Menlo Security

BRIEF

Secure Remote Internet Access for Financial Services Institutions

Fortify your workforce for remote working.

Benefits:

- Prevent phishing attacks with read-only mode
- Prevent web-based ransom and malware attacks
- Deploy protection to very large deployments quickly

The Era of Remote Working

Global business deals, the need for local representation, and years of investment in cloud security have all contributed to a world where working inside a physical office is no longer a necessity for many occupations.

Financial services institutions (FSIs) have been particularly quick in cloud-based and remote-working solutions, with more than 35 percent of its security applications already delivered via the cloud in 2020 (CyberEdge).

All of these factors have created a work environment for FSIs in which employees connect to the corporate network from outside the safety of a central firewall and thereby become a target for cyberattacks.

Cyberattacks against Financial Services Institutions Are Adapting

Cybercriminals attack FSIs using ransomware for the same reason bank robbers have attacked financial institutions for generations—their unique ability to pay. Often, many FSIs decide it's easier to quietly pay off the criminal than to incur greater harm to the reputation of the company and lose customer confidence. New technology and work practices will not change the threat environment inherent to FSIs as a business category.

The ability of FSI employees to work remotely only increases the threat of attack in the digital age. In 2020, FSI employees experienced a 38 percent increase in attacks when many were pushed out of the office because of the global health emergency (Financial Stability Institute Brief). Credential theft is on the rise because remote workers may fail to check with coworkers or their IT department when interacting with suspicious content, as they once did when they worked in the office.

In addition, because employees have adapted to working outside the office, they are less likely to want to return. Analysts predict that up to 30 percent of employees will work remotely on a permanent basis after 2021 (Deloitte). When combined with the desire for greater convenience, the security issues of remote working will likely only increase with time.

Secure Your Remote Workforce against Cybercrime with Isolation

A cloud proxy with isolation enables admins to provide security against credential theft as well as ease of connectivity.

- Isolation enhances the security of a cloud proxy by sanitizing incoming web code against malware and blocking phishing attempts by placing suspicious web pages into read-only mode.
- Globally available cloud proxies enable remote working by allowing users to connect to the network from wherever they are.

For financial services, both tools enable companies of all sizes to enjoy the convenience and productivity benefits of remote working without the risk of compromise through the web and email.

FSIs Are Concerned about Fast Deployments

Security teams also worry about the speed of deploying new technologies because of the large number of global and remote users who need to be secured.

Any security solution should be effective and deliver on its protective promises. However, effectiveness is not the only metric that security professionals care about. As FSIs look to new platforms to combat cybercrime, their security teams also worry about the speed of deploying new technologies because of the large number of global and remote users who need to be secured.

Implementing new technologies is costly. Assuming a successful test, deployment rollouts might last months or years for thousands or millions of users. Time spent testing then becomes a SOC manager's most valuable resource. Learning new UIs and APIs and configuring quarks can be significant time sinks that create barriers for organizations' willingness to try new technologies.

To reduce the time required to jumpstart new security deployments like isolation, we created some handy guides to help security teams configure their deployment with the latest in isolation best practices.

To find out how Menlo Security can help you protect your remote working environment, contact us at ask@menlosecurity.

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 Menlo Security Cloud 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.

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