Menlo Security

BRIEF

Email Isolation for Financial Services and Insurance Institutions

Menlo Security Internet Isolation Gateway protects FSI users from phishing attacks.

Benefits:

- Users are protected from email-based attacks, including malware, credential theft, and ransomware
- No impact on the user's email performance and experience
- Integrates with existing email infrastructure—including Microsoft Exchange, Gmail, and Office 365
- No special email clients or plug-ins to install

Financial services and insurance institutions (FSIs) are tempting targets for phishing attacks. Attackers can easily spin up an authentic-looking email with a fake logo and entice an unsuspecting FSI employee to click on a link. At the same time, the potential financial payout from a successful attack on an FSI firm can be enormous. Unfortunately, the problem isn't going to be resolved without fundamentally rethinking how FSIs protect users from email-based attacks.

Traditional Email Security Solutions Fall Short

Despite deploying an array of email security products including anti-spam, anti-virus, data security, and encryption, FSIs and their employees—and even customers—continue to be severely impacted by phishing. Phishing attacks on FSIs range from pinpoint, surgical spearphishing attacks targeting specific executives with personally crafted emails to broader phishing attacks directed at more vulnerable departments, all using social engineering. These attacks often result in credential theft and the installation of malware and ransomware.

Legacy email security products deployed by FSIs rely on a good versus bad determination provided by third-party data feeds or internally via large-scale email traffic and data analysis. Because spearphishing attacks target specific individuals within an FSI, the email link is usually unique, as is the target user. Therefore, no third-party reputation data is available, nor is there enough data for internal analysis to make an accurate good versus bad determination. And if the determination is incorrect, the first targeted "patient zero" individuals are sent directly to a website where their credentials can be stolen, malware can be downloaded, or a ransomware attack can be launched. A single false negative—as well as a single employee or contractor clicking on a link embedded in an email—can initiate a string of costly and damaging cyberattacks.

Attackers are much more clever when launching attacks on FSIs. Increasingly, targeted spearphishing or broader phishing attacks are a smokescreen for a more dangerous cyberattack. Avoiding or quickly alleviating the camouflaged phishing attack can help stop the more insidious cyberattack.

Email isolation directs email links and attachments through a cloud-based isolation environment where an isolate versus block determination can be made—effectively cutting malware off from any access to the endpoint.

The Solution: Menlo Security Email Isolation

Email isolation avoids the complexity involved in distinguishing between legitimate and malicious emails and content. Isolation inserts a secure, trusted execution environment, or isolation platform, between the FSI's users and potential sources of attack. By executing user sessions away from the endpoint and delivering only safe rendering information, users are protected and their devices are insulated from malware and malicious activity.

Menlo Security's email isolation solution sits within the Menlo Security Internet Isolation Gateway and eliminates the credential theft, drive-by malware exploits, and ransomware instigated by email attacks. By integrating email isolation with an FSI's existing mail server infrastructure—such as Microsoft Exchange, Gmail, or Office 365—all email links can be directed to pass through a cloud-based isolation environment where an isolate versus block determination can be made. Malware has no avenue for accessing endpoints or the rest of the network.

Preserve Users' Native Email Experience

With the Menlo Security Internet Isolation Gateway, deployment is streamlined, requiring no changes to existing email platforms or the user's experience. When users click on an email link, they are 100 percent isolated from all malware threats, including ransomware. As cyberattackers are becoming more sophisticated in their phishing methods, Menlo's solution also ensures that zero-day and emerging phishing techniques are stopped. Websites opened from links within emails may also be rendered in read-only mode, preventing users from entering critical credentials or sensitive information into malicious web forms.

With users safely isolated, administrators can monitor behavior statistics and customize time-of-click messages to help reinforce anti-phishing awareness training in real time. Administrators can also define workflow policies for groups or individuals to determine if or when read-only mode may be relaxed. With zero dependency on error-prone threat detection methods, such as data analytics, Menlo Security Email Isolation is the only email security solution that protects every FSI user's email the instant it's deployed.

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