WHITE PAPER

Securing the Vault: How SSE Platforms Fortify Data Protection for Financial Services Institutions

Table of Contents

Framing Challenges for Financial Institutions in the 21st Century

In the twentieth century, a bank vault represented the most robust security money could buy. But in the twenty-first century, steel doors have become a relic of the past. High-value data generated, collected, and stored by financial services institutions (FSIs) in the cloud is accelerating exponentially—from digital currencies to daily transaction information—and must be protected. Today's FSIs worry less about bank robbers and more about how to secure sensitive data—from internal information and customer data to application source code and new banking products. With threats increasing in volume and sophistication at an accelerated pace, it is no surprise that 78% of financial services firms have experienced a cybersecurity breach, threat, and data theft.[1]

With the evolution of the cloud, protecting growing volumes of data poses a big challenge for FSIs. Rising compliance regulations, hybrid work environments, and interest in leveraging generative artificial intelligence (AI) and other innovations create new security challenges. Financial service leaders know their data is a favored target for profit-driven attackers and nation-state actors. However, the majority of data breaches result from insider threat vectors through intentional malicious actions or unintentional error due to a lack of end user awareness.

While FSIs are trying to leverage emerging technology to streamline and simplify work, 48% of banking executives don't believe their organizations have a mature understanding of the security technology required to safeguard sensitive data in the cloud.[2]

Clearly, a fresh approach is required. A single breach can have a massive impact on an FSI's reputation, hampering business and investment for years. Managing reputation and maintaining regulatory compliance standards demands strong data visibility and protection capabilities, including a Zero Trust Framework, to close the data protection gap.

1 Source: Skyhigh Security, 2023: The Data Dilemma: Cloud Adoption and Risk Report Financial Services Edition
2 Source: BankDirector: 2022 Technology Survey

Growing Volumes of Data Make It Harder to See and Manage

As FSIs continually generate more data in the cloud, they need to gain visibility into where data is stored, where it goes, how it is used, and whether it is properly secured. In addition to taking proactive measures to prevent breaches, meeting regulatory requirements remains challenging as the attack surface expands.

Until recently, many FSIs maintained a castle-and-moat security approach, securing data across both emerging software-as-a-service (SaaS) and legacy tools by focusing on network security and maintaining strong perimeter defenses. However, hybrid work and cloud computing have compelled FSIs to rethink their security strategies. Gaining visibility across IT infrastructures and securing data beyond the physical perimeter are key drivers behind their current cybersecurity modernization initiatives. In 2023, 95% of FSIs that use SaaS applications and services report that they have experienced security issues.[3] Shadow IT, including data storage outside the organization's country of origin, and the rising risk of threats are critical factors that drive the need for greater visibility and control over cloud data.

Some FSIs have implemented unintegrated point security solutions to manage individual applications within their complex infrastructures. While this may have been a positive first step in the past, these solutions often can't communicate with each other, so data tends to fall through the cracks, unseen and unclassified or inconsistently classified across security technologies. In addition, this approach diminishes the effectiveness and efficiency of security operations centers (SOCs) and adds complexity and 'false-positive' fatigue. Short-staffed teams end up juggling multiple consoles with different interfaces and divergent policies. Using best-of-breed point solutions also degrades security effectiveness because of protection gaps and inconsistencies in policy. This makes securing data less effective and significantly more difficult, time-consuming, and expensive for FSIs.

3 Source: Skyhigh Security, 2023: The Data Dilemma: Cloud Adoption and Risk Report Financial Services Edition

FSIs are Under a Microscope

For FSIs, stricter compliance regulations have elevated the need for more robust data protection. Staying current with complex regulations can be challenging, especially since almost every region has ever-evolving laws for managing and securing personally identifiable information (PII). Failure to comply with these laws could lead to hefty financial penalties.

With a highly complex environment comprising a diverse array of endpoint devices, networks, clouds, and applications, FSIs know they must introduce new processes and security technologies to manage data across multiple systems and environments. However, overburdened staff often lack the resources and time needed to automate controls and reduce their workload. Teams also waste a significant percentage of their time investigating false-positive alerts instead of focusing on genuine threats. In addition, compared to other industries, the cybersecurity talent shortage significantly affects this sector: 96% of financial services IT decision-makers say this impacts their ability to secure usage of cloud computing.[4]

And all of these factors amplify the potential for a breach. For instance, cloud migrations and misconfigured cloud security expose common security gaps for FSIs. Considering these organizations store an average of 61% of sensitive data in the public cloud,[5] the risk is further magnified.

To protect vital data and meet regulatory requirements, FSIs need support to optimize and automate operations. Security Service Edge (SSE) can provide that support. Initially defined by Gartner, Inc. in 2021, SSE is considered a transformative cloud-centric platform that consolidates multiple integrated security services to protect data, increase visibility, and vastly reduce complexity.

4 Source: Skyhigh Security, 2023: The Data Dilemma: Cloud Adoption and Risk Report Financial Services Edition
5 Source: Ibid.

Data Breaches Impact FSI Reputation

For FSIs, reputation is everything, especially when it comes to maintaining customer confidence. Considering the financial services industry experiences an average of 1.5 data breaches every day,[6] it's no wonder that customer trust is low. In 2022 alone, FSIs leaked over 254 million customer records due to data breaches.

Most FSIs have seen reputational fallout from the 2017 Equifax breach and the 2020 Flagstar Bank breach. FSIs can't afford to risk their reputations in heavily publicized breaches, especially as customers grow increasingly aware of security breaches: 47% of customers say they will permanently stop working with a company after a single data breach.[7]

Reputational threats have driven financial firms to invest in more cybersecurity each year. But building an arsenal of point products often creates more risk than it alleviates and can result in missed alerts, management headaches, and even downtime.

Technologies like generative AI, which can create various types of content such as text, images, and other media, raise new challenges. While FSIs are eager to leverage these technologies to improve productivity and speed innovation, there's also a need to ensure they have the proper visibility and security controls in place to protect sensitive data.

6 Source: Bank Info Security, 2022: Financial Services Was Among Most-Breached Sectors in 2022
7 Source: Okta, 2021: The State of Digital Trust

Zero Trust Provides Stronger, Coordinated Controls

Today's FSIs need a more mature cybersecurity strategy and stronger controls to prevent cyberattacks and data exfiltration. Companies are discovering that one of the best ways to secure their data is to adopt a Zero Trust Framework based on the principle of "trust no one and verify everything." Financial institutions thrive when customers believe their data privacy is a top priority, compliance requirements are met, and data is handled safely across the entire infrastructure.

By adopting widely accepted industry standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Payment Card Industry Data Security Standard (PCI DSS) FSIs can increase customer confidence. These cybersecurity guidelines fully align with a zero trust approach. FSIs must put controls and policies in place to enforce the principle of least privilege access and reduce data exposure.

Given the current state of affairs, where the average new FSI employee gains access to nearly 11 million files on their first day on the job,[8] tightening access management is crucial. Limiting privilege and implicit trust prevents data loss by verifying user identities before granting access to files and data. This works hand-in-hand with stringent policies to minimize the number of employees with access to sensitive data.

Together, these capabilities protect organizations against external threats, such as credential theft, which allows infiltrators to access multiple systems without further verification. And it reduces intentional and unintentional internal threats by controlling employee access to PII and other sensitive data.

As FSIs work to formulate a new security strategy and strengthen controls by adopting zero trust, they must also take into account other emerging risks.

8 Source: Varonis: 2021 Data Risk Report Financial Services

New Technologies Present Rising Risks

Many FSIs are eager to try new technologies despite reliance on legacy software. As some businesses report 66% higher productivity from using AI tools,[9] the temptation to optimize workflows, generate revenue streams, and explore new operational or promotional opportunities can be too great to resist. However, introducing new technologies also brings risks that threaten an FSI's security posture.

For example, many employees at FSIs want to explore the opportunities generative AI tools provide.[10] However, without existing controls in place to limit or monitor use, FSIs risk exposing sensitive data and violating compliance regulations—despite their best intentions.

Some companies have already discovered the implications of sharing data with the natural language AI tool, ChatGPT. Employees rarely consider that sharing data with increasingly popular AI tools means permanently introducing company data into the tool's training model, including customer PII, trade secrets, or internal metrics. This dramatically limits how employees can securely leverage AI without unintentional data exfiltration.

FSIs need a way to simplify monitoring, alert management, risk management, and data security without or adding new layers of complexity.

9 Source: Nielsen Norman Group, 2023: AI Improves Employee Productivity by 66%

10 Skyhigh Security, 2023: Adopt ChatGPT Without Putting Your Business-Critical Data at Risk

Achieving the End-to-End Visibility with Skyhigh Security

KEY BENEFITS FOR FSIs

- Skyhigh Secure Web Gateway (SWG) for Cloud protects remote users from malicious websites, zero-day threats, and data exfiltration with secure web connectivity for every device, user, and location. It provides expanded visibility and control over access to cloud applications, including Shadow IT. Skyhigh Security's unique hybrid capability seamlessly migrates Skyhigh SWG for On-Premises web policies to the cloud with the click of a button, benefiting those bound by legacy infrastructures, data sovereignty, or compliance regulations.
- Skyhigh Cloud Access Security Broker (CASB) provides visibility and control over data, context, and user behavior in SaaS, PaaS, and IaaS cloud services to prevent sensitive data exfiltration and stop security threats.

Continued on next page.

FSIs need to know that not all SSEs are created equal. They need a security solution to meet their unique requirements, offering the end-to- end visibility required to safeguard their reputations and vital data. That's why 80% of global banks and 25% of Fortune 500 companies trust Skyhigh Security.[11]

Skyhigh Security's industry-leading SSE portfolio has helped over 3,000 organizations enable their workforce with unmatched data protection capabilities across the web, cloud, private applications, email, and endpoints—all from a single, converged console. By taking a data-first approach, Skyhigh Security secures data-at-rest, in-use, and in-motion across every control point, from anywhere, in any application, and on any device. This gives FSIs the benefits of a hybrid or remote-first work environment without compromising security.

Multi-vector data protection, a hyperscale service edge, and advanced threat protection come together in a single platform, creating a powerful security solution FSIs can count on. Some Zero Trust Frameworks[12] focus primarily on access restrictions, which may affect productivity and collaboration.

Skyhigh Security, on the other hand, goes beyond this, helping FSIs define optimal data protection rules and then applying them organization-wide.

True end-to-end data protection means that data is always visible and unified security controls are in place to protect it. Skyhigh SSE provides unified data classification and leverages AI and machine learning to automatically categorize content across multiple key exfiltration vectors. This gives FSIs the power to ensure sensitive data doesn't end up in the wrong places. If an incident occurs, detailed information enables security teams to mitigate the issue and apply stronger controls quickly.

Skyhigh Security consolidates multiple powerful cloud-native security technologies into a single platform to enable FSIs to move their business forward while minimizing the impact on security, performance, complexity, and cost.

11 Source: Skyhigh Security, 2023: Security Service Edge
12 Source: CIO, 2022: Beyond Zero Trust: Protecting Data Wherever It Resides with Data-Aware Security

Creating a More Secure Future for FSIs

KEY BENEFITS FOR FSIs (CONTINUED)

- Skyhigh Private Access ensures data safety and integrity by continually verifying all users and devices before granting access to private applications and other sensitive resources. Skyhigh Private Access provides DLP scanning, anti-malware inspection, and seamless RBI integration for robust data protection.
- Skyhigh Cloud-Native Application Protection Platform (CNAPP) identifies risks from misconfigurations, threats, and vulnerabilities while protecting FSI data—all from a single, frictionless platform.

Skyhigh Security also significantly streamlines compliance. This pays big dividends, such as increased efficiency, greater transparency, and better reporting accuracy. Automated controls allow security teams to focus on high- priority security gaps and advance security maturity. Together, these elements effectively prevent data breaches and ensure a financial organization's reputation remains intact.

For more information about how Skyhigh Security helps Financial Services Industries, please visit www.skyhighsecurity.com.

Skyhigh Security's cloud-native SSE solution converges multi-vector data protection, hyperscale service edge, and advanced threat protection into a single platform to provide FSIs with assurance that their data is protected as they explore new technologies. From artificial intelligence (AI) to cloud computing, FSIs need innovations to drive business efficiencies, provide better services, and stay competitive. To confidently embrace these technologies, FSIs must be able to leverage the benefits without putting sensitive data at risk by implementing a single-vendor SSE solution. They can now safely adopt emerging technologies knowing that their investment in Skyhigh Security scales to "futureproof" application and data protection controls.

Schedule a demo today to discover how the Skyhigh Security SSE portfolio can simplify your security operations.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

About ITB

At ITB, your cybersecurity is our priority. Since 2008, you've trusted us to secure your business, data and people against ever-evolving threats, backed by our partnerships with leading IT providers.

Whether you're in the private or public sector, we've supported hundreds of businesses like yours across a wide range of industries, helping you stay protected.

You can count on our team of cybersecurity experts to understand the latest hacker tactics and guide you through building a future proof strategy that fits your unique needs.

For more information visit us at it-b.co.uk

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

November 2023. WP-EN-000020-01