4 Keys to Cloud Security for Financial Services

How to Secure Customer Data and Build Trust

4 Keys to Cloud Security for Financial Services

Increasing compliance and risk management requirements, coupled with a disproportionate amount of cyberattacks, are creating a need for more robust security defenses.

As the financial services industry embraces digitization, cloud applications, and new ways to engage customers, criminals are capitalizing with more innovative attacks. Fraud, account takeover, spear phishing, compromised credentials, ransomware, and sophisticated malware are driving an increase in data breaches.

This ebook offers practical advice for financial organizations looking to securely embrace the cloud while maintaining customer trust and the availability of business processes and services.

Financial industry cyberattacks cost more than the cross-industry average

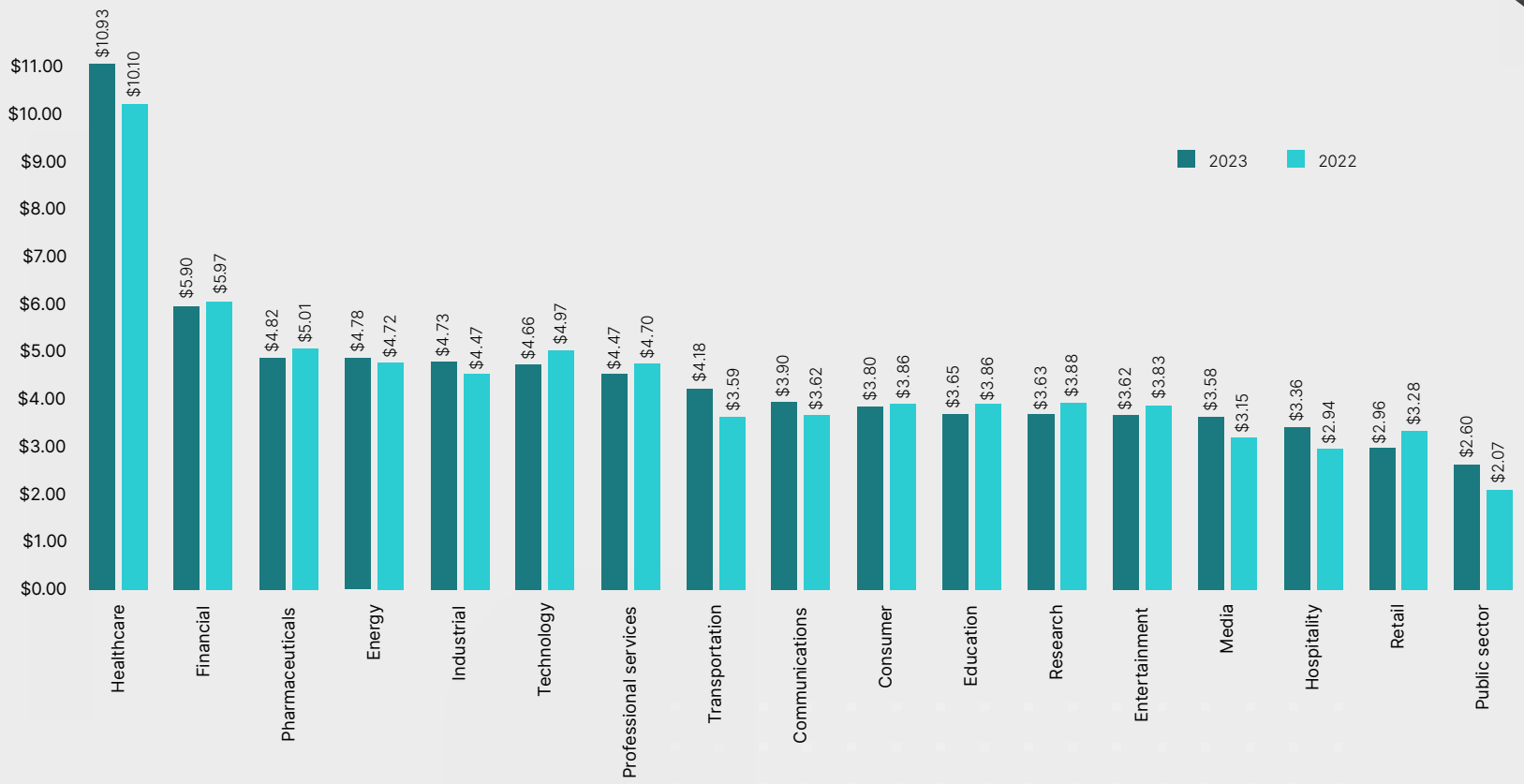
$4.45M

Global average total cost of a data breach across all industries[1]

$5.9M

Global average total cost of a data breach within financial services[2]

Cost of a data breach by industry (Measured in USD millions)[3]



A Prime Target for Cybercrime

The proliferation of connected networks and devices spanning multiple platforms provides an ideal attack vector for cybercriminals to go unnoticed. With online banking, personal financial management tools, and the benefits of big data on global markets, hackers take advantage of organizations that fail to continuously monitor their users, data, and cloud infrastructure. Adding to the lure is the dark web and the abundance of accessible financial data to capitalize on.

Top attack vectors for cybercrime

Phishing

Phishing was the most prevalent attack vector (16%) of all initial attack vectors.[4]
Attackers trick organizations or consumers into handing over sensitive information to penetrate networks, impersonate, or defraud.

Compromised credentials

The second largest attack vector involved stolen or compromised credentials, with 15% of all initial attack vectors.[5]
Over the last few years, the market for valid credentials has grown. Here, attackers buy and sell personal and business credentials used for cyberattacks.

Cloud misconfigurations

Cloud misconfigurations, a relatively new attack vector, ranks third, with 11% of initial attack vectors.[6]
As more companies move and sometimes rush to the cloud, attackers know that security is often forgotten and access to misconfigured cloud services is quick and easy.

The Fragility of Customer Trust

For financial services companies, the most crucial asset stolen by cybercriminals isn't data—it's customer trust.

Much like healthcare, finance is an industry where companies deal with livelihoods. Mishandling this heavy responsibility can have an immense negative impact on a business. The only other sector that surpassed financial was, unsurprisingly, healthcare (40%). The next closest sector to the two was food and beverage, with less than 10% of the votes.[7]

Three large consulting firms recently sponsored independent research around trust and finance. And each research firm seemed to land on two interconnected truths: in finance, 1) trust is difficult to earn, but 2) trust is easy to break.

Trust is difficult to earn

- **Thirty percent** of American consumers stated trust was the primary factor when considering a financial institution.[7]

- **Eighty-seven percent** of consumers said their trust in financial institutions hinged on their ability to secure personal data.[8] Similarly, according to Ernst & Young, the biggest driver of financial trust is confidence in securing customer data.[9] This is the unanimous top driver across all age groups when choosing among 14 other drivers.

Trust is easy to break

- **Sixty-six percent** of consumers said they would stop using a financial institution if a data breach affected their data.[10]

- **Twenty-one percent** of consumers verified that they have stopped using a financial service on account of a data breach.[11]

CYBER RISK INSTITUTE

Develop a baseline cybersecurity profile specifically for financial institutions of all sizes, based on the NIST cybersecurity framework. Learn more about the Cyber Risk Profile at cyberriskinstitute.org.

Finance Being Held to Account

In the past, financial service companies may have been tempted to withhold data breach information from consumers. However, because the mishandling of financial data can drastically impact customers, many international governments now require disclosure of cyber incidents within days of their occurrence.

For example, in the United States, the Presidential Policy Directive on Critical Infrastructure Security and Resilience recognized the financial services industry as critical infrastructure. Now, U.S.-based financial institutions face even more stringent cybersecurity requirements, including notifying their regulator of record within 36 hours after an incident has been identified. These entities must also notify each affected banking organization customer when it determines a computer-security incident has caused, or is reasonably likely to cause, a service disruption lasting four or more hours.

Similarly, the NIS 2 regulations in Europe have named "banking" and "financial market infrastructures" two high-criticality sectors. The regulation states that companies must take proactive steps to minimize disruption. They must also disclose incidents or cyberthreats to the national authority within 24 hours, followed by an official public-facing notification within 72 hours. Offenders of these policies could suffer fines of either €10 million or 2% of global annual turnover (whichever is higher).

4 Keys to Financial Cybersecurity

In financial services, there's a lot at stake. But there are ways to keep your cloud security in check. You can reduce risk by improving your visibility and can detect and isolate attackers with enhanced threat detection methods. Exploited vulnerabilities can be fixed, but it's even better if you identify and address these problems during development, not production, to save time and money and reduce friction between security and DevOps teams.

Luckily, there are some practical steps you can take to ensure that your data—and your consumers' data, by extension—remains protected. These steps range from solutions that can be implemented as soon as you close this ebook to others that may require some time and effort to deploy.

- **Get Risks Under Control**, Including the "Human Element"
- **Improve Detection** to Find Threats Faster
- **Consolidate and Automate** to Increase Efficiency
- **Make compliance** a continuous effort

Read on to learn how.

Get Risks Under Control, Including the "Human Element"

To reduce exposure and improve efficiency, you must continually monitor your cloud infrastructure and applications, find weak spots, and prevent mistakes from being deployed into production. You must gain complete visibility into what is running, what has been added, how it is configured, and what workloads are doing to pinpoint and prioritize the most critical vulnerabilities and misconfigurations to remediate.

But risk reduction efforts extend beyond the technology itself. According to Verizon, 74% of breaches involve the use of stolen credentials, phishing, or simply an error—what it has labeled as "the human element."[12]

Financial services is arguably the perpetual leader in cyberattack frequency. These institutions should educate employees on the different ways attackers can successfully execute a phishing attack beyond suspicious emails. This is a practical tip you can act on starting tomorrow.

74%

of breaches involve using stolen credentials, phishing, or simply an error—what it has labeled as “the human element.”

Improve Detection to Find Threats Faster

Out with the old and in with the new. You can uncover threats within your dynamic cloud environment by leveraging anomaly detection and threat intelligence. These innovative detection methods enable you to gain rich context around each alert to quickly investigate and remediate threats, whether or not they're tied to known rules or signatures.

Historically, companies have focused on protecting their systems from known threats by using indicators of compromise. Unfortunately, this strategy depends on rules, on companies knowing exactly how they will be attacked, and on manually updating their cybersecurity defenses against those threats.

Rules-based security tools can't keep up with the cloud. Such tools take considerable time and effort to configure, implement, and fine-tune, especially when considering the size of a modern cloud environment. With the increasing technological complexity and the speed at which attackers can gain access to a company's network, internal teams struggle to even detect a breach.

Financial services institutions should consider cloud-native security solutions built specifically for the cloud. These tools often feature anomaly-based, rules-optional approaches to cybersecurity. Rather than manually inputting rules to detect threats and vulnerabilities, modern tools learn the ins and outs of a cloud environment and automatically surface anomalies—anything that looks out of the ordinary.

20%

Financial services is one of the most targeted industries in the world for cyberattacks, suffering nearly 20% of all attacks.[13]

Consolidate and Automate to Increase Efficiency

Efficient cloud security has never been more critical. But often, it may seem like cloud security "solutions" are just adding to the problem. As cloud adoption increased, security issues became clear. Every new problem has brought forth a new solution category. And, before we knew it, the cloud security solution marketplace was extremely fragmented, saturated, and confusing.

Unlike many modern organizations, the cloud is not full of siloes. Changes to data on one side of the cloud can have reverberating effects across the entire environment. Yet many cloud security tools focus on one specific area of the cloud—posture management, vulnerability management, workload security, and infrastructure security.

Efficient security can't involve piecing together data across tools. But, if cloud security was handled in one place, how would one make sense of all that data?

The future is the automated platform, ingesting data from across the environment into one place and then using automation to connect the dots and enrich context wherever possible. Investing in one automated tool to cover an entire cloud environment is a safe bet for financial institutions looking to safeguard data and maintain consumer trust.

46%

of respondents cited a greater need for automation as the most common barrier to combat fraud.[14]

Make Compliance a Continuous Effort

Technology is accelerating, yet governmental regulatory processes often lag behind. FFIEC IT, the Gramm-Leach-Bliley Act, NYDFS, GDPR, PCI, SOC 2, NIS 2, SEC guidance, and other regulations place pressure on financial services companies to build and enforce cyber risk management programs.

Violations of these guidelines can lead to possible financial losses, fines, or business delays. To reduce the risk of these challenges, make compliance a continuous effort rather than a moment-in-time activity. This can lead to increased revenue and consistent auditing cycles and can open doors to new market opportunities and faster deal cycles.

By investing in an automated compliance solution, you can continuously evaluate configurations against custom enterprise policies and industry best practices and readily maintain traceability of cloud service checks to enterprise controls and industry frameworks. This streamlines compliance evidence collection and simplifies the process for on-demand reporting.

Make compliance a continuous effort versus a moment-in-line effort.

6 Steps to Get Started

The cloud opens up unlimited opportunities for traditional brick-and-mortar banking institutions and digital financial services organizations. Cloud computing offers speed, scalability, accessibility, and unlimited storage capacity. Perhaps most appealing is the cost savings from not having to maintain hardware and only having to pay for what cloud resources are used.

However, cloud computing also carries a certain amount of risk, especially in the financial services industry. As more financial institutions embrace hybrid work, they face increasingly sophisticated cyberthreats targeting remote workers, customers, and third-party suppliers across an expanding attack surface. Organizations can get ahead of evolving threats by embedding cybersecurity requirements into the architecture and build stages of development.

Tips to Secure Success

1. Engage with senior business leaders to discuss cloud strategy and build security into the plan
2. Document your company plan for cyber risk assessment, identification, and management from code development to runtime
3. Create a cybersecurity disclosure plan on how to communicate with customers and investors
4. Understand the impact of your company's cybersecurity posture
5. Continually assess your cloud security policy and identify areas of improvement
6. Invest in a cloud security platform that can support every facet of your cloud security strategy

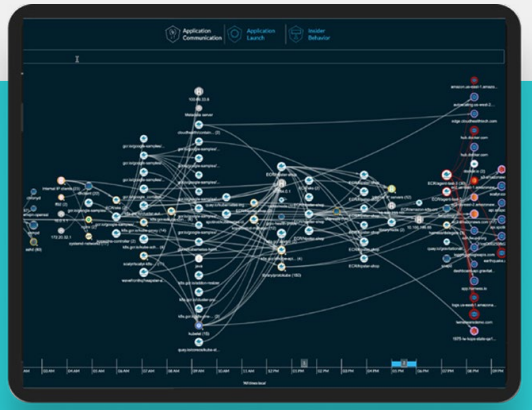
Take the Next Step

From insurance providers to retail banking and fintech to financial markets, Fortinet can help you embrace the cloud and keep your customers safe. Find out how Lacework FortiCNAPP can help you grow your business securely.

Fortinet keeps organizations secure in the cloud, allowing them to innovate faster and with greater confidence. Cloud security requires a fundamentally new approach and Fortinet's Lacework FortiCNAPP platform is designed to scale with the volume, variety, and velocity of cloud data across an organization's cloud environment: code, identities, containers, and multi-cloud infrastructure. Only Lacework FortiCNAPP provides security and development teams with a correlated and prioritized end-to-end view that pinpoints the most significant risks and handful of security events that matter most.

Ready to chat?

REQUEST A DEMO



[1] IBM. "Cost of a Data Breach." July 24, 2023.

[2] Principato, C. "Most Trusted Brands 2022—Trust in banking, investment and payments. Morning Consult." June 2022. Morning Consult Pro.

[3] IBM. "Cost of a Data Breach." July 24, 2023.

[4] Krivkovich, A., White, O., Townsend, Z., & Euart, J. "How US customers' attitudes to fintech are shifting during the pandemic." January 19, 2021. McKinsey & Company.

[5] Lele, N., & Mannamkery, R. J.. "How financial institutions can win the Battle For Trust." June 11, 2021. Ernst & Young.

[6] Verizon. "2023 Data Breach Investigations Report." June 6, 2023.

[7] IBM Security. "X-Force Threat Intelligence Index 2023." February, 2023.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[11] Verizon. "2023 Data Breach Investigations Report." June 6, 2023.

[12] IMF. "Rising Cyber Threats Pose Serious Concerns for Financial Stability." April 9, 2024.

[13] Alloy. "2023 State of Fraud Benchmark Report." November, 2022.

FORTINET

www.fortinet.com

August 29, 2024 10:08 AM / 2801672-0-0-EN