



Fortune 50 Global Investment Firm

Investment banking leader serves millions of customers worldwide, resulting in tens of billions of dollars in annual transactions.

Challenges

- Existing email security solutions weren't stopping targeted spearphishing attacks
- Resulted in ongoing credential theft and malware exploits
- Once they gain access to endpoints, cybercriminals are able to launch sophisticated network attacks

Solution

- Menlo Security Internet Isolation Gateway
- Integrated within existing email infrastructure
- All email links are isolated in the cloud, reducing phishing attacks

Fortune 50 Global Investment Firm Counters Phishing Threats with Menlo Email Isolation

Menlo Security Email Isolation closes the gaps in email security infrastructure.

Despite multiple security defense layers and many hours and dollars spent on end-user training, phishing continues to be one of the most effective attack vectors for cybercriminals. To combat email threats, a Fortune 50 global investment firm deployed multiple layers of security, each intended to address a specific part of the email security problem. Its architecture was similar to that used by many other large enterprises, combining cloud and on-premises versions of anti-spam, anti-virus, data security, encryption, and sandboxing solutions. Although these solutions are capable of defending against a broad variety of threats, they remain highly vulnerable to two of the most insidious attacks—spearphishing and drive-by malware exploits.

The security team for the large investment firm observed an increase in spearphishing attacks that targeted specific individuals within the organization. Unfortunately, legacy email security solutions weren't able to stop these attacks because they are largely based on reputation; that is, whether an email link is known to be "good" or "bad." Each email link was unique, providing no third-party reputation data for threat intelligence to detect or analyze internally to make an accurate determination. One false determination, and users were sent directly to a site where credentials were



Menlo provides protection from email-based malware embedded in links and attachments—including spearphishing and credential theft attacks—without impacting the user's native email experience.



attempted to be stolen or malware downloaded to the endpoint. The risk was simply too great, as a single error could facilitate a pervasive attack that would have cost billions of dollars in damage.

The investment firm knew that it had to rethink how it kept users safe from email-based attacks.

Menlo Security Internet Isolation Gateway Closes the Gap

Since the investment firm was already using the Menlo Security Internet Isolation Gateway to protect users from web-based threats, they discovered that Menlo could also isolate links and attachments in users' emails. Menlo Security worked closely with the firm to develop a scalable architecture that would support hundreds of thousands of users across the globe.

Any links originating from an email are now isolated and executed in the Menlo cloud, preventing malware from accessing the user's browser. At the same time, suspicious web forms are rendered as read only, preventing users from entering their credentials into a bogus sign-in page. With this unique approach, users can safely view sites with input field restrictions, while they are provided with information that helps them determine a site's legitimacy. This information is delivered via configurable messages that can provide additional corporate phishing awareness training.

The Result: 100% Protection from All Email Link- and Attachment-Based Attacks

By isolating all email links in the cloud away from users' devices, the Menlo Security Isolation Gateway closes the email security gap created by shortfalls in legacy solutions' detect-and-respond approach. Menlo provides protection from email link- and attachment-based malware, spearphishing, credential theft, and ransomware—without impacting the user's native email and browsing experience. Users can trust that any link in an email they click on—whether it is risky or not—will not result in an infection or stolen credentials.

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.

© 2019 Menlo Security, All Rights Reserved.

Contact us

menlosecurity.com

(650) 614-1705

ask@menlosecurity.com

