AMERICAN BANKER

Sponsored by Akamai

WHITE PAPER

# Better Visibility Is the Key to Better Cybersecurity Protection

Safeguarding financial services enterprise data requires enhanced insight and awareness

Cybersecurity threats remain a critical concern for financial services leaders. Their defensive measures must simultaneously deal with the latest threats and an evolving regulatory landscape, while minimizing impact on the customer experience. It's no surprise that financial institutions (FIs) face significant challenges meeting their cybersecurity protection and compliance goals.

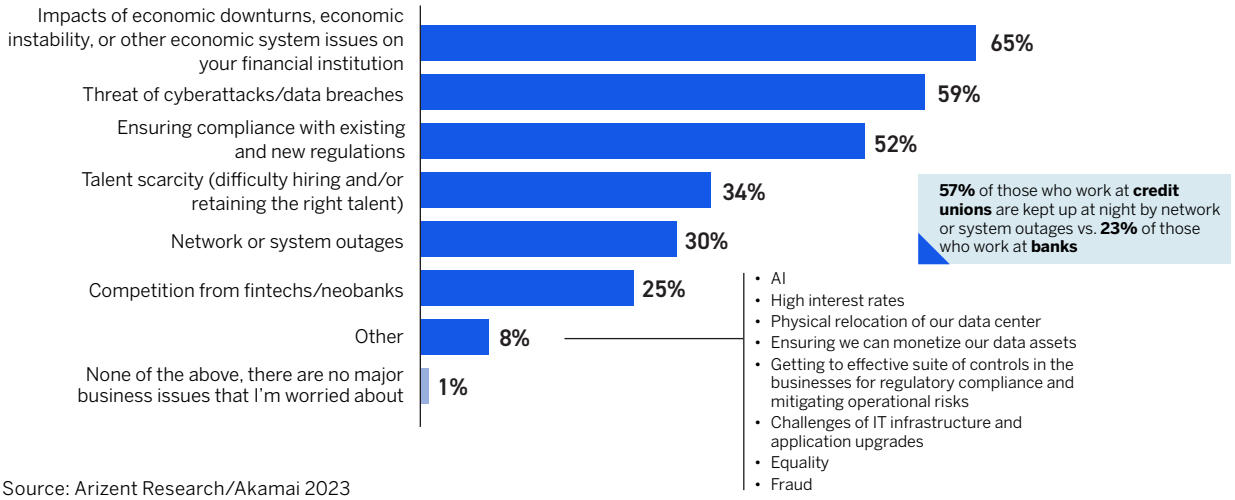
In November 2023, Arizent, parent company of American Banker, surveyed 102 financial services leaders to explore how they understand current cybersecurity threats and what actions they are taking to protect themselves while ensuring regulatory compliance. The results suggest a lack of visibility across their entire networks may hamper their ability to identify and adapt to ever more sophisticated cybersecurity threats.

## Cyberattacks remain a persistent threat

Financial services leaders remain heavily focused on cyberthreats. Data breaches and attacks from cybercriminals are among the top three business problems these executives face (see Figure 1). Half of these leaders also see ensuring compliance with existing and new regulations as a major challenge. As FIs increasingly rely on a growing array of supply chain vendors, the regulatory burden of due diligence and fraud protection is poised to become even greater.

### Figure 1: Cyberattacks remain a top business concern

What are the top three business problems that are keeping you up at night?




Source: Arizent Research/Akamai 2023

Complexity across multiple dimensions makes it challenging for FIs to implement and maintain their cybersecurity protection and mitigation strategies. More than 4 in 10 cite difficulties in each of these areas:

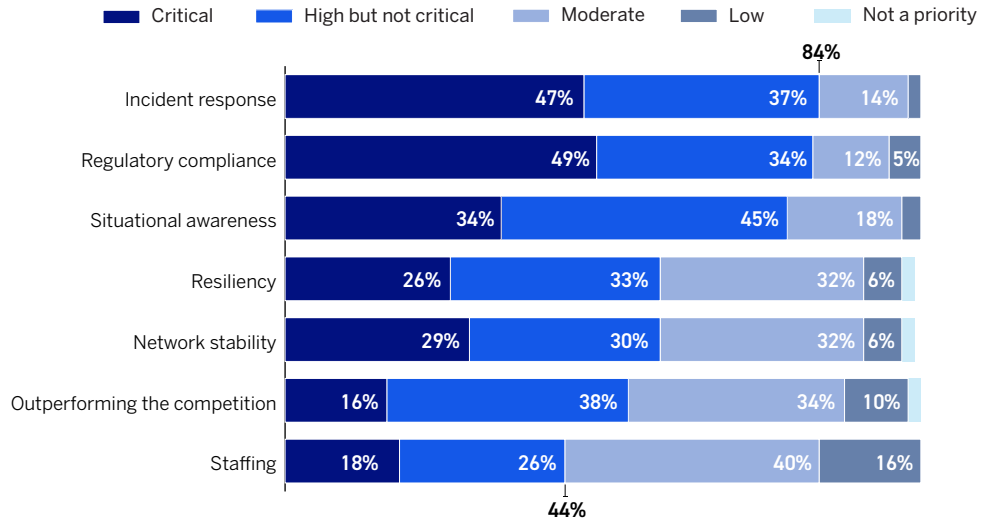
- Responding to regulatory complexity (44%)
- Effectively managing the number of security systems they have in place (43%)
- Integrating technology platforms with legacy systems (42%)
- Managing conflicting priorities within the institution (41%)

## Incident response is a high priority

As they manage through these complexities, incident response and regulatory compliance top the list of most FIs' goals in 2024 (see Figure 2).

### Figure 2: Incident response and regulatory compliance are top goals in 2024

Thinking about your institution's cybersecurity and network infrastructure, to what extent are the following a priority for your organization in the coming year?




Source: Arizent Research/Akamai 2023

More than three in four FIs consider incident response (84%), regulatory compliance (83%) and situational awareness (77%) critical or high priorities this year. Rapid changes in the threat and regulatory environments make the urgency around incident response and regulatory compliance easy to understand. The lack of situational awareness suggests a deeper problem, however.

The better that FIs can see and analyze what's going on across both their own and their partners' networks, the better their ability to respond effectively when threats do occur. But nearly 7 in 10 banks (69%) lack a centralized, real-time dashboard for tracking their security systems.

## You can't protect what you can't see

The inability to view their security systems in one place is a symptom of a broader problem: FIs lack full visibility across their networks and systems. For example, 89% of FIs face one or more security issues related to the application programming interfaces (APIs) they have in place to connect their systems. This is a particularly dangerous situation, as APIs can give threat actors an entry point to an FI's network.

Because APIs create links across an FI's cyber footprint, any network or system that an organization can't monitor represents a potential threat. These types of threats only stand to grow as attacks get more complex and sophisticated. The pandemic-era acceleration of remote work expanded the number of API-driven products FIs use. The expanded digital supply chain that gives FIs access to a variety of valuable services also broadens the potential attack surface for threat actors.

> **"For financial institutions, cybersecurity situational awareness demands vigilant, comprehensive monitoring of network traffic beyond traditional boundaries."**
>
> **— Steve Winterfeld**, Advisory CISO at Akamai

In this environment, cybercriminals have also become increasingly savvy about where and how they enter networks. Strategies that prevent attacks from outside the network may not be able to identify cybercriminals who breach systems in one area (e.g., via an unmonitored API) to gain access to sensitive information in some other system. Microsegmentation can help mitigate these types of attacks, but it can't detect them. Monitoring traffic across the entire network can.

"For financial institutions, cybersecurity situational awareness demands vigilant, comprehensive monitoring of network traffic beyond traditional boundaries," says Steve Winterfeld, Advisory CISO at Akamai. "Safeguarding both institutions and customers requires a holistic approach, observing data flows across diverse environments, from data centers to the cloud and third-party SaaS providers, transcending network perimeters."

## The power of visibility

Having visibility into network traffic can help detect and prevent cyberattacks in a number of ways. Firms that can detect activity across all of their APIs can more easily detect and disable potential vulnerabilities. The ability to see traffic patterns also means FIs can proactively defend themselves against attacks seen in other regions. By matching current network activity against attack patterns identified elsewhere in the world, banks can identify potential warning signs of an impending attack before it takes place.

This level of visibility can help FIs manage their compliance landscape as well. Regulators base their decisions in part on global data. Learning from and implementing tools to protect against known attack vectors can help demonstrate resilience to regulators — an increasingly important component of compliance in a world where breaches are almost inevitable. These capabilities also help banks prepare for new regulatory requirements that get built out in response to successful attacks.

Without visibility into the broader threat landscape and experience with the current regulatory landscape, this type of resilience is impossible to achieve. For most organizations, amassing these capabilities would be prohibitively resource-intensive without an experienced partner. Cybersecurity partners with access to global data and experience with a wide range of third-party providers can help FIs gain a comprehensive view of their security posture, detect potential security holes, and mitigate issues proactively. This knowledge and experience can also ensure banks adopt best practices and effective processes as early as possible — ideally before a breach happens.

Partners should also be able to help FIs achieve full visibility of their own networks, as well as the vendors and services with which they interact. That visibility should extend to all the APIs that feed an FI's network. Partners should also be able to offer a level of visibility that goes beyond the network's entry points so that they can help detect and identify suspicious traffic patterns within FIs' networks. This information can also be used to fortify FIs' networks against lateral attacks through microsegmentation.

Ultimately, full visibility across networks should allow partners to help FIs defend against the widest possible range of vectors, including those that require real-time detection and mitigation, such as distributed denial-of-service attacks.

Working with industry consortiums like FS-ISAC can give FIs additional insight about current regulatory concerns and potential regulatory updates. By keeping a finger on the pulse of the regulatory agencies, these types of partners can help FIs identify and deploy solutions in line with evolving industry best practices. In other words, the right partner can help an FI address its most pressing priorities simultaneously with helping FIs achieve the situational awareness necessary to bolster their incident response and resilience, as well as making it easier to keep up with regulatory changes.

"Trust, business insights, adaptability, and shared accountability form the bedrock of a strong security posture," says Winterfeld. "An experienced partner, leveraging global intelligence, is crucial for financial institutions to successfully navigate the complexities of the ever-evolving threat landscape."

## Methodology

In November 2023, Arizent, parent company of American Banker, surveyed 102 banking leaders to explore how they understand current cybersecurity threats and what actions they are taking to protect themselves while ensuring regulatory compliance. To qualify, respondents must work at a bank or credit union with at least $1 billion in assets and have at least a management-level role in a business area related to the research.


## About Akamai

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible.

Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn.


## About Arizent Research

Arizent delivers actionable insights through full-service research solutions that tap into their first-party data, industry SMEs, and highly engaged communities across banking, payments, mortgage, insurance, municipal finance, accounting, HR/employee benefits, and wealth management. They have leading brands in financial services including American Banker, The Bond Buyer, Financial Planning, and National Mortgage News, and in professional services, such as Accounting Today, Employee Benefit News, and Digital Insurance.

For more information, please visit arizent.com.

Published 02/24.