splunk>
a CISCO company

Fighting Fraud Before It Hits with Data-Driven AI Solutions from Splunk

For financial institutions, the stakes couldn't be higher when fighting fraud. AI-powered security and observability tools from Splunk can help these organizations stay ahead of financial criminals, but how?

Let's find out how a fictional financial services company, Acme Bank, might deploy Splunk's machine learning (ML)-based analysis capabilities to revolutionize its fraud detection and prevention effort — ultimately safeguarding its financial integrity.

The fraud challenge: when traditional methods just won't cut it

Acme Bank is a medium-sized organization with 30,000 employees and has a team to manage case overflow. But they struggle to handle rising fraud cases, especially spotting emerging fraud tactics.

Traditional fraud detection methods rely heavily on manual processes, legacy systems that don't scale well, and siloed applications that do not share information readily.

The bank's in-house application tries to create a unified view of data across all its systems. It isn't working well because the static rules of the in-house application quickly become outdated compared to sophisticated vendor tools that use ML to update rules dynamically. Financial fraud is a moving target, with new schemes emerging as quickly as old ones are shut down.

This problem has become more acute since a banking partner abroad informed Acme Bank that an overseas organization, Alpha Trading Co, has been using it to evade international sanctions. The organization uses Acme Bank as an intermediary to facilitate its transactions, exploiting weaknesses in its compliance checks. It then routes transactions through a series of shell companies. It uses smaller, frequent transactions with front companies registered in neutral jurisdictions to obscure its financial trail further, ultimately funneling money back to its domestic accounts.

The most disruptive incidents of fraud in financial services institutions can cost as much as

$50 million

A 2024 study of financial service fraud shows more than 50% of banks, fintechs, and credit unions reporting an increase in business fraud and over 2/3 reporting an increase in consumer fraud.

How Splunk turns the tables on fraudsters

Acme Bank recognizes that it needs a more holistic view of its processes. The bank turns to the Splunk platform, which gathers data seamlessly from across the organization and then powerful AI models can be used to detect and even predict suspicious activity across a financial service organization's entire infrastructure.

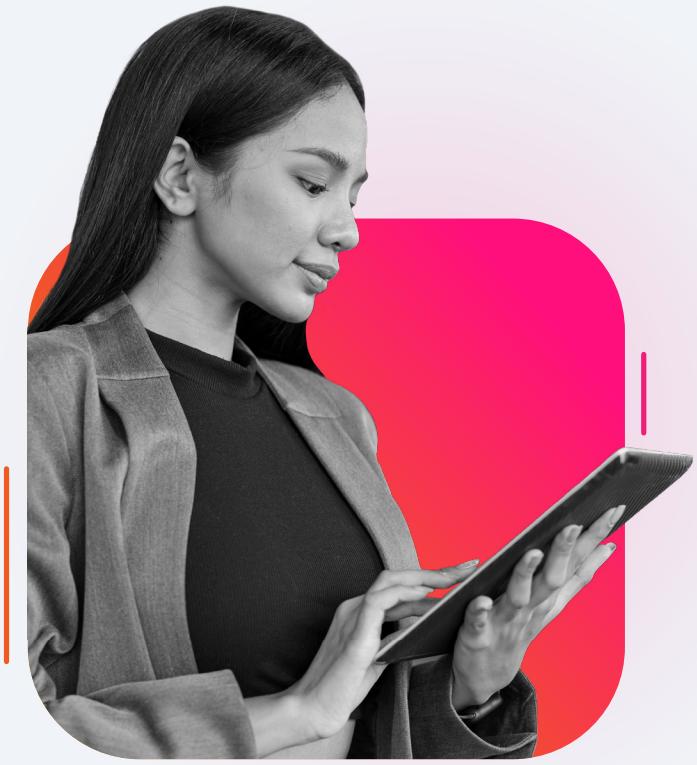
Acme Bank uses the Splunk AI Assistant for SPL to help create saved searches in the Splunk Search Processing Language (SPL). These searches regularly gather data that provides context on transactions. The fraud team uses this information to create an index of scores indicating each customer's aggregated level of risk based on multiple data points. It then uses the Splunk App for Anomaly Detection to apply ML algorithms to find outliers in these risk scores that warrant further attention.

As it gets used to this workflow, Acme Bank uses the Splunk Machine Learning Toolkit to apply more sophisticated ML procedures to its risk index. This includes predicting a user's future risk scores and identifying which users frequently nudge the risk score threshold but never exceed it.

Splunk enables Acme Bank to map user behaviors, transaction histories, and network anomalies with a precision that traditional manual or static rules-based methods simply can't match. Using these tools, the bank constantly updates its data to achieve an up-to-the-second view of what's happening.

This proves invaluable when Acme Bank begins investigating the Alpha Trading Co case. Splunk's platform enables it to monitor customer activities by looking at individual accounts and monitoring chains of transactions to find anomalies that indicate potential fraud. The app provides Acme Bank's fraud department a comprehensive view of this transaction data. At the same time, a generative AI assistant makes it easier to query that data, highlighting the connections between seemingly unrelated transactions and revealing the larger fraudulent operation at play.

Splunk offers a specific fraud detection application to complement the AI capabilities of its core platform. The Splunk App for Fraud Analytics (SFA) is an add-on to its Splunk Enterprise Security product that helps financial institutions handle account takeover, account abuse, and money laundering detection.



Betting on Splunk for long-term success

With help from AI-powered transaction analysis, Splunk enables Acme Bank's fraud department to build a base of solid evidence identifying several accounts and transactions as fraudulent. It can then pass these on to correspondent banking partners and local law enforcement.

Acme Bank uses the Splunk platform to be even more proactive. Financial criminals create new accounts constantly, accessing many of those after stealing legitimate account holders' information. Law enforcement officials ask the bank to notify them as quickly as possible if it detects groups of transactions matching specific patterns. Acme Bank can do so, thanks to Splunk's automated risk-based alerting mechanisms.

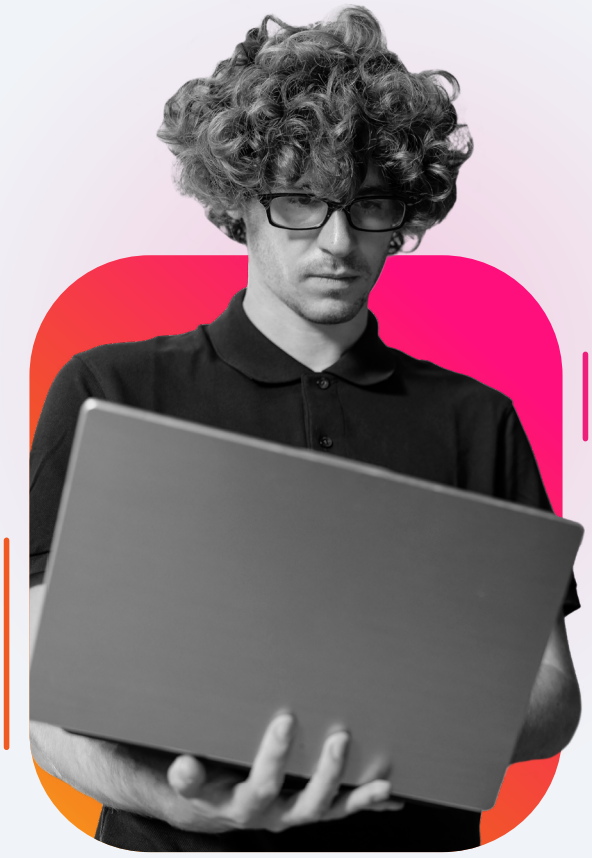
As the financial industry grapples with increasingly sophisticated fraud tactics, it's clear that traditional methods are no longer enough. Acme Bank's hypothetical journey demonstrates how Splunk's AI-powered security and observability platform can provide game-changing solutions for financial institutions. The latest ML-based fraud detection and observability algorithms enable Acme Bank to protect its customers from financial theft while preserving its integrity and reputation.

Deutsche Kreditbank (DKB) used Splunk to gain visibility into all parts of its complex hybrid infrastructure, leading to

90% faster
threat detection and investigation

Increased visibility
across tools and environments

Fewer
false positives



Stop fraud before it hits with data-driven AI solutions

AI-powered security and observability tools from Splunk help financial organizations track end-to-end digital journeys and detect, investigate, and respond to financial crime.

Splunk App for Fraud Analytics

The Splunk App for Fraud Analytics (SFA) is a comprehensive fraud detection solution built on the existing development frameworks of Splunk Enterprise Security. SFA offers your fraud team a standardized workflow, extensive interactive visual investigation capabilities, and a robust risk-based alerting framework, which is completely customizable and extensible.

With the risk-based alerting framework, SFA uniquely provides fraud prevention teams with the ability to improve alert fidelity and reduce false positives, ensuring that financial, legal, compliance, and reputational losses are minimized.

Splunk App for Anomaly Detection

Splunk App for Anomaly Detection works with any time series dataset that can be ingested into the Splunk platform. Using ML to detect seasonality in the data without user input lowers the barriers to realizing value.

Find anomalies in time series datasets and experience an end-to-end workflow to manage and operationalize anomaly detection tasks. The app detects seasonal patterns and finds anomalies in just a few clicks. Create anomaly detection jobs that run on a regular cadence, view SPL queries, and create alerts to detect fraud — faster.

Splunk AI Assistant for SPL

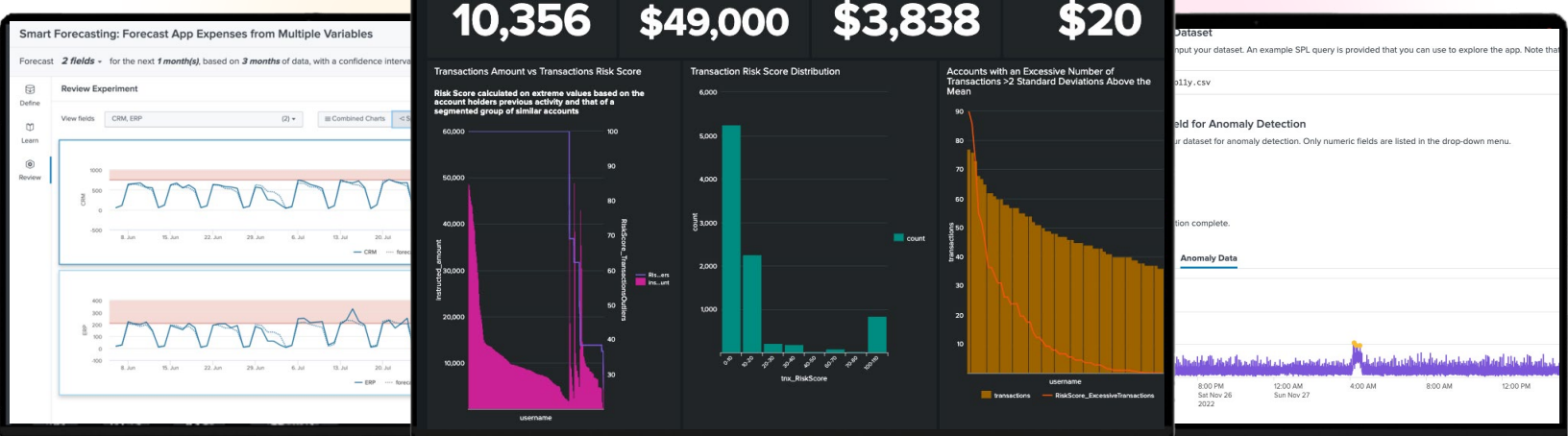
Splunk AI Assistant for SPL offers bi-directional translation between natural language (NL) and Splunk SPL. Compose what you want to search in plain English, and the Splunk AI Assistant for SPL translates the request into SPL. You can execute or build on that SPL search, all within a familiar Splunk interface.

Information from saved searches can provide more context on transactions and your team can use this data to better assess risk.

Splunk Machine Learning Toolkit

The Splunk Machine Learning Toolkit helps you apply various ML techniques and methods, such as classification (predicting a yay or nay), regression, anomaly detection, and outlier detection against your data. The different showcases in this app illustrate how to apply these methods to a sample of datasets, which are included in the app for you to use as a starting point for building your own analysis.

Each assistant includes end-to-end examples with datasets, plus the ability to apply the visualizations and SPL commands to your own data. You can inspect the assistant panels and underlying code to see how everything works.



The expanding digital attack surface in financial services has increased the range of data sources required to identify suspicious activity and points of system vulnerability accurately

Data-driven AI solutions empower financial services companies, like the fictional Acme Bank, to fight fraud more efficiently with better visibility and automated processes. With fraud on the rise, financial institutions need to detect, investigate, and respond quickly to protect your organization's balance sheet and reputation.

Learn more about how Splunk's solutions for financial services help to fight financial crime and fraud.

splunk> a CISCO company