SailPoint

eBook

Intelligent identity security

How financial services can reduce costs and empower IT teams

The financial services industry continues to face significant challenges related to identity security.

According to a recent state of identity security report, 93% of financial services report that their organization has faced a breach in the last 2 years.

Source: The state of identity security 2023:
A spotlight on financial services

Additionally, U.S. banks and financial institutions have processed more than $1 billion in potential ransomware-related payments.[1]

IT skills-gaps, strict regulatory compliance requirements, mergers and acquisitions, and rising cyber-insurance costs—these contributing factors are creating environments both difficult to secure and expensive to maintain.

Despite the challenges, it is essential for banks and financial firms to maintain customer trust by protecting their sensitive data through a robust identity security program. The question the industry must answer then is, how to implement and maintain best-in-class identity security while also lowering costs and streamlining IT processes.

[1] https://www.fincen.gov/news/news-releases/fincen-analysis-reveals-ransomware-reporting-bsa-filings-increased-significantly

How do you maintain best-in-class identity security while also lowering costs and streamlining IT processes?

This is where AI-driven identity security comes in.

In this eBook, you will learn why leading financial services organizations are turning to AI to modernize identity security, gain efficiency, comply with regulations, and evade data breaches that have serious financial implications and cause reputational harm.

We will provide adoption strategies and ways AI-driven identity security can result in significant cost savings for your organization.

When you finish reading, you will understand the many advantages AI-driven identity security offers, how to conduct a discovery process with various stakeholders, and the best practices for moving forward.

Let's begin.

Why AI?

Despite being a highly regulated and risk-averse industry, financial services regularly face costly ransomware attacks that target over-entitled or orphaned identities.

Over-entitled identities typically arise from the need to grant employees and third parties access quickly while orphaned identities, or dormant accounts, most often result from workers leaving the organization without access being deprovisioned. Both introduce serious security vulnerabilities attackers use to exploit security gaps and gain access to sensitive data and private environments.

Financial services also face the risk of insider breaches—from fraud to accidental access–due to complex corporate structures and departmental silos. This type of environment is ripe for inefficiencies and security risks, and requires constant oversight and scrutiny by teams already stretched thin with limited budgets to hire specialized expertise. This is why reducing the IT/Security skills gap is a top priority for many banks and financial firms.

Finally, the financial services industry must meet complex compliance and regulatory requirements. This is often a time-consuming process that drains resources, but is critical when it comes to maintaining customer trust and industry allegiance.

Top these pain points off with manual processes that introduce risk of inaccuracies and increase costs. It is plain to see why banks and financial firms need AI-driven identity security that can go beyond human capabilities.

Without question, these are real and difficult challenges, but the industry has an opportunity to strike back—to resolve today's most pressing issues while ensuring improved outcomes for tomorrow.

Using AI-driven identity security, organizations can develop highly efficient and effective access processes, dramatically reduce the chances of a security breach, simplify compliance, lower costs and gain cross-team efficiencies—all while preserving customer trust and business reputation.

A better way forward

Security and IT teams have a mandate to uncover a better way forward, to keep costs down and improve efficiency. Intelligent identity security answers this mandate in several positive ways:

1. **Provides secure access on Day 1:** Ensures faster and more secure access for employees and third parties.
2. **Protects brand reputation:** Eliminates overprovisioning, reducing risk and reputational harm caused by data breaches.
3. **Simplifies compliance:** Automates reporting and implements access controls to easily manage SOX, GDPR, and GLBA requirements.
4. **Reduces compliance time and costs:** Reduces the time spent on multiple IT audits for a wide array of various regulatory initiatives (e.g., SOX, GLBA, FDIC, FINRA, NAIC, NY DFS, etc.) through intelligent automation. Reduces the cost of compliance by automatically generating audit trails and access reports on all key applications and data.
5. **Improves the operating effectiveness of controls:** Reduces certification fatigue and rubber stamping user access certifications.
6. **Mitigates insider threats:** Reduces the risk of error or fraud with easier execution of Separation of Duty (SoD) policies that enforce access controls, preventing conflicts of interest and information theft.
7. **Lowers operational costs:** Relieves IT and security teams of manual access management processes, freeing up valuable resources and time.

Begin the Journey

The goal of reducing costs and improving identity security is essential, but it's equally important to answer the following questions before making a move. Ultimately, a thorough discovery process can help ensure your transition is smooth and secure.

- **Identify pain points:** What is your current identity security program approach? Do you have IT staffing gaps, manual provisioning causing access delays, and instances of over-entitled or orphaned identities?
- **Assess existing identity access governance:** Where can your existing identity security process improve, and can a new solution complement or replace existing security measures?
- **Gauge attack surface:** Have excess privileges increased your attack surface? Assess if your policy-based access is in accordance with employee events—including joining, moving or leaving the organization.

- **Understand regulatory requirements:** Consider the time and cost spent trying to comply with regulatory requirements for identity security; where would you like to gain efficiency while ensuring you meet compliance and avoid potential legal liabilities?
- **Evaluate identity security technologies:** What capabilities are the most appropriate for your specific needs?
- **Consider scalability:** Is your organization planning to scale (either up or down), and if so, which solution can best accommodate the potential changes in the size or scope of the organization?

Overall, it's wise to take a holistic approach and consider your specific needs, regulatory requirements, and available technologies. This approach builds the foundation on which your organization will operate, so it's critical to allot time and leverage the necessary resources.

When the discovery process is complete and you have selected a solution, it's time to make a plan for implementation. A comprehensive plan that outlines your goals, objectives, and timelines optimizes success and helps you quickly realize the many benefits AI-driven identity security delivers.

Consider the following strategies as you move into the implementation phase:

- **Begin with the end in mind:** Design a roadmap showing how specific identity security investments can facilitate your desired future state and support business goals.
- **Engage stakeholders and champions:** Create an identity security program charter and steering committee that includes IT personnel and management, application owners, internal audit, human resources, and other key executives that can help drive overall program adoption.
- **Communicate business value:** Demonstrate the need for a centralized system so security teams have broader visibility into resource and application access, user behavior and anomaly tracking across the entire organization
- **Start small:** During the initial implementation, create smaller projects—this helps keep timelines short and focused, while also giving periodic achievements to celebrate. A "short sprint" approach will help when additional modules need to be integrated or the identity security program expands to include more aspects of the digital ecosystem.
- **Provide training:** Provide training to key employees, administrators, and other staff on the proper use and management of the solution; confirm that each can navigate the technology effectively in real-world situations, understand the value, and endorse its adoption.
- **Remember that identity security as a program needs to continue to evolve** with your organization well after the initial implementation is complete.

The big question on an organization's mind at this point is time-to-value. When can you expect to meet the objectives you declared, how long will it take to comprehensively on-board users across your environment, what is the timeframe for reducing costs?

Several factors determine the answers to these questions, each of which is unique to your organization. One thing is certain, however: regardless of your size or current technology landscape, AI-driven identity security provides the tools you need to dramatically reduce costs quickly, all while empowering IT teams, preserving customer trust, and protecting your bank or financial firm's reputation.

Conclusion

It's clear why leading financial service organizations are turning to AI-driven identity security. Streamlining security tasks, reducing costs, gaining efficiency, and maintaining customer trust are mission-critical objectives in the industry.

Automation accelerates and simplifies the process of ensuring the right people have the right access to important financial data and personal identifiable information (PII). It alleviates highly manual and complex provisioning efforts by executing access requests automatically, and reduces such help desk tickets as resets, access requests, and password changes.

AI-powered identity security preserves scarce resources and allows IT to focus other key priorities. It is possible to accelerate new user access from a matter of days to seconds, and adjusting access levels in accordance to predefined security policies occurs immediately.

With robust identity security controls in place, organizations gain security and efficiency around mergers and acquisitions, digital transformations, and shifts to the cloud. What's more, the elimination of redundant overhead, infrastructure, and third-party consulting services simplifies processes and consolidates user access.

An AI-based identity solution reduces the cost of compliance by automatically generating audit trails and access reports on all key applications and data, and easily demonstrates security controls to cyber insurance underwriters.

In closing, financial service organizations that adopt AI-driven identity security can proactively identify and manage risky access, ensure customer trust, empower IT teams, and deliver significant cost savings.

How does your identity security program compare to other healthcare organizations?

Take the identity security assessment →

SailPoint

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.