FINANCIAL SERVICES

Thriving Despite Compliance Challenges

Boosting resilience in financial services

splunk>
a cisco company

The evolving compliance landscape for financial services

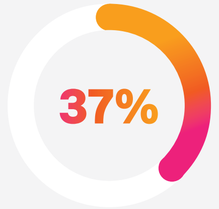
In today's financial services industry, compliance is no longer just a checkbox exercise. It's a critical business function that touches every aspect of operations. At the heart of this compliance challenge lies the complex interplay of assets and identities:

- **Assets:** Information or information systems that are critical to the operation of the business, such as customer data, financial instruments, IT infrastructure, and third-party services.
- **Identities:** A set of details that identify individual users or accounts, including employees, customers, partners, and even automated systems and APIs.

Financial institutions are facing a wave of new mandates. For example, our research from The State of Security in Financial Services found that 62% are already affected by regulations requiring timely disclosure of material breaches. In response to increasing regulation, financial institutions are making asset and identity intelligence the cornerstone of their compliance strategy.

Several compelling forces are propelling this shift. Regulatory scrutiny focused on data governance and access controls keeps increasing while digital assets and services steadily proliferate. Organizations are also encountering more sophisticated cyber threats targeting financial data and systems and rising costs associated with compliance failures.

It's a complicated puzzle. But financial institutions can elevate their efforts to stay on top of compliance mandates.



Only 37% of financial institutions around the globe monitor cost of compliance with regulations, despite reporting the need to balance cost pressures as a top compliance challenge.

Source: Thomson Reuters

Financial services compliance challenges

Financial institutions manage an array of data that creates unique compliance challenges.

They grapple with a **dynamic asset landscape** that is constantly evolving to incorporate new financial products and services. At the same time, they're facing pressure to integrate legacy systems with modern digital platforms. The rapid adoption of cloud and hybrid infrastructures is bringing efficiencies but introducing new security risks.

Additionally, financial organizations have a **complex identity ecosystem** with multifaceted customer identities across various services. As organizations work with more third parties, sharing data access through integrations, they experience new challenges and heightened risk. Embracing privileged access management for high-risk operations is a key safeguard that protects against compromising identities and systems.

Dynamic asset landscape

Constantly evolving financial products and services

Rapid adoption of cloud and hybrid infrastructures

Integration of legacy systems with modern digital platforms

Complex identity ecosystem

Multifaceted customer identities across various services

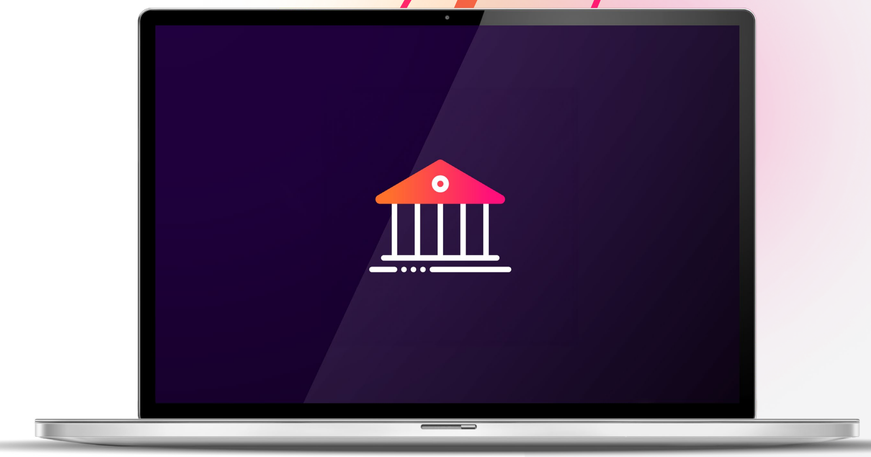
Privileged access management for high-risk operations

Expanded APIs and third-party data access and integrations

A complex compliance landscape

Financial organizations are navigating an ever-evolving web of regulatory mandates designed to protect consumers and businesses, stabilize the world's financial systems, and safeguard against financial crime.

Keeping up with compliance standards isn't optional. It's essential to maintain reputations and customer trust while avoiding legal consequences and hefty fines. What's more, financial institutions need to be able to adapt to regulations — both globally and in the specific markets where they do business.



Global compliance mandates

Know Your Customer (KYC)

In brief: KYC is a set of standards financial institutions use to verify customers' identities, assess their financial activities, and mitigate risk.

What this means for you: This foundational control ensures financial institutions perform due diligence by collecting and verifying customer identity information to assess their risk profile and protect against corruption, fraud, and money laundering.

T+1 Settlement Cycle

In brief: T+1 requires financial institutions to close most routine settlement transactions on the next business day after their transaction date.

What this means for you: In many cases, to meet this requirement, financial institutions need to adjust their operational and technological infrastructures to shorten trade settlement time. This acceleration can occur through eliminating manual intervention and pursuing straight-through processing to automate the settlement processes.

United States compliance mandates

Sarbanes-Oxley (SOX)

In brief: SOX is a federal law that safeguards investors from fraudulent financial reporting by mandating strict recordkeeping processes for all public and some private companies.

What this means for you: Internal controls are needed to prevent tampering with financial records, and file regular reports with the SEC attesting to the effectiveness of security controls and the accuracy of financial disclosures.

California Consumer Privacy Act of 2018 (CCPA)

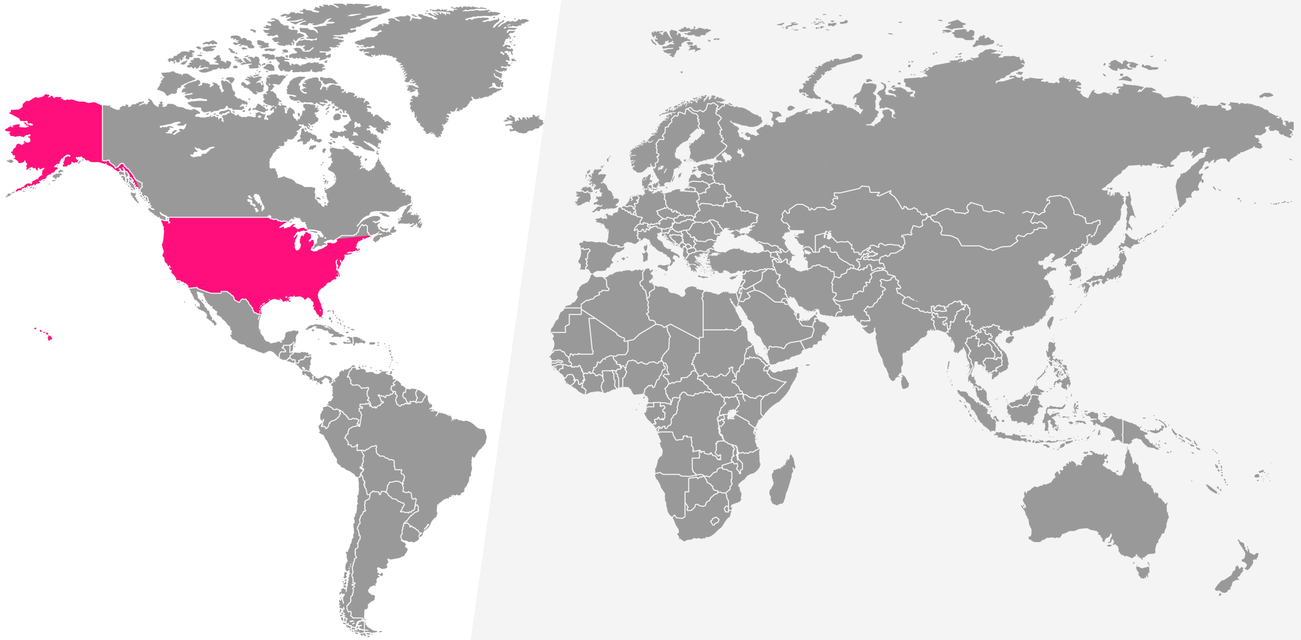
In brief: CCPA enhances consumer privacy by providing California residents with control over how businesses collect and use personal information.

What this means for you: Financial institutions operating in California are required to comply with CCPA's prescriptive data collection and opt-out measures and must stop selling consumers' private data upon request.

Payment Card Industry Data Security Standard (PCI DSS)

In brief: PCI DSS defines baseline technical and operational security standards to safeguard environments where payment information is processed, transmitted, or stored.

What this means for you: Maintained by payment card brands, PCI DSS outlines a set of standards for financial organizations to safely accept payment card data to secure cardholders' sensitive information and protect against fraudulent activity and data breaches.



Europe, Middle East, and Africa compliance mandates

Digital Operational Resilience Act (DORA)

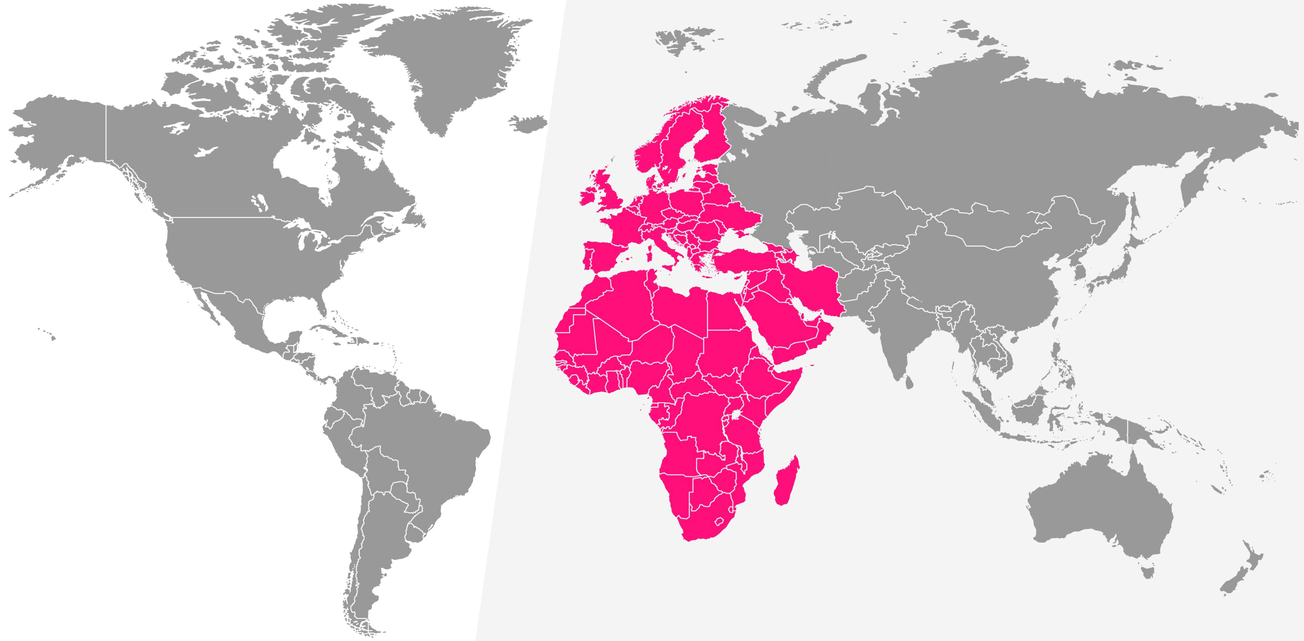
In brief: DORA creates a regulatory framework on digital operational resilience for the European Union, requiring all financial firms to make sure they can withstand, respond to, and recover from all types of information and communications technology disruptions and threats.

What this means for you: The DORA compliance process is an opportunity for financial institutions to review current security policies and procedures, with an emphasis on the regulation's five pillars: risk management, third-party risk management, incident reporting, information sharing, and resilience testing.

Bank of England (BoE) Rules and Guidance

In brief: Financial institutions operating in the United Kingdom must comply with a wide range of requirements, including the Prudential Regulation Authority Rulebook, the Financial Conduct Authority Handbook, and various pieces of legislation.

What this means for you: BoE requires financial institutions to maintain adequate capital and have strong governance and model risk management controls to avoid risks associated with using inappropriate or flawed models. BoE also supervises firms and can step in if firms are not being run in a sound way.



Asia Pacific (APAC) compliance mandates

CPS 230 Operational Risk Management (Australia)

In brief: CPS 230 aims to strengthen operational resilience and risk management, as well as resilience, for financial services organizations regulated by the Australian Prudential Regulation Authority (APRA).

What this means for you: This standard sets out essential security practices for ARPA-regulated entities to fortify resilience by establishing policies, procedures, and controls aligned with international cybersecurity best practices.

CPS 234 Information Security (Australia)

In brief: CPS 234 institutes requirements for information asset identification, security team roles and responsibilities, controls testing, incident management, audit, and breach notification.

What this means for you: To meet these requirements, financial organizations need information security strategies, governance, and risk frameworks, clarity on the scope of their information assets and third-party relationships, and a regularly tested incident response program.

Five critical capabilities for compliance monitoring

Gaining and maintaining a complete view of complex systems and customer identities is essential for effective security decision-making and efficient compliance management. The following pages detail five critical capabilities that help financial services security and compliance teams proactively mitigate risk by discovering and closing security gaps in real time.

Financial services is a heavily regulated industry, and this can make it difficult to move as quickly as financial institutions would like. They must address the constantly increasing customer demands, battle competitive pressures (especially from less-regulated players such as some fintechs), and keep costs down, all while maintaining regulatory compliance, operational resilience, and security. Responding to market and customer demands while maintaining digital trust is a key factor in an institution's brand, reputation, and success in the market.

— Jerry Silva, Program Vice President, IDC Financial Insights

1. Comprehensive and continuous visibility

The challenge: Data silos create a number of challenges for security and compliance teams — and those challenges can snowball. When information is fragmented and scattered, it makes it hard to get visibility into potential attack surfaces, ask related questions, get answers, and take action. It's also difficult to aggregate and maintain customer data across multiple sources to create accurate customer profiles. Working around these disconnects takes time and resources, which can overwhelm teams as they are forced to manually track and reconcile data.

These challenges are then compounded by inefficiencies in the tools themselves — many of which only offer partial insights. This leaves gaps in understanding an organization's complete infrastructure or getting a full view into customer identity information. As the saying goes: You can't secure what you can't see. The lack of a comprehensive, unified view makes it harder to secure systems and thwart fraud.

Critical capability: To navigate today's regulatory environment, stale data can mean the difference between compliance and noncompliance. Security and compliance teams need a **continuously updated inventory of technology assets across multiple sources**, including network, endpoint, cloud, and scanning tools. By eliminating stale data, teams can be secure in the knowledge that the data about their assets and the identities they manage is always accurate and comprehensive — a foundational insight that's crucial for reducing risk exposure and eliminating blind spots.

Security and compliance teams also benefit from a centralized platform for collecting and analyzing data. With real-time integration and identity resolution, teams gain a single, unified view of each customer. Automated KYC workflows, risk scoring, and ongoing monitoring further enhance customer experience and security.

2. Out-of-the-box use cases to meet compliance requirements

The challenge: When it comes down to it, one of the biggest challenges financial services security and compliance teams face is a lack of time — and uncovering compliance gaps in security controls can eat up a tremendous amount of resources.

No organization wants to risk that. Noncompliance can result in substantial fines. For example, the first half of 2024 saw fines for noncompliance with anti-money laundering regulations (including KYC), sanctions, suspicious activity reports, and transaction monitoring violations eclipsing $263 million globally — up 31% from the prior year.

Notably, the highest value fine levied against a single institution was $65 million, nearly one-quarter of the half-year total.

Yet teams can struggle, thus making it hard to measure compliance against their security controls. Security and risk teams also spend many (many, many) hours each quarter preparing compliance reports for external audits as well as for a rapidly expanding roster of people within the organization who care deeply about compliance.

Critical capability: An easy button. Well, not quite. But, by being able to **measure compliance against major compliance mandates** with out-of-the-box security and observability use cases, which solve for compliance requirements, teams can quickly understand their compliance posture without wasting precious time. This way, they also have time to be more strategic and proactive.

3. Customizable security and observability use cases for compliance

The challenge: No two architectures are exactly alike. Security and compliance teams can spend a lot of time trying to gain foundational visibility over their entire asset inventory and make sure that they have the most up-to-date view of customer identity information. Often, an organization will opt to onboard multiple tools to get the necessary visibility, but those tools don't always integrate with each other very well (or at all), meaning a lot of late nights and fire drills due to manual processes.

Critical capability: Security and compliance teams need the ability to build **custom compliance metrics** (total incidents, time between issues, compliance cost, resolution time, etc.) to reduce risk exposure and report on real-time compliance against security controls and other compliance requirements.

> **Resources are my only real weakness — actually having enough hours in the day and having enough people to handle all the responsibilities.**
>
> — CISO, financial services company, The Ciso Report

48%

of financial services CSO/CISOs say their team spends the majority of their time working on cybersecurity posture and risk mitigation (vs. 25% all others).

4. Real-time compliance reporting

The challenge: More people care about compliance than ever before, and static risk and compliance assessments simply aren't enough anymore. With the rise of personal accountability over compliance posture, it might not be too far-fetched for a stakeholder to ask who in an organization wrote a specific line of code.

Security and risk teams can spend considerable time preparing for audits or digging through transactions, payments, and customer data, but today's stakeholders want a clear picture of compliance posture — now.

Critical capability: Security and compliance teams need to be able to give real-time reports on an organization's compliance posture. It's important for them to quickly identify and report on systems, data, and processes that are noncompliant across several metrics, get an executive-level metrics compliance view, and demonstrate a plan to proactively address any areas that are missing controls. With a unified platform that automates the collection, analysis, and reporting of data from across systems and partners, teams can achieve **real-time transaction monitoring and proactive compliance management**. It'll help everyone sleep better at night.

of financial services organizations say that the complex web of global regulations and sanctions has begun to restrain their business activities.

are looking to increase their operational resilience to set their organizations up to withstand disruptions, recover quickly from challenges, maintain continuity, and ensure long-term sustainability.

Source: True Cost of Financial Crime Compliance Study, 2023, Forrester Consulting

5. Contextualized, accurate asset data

The challenge: Security and compliance teams face significant challenges correlating alert data with specific systems during investigations. This process is hindered by the absence of a real-time, comprehensive overview of systems, applications, and data, requiring them to cross-reference multiple tools and often make assumptions. This not only slows down the investigation process but also delays alert triage and incident response.

The complexity increases when an alert involves a system that has undergone changes, such as different IP addresses, network locations, or user associations, especially over extended periods of time. This raises a critical question: How do you accurately attribute an investigation to a specific concern at any given time?

Critical capability: With **accurate query context**, teams can focus and shorten their investigations. And, by mapping relationships, they can quickly identify **who** is associated with **what** system or identity and **when**. Pre-built compliance dashboards and proactive alerts help automate analysis and reporting processes and ensure data integrity.

The pace of regulatory change in financial services shows no signs of slowing down, so it's important for financial institutions to stay one step ahead. An up-to-date, comprehensive compliance management strategy is a great foundation to help close security gaps and demonstrate improvements.

View this on-demand webinar to learn strategies to enhance your security and reliability posture in an increasingly complex landscape.

splunk>
a cisco company

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.