Menlo Security

Data Sheet

Email Attachment Isolation

Prevent email attachment–based attacks that download malware on users' computers.

Email continues to be the most popular and successful attack vector for cybercriminals to distribute malware—mainly because traditional email security solutions fail to fully protect the user from weaponized email attachments. The answer? Menlo Security Email Attachment Isolation.

Weaponized Email Attachments Continue to Threaten Today's Enterprises

Email is the most common attack vector for threat actors today. The reason is simple. Everyone uses email, and traditional security solutions have a hard time identifying—much less preventing—an attack. Despite operating a full spectrum of email security solutions that include anti-spam, anti-virus, data security, and encryption, organizations continue to fall prey to these types of attacks. These solutions typically rely on detection to make a "good" versus "bad" determination based on third-party threat intelligence feeds. Unfortunately, email attacks—especially weaponized attachments—are unique and targeted to just one person or only a few users, leaving no reputation footprint that can be detected in order to prevent future attacks.

It's clear that a new approach is needed.

Menlo Security Email Attachment Isolation

Menlo offers protection from malicious attachments in two ways. Known malicious attachments are automatically blocked while all others—even those deemed safe—are isolated, thus cutting off any access to users' devices. At the same time, the solution is seamlessly integrated with existing email server infrastructure to give users a consistent, native email experience. There are no new email systems to learn or software to install. All documents are simply routed through the Menlo Security Isolation Platform (MSIP), giving malware

Today's Email Attachment Security Landscape

- Weaponized documents masquerading as legitimate email attachments can download malicious malware onto users' devices.
- From there, threat actors can gain access to critical business systems and steal data or wreak havoc on the network.
- Traditional security solutions that rely solely on detection aren't able to act fast enough to prevent infections in real time.

Phishing and pretexting represent **98%** of social incidents and **93%** of breaches.

Email continues to be the most common vector **(96%)** for launching social engineering attacks.

Verizon
Data Breach Report 2018

no viable path to reach the user's device—an industry first not offered by any email protection service.

When users open a received email and click on an attachment, the document can be immediately viewed with 100 percent safety in isolation, without disrupting established workflows or negatively impacting user experience. In addition, administrators can provide users with an option to download a safe, macro-free PDF version of the attached document, or, in rare cases, allow certain users to download the original document attachment after it has been checked by an advanced anti-virus scan and placed in a sandbox—even if the attachment is password protected.

Menlo Security—
Email Attachment Isolation Key Features and Benefits

Feature	Benefits
Safe or Original Attachment Download	• As an option, administrators may allow users to download safe PDF versions of rendered attachments or allow designated users to download original document attachments.
Anti-virus Document Scan and Sandbox Options	• If users are permitted to download an isolated original attachment, Menlo Security offers cloud-based anti-virus scanning and sandboxing of the original document. • Workflow is fully customizable by administrators on a policy-controlled basis (per user, per group, per domain, per category, etc.). • Infections are prevented by scanning documents in ZIP files, even if they are password protected.
Integrates with Existing Email Infrastructure	• Easily integrates with existing mail server infrastructure, such as Exchange, Gmail, and Office 365. • Significantly reduces deployment and installation time. • Maintains known user experience and does not interrupt existing user email workflows.

About Menlo Security

Menlo Security protects organizations from cyberattacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com