Menlo Security

M1: COMMUNICATIONS

A New Approach to Web Malware and Phishing Problems

CASE STUDY

OVERVIEW

Introduction

M1 is Singapore's most vibrant and dynamic communications company, providing mobile and fixed services to more than 2 million customers. M1 was the first operator to offer nationwide 4G service to Singapore, and ultra-high-speed fixed broadband, fixed voice, and other services on the Next Generation Nationwide Broadband Network (NGNBN). With its continual focus on network quality, customer service, value, and innovation, M1 links anyone and anything, anytime, anywhere. M1 is publicly listed on the Singapore Exchange Limited (SGX).

Challenges

Like many businesses, M1 employees receive training to recognize and react to phishing, malware, and ransomware attacks. With a constantly evolving threat landscape, though, training can only reduce cybersecurity risks, but never eliminate them.

Solution

After learning about the Menlo Security Isolation Platform (MSIP), M1 worked together with Menlo Security on a short Proof of Concept (PoC) before adopting the solution to provide end-user cyber-security protection.

Benefits

- Since deploying Menlo Security's Isolation Platform, M1 has enjoyed a reduction in pressure and demands regarding updates and patching, lower remediation requirements, and decreasing cost.
- By supplying borderless endpoint protection for their users' web access, M1 has enjoyed greater peace of mind and enhanced security from web-borne malware attacks, including drive-by attacks and watering-hole attacks.
- Users are now able to access all websites, regardless of whether they are categorized or uncategorized, with the assurance that they will not be the catalyst for a devastating attack on their company.
- Peace of mind, through 100 percent web security. That's what Menlo Security delivers.

CHALLENGES

Defenses Must Be Right Every Time

Employee security training can be helpful in engaging employees and users to identify potential cybersecurity threats—especially phishing and spear-phishing emails—before they can be unleashed. But, in today's fast-paced workplace, all it takes is a single, well-crafted, well-thought-out email, with the appropriate amount of social engineering to breed a sense of familiarity, aimed at an employee or a user who is tired, stressed, or overworked, and an attack begins.

Most security products deployed today rely on detection and response. They use a simple decision tree and comparison to determine whether web traffic, emails, attachments, downloads, links, and more are "good" or "bad." But a "good versus bad" determination is not foolproof. The sources for any comparison made to determine whether something or someone is good or bad need to be kept updated almost to the second. A security solution that uses detection and response may not be able to capture and stop a zero-day attack, for example, because the source for comparison hasn't been updated with the latest data. While many detect-and-respond solutions can trace back and remediate the attack, the attack has already happened; information, data, and time have been lost; and costs to remedy the incident have increased.

SOLUTION

Menlo Security Isolation Platform

A new approach to cybersecurity, providing peace of mind, is needed.

Menlo Security's Isolation Platform does not use a "good" versus "bad" decision process. It simply ensures that any web page is stopped and re-rendered in the Isolation Platform. A user receives the same web page on their device that they did before MSIP was implemented, with all links and videos interactive—except any malware or other dangerous content is stopped and contained in the Isolation Platform. The user experience is preserved, without jitter, stutter, or latency.

A New Approach to Web Malware and Phishing Problems

After viewing a demonstration of the Menlo Security Isolation Platform, M1 understood the benefits of isolation, and how it would help manage potential gaps in their cybersecurity infrastructure. After a successful PoC trial, M1 saw firsthand the feasibility of isolation in preventing threats.

> "Menlo Security's innovative solution provides practical security protections for user Internet access, without sacrificing convenience. As a cloud service, it was deployed and has been easy to maintain. The platform has decreased our remediation needs, while reducing patch pressure."
>
> **ALAN GOH, CHIEF INFORMATION OFFICER**

M1 is using the Menlo Security Isolation Platform to isolate all web traffic. With isolation, M1 users can access the Internet safely, as any malware or malicious content on any website is stopped and contained in the isolation platform, and cannot do any harm to a user's device or browser.

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