PARTNER:
SOLUTION BRIEF

MENLO SECURITY

OPSWAT.
MetaDefender

Menlo Cloud Security Platform Powered by an Isolation Core™ and OPSWAT MetaDefender

View and download files in their original format without compromising security.

The challenge

In the new normal, most content creation and consumption activities can be completed in a web-based interface—moving workloads from the secured data center to the cloud. Threat actors know this, of course, and are using Software as a Service (SaaS) platforms and web apps to mislead users to open a malicious website or document. Given the ubiquitous nature of SaaS and threat actors' ability to spin up branded emails at scale, it is extremely difficult to make an accurate point-of-click determination between fake and legitimate communications. Simply limiting users' browsing access may improve security, but blocking access would severely impact their productivity—especially given that most work is happening in the web now.

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

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.

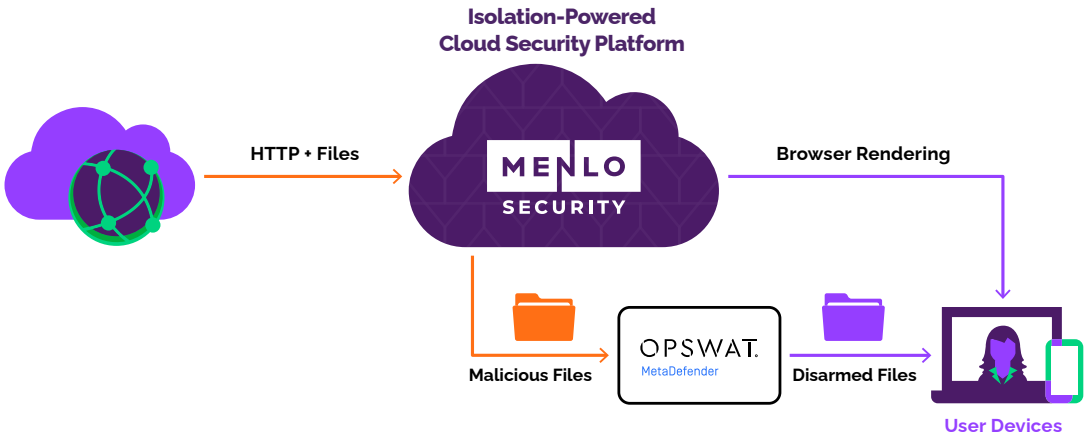
OPSWAT MetaDefender

Not everything can be done in a web session, and some collaborative work functions require files to be downloaded in their native format to the endpoint and opened locally. This step creates a major risk for the user, since the file will no longer run in an isolated environment but on the user's device—most probably located within the corporate network.

OPSWAT MetaDefender addresses this risk by analyzing the downloaded files to detect malware and, even more importantly, sanitize them. The sanitization process implies that all active content in a file is removed, ensuring that the final content is safe to consume on the end user's device.

Menlo Cloud Security Platform Powered by an Isolation Core™ Combined with OPSWAT MetaDefender ONE

Provides end-to-end security enforcement for files accessed via the web or email.



Integrating the Menlo Cloud Security Platform with OPSWAT MetaDefender provides end-to-end security enforcement by isolating active content in a remote environment, where it can be sanitized entirely without stripping out vital content or capabilities. MetaDefender detects malicious files by scanning them with more than 30 AVs, including next-gen AV. The files are then sanitized through Deep Content Disarm and Reconstruction (Deep CDR), effectively removing possible attacks hidden in files while keeping the files' functionality and usability intact. MetaDefender can also restrict the allowed file types that can be downloaded.

File-based attacks continue to evolve, making it difficult to stop them using a detect-and-respond approach to cybersecurity. Menlo Security has teamed up with OPSWAT 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.

MENLO SECURITY

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.