splunk>
a CISCO company

Detect, Investigate, and Respond: Reduce Financial Crime and Fraud in Financial Services

Competition is high for financial services organizations — with big tech, financial infrastructure, and technology services taking a larger share of the industry.

Organizations that prioritize customer trust and reputation are better positioned to remain competitive and profitable.

At the same time, evolving compliance regulations and efforts to guard against financial crime and fraud can make it harder to deliver on customer expectations.

CHALLENGE

Prioritize and reduce financial crime and fraud risks

The threat landscape is ever changing — with new types of fraud cropping up all the time. Threats are becoming increasingly sophisticated, complex, and difficult to detect. This is especially true with the introduction of generative AI, which can be beneficial to both defenders and attackers.

With more customer-facing applications and third-party integrations, the expanded attack surface requires more data sources to quickly and accurately identify suspicious activity and points of system vulnerability.

While data is key to protecting against fraud and financial crime, it tends to be siloed amongst point solutions, making it difficult for organizations to analyze and act on that data.

SOLUTION

Splunk for financial crime and fraud

To protect both their reputations and their balance sheets, organizations are looking to improve how they detect, investigate, and respond to financial crime and fraud. Splunk provides powerful data aggregation and correlation capabilities to help identify anomalies and potential threats. With Splunk, organizations can operationalize financial crime and fraud data by ingesting and extracting information from various sources, allowing them to monitor and search for suspicious activities across the entire organization.

For financial institutions, the cost of fraudulent transactions can add up to a lot of lost revenue, so every basis point of fraud reduction is a massive win for the organization. With improved visibility, financial services institutions can reduce business risk and effective fraud rates — ultimately improving top line revenue.

Transaction fraud

Identify suspicious wire transfers through statistical analysis

To optimize operations, financial institutions want real-time transaction details. With greater visibility into transaction fraud, organizations can gain insights around authorized, cancelled, or denied attempts, all mapped to customer experience and response times.

Getting ahead of transaction fraud requires accurate, up-to-date tracking of customers' end-to-end journeys — a key part of Know Your Customer initiatives designed to fight fraud, as well as protect customers' finances and preserve their trust in the institution.

With Splunk, each transaction can be scored based on the wire transfer value, with amounts deemed statistical outliers compared to the account holder's previous transfers and peer group transfers receiving higher risk scores. Taking the risk scores into account, this model helps identify potentially fraudulent transactions.

Money laundering

Detect and identify unusual activities

Money laundering is a huge problem: the estimated amount of money laundered globally in one year is 2-5% of the global GDP, or $800 billion to $2 trillion in current US dollars. Anti-money laundering (AML) regulations have strict requirements designed to combat these financial crimes, with regulations such as the U.S.' Bank Secrecy Act and the EU's 6AMLD laying the framework for compliance.

For the financial services industry, it's critical to detect the placement, layering, and integration of funds to shut down money laundering schemes.

Splunk's money laundering use case is built on a model highlighting account holders colluding to launder money in high-risk destination countries. It identifies recipient accounts in high-risk areas where multiple accounts have wired money, uncovering potential money laundering schemes involving account collusion and transactions just under AML thresholds.

Account takeover

Target and act on suspicious accounts

From online banking to alternative payment and remittance platforms, many digital applications now have a payment component. And they all have one thing in common: an account.

Unlike stealing a single bank account or credit card number, an account takeover gives attackers access to every aspect of the account's capabilities, resulting in financial damages for customers and reputational damage to organizations that's hard to bounce back from.

To help combat this, Splunk creates an account takeover (ATO) risk score by correlating multiple ATO-related Splunk searches that result in a weighted risk score. With aggregated results, teams can identify and prioritize the most important accounts, while significantly reducing alert noise that occurs when reviewing individual ATO indicators in isolation.

Wire transfer

Monitor and mitigate fraudulent transfers

Financial services customers are often at risk for common scams, such as fake rental deposit requests, lottery winnings that supposedly require a tax prepayment, or overpayments on bad checks.

Identifying suspicious wire transfers can help protect customers from financial ruin at the hands of scammers — and protect both the reputation and financial status of the institution.

With Splunk, users can analyze MT103 Swift messages using the "Swift Wire Transfers Overview" dashboard to better understand where money is being transferred and by whom. The dashboard allows users to drill down and view raw Swift messages, which are composed of multiple blocks holding specific information about the wire transfer.

Take action against fraud with Splunk

"I need a comprehensive view of the fraud journey to identify gaps and anomalies."

With Splunk, users can create a range of financial crime and detections using algorithms and guided workflows to track end-to-end digital journeys. After analyzing user behavior and transaction history, solutions like Splunk's Machine Learning Toolkit can identify atypical patterns to preemptively raise a red flag.

"I need to bring teams together to fight fraud more effectively."

Splunk helps break down silos between people and technology by collecting data from point solutions, consolidating the fraud scores they produce, and facilitating consistent, collaborative investigations into fraud events. Powering a fusion center approach, Splunk helps financial services institutions establish a shared data environment for SOC and fraud teams where insight is aggregated, reusable, and easily repurposed.

"I need to improve operational efficiency and fight fraud faster."

Splunk has the unique ability to correlate data based on risk and aggregation, helping organizations catch and remediate fraud faster. And with Splunk's out-of-the-box AI/ML tools, organizations can get a jump start on monitoring customers' transactions and internal systems, so they can identify and mitigate threats more quickly.

Aflac adopts Splunk platform for analytics-driven security

CHALLENGE

Facing a rapidly changing threat landscape, Aflac needed a robust security platform to protect its customers, 10,000 employees, and brand reputation.

SOLUTION

Aflac orchestrated threat intelligence across 20 security technologies and created an analytics-driven security approach that provided immediate return on investment.

OUTCOMES

2 wks
to enterprise-ready implementation

2M
security threats blocked in one six-month period

40 hrs
saved every month by replacing manual processes

> We were able to do extraordinary things in a very short period of time to detect advanced threats. Ultimately, that was the decision point for us to make a much larger investment in Splunk Enterprise Security and UBA across our different security use cases.
>
> **D.J. Goldsworthy,**
> Director of Security Operations and Threat Management, Aflac
>
> Aflac.

Keystart improves productivity and ensures compliance remains paramount

CHALLENGE

With limited security staff, a lack of formalized security programs or systems, and strict auditing processes, Keystart needed a platform that would support customers across numerous data-driven channels, while adhering to specific legal requirements and ensuring compliance within government standards.

SOLUTION

Keystart deployed Splunk technology to enhance security measures through a unified view of systems, reduce cost and resources in managing large data sets, and help monitor compliance against security standards.

OUTCOMES

75%
reduction in incident response time

4x
increase in productivity

> Prior to Splunk, we had to internally write some applications to get a comprehensive overview of our siloed system. Now with Splunk's alerts and a unified view across systems, we've reduced incident response time by 75% and increased our productivity at least four-fold.
>
> **Sean Smart,**
> Information Security Officer, Keystart
>
> **Keystart.**

Find fraud faster with Splunk

Splunk helps financial institutions accurately detect, investigate, and respond to fraud and financial crime. With Splunk, organizations can improve topline revenue by reducing business risk and effective fraud rates with greater visibility across all parts of the business.

Visit splunk.com/financialservices for more information or contact Splunk to arrange an in-depth review of your goals and challenges.

splunk> a CISCO company