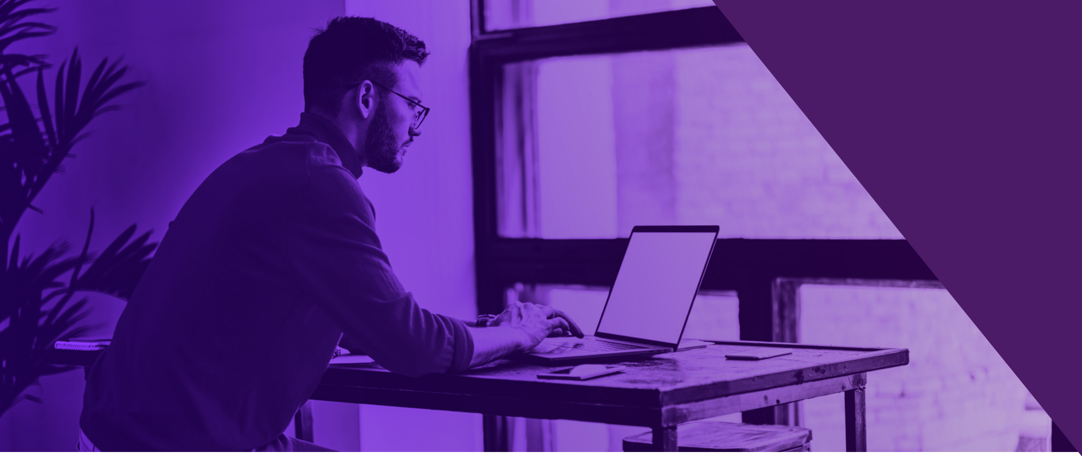


PARTNER:

SOLUTION BRIEF

Menlo Cloud Security Platform Powered by an Isolation Core™ and ReSec ReSecure Web

Protect users from threats originating from file downloads.

The challenge

File-based attacks 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 laterally to other devices, steal data, and disrupt business continuity. Simply limiting browsing access may improve security, but limiting access would also severely impact users' productivity—especially given that most work leverages cloud and web-based applications.

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.

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

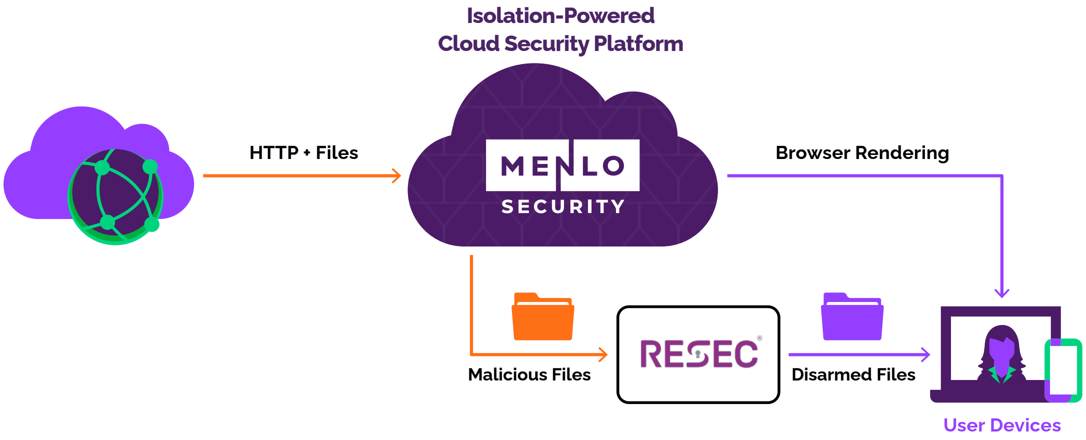
ReSec ReSecure Web

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.

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 format 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.

Menlo Cloud Security Platform Powered by an Isolation Core™ Combined with ReSec ReSecure Web

View and download files in their native format.



The joint solution from Menlo Security and ReSec Technologies ensures that the user is fully protected when accessing files in native format from the web. It combines Menlo's industry-leading isolation technology and ReSec's Content Disarm and Reconstruction (CDR) technology to retain full functionality of the downloaded files without compromising security. Unlike legacy security products, the Menlo Cloud Security Platform and ReSec's ReSecure Web 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 ReSec Technologies 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.