Protect Users from Threats Originating from File Downloads on the Web

Menlo Security's Isolation Core™ Seamlessly Integrates with ReSec's ReSecure Web

Benefits:

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

File-based attacks spread on the web are growing in sophistication and volume as knowledge workers increasingly work from branch offices, home offices, customer sites, and places with public Wi-Fi. Threat actors are able to seamlessly spin up phishing emails at will and at scale to trick users into opening a malicious document that is designed to compromise their device. Once the document reaches the endpoint, the attacker can easily infect business systems, spread the attack to other devices, steal data, and disrupt business continuity. Simply limiting browsing access may improve security, but cutting access would severely impact users' productivity—especially given that most work now leverages the cloud and web-based applications.

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.

However, organizations sometimes need to allow user access to original content (such as PDFs, Excel files, etc.). Organizations were limited to a simple sandbox check of these files—an approach that still relies on detection of known threats. Now a third option—in addition to AUPs and sandboxing—allows the safe download of files while preserving the native file format, and is offered through the Menlo Security and ReSec Technologies 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.

The Menlo Security Global Cloud Proxy with an Isolation Core™ seamlessly integrates with ReSec's CDR technology, enabling the return of a disarmed file.
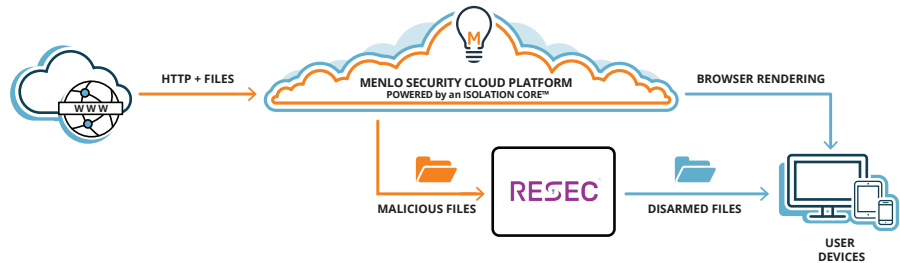
ReSec's ReSecure Web solution completely stops known and unknown malware that uses downloaded documents from the web as an attack vector. The solution maintains the original file outside the organization's network and creates a threat-free and fully functional replica of the file in real time that can be safely accessed by the user. A granular and rich policy editor offers diverse alternatives to exclude file types, treat URLs, and configure security setting levels.

Integrating Two World-Class Prevention Technologies

This joint prevention offering from Menlo Security and ReSec Technologies ensures that the user is fully protected when accessing files in native format from the web. The solution combines Menlo's industry-leading isolation technology and ReSec's CDR technology to retain full functionality of the downloaded files without compromising security. Unlike legacy security products, both Menlo Security and ReSec offer prevention platforms that do not rely on a detect-and-respond approach.

File-based attacks continue to evolve, making it difficult to stop using a detect-and-respond approach to cybersecurity. Menlo Security has teamed up with ReSec's ReSecure Web solution 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.

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