MENLO SECURITY

M1: Communications

A new approach to web malware and phishing threats.

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 Secure Enterprise Browser solution, M1 worked together with Menlo Security on a short Proof of Concept (PoC) before adopting the solution to provide end-user cybersecurity protection.

Benefits

- Since deploying the Menlo Security Enterprise Browser solution, 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 reliable, scalable browser 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 to launch an attack is a single, well-crafted, well-thought-out email. With the appropriate amount of social engineering to breed a sense of familiarity and aimed at an employee or a user who is tired, stressed, or overworked, an attack can succeed.

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 systems 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 Enterprise Browser solution

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

The Menlo Secure Cloud Browser does not use a “good” versus “bad” decision process. It simply ensures that any web page is stopped and re-rendered by the Menlo Cloud. A user receives the same web page on their device that they did before cloud browsing was deployed, with all links and videos interactive—but any malware or other dangerous content is blocked by the Menlo Cloud. The user experience is preserved, without jitter, stutter, or latency.

A new approach to web malware and phishing threats.

After viewing a demonstration of the Menlo Security Enterprise Browser solution, M1 understood the benefits of browser 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 users’ 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 Secure Cloud Browser 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 Menlo Cloud and cannot do any harm to a user’s device or browser.

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

MENLO SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
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 while 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.