Menlo Security
IT'S SAFE TO CLICK

CASE STUDY

Premier Asset Management

Premier Asset Management Adds Isolation to Protect Against Cyber Attack

Menlo Security's Isolation Platform helps to ensure that no web-based or email attacks get through a layered security approach

"Menlo Security's Isolation Platform is helping to protect us from web-based cyber attacks hitting our users or their inboxes. Our users' response to our Menlo Security installation has been very good from the moment it was deployed."

KEVIN STRANGE,
HEAD OF IT, PREMIER ASSET MANAGEMENT

Premier Asset Management is a UK retail asset management group wholly focused on asset management and client service. With £5.8 billion of assets under management (as of June 30, 2017), Premier Asset Management offers a broad range of investment solutions covering multi-asset, UK equity, global equity, absolute return, and fixed income strategies.

Challenges

Premier Asset Management juggles security and privacy of customer data and employee information with government and industry regulatory compliance. But, like many financial services organizations, ransomware and all forms of phishing, including spear phishing attacks, are major threat risks to the security of customer information.

Solution

After reading an article about Menlo Security and the Menlo Security Isolation Platform (MSIP), as well as reading a press release about a large deployment of MSIP at a Fortune 25 financial institution, Premier Asset Management decided to deploy Menlo Security's cloud-based Isolation Platform to address their ransomware and phishing threats.

Benefits

Even though Premier Asset Management was protected by leading email spam, phishing, and URL filtering solutions, Menlo Security's Isolation Platform helps to ensure that no web-based, email-delivered cyber attacks will get through their layered protection approach. This is accomplished without affecting the user experience or impacting the IT team.

"Good Enough" Security?

Today, there are many approaches and methods for an organization to defend itself against the daily onslaught of malware, phishing, ransomware, and other cyber attacks. There are traditional network perimeter products, such as firewalls. There are newer products that incorporate a variety of capabilities, such as next generation firewalls (NGFW). Then, there are the appliances and software that attempt to protect organizations from web-based cyber attacks; these include secure web gateways, URL filters, and unified threat management (UTM) products. Finally, there are products that address specific endpoint-related challenges, such as appliances and software for anti-virus, anti-malware, email security gateways, and more.

These products operate on a simple decision tree: Is the traffic, information, email, weblink, etc. 'good' or 'bad'? This decision process is engrained in most security products available today. And, while the 'good' or 'bad' decision has generally worked to protect against cyber attacks, it isn't foolproof. There is a need to ensure that the sources for the 'good' versus 'bad' decision are up-to-date. If the cyber attack is a zero day attack, the 'good' versus 'bad' may not catch it. There is also the issue of false positives, which can bring a security operations center (SOC) to its knees with false alerts, not to mention the false negatives which are even worse—as it means that an attack has gotten through the defenses.

Most cybersecurity providers will assert that their solutions will protect an organization, its users, endpoints, and customer information up to 99.9 percent of the time. But unfortunately, all the attackers need to succeed is that remaining 0.1 percent, and an organization's network, user endpoints, and—worst of all—customer information is at risk of being encrypted and ransomed, stolen and sold, or simply deleted.

Thus, the best approach for protecting organizations, users, and their endpoints from cyber attack is a layered approach, deploying and integrating solutions that will provide levels of security and which are best-in-class offerings in the cybersecurity areas they address.

Menlo Security Isolation Platform

With their primary focus on securing and keeping customer financial information private, Premier Asset Management took a layered approach to protecting their organization, users, and endpoints from cyber attack and intrusion. They had deployed solutions to address email spam, phishing, and web filtering. But emails with web links to malware-laden websites, as well as web-based documents loaded with malware exploits were somehow still infiltrating their network and ending up in employee inboxes. Something had to be done to address these active threats to the security of the company and its customers' information.

A new approach to security was needed.

Menlo Security's Isolation Platform doesn't use a 'good' versus 'bad' decision process. It ensures that any web page is stopped and re-rendered within its Isolation Platform, and that the user receives the same web page on their endpoint, with all links and videos interactive—except for any malware or other nefarious content that has been stopped and contained in the Isolation Platform, and will be destroyed in the cloud, far away from the user's endpoint once the user ends their web session. No jitter. No screen-scraping. No stutter. No latency.

The Solution for Premier Asset Management

To enhance their security capabilities, Premier Asset Management decided to deploy Menlo Security. To test out its capabilities and claims, Kevin Strange, Premier Asset Management's head of IT, tested the Menlo Security Isolation Platform against websites that were known to be bad and full of malware. The platform worked, allowing users to access the content on a web page, re-rendering the web page and its content to make it safe and secure from any malware or exploit before it was served and delivered to the user's endpoint device.

"Menlo Security's Isolation Platform is helping to protect us from web-based cyber attacks hitting our users or their inboxes. Our users' response to our Menlo Security installation has been very good from the moment it was deployed," said Mr. Strange. "We've seen no impact to the speed of web pages. I have no complaints, and neither do my users."

In addition, the Menlo Security Isolation Platform had no negative impacts on Mr. Strange's IT team. In fact, the Isolation Platform has helped raise the confidence level of the team, because of how the Menlo Security Isolation Platform is helping to protect customer information.

"[Premier Asset Management] is happy to have deployed Menlo Security's Isolation Platform. It is an important part of our security infrastructure," said Mr. Strange.

Menlo Security delivered Premier Asset Management increased peace of mind that they—and their customers' information—will be safe and protected from web-borne and email-based attacks.

2300 Geng Rd, Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1795
info@menlosecurity.com