Menlo Security

CASE STUDY

Fortune 50 Bank Takes New Approach to Prevent Web Risks

Menlo Security Isolation Platform completely eliminates the most prevalent path of malware.

"Internal analysis showed that more than 60% of malware infections stemmed from visits to sites that our web security gateway was unable to classify as good or bad. Now that we route those connections through the Menlo Security Isolation Platform, we haven't seen any more incidents stemming from uncategorized sites. Menlo Security has eliminated a significant security risk, while saving us a material amount of money and time in our fight against malware."

CISO,
GLOBAL FINANCIAL SERVICES FIRM

Challenges

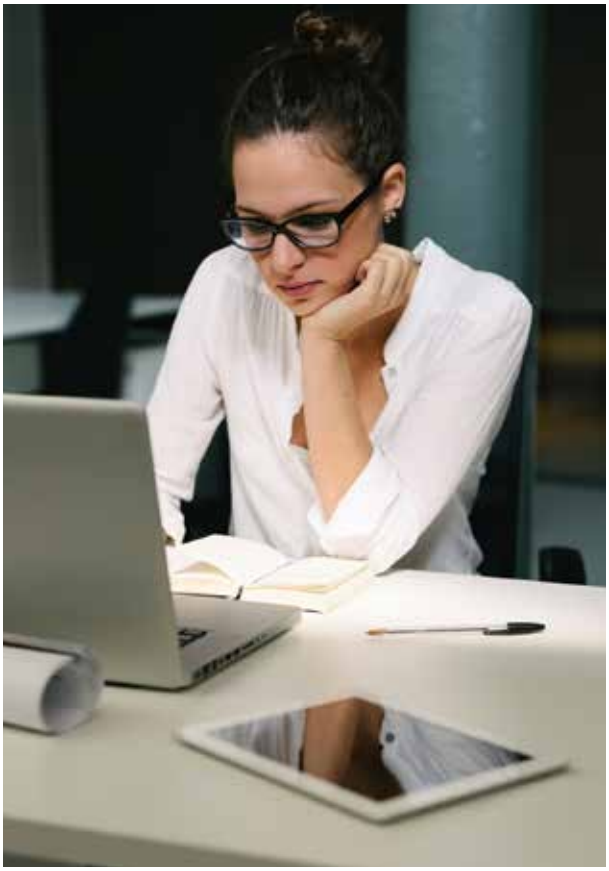
Even with a web security gateway and other security measures in place, the web remained the overwhelming source of malware infections. Blocking access to sites that were unclassified by the web security gateway resulted in reduced user productivity, as access to many of these sites was required for legitimate business needs.

Solution

Routing connections to uncategorized sites through the Menlo Security Isolation Platform isolates all active content and eliminates malware in the cloud. The user experience is unchanged, providing a completely safe experience without the need to deploy and update software to their endpoints.

Benefits

- Completely eliminated the most prevalent path of malware infection, dramatically improving the company's security capabilities
- Freed IT staff from reviewing access requests to business-critical web sites
- Eliminated the expenses tied to reclassifying web sites with their Secure Web Gateway vendor
- Empowered employees to do their jobs without impacting their user experience or requiring client software
- Solution scales to isolate e-mail links and attachments in future deployment phases



Protecting Assets and Users

With trillions of dollars in assets and operations worldwide, no one takes security more seriously. But the reality of easily compromised web servers and a seemingly unending stream of browser vulnerabilities have made the web the primary threat vector for malware infections. According to a recent report[1], 34% of the top one million websites are considered risky, with 20% running software that is vulnerable to attackers. These percentages escalate dramatically when you consider the vulnerabilities in the software run by third party contributors to sites such as ad networks.

To keep malware out of its networks, the firm deployed a sophisticated layered security solution. A web security gateway provided website categorization; desktop antivirus detected suspicious downloads to endpoints; and a sandbox firewall product added another layer of malware detection.

Frustrated by the declining efficacy of their existing products, they performed an in-house analysis that unearthed an interesting data point. Security administrators found that over 60% of malware infections at the company emanated from uncategorized websites. Uncategorized sites (sites that don't fall into any category for which a security policy applied) can be a security issue because many malware sites are quickly shuttered when discovered, only to re-emerge hours later under a new name. These new sites are unknown and thus uncategorized. However, there are also many legitimate business sites that do not generate broad amounts of web traffic that are also uncategorized.

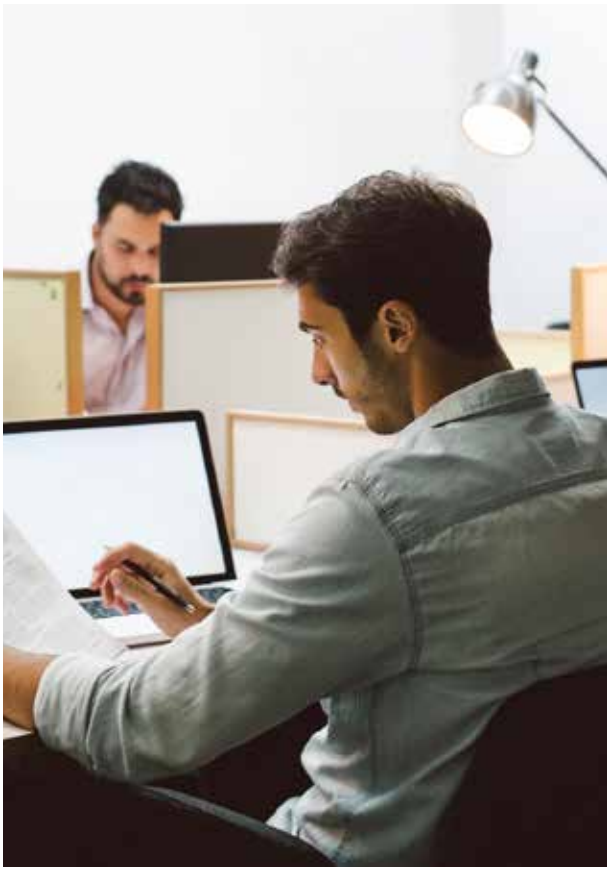
A natural response to this finding was to block access to all uncategorized sites. This blocked the malware vector, but also blocked legitimate sites. The resulting storm of user complaints led to thousands of requests to the security team each day from users seeking access to sites that were relevant to their business, but now blocked by the secure web gateway. The customer needed an efficient way to limit its exposure to threats from websites containing malware, and to reduce the costs and headaches associated with remediation. The need to find a better solution became imperative.

[1]State of the Web 2015: Vulnerability Report: https://www.menlosecurity.com/news-events-press-release-march-24-2015

A New Approach to Solving the Malware Problem

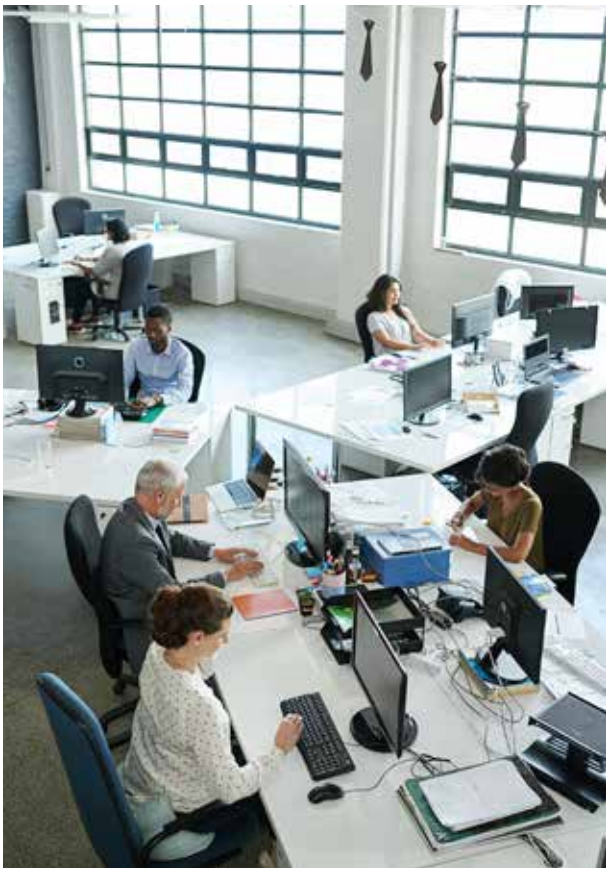
The financial services firm considered many alternatives for restoring broader web access, including purchasing separate devices for viewing uncategorized sites; however, the management of these devices would present yet another round of support problems. Fortunately, they discovered that Menlo Security has taken an entirely different approach to securing end users from the threat of malware.

The Menlo Security Isolation Platform (MSIP) provides a new level of security that prevents malware from ever reaching user devices via compromised or malicious websites. The platform isolates all web content by running it in a disposable virtual container in the cloud (public or private), 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 interference with the user's experience. Menlo Security's Isolation platform was selected because it eliminates the need for client software, deploys within minutes and can easily scale to provide comprehensive protection across organizations of any size without impacting user experience.



Deploying a Technology in a Globally Distributed Enterprise

Once Menlo Security's solution was selected, Menlo Security worked with the financial services firm on a scalable architecture to support a truly global enterprise. In the new architecture, when a user tries to access an uncategorized web site, the Secure Web Gateway notifies the user with a warning that the site is uncategorized and that the resulting connection will flow through the Menlo Security Isolation Platform. The web session is handled



by the MSIP and executed in a disposable virtual container in the data center for completely secure access to the site, with the user endpoint receiving a real time rendering of the resulting content.

Further integration with the organization's infrastructure includes Syslog messages and SNMP information sharing from the MSIP to the appropriate collectors and NMS on the customer side. The isolation platform is also connected to the firm's user directory service, to validate that the user is in a role with a legitimate business need to connect to these sites. In order to scale this design to users around the world, the MSIP is run in conjunction with a multi-tier load balancing solution that distributes traffic across global data centers complete with multi-geo and multi-data center redundancy.

Problem Solved

The Menlo Security Isolation Platform solution has completely eliminated malware infections coming from uncategorized web sites, and the flood of requests for access to uncategorized sites has slowed to a very manageable trickle. The company 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

934 Santa Cruz Avenue
Menlo Park, CA 94025
Tel: 650 614 1795
info@menlosecurity.com

menlosecurity.com