandbox check of these files, but this approach still relies on detection of known threats.

Menlo Security and Sasa GateScanner

To solve this problem, the Menlo Security Global Cloud Proxy with an Isolation Core™ seamlessly integrates with GateScanner CDR by Sasa Sofware, enabling the return of a disarmed file. This partnership offers a powerful synergy to prevent both browser- and file-based threats when administrators need to allow access to original content.

Menlo Security Global Cloud Proxy with an Isolation Core™ seamlessly integrates with GateScanner CDR by Sasa Sofware, enabling the return of a disarmed file.



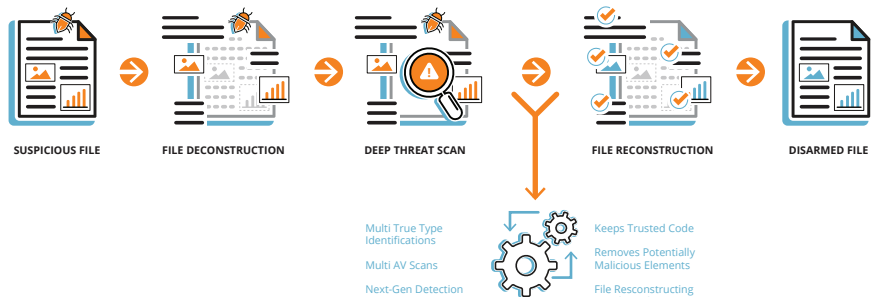
Menlo Security Global Cloud Proxy with an Isolation Core™

Menlo Security's Global Cloud Proxy with an Isolation Core™ enables safe viewing of web content and documents by executing all active content in the cloud—away from the endpoint device—while providing a native and seamless user experience.

In addition to providing 100 percent security with its cloud-delivered isolation approach, Menlo Security gives administrators the ability to set and enforce acceptable use policies (AUPs), such as for posting on social media sites, and to block malicious activity, including file uploads and downloads. Policies can be applied by user, group, file type, or website categorization to determine when the content is blocked or rendered in read-only mode. Menlo Security provides two tiers of functionality to combat these threats. First, users can be restricted to viewing a "safe PDF" version of the file, meaning that it has been stripped of any malicious content. Second, if the user requires access to the original file, it can be sent to a sandbox. If the sandbox detects malicious activity, then it will block the original file. Now a third option, which determines when the original content should be accessible by the user, is offered through the Menlo Security and GateScanner integration.

GateScanner CDR Pre-Filters Malicious Files to Stop Them

Sasa Software's GateScanner Content Disarm and Reconstruction (CDR) technology ensures security by combining highly optimized scanning and detection technologies to pre-filter malicious files, as well as proprietary file disarm technology to transform files into safe and neutralized (harmless) copies.



GateScanner CDR prevents advanced, undetectable weaponized content—including zero-day exploits, APTs, and ransomware—while maintaining full file fidelity and usability. The technology can leverage existing security assets such as network sandboxes to maximize their usage. Security policies are adjustable according to the organization's needs and can be applied to both downloads and uploads.

File-based attacks continue to evolve, making them difficult to stop using a detect-and-respond approach to cybersecurity. Menlo Security has teamed up with GateScanner CDR to prevent these threats while allowing users to access original files when appropriate.

To find out how Menlo Security can provide your company with protection against cyberattacks, visit menlosecurity.com or contact us at ask@menlosecurity.com.

GateScanner CDR prevents advanced, undetectable weaponized content—including zero-day exploits, APTs, and ransomware—while maintaining full file fidelity and usability.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The Menlo Security Cloud Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
1 650 695 0695
ask@menlosecurity.com