Menlo Security

BRIEF

Prevent Email-Based Cyber Attacks with Menlo Security Email Isolation.

Email is the most popular attack vector, yet it remains the most vulnerable link in the enterprise.

Benefits:

- Safeguard against users entering critical user credentials into web forms
- Identify the users who are clicking on potentially risky links and causing the most risk to the organization
- Deliver configurable, real-time warning messages that offer additional corporate phishing-awareness training
- Set policies that allow users to download safe or original document attachments
- Automatically scan allowable original documents in a cloud-based, anti-virus sandbox environment—even password-protected ZIP files
- Integrate with existing mail server infrastructure without impacting user experience or existing workflows

Traditional Security Solutions Fail to Protect

Email continues to be the most popular and successful attack vector for cybercriminals to distribute malware. Traditional email security solutions rely on a sandbox to make a "good" versus "bad" determination based on internal and third-party threat intelligence feeds. However, most email attacks today are highly-targeted to a small group or a single individual—leaving no reputational footprint that makes detection possible in the future.

The result? A detection only approach fails to protect users and organizations from these types of attacks.

Menlo Security Email Isolation

Menlo Security uses isolation to prevent threat actors from delivering malware to users' endpoints through malicious links or email attachments. Integrated directly in the Menlo Cloud Isolation Gateway, Menlo Security Email Isolation relies on a block or isolate approach where known malicious links and attachments are automatically blocked while all others are isolated—even those links and attachments that are deemed safe. This zero trust strategy ensures that no malicious content originating from email is able to access users' endpoints.

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 web content and email attachments are routed through the Menlo Cloud Isolation Gateway (MCIG), giving malware no viable path to reach the user's device—an industry first not offered by any email protection service.

Email Links

Rather than determine which links in an email are legitimate and which are not, Menlo isolates all web content through the Isolation Gateway—eliminating the need to make an allow-or-block determination based on coarse categorization. Instead, the fetch and execute commands are conducted in the cloud far away from users' browsers.

Administrators can set customized policies in Menlo that render web pages and forms as read only—preventing users from accidentally exposing their credentials. Analytics also provide valuable insight into the users most susceptible to phishing attacks, and configurable, real-time messages can be used as teachable moments and enhance anti-phishing training.

96%

Percent of social engineering attacks launched via email

—Verizon 2018 Data Breach Report

Email Attachments

When users open a received email and click on an attachment, the document can be immediately viewed with 100 percent safety in isolation—and Menlo does this, 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's Zero Trust Approach

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 email-based cyberattacks. Rather than rely on a detection-only approach, organizations should integrate email isolation directly in their SWG solution. This would ensure that all web content and documents originating from email--whether it is deemed risky or not—is kept far from users' endpoint devices. This zero trust strategy is the only way to protect users and the organization from web-based attacks without impacting the browsing and email experience.

To find out how Menlo Security solutions can protect your organization, contact us at ask@menlosecurity.com.

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