Menlo Security

LEADING NONPROFIT HEALTHCARE ORGANIZATION ISOLATES MEDICAL PROFESSIONALS AND STAFF FROM WEB THREATS

CASE STUDY

OVERVIEW

Challenges

Faced with a rapidly evolving threat landscape, a complex network, and a decentralized management structure, a leading nonprofit healthcare organization (HCO) with tens of thousands of users was challenged to protect medical professionals and staff from mounting web threats. A single click on a compromised or malicious website could have resulted in a malware infection that would lead to the theft of millions of electronic healthcare records (EHRs), the value of which would surpass Social Security or credit card numbers if sold on the dark web.

Solution

The HCO adopted a new approach—web isolation—to prevent malware infection. Web isolation inserts a secure, trusted execution environment, or isolation platform, between the user and potential sources of attacks. By executing sessions away from a user's endpoint and delivering only safe rendering information to their devices, the isolation platform protects users from web malware.

Benefits

Even though the HCO was protected by leading email spam, phishing, and URL filtering solutions, Menlo Security's Isolation Platform helps ensure that no web-based cyberattacks will get through their layered security approach. This goal is accomplished without affecting user experience, and without negatively impacting the HCO's IT team.

CHALLENGES

Protecting a Diverse Set of Users and Locations

With more than 50,000 employees across six states, the HCO required a security solution that was not only secure, but also flexible and scalable enough to accommodate healthcare professionals such as doctors and traveling nurses, as well as business partners, vendors, facilities staff, and administrative personnel.

These individuals rely on the web not only to do their jobs, but also to manage their lives. Limiting their web access in the name of security had the potential to negatively impact morale in the midst of an industrywide shortage of physicians and nurses. HCOs regularly compete for talent, and ease of access to web and email can influence a professional's decision to work for a particular provider.

Given the HCO's sheer number of users, the organization could not deploy a product that had an adverse effect on productivity, increased help-desk tickets, required additional employee training, or gave employees an excuse to evade security measures altogether. In addition, because the deployment would need to cover six states, racking, stacking, configuring, and maintaining appliances was not an option.

“Good Enough” Security Was No Longer Good Enough

Today, organizations can use many approaches to defend itself against the daily onslaught of malware, phishing, ransomware, and other cyberattacks. There are network perimeter products, such as firewalls and next-generation firewalls (NGFW). There are also appliances and software that attempt to protect organizations from web-based cyberattacks, such as 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”? While the “good” or “bad” decision has generally worked to protect against cyberattacks, 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 cyberattack is a zero-day attack, the “good” versus “bad” approach may not be able to catch it or stop 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 because they indicate 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, users, endpoints, and—worst of all—customer information is at risk of being encrypted and ransomed, stolen and sold, or simply deleted. With this in mind, the HCO in this case study came to the conclusion that although the basics were still helping to prevent many attacks, they could not address all threats. A new approach was needed.

SOLUTION

The Solution: Isolation

Whatever solution the HCO would eventually deploy would need to meet three criteria:

- ➔ **Do we need it?**
- ➔ **Does it work in our environment?**
- ➔ **Can we afford it?**

The cloud-based Menlo Security Isolation Platform (MSIP) not only satisfied these criteria, but also provided a new level of security, by preventing malware from ever reaching user devices via compromised or malicious websites. The platform isolates all web content by opening it in a disposable virtual container in a public or private cloud, enabling users to safely interact with websites, links, and documents online without compromising security. Traditionally, attempts to use isolation technology to prevent malware suffered from several key limitations, such as the need to deploy and manage endpoint software and upsetting or changing the user's experience. Menlo Security's cloud-based Isolation Platform was selected because it is 100 percent effective, eliminates the need for client software, deploys within minutes, and can easily scale to provide comprehensive protection across organizations of any size, worldwide, without impacting user experience.

Happy Users Mean Happy IT

During the relatively quick rollout, the HCO's IT staff received positive feedback from users, and received no complaints. Even the IT administrators who were using the products remarked that they often forgot their web sessions were being isolated. This is because Menlo Security's patented Adaptive Clientless Rendering™ (ACR) maintains an entirely native user experience. Functions such as scrolling, copy and paste, right-click menus, streaming videos, and printing are all accessed the way they always have been, and work the way they should.

Menlo Security's patented Adaptive Clientless Rendering™ (ACR) maintains an entirely native user experience.

Problem Solved

The Menlo Security Isolation Platform solution has eliminated malware infections coming from uncategorized websites, and drastically reduced the probability that a breach will compromise the organization's electronic health records (EHR).

In addition to peace of mind, the HCO estimates that this solution will result in material savings in both dollars and staff costs for remediating infected endpoints and processing site categorization requests.

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Menlo Security's 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, and backed by General Catalyst, Sutter Hill Ventures, Engineering Capital, Osage University Partners, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Palo Alto, California.

2300 Geng Rd., Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1705
info@menlosecurity.com

menlosecurity.com