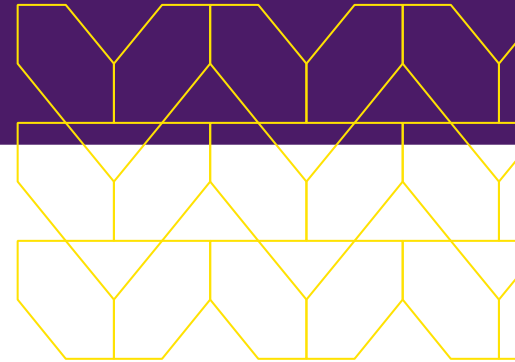




**PARTNER:
SOLUTION BRIEF**

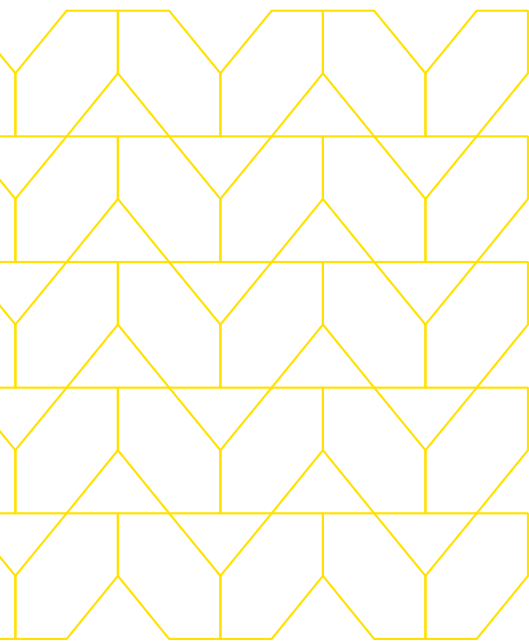


Menlo Cloud Security Platform Powered by an Isolation Core™ and Sasa GateScanner® Content Disarm and Reconstruction

Give users safe access to original files
without putting the organization at risk.

The challenge

The speed of business requires fast, reliable access to mission-critical systems, files, applications, and data, but as users continue to increasingly access resources 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 can delay file access, and stripping out the malicious code affects the powerful capabilities of these applications. Either way, the native user experience suffers and productivity is impacted—especially for remote workers.



Benefits

- Provides a true Zero Trust approach for all file downloads
- Secures downloaded files in their original file format
- Preserves the native end-user experience

True agility requires real-time access to original files in their native format without putting the organization at risk. The Menlo Cloud Security Platform Powered by an Isolation Core™ combined with Sasa's GateScanner® 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.

Menlo Cloud Security Platform— Powered by an Isolation Core™

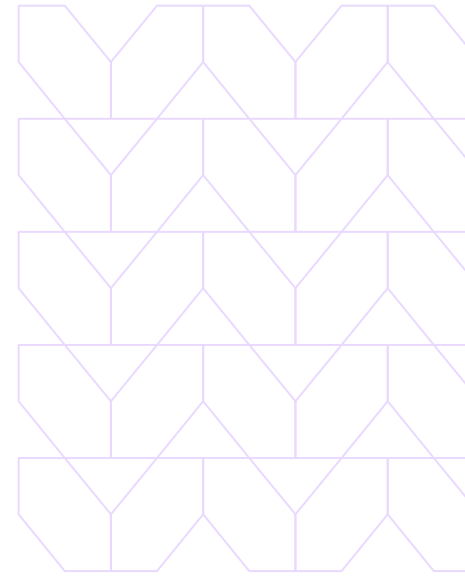
The Menlo Cloud Security Platform enables safe viewing of web content and documents by executing all active content in the cloud—away from the endpoint device—while providing a native and seamless user experience. Unlike legacy solutions, the Menlo Cloud Security Platform does not rely on a detect-and-respond approach, but rather on the assumption 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.

The Menlo Cloud Security Platform instead offers an option to “isolate” potentially risky or uncategorized websites. Once content is isolated, malware-free content is delivered safely and efficiently to the end user's browser, with no impact on user experience or productivity, and without requiring an endpoint agent or browser plug-ins. All active content such as JavaScript and Flash, whether good or bad, is fully executed and contained within Menlo Security's cloud-based Isolation Core™. This eliminates the possibility of malware ever leaving the isolated web browsing session and infecting the endpoint. This approach restores 100 percent confidence in the security posture and enables security teams to empower worry-free and productive clicking, downloading, and browsing for end users.

The Menlo Cloud Security Platform also gives administrators the ability to set and enforce acceptable use policies to block malicious activity, including file uploads and downloads. Policies can be applied by user, group, file type, or website categorization to determine when content is blocked or rendered in “safe preview” mode.

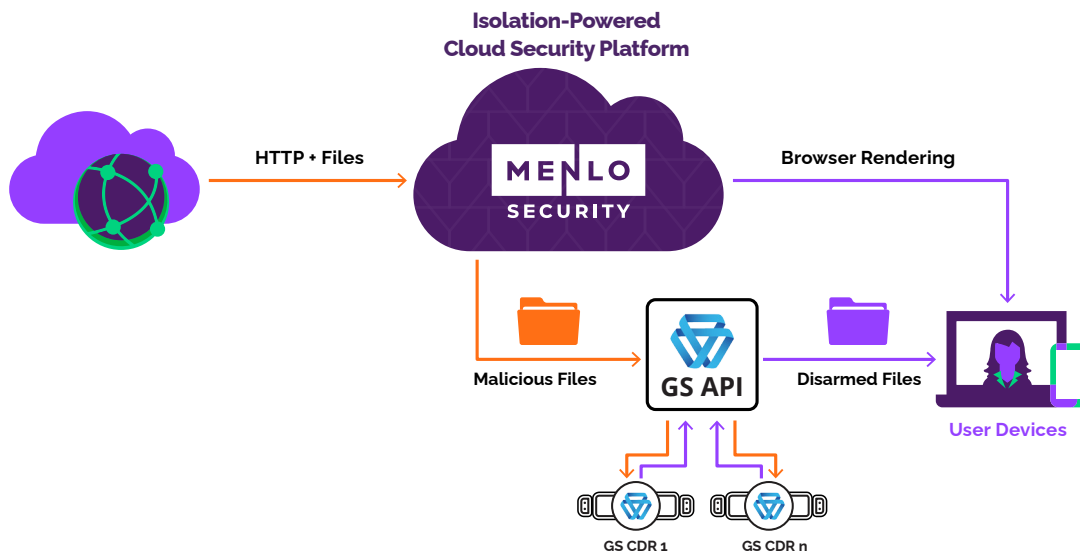
Sasa GateScanner® Content Disarm and Reconstruction (CDR)

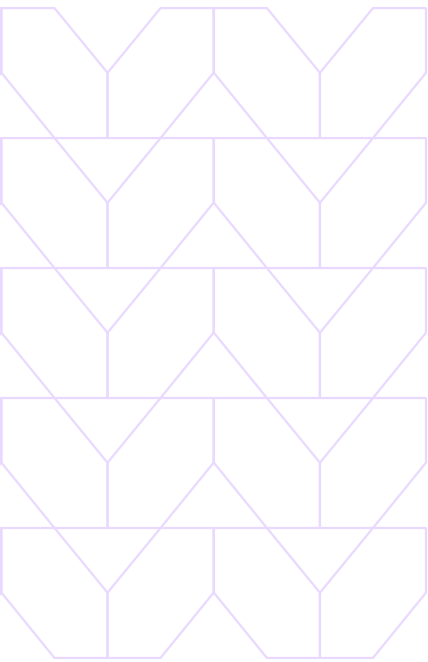
Sasa Software’s GateScanner® Content Disarm and Reconstruction (CDR) technology ensures security by combining highly optimized scanning and detection technologies to pre-filter malicious files, as well as proprietary file disarm technology to transform files into safe and neutralized (harmless) copies. GateScanner® CDR prevents advanced, undetectable weaponized content—including zero-day exploits, Advanced Persistent Threats (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.



Menlo Cloud Security Platform Powered by an Isolation Core™ Combined with Sasa GateScanner®

View and download files in their native format.





Integrating Menlo Cloud Security Platform with Sasa's GateScanner® Content Disarm and Reconstruction (CDR) provides a total security solution for web access, as well as for viewing and downloading files in their native format. This is achieved by isolating all content in the Menlo Cloud Security Platform and sanitizing files that need to be downloaded by routing them through Sasa's GateScanner®. This ensures that the downloaded files present no threat and are available in native file format to enable collaboration. Unlike legacy security products, the Menlo Cloud Security Platform and Sasa's GateScanner® are solutions that do not rely on a detect-and-respond approach.

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 Sasa 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.



To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com



About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

© 2021 Menlo Security, All Rights Reserved.