Akamai

WHITE PAPER

Financial Services and Post-Pandemic Cybersecurity

Introduction

The shift toward remote work and virtual customer engagement fueled digitalization and changed the cybersecurity landscape in financial services. Faced with an abrupt need to rethink existing business models, financial institutions accelerated digital transformation efforts to streamline approval and compliance processes, with a heavier reliance on automation, all while committed to providing personalized, secure digital experiences to their customers. The need has never been greater for simple and creative solutions to reduce risks, meet compliance requirements, and safely embrace new technologies.

> "Trying to outpace evolving cyberthreats diverts resources from a financial firm's core business"

Financial institutions continue to be lucrative targets for threat actors. The threats are becoming more complex, whether from nation-state actors — who are highly trained, motivated, and resourced — or financially motivated cybercriminals, it has never been more important to understand your attack surfaces and risk exposures to help you devise mitigation plans. As stated in a report from the Financial Services Information Sharing and Analysis Center (FS-ISAC), "Trying to outpace evolving cyberthreats diverts resources from a financial firm's core business." [1]

Also, financial institutions have validated this trend by reporting that losses due to operational disruption and losses in customer trust are more financially damaging than losses due to regulatory fines.[2]

> "The modern CISO needs to focus on an expanding attack surface created by digital transformation initiatives. Demand for technologies and services such as cloud security, application security, ZTNA, and threat intelligence has been rising to tackle new vulnerabilities and risks arising from this exposure."
>
> — Ruggero Contu, senior director analyst at Gartner

1 FS-ISAC, "Navigating Cyber," 2021

2 Deloitte and FS-ISAC, Cybersecurity Benchmarking Analysis, 2019

Unique security challenges

As they seek to achieve security at scale, financial institutions face challenges in five key areas:

Third-party access: The rapid growth of remote work has increased the challenges that financial institutions face in securing their ecosystem. There was an almost overnight transition from one managed network to managing hundreds of networks, depending on the size of your remote staff. Additionally, financial institutions are often reliant on a network of partners, service providers, and data providers. They need the means to isolate, protect, and enforce third-party access routes, while limiting access only to approved applications, systems, and environments — all without sacrificing flexibility. Attackers frequently exploit weak third-party connections, including access through IoT devices, to gain access to a bank's network and start moving laterally.

> Attackers frequently exploit weak third-party connections to gain access to a bank's network

Cost reduction: According to Accenture,[3] while the per-company cost of cybercrime is over $18 million for financial services, investments in security intelligence and threat sharing technologies, for example, have an estimated annual return on investment of 22.5%.

> About 15 different agencies impose cybersecurity requirements on banks

In a recent Deloitte survey,[4] 33% of respondents said the biggest impacts of cyber incidents or breaches were revenue losses and regulatory fines.

Cybersecurity compliance: Financial institutions are regulated by at least 15 different agencies that impose cybersecurity requirements on federal, state, and local levels. Recent years have seen several high-profile cases in which criminals have compromised electronic funds transfer and payment systems, not by penetrating those systems themselves, but by gaining access through the client bank's network. Therefore, third-party core banking service providers often include specific cybersecurity requirements in their contracts. Banks must figure out how to efficiently address these requirements and regulations.

> Regulatory and compliance requirements are, at once, a significant challenge for the financial sector and the single most important reason that consumers trust the industry with their money.

Cloud migration and new technologies: Financial institutions are looking to reduce their IT footprint and gain operational efficiency by moving their operational workloads to the cloud, often combining on-premises data centers with private or public clouds. They are further looking to create a differentiated digital customer experience with cutting-edge technologies. In fact, a McKinsey analysis found that Fortune 500 financial institutions alone could generate as much as $60 billion to $80 billion in run-rate EBITDA in 2030 by

3 Accenture, "Unlocking the Value of Improved Cybersecurity Protection," 2019
4 Deloitte, "2021 Future of Cyber Survey"

making the most of the cost-optimization levers and business use cases unlocked by cloud.[5] Banks must be aware of, and take measures to mitigate, the security risks that accompany new technology adoption.

> **Within 24 hours, exploitation of zero-days reach multiple thousands of attacks per hour**

Breach mitigation: It's no surprise that financial institutions are prime targets for cybercriminals, who are looking not only for easy money but also for the wealth of private information that customers entrust to their banks. Perimeter defenses are essential, but unfortunately, breaches have become business as usual. In fact, the financial services industry consistently ranks in the top three targeted verticals for web application and API, zero-day, and DDoS attacks.[6] Phishing is the most common breach vector leading to a financial institution's network being compromised with malware or ransomware, or to confidential information being leaked. An attack that begins with an employee clicking a link in a phishing email can end up with the business suffering significant financial and reputational damages. As the modern perimeter becomes harder to define and defend in a hybrid infrastructure, financial institutions need to take measures to mitigate the impact of breaches by preventing intruders' lateral movement and ringfencing their critical assets.

> **"The five most efficient cyber defenders are anticipation, education, detection, reaction, and resilience. Do remember: Cybersecurity is much more than an IT topic."**
>
> **— Global Head, Information Security, multinational financial services company**

5 McKinsey, "Cloud's trillion-dollar prize is up for grabs," 2021
6 Akamai, "Enemy at the Gates: Analyzing Attacks on Financial Services," 2022

The common theme running through these challenges is the need to separately secure critical application workloads and many of their third-party-provided applications and infrastructure — commonly referred to as segmentation. It allows financial institutions to achieve security at scale by addressing several key requirements, while still moving at the speed their business demands.

Visibility and segmentation address key challenges in financial services

Secure cloud adoption: Lack of visibility into network traffic and digital assets can make the move to the cloud virtually impossible. As a starting point in the digital transformation journey, financial institutions need to have an accurate inventory and map of all their core and critical applications, their dependencies, and the network traffic they generate. This visibility will provide a foundation for the ringfencing controls to allow seamless migration of the applications into the cloud, along with their security policies.

Protecting third party access: Third-party outsourcing or software provider traffic needs to be properly routed, usually through a "jump-box" in the DMZ to a single termination point within the data center, and restricted from traveling across the bank's network. This is essential to prevent attackers from "landing and expanding" through a third party's compromised system.

Isolating money transfer and payments systems from general IT: Providers of electronic funds transfer and payment systems, notably the Federal Reserve's FedLine service, typically demand strict separation of their services from the institution's general IT environment. Segmentation enables bank IT teams to set boundaries around the service provider's "zone" and prevent unauthorized access.

Reducing risk by limiting lateral movement: Providers of electronic funds transfer and payment systems, notably the Federal Reserve's FedLine service, typically demand strict separation of their services from the institution's general IT environment. Segmentation enables bank IT teams to set boundaries around the service provider's "zone" and prevent unauthorized access.

Addressing compliance and cyber regulation: Segmentation gives banks an efficient way to comply with the vendor requirements and cybersecurity regulations from multiple agencies. Accompanied by deeper visibility with a single pane of glass, it allows them to demonstrate that they are taking effective measures to secure critical assets, mitigate fraud risk, and protect customer privacy.

Where conventional segmentation approaches fall short, and where software-defined segmentation succeeds

If segmentation answers many of the challenges facing financial institutions, why hasn't it been more widely embraced and deployed? Many CISOs at smaller institutions are hesitant to pursue segmentation initiatives, citing that they take too long and require multiple teams and resources. This hesitancy is understandable. Traditional methods of achieving segmentation are both complicated and time-consuming. For example, configuring VLANs, ACLs, and firewalls across multiple locations and environments is a laborious, slow, and error-prone process. If workloads extend into the cloud, the process is complicated significantly. Placing a firewall at every data egress point is cost-prohibitive, and further management challenges arise with the complex networking configurations required to route traffic and place firewalls in virtual environments.

Organizations are further stymied by a lack of visibility into east-west traffic, making it difficult to identify intersegment dependencies and create segmentation policies. Even using traffic taps or similar technologies, the resulting view likely lacks the context and sophisticated translations between IPs and ports required for effective segmentation. In dynamic environments, such as platform as a service (PaaS), it's all but impossible.

> Traditional methods of achieving segmentation are both complicated and time-consuming

A different approach

In recent years, software-defined segmentation has emerged as a more flexible, streamlined, and cost-effective approach to application-level security — one that dramatically accelerates implementation, simplifies ongoing maintenance, and is ultimately more effective in mitigating threats. A leading example of this methodology is Akamai Guardicore Segmentation. Akamai takes the concept of segmentation to a very granular level, enabling the creation of security policies

around individual or logically grouped applications, regardless of where they reside in the hybrid data center. These policies dictate which applications can and cannot communicate with each other — true Zero Trust at the application level.

> **Segmentation with Akamai allows for protection of applications, threat detection, and prevention of lateral spread of attacks**

Besides protecting applications from malicious access, software-defined segmentation with Akamai has the additional benefit of threat detection and preventing the lateral spread of attacks. Any attempt at unauthorized communication is an instant indicator of the likely presence of a threat.

To affect this level of segmentation, Akamai provides a visual map of all applications running in the data center and the dependencies among them. Operators can then create and enforce network and individual process-level security policies to isolate and segment critical applications and assets. With a software-defined overlay approach, it is independent of the underlying infrastructure and protects workloads that span on-premises facilities, legacy systems, VMs, containers, and clouds.

This simplifies and accelerates segmentation efforts by:

- Detecting and interpreting workload dependencies automatically at the process level, with additional identity and domain name granularity
- Enforcing one consistent policy expression as applications migrate across heterogeneous environments with zero changes to infrastructure
- Avoiding application modifications and production downtime through a software-defined overlay approach
- Future-proofing policies with platform-independent contextual traffic visibility and segmentation
- Ensuring and continuously validating compliance with real-time and historical traffic visibility

Case study: Speeding the transition to hybrid cloud

A financial institution located in the midwestern U.S. was looking to securely adopt hybrid cloud while strengthening controls over third-party access and ringfencing critical applications and systems. With limited IT resources, they were looking for a solution that would allow them to accomplish these objectives with minimal impact on their infrastructure and resources while providing maximum cyber-risk reduction.

The project specifically targeted the bank's digital "crown jewels": 10 critical applications requiring ringfencing and preparation for migration. In addition, they needed to completely isolate the FedLine environment from the general IT infrastructure, in line with the requirements of the Federal Reserve Bank, the provider of the FedLine Services.

With Akamai, the team was able to:

Gain granular visibility into east-west traffic, with a "single pane of glass" view of all applications and assets regardless of their location and environment

Compliant with FIDO2 to ensure that user credentials are decentralized, isolated, and encrypted on users' personal devices, which is particularly important in fending off phishing attacks

Able to verify users via their smartphone without relying on a physical key

Inventory all applications and their dependencies quickly and accurately

Migrate applications between environments without creating service disruptions

Implement a unified security standard across the hybrid infrastructure

> "Akamai has provided us with the fastest and most elegant path to application segmentation while delivering the added benefit of breach detection for lateral traffic."
>
> — Chief Information Technology Officer, Midsize Regional U.S. Bank

Akamai helped this midsize financial institution become cloud-ready without putting extra stress on their limited IT resources and without any impact on the underlying infrastructure.

Had the IT and security teams chosen to take the VLAN or firewalling route, they estimated the project would have taken a full team 18 months, without any gain in visibility or third-party access restrictions. With Akamai, they completed all of the project's objectives in two months with only one information architect. More importantly, the bank was able to start reaping the benefits of the cloud and operational cost savings more quickly.