

CASE STUDY

JAPAN POST HOLDINGS

Japan Post Holdings is the largest corporation in the country in terms of employees and total assets.

Challenges

- Attacks from compromised websites posed a serious, persistent security threat
- URL and content filtering was not sufficiently secure and disrupted end-user access to the Internet
- Alternative solutions required massive investment in hardware, software, or both and complicated the end-user experience

Solution

- The Menlo Security Cloud Platform powered by an Isolation Core™ allows access to the entire Internet while eliminating malware threats
- Centralized visibility and control of all Internet traffic for all users

Japan Post Holdings Implements Internet Isolation to Eliminate Web-Based Attacks

Largest corporation in Japan achieves 100% malware protection without impacting end-user experience or convenience

Founded nearly 150 years ago, Japan Post Holdings owns and operates Japan Post, Japan Post Bank, and Japan Post Insurance and is the largest corporation in the country in terms of employees and total assets. Its size, importance to the country's economy, role in the lives of the Japanese people, and diversity of customer-facing services make Japan Post Holdings an enticing target for cyberattacks.

The Japan Pension Service experienced a massive cyberattack in 2015 when an employee unknowingly opened a virus-laced email attachment. The attackers were able to steal the data of 1.25 million people, the largest successful attack in Japan. After the attack, the Ministry of Internal Affairs and Communication created the Internet Isolation Guideline for businesses. Japan Post Holdings began to adopt the guidelines, which required the company to separate their enterprise network from the public web while providing their employees with Internet access to perform their duties.

Japan Post Holdings's cybersecurity strategy focused on three key areas: email attachments or external devices, data theft or loss, and web-based attacks on the Internet. Though solutions for email attachments and data loss prevention have made tremendous progress in the industry, Japan Post Holdings did not



The biggest benefit is that we have improved security and usability at the same time.

Takuro Yoshida,

Information Security Office,

Group IT Management Department



have a good solution for web-based attacks. At the time, the company was relying on URL filtering and blocking to limit access to bad sites, while allowing access to good sites, by using whitelists or blacklists. The problem with this approach is that many legitimate sites are actually categorized as risky or worse, and known good sites can be compromised with malware. Users who were following the company's policies and exercising extreme caution could have their devices get infected anyway, through no fault of their own.

"We're particularly focused on preventing attacks that use email attachments, external devices such as USB memory sticks, and Internet-based watering-hole attacks to infect user systems," said Tsutomu Shomura, executive officer of the company's Information Security office. "We felt that we had good protection against email and external media attacks, but our defenses against watering-hole attacks were based on an allow-or-block approach using web content filters and blacklists. We felt this approach was too disruptive to user productivity, while not providing 100 percent total protection."

Internet Isolation with Menlo Security Improves Security and Usability

Japan Post Holdings considered various methods, such as physically separating devices for the Internet and those for internal operations, as well as using Virtual Desktop Infrastructure (VDI) to enable applications to be operated from different locations. Both of these solutions were ruled out because they require extensive hardware and software to be purchased, installed, and maintained. Users would also have to be trained and adjust the way they do their jobs, which would be a massive training exercise for Japan Post Holdings to undertake.

Physically separating devices would double the number of devices as well as the associated costs and desk space. In addition, installing additional tools on existing devices would prove to be cost-prohibitive, as the devices are geographically distributed across the country and regular updates and maintenance would be costly. VDI could also potentially require network upgrades, which would further increase costs.

The Menlo Security Cloud Platform solution did not have the shortcomings of VDI or physical separation. After rigorous testing and evaluation, Japan Post Holdings selected the Menlo Security solution because it is delivered as a SaaS service and provided 100 percent protection against web-based malware attacks. "We improved security and usability at the same time." said Takuro Yoshida from Information Security Office.

Secure Cloud Transformation with the Menlo Security Cloud Platform

Japan Post Holdings understands that SaaS services provide many benefits, and they view Menlo Security as part of a broader strategy that allows them to achieve Secure Cloud Transformation, which includes the following:

- 100 percent malware protection and autoscaling with growth in the number of users, devices, and applications
- Secure direct-to-Internet architecture without limits and no change to the end-user experience
- Centralized security controls and visibility for data protection

The Menlo Security Cloud Platform is the only solution in the industry with an Isolation Core™, and it was built in the cloud for the cloud. The global cloud is built on a native cloud architecture that allows enterprises to access the Internet safely and adopt SaaS applications securely, without having to worry about greater traffic volumes or network issues.

NTT Communications worked with Japan Post Holdings and Menlo Security to roll out the new solution in less than six months, despite this project being the largest Internet Isolation project ever implemented in Japan. The deployment included hundreds of thousands of employees and endpoints.

Shomura added, “NTT Com was constantly communicating with Menlo Security headquarters in the U.S., which provided a very smooth deployment. Typically with other providers, deployments of this size might take several years. However, NTT Com had detailed knowledge of our network and got everyone working very quickly. Menlo Security is an outstanding product, and we believe other Japanese corporations should also implement it.”

Internet Isolation with the Menlo Security Cloud Platform has resulted in 100 percent malware-free web browsing for Japan Post Holdings users across the entire organization. Most importantly, Internet Isolation does not impact the user experience and requires no additional browsers or plug-ins to be installed on devices—and users don’t have to worry about whether they should click on links in an email or on the web. The improvement of services to end users at a low cost enabled by cloud technology means Japan Post Holdings has begun to realize the benefits of Secure Cloud Transformation.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

© 2020 Menlo Security, All Rights Reserved.



Menlo Security is an outstanding product, and we believe other Japanese corporations should also implement it.

Tsutomu Shomura

Executive Officer
IT Systems Division



Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com

