Zero Trust is the foundation for securing fiserv and fintech

How to protect cyberthreats and unlock productivity

eBook

MENLO SECURITY

Contents

Few industries have changed as dramatically as financial services (fiserv) in the last decade. Banking and financial transactions were once an exclusively in-person process; now customers regularly conduct their financial affairs digitally, and employees of fiserv companies increasingly rely on websites and cloud and SaaS apps, as opposed to the walled gardens of the past. Bad actors know that the reward is high if they can steal data or assets from a financial firm; in fact, the Ponemon Institute's most recent Annual Cost of Cybercrime report[1] finds financial services saw the highest cybercrime costs among all industries studied, over $18B USD and rising year over year.

These hacks cast doubt on the security and reliability of financial services and fintech firms overall. But the security tools and strategies these businesses have typically turned to over the years are no longer enough to stand up to today's threats. Current security methods and tools are reactive focusing too much on perimeter security when many threats are often already within the network. As businesses become more innovative, so do criminals. Phishing, ransomware and other malicious code are all constant threats to productive employees who simply want to get their jobs done.

In this ebook, we will look at the factors behind current security risks in fiserv and fintech, and how security leaders can tackle them effectively.

The European Systemic Risk Board[2] estimated the cost of cyberattacks worldwide at somewhere between **$45B and $654B USD**. The president of the European Central Bank raised concerns[3] that attacks targeting multiple banks could trigger a financial crisis.

1 https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
2 https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html
3 https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html

SECTION 1

The visibility and trust barrier in fintech

There are a number of elements that combine to create a challenging security and risk environment in financial organizations today.

Remote work makes the attack surface even larger

The new, largely remote environment created a perfect storm for security; one survey[4] found that nearly a quarter of security pros said cybersecurity incidents at their organization have increased since transitioning to remote work – with some tracking as many as double the number of incidents.

Supporting – and securing – a work-from-anywhere model also meant new risks, as security teams have less visibility into teleworkers' systems and home WiFi and video conferencing platforms can be considerably less secure than an organization's onsite network. Bring your own device (BYOD) policies had to adapt as well, yet securing personal devices was not part of the original security strategy for many financial organizations, leaving them vulnerable at first.

Most security tools fail to address the underlying issue here: for malware, spyware and ransomware to impact the organization, there needs to be a direct connection from website to networked device.

Fraud attempts skyrocket in finance

In fintech and financial services, the often transactional nature of what employees do means productivity cannot be interrupted – and trust needs to be a given.

Unfortunately, in the weeks following the start of the pandemic, criminals found new ways to exploit the increased reliance on digital payments and communication. Overall, according to Advisen, the combined Finance and Insurance sectors were hit with 25 percent of COVID-19-related cyber events. Financial institutions of all kinds also saw increased fraud related to stimulus funds, wire transfers and phishing attempts, while payment firms, insurance companies and credit unions were most impacted by hacking attempts.

4 https://blog.isc2.org/isc2_blog/2020/04/survey-covid-19-response-sees-nearly-50-of-cybersecurity-workers-reassigned-to-it-tasks.html

SECTION 2

Factors at play: Disruptors and security challenges

As the events of the last year unfolded, one thing became clear: the future of finance, banking and fintech is digital, and so is how work gets done within these organizations.

Financial institutions are increasingly moving applications to the cloud and embracing hybrid cloud infrastructure, refactoring applications and more freely sharing data between departments and partners.

A rapid adoption of SaaS[5] is occurring, introducing numerous issues. In 2017, only 38 percent of companies were operating on mostly SaaS. But now, research shows that a majority of organizations (68 percent) operate on mostly or all SaaS. Yet speed and productivity are often impacted by barriers to online and cloud-based information.

Also with this move to the cloud and Software as a Service (SaaS) solutions, security and regulatory compliance become a concern: synchronizing regulations[6] throughout regions adds an extra burden, particularly within APAC, where financial operations are closely integrated across borders; bad actors could seize opportunities to exploit different security standards that could then impact a large part of the world economy.

5 https://www.blissfully.com/saas-trends/2020-annual-report/
6 https://www.csis.org/analysis/financial-sector-cybersecurity-requirements-asia-pacific-region

This layering of new systems into infrastructure makes an organization more vulnerable to new threats and also introduces new compliance concerns, as it creates visibility challenges. Teams are often uncertain if their applications and data management are in compliance with current regulatory demands.

But the security tools and strategies these businesses have typically turned to over the years are no longer enough to stand up to today's infrastructure demands and an ever increasing threat landscape. Endpoint protection, enterprise antivirus, intrusion detection and other technologies fail to fully protect applications, data, customers and employees, as these tools are reactive, often only notifying security teams of threats that fit known profiles or generating false alarms in response to any unusual activity.

Fintech and financial services teams need solutions that can prevent attacks from reaching the network perimeter in the first place.

State-sponsored and organized crime attacks can not only disrupt financial operations[7] but are responsible for the theft of billions of dollars. Since 2016, North Korea alone has been behind the loss of approximately **$2B USD from 38 countries**.

7 https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

SECTION 3

Common attack vectors in fiserv and fintech

Web use by employees in the financial space is a double-edged sword. While it's a vital source for research and news, the web also exposes users to malicious code. There are multiple challenges that need to be managed when it comes to protecting employees' web usage.

Increased web access increases risk of malware

Employees in fintech need to perform any number of online tasks that come with inherent risks. Even well-known sites that appear to be safe may, in fact, be compromised. If a security strategy relies on blacklisting and whitelisting to block known threats, it impacts productivity, as employees are delayed or prevented from accessing content they need to do their jobs.

Phishing can bait workers into trouble

Another common attack conduit is phishing — fraudulent emails in which criminals try to trick unsuspecting users into clicking a link to an infected site or downloading a malicious attachment. For users of SaaS office applications, it may seem like these files are safe, since they come from the cloud environment. But, in most cases, there is still a live connection to the user's device, which means the potential exists for malware to be downloaded. The Verizon Data Breach Investigations Report[8] finds 25 percent of breaches involved phishing — and 22 percent involved human error.

Mobile security Is a moving target

Mobile security is a top concern in financial services and fintech because so much now takes place on smartphones, tablets and laptops. Most workers routinely access the web, as well as corporate data from smartphones, and that has grown amid the ongoing remote work trend.

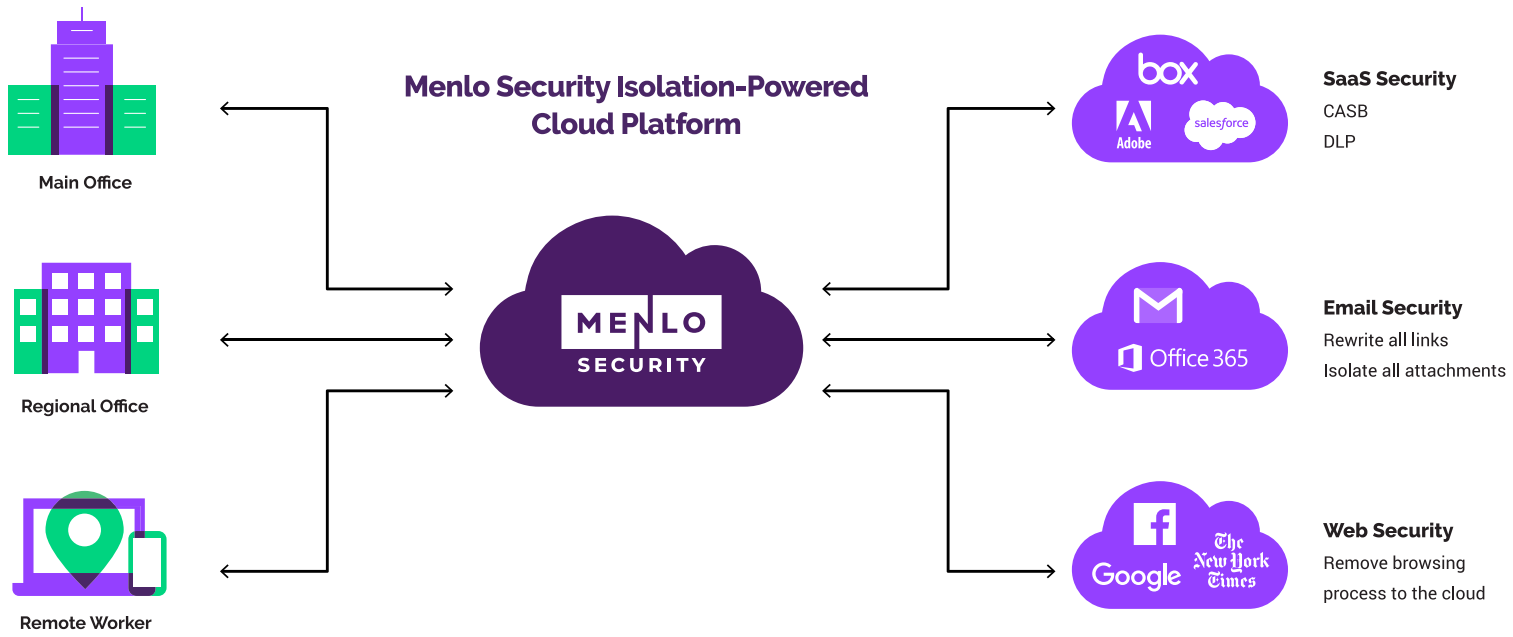
8 https://enterprise.verizon.com/resources/reports/dbir/

SECTION 4

Enabling Zero Trust through isolation

A security strategy that relies on stopping attacks at the perimeter won't stop a phishing email, won't protect employees from a drive-by download attack on the web, and won't protect them from multiple other types of web-based exploits while they work remotely. Traditional "detect and respond" approaches fail to provide the safety that users and businesses need. Prevention stops attacks before they start, whereas detection and response means it is already too late.

The answer is an approach that keeps malicious code from ever reaching the network perimeter — one that relies on isolation-powered cloud security and Secure Access Service Edge (SASE)-based solutions.



Using this approach, organizations can address productivity issues by opening up access to SaaS apps and websites without restriction. Isolating all web content, including sites, videos and documents, in a remote browser mitigates this risk by creating a virtual air gap between the user and malicious content on the Internet — effectively shutting off access to endpoint devices. Organizations no longer need to block employees from visiting sites to maintain their security posture.

But in order to do this effectively usability and scalability are key. An isolation-by-default approach eliminates malware without impacting user productivity. It is also essential to ensure that your isolation strategy can scale and meet the massive scalability required by SASE deployments so that cloud security can be assured with new deployments.

Built for the remote workforce

Employees logging in from outside the corporate firewall (an everyday occurrence these days) need reliable, secure Internet access that, unlike VPNs, won't impact performance or degrade the native browsing experience. The demands of work now require an architecture that can offer optimal, secure performance, regardless of where a user connects.

The Menlo Security Secure Web Gateway, powered by an Isolation Core™, provides a ubiquitous security layer in the cloud through which all web traffic flows, including email links and attachments. It's here where security policies can be applied, ensuring enforcement regardless of whether the user is at the office, home or a public cafe.

The cloud-based Isolation Platform quickly scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software. The service deploys quickly, reduces SOC tickets, and optimizes the end-user's browser experience and reduces the burden on IT and security teams through fewer false positives and help desk requests and greater control.

Menlo Security protects financial services and fintech organizations from cyberattacks by eliminating the threat of malicious code from the web, downloaded documents, and email. Menlo provides a secure Zero Trust approach to preventing malicious attacks, making security invisible to end users while they work online. This also removes the operational burden for security teams as they innovate quickly and respond to dynamic customer demands. At the same time, it preserves a native web-browsing and SaaS app experience for users, which means employees can stay focused on critical tasks.

Isolation powers security and productivity

Menlo Security's isolation-powered platform provides fast, secure Zero Trust access to cloud-based applications and websites without impacting the user experience.

Features:

- 100% Malware and Phishing Protection: Eliminate malware, ransomware, phishing and zero-day attacks.
- Makes online work your safe space: Managed solutions for web, email and SaaS protection.
- Fast Deployment: 100% cloud-based solution with no hardware or software to purchase or deploy.
- Global Elastic Cloud: Auto-scaling architecture to add users and devices instantly from anywhere in the world.

Benefits:

- 100% malware-free web browsing for remote workers.
- 100% protection from ransomware and phishing for Office 365/G Suite users.
- Consistent security protection for all users across any device.
- Fast direct-to-Internet connectivity with no need to backhaul web traffic.

Learn how you can eliminate web-based cyberattacks and dramatically decrease your attack profile.

Visit menlosecurity.com or contact ask@menlosecurity.com

MENLO SECURITY