Menlo Security

Data Sheet

Email Link Isolation

Stop email-based attacks in their tracks before a user clicks on a malicious link.

Getting users to click on a malicious link embedded in an email is a tried-and-true tactic used by cybercriminals to gain access to critical business systems. Yet, traditional security solutions fail to identify, much less block, email-based attacks. The answer? Menlo Security Email Link Isolation.

Detect and Respond Fails to Protect Users from Malicious Email Links

Traditional legacy security solutions that rely solely on detect-and-respond tactics have failed to keep up with the evolving nature of sophisticated email attacks. These solutions analyze web links in an email and make a "good" versus "bad" determination. However, attacks today target specific individuals within an organization, and the email link is usually unique, as is the target user. Therefore, no third-party reputation data is available, nor is there enough data to analyze internally to make an accurate determination. If the determination is incorrect, the first targeted "patient-zero" individuals are sent directly to a site where credentials can be stolen or malware can be downloaded. A single error can facilitate a costly and damaging cyberattack.

Clearly, a new approach is needed.

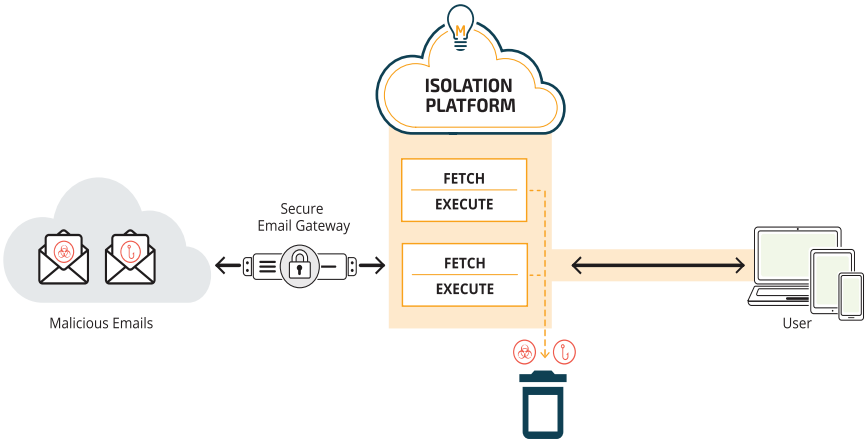
Menlo Security Email Link Isolation

Rather than determining which links in an email are legitimate and which are not, organizations should just assume that all web content is risky and hosts potentially malicious content. The resulting zero-trust approach eliminates the need to make an allow-or-block determination based on coarse categorization. Instead, Menlo renders all web content—including email links and attachments—in read-only mode, preventing any malicious content from ever reaching users' devices, where it can do real damage.

Today's Email Link Security Landscape

- Threat actors use email to deliver web links to users that, when clicked, download malicious content onto their device.
- From there, cybercriminals can gain access to the corporate network and critical business systems, where they can do a lot of damage.
- Links can be spoofed or contain similar branding to that of a legitimate, trusted site.

By opening all email links in safe isolation sessions, MSIP protects every user against targeted spearphishing and drive-by exploits, thus eliminating "patient-zero" infections.



With Menlo, web content is fetched and executed in the Menlo Security Isolation Platform (MSIP) in the cloud instead of on users' browsers. Menlo efficiently delivers only safe and authorized content to end-user browsers, with no impact on email or browsing experience. There are no new email systems or browsers to learn or software to install.

Menlo Security—Email Link Isolation Key Features and Benefits

100% Protection from Malicious Email Links

Feature	Benefits
Read-Only Mode	• Safeguards against users entering critical user credentials into web forms on isolated websites. • Alleviates the threat of credential theft. • Policy can be assigned by user, group, etc.
Visibility into User Behavior	• Allows administrators to determine which users are clicking on potentially risky links, causing the most risk to the organization.
Teachable Moments	• Provides configurable, real-time warning messages for users that offer additional corporate phishing-awareness training.

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS (M) SDN BHD (72640-P)
Infinite Centre, Lot 1, Jalan 13/6, 46200 Petaling Jaya, Selangor, Malaysia.

Contact Us:
Sales & Marketing: +603-7801 2611 marketing.1@konicaminolta.com
Technical Support: National Service Contact Center: 1-300-Call-KM (2255-56)