

Consume Content Downloaded from an Isolated Environment

Menlo Security's Isolation Core™ Seamlessly Integrates with OPSWAT MetaDefender

Benefits:

- Provides a true Zero Trust approach for file downloads
- Secures original downloaded files
- Preserves the native user experience

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 browsing access may improve security, but cutting access would severely impact users' productivity—especially given that most work is happening in the web space now.

Isolation Provides Security without Compromise

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.

Now a third option, which determines when the original content should be accessible, is offered through the Menlo Security and OPSWAT integration.

Enhance Isolation with Content Disarm and Reconstruction (CDR)

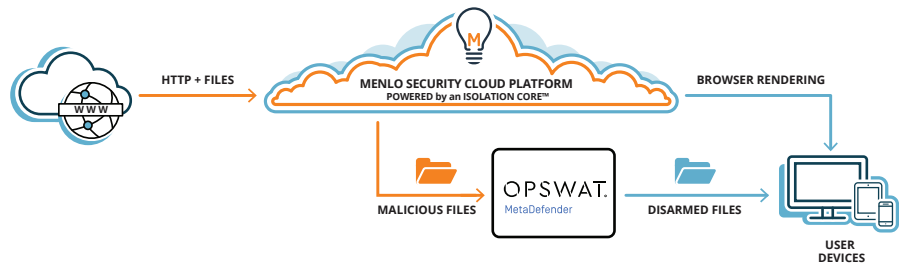
Not everything can be done in a web session, and some workloads require files to be downloaded to the endpoint and opened locally. This step creates



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 in 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.

Integrating MetaDefender into the Menlo Security Global Cloud Proxy with an Isolation Core™ provides end-to-end security enforcement for files accessed via the web or email.



End-to-End Security Enforcement

Integrating MetaDefender into the Menlo Security Global Cloud Proxy with an Isolation Core™ 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 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 MetaDefender 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.

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.
© 2020 Menlo Security, All Rights Reserved.

Contact us
menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

