CUSTOMER CASE STUDY

MENLO SECURITY

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, antivirus, data security, encryption, and sandboxing solutions. Although these solutions can defend against a wide 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 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."

COMPANY

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

Implemented the Menlo Security Internet Isolation Gateway.

Integrated within existing email infrastructure.

All email links are isolated in the cloud, reducing phishing attacks.

*Because of confidentiality agreements, the names of personnel and the company remain anonymous in this case study.

> 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.

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 attempted to be stolen or malware downloaded to the endpoint. The risk was simply too great, as a single error might facilitate a pervasive attack that could 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 a 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 Percent 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.

Learn how Menlo Security is securing work. Visit menlosecurity.com or contact us at ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users as they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.

Learn more: https://www.menlosecurity.com

Contact us: ask@menlosecurity.com