

Splunk App for Fraud Analytics

Detect, Analyze, Investigate and Respond to Fraud





- **Patterns of fraud** are often found across different silos of both structured and unstructured machine data.
- **Traditional anti-fraud tools** can't scale, give a narrow view that creates siloes and the ability to centralize data of all types, including Structured and Machine Generated Big Data.
- **The Splunk® App for Fraud Analytics** helps with many needs of anti-fraud teams from fraud detection and monitoring, investigations, analytics and reporting, to enhancing your existing fraud tools.
- **Gain insight** into transaction and behavioral red flags over disjointed data sources.
- **Flexibility** to index relevant machine data across all data sources to search and correlate, making is easier to identify fraudulent patterns, so an organization can detect and alert on fraud in real time and act to prevent it.

Fraud has become a global problem and the impact, and cost remains higher than pre-pandemic levels. The effect is felt by organizations of all sizes, across many industries. Fraudsters are increasingly sophisticated and successful, especially as commerce and financial transactions move online, where it's easier to evade detection, use stolen credit card information, impersonate individuals and take over online accounts. Many existing anti-fraud solutions create a siloed approach to fraud detection and response, and do not provide the visibility or flexibility to detect and respond to fraud.

Fraud detection and prevention is a big data challenge that organizations can use to implement process and actions based on fraudulent activity. As business moves online, the evidence of internal or external fraud often lie in the massive amounts of unstructured machine data, commonly log files, generated within business applications, IT infrastructure and security systems.

This data comes from multiple sources, such as web proxies, firewalls, authentication systems, transaction processing systems, payment and billing systems, databases, point of sale systems and operating systems.

By indexing relevant machine data and searching and correlating on it to identify the patterns of fraud, an organization can detect fraudulent activity, alert teams in real time, and prevent it before bottom lines are impacted.

<p>Compliance</p> 	<p>The act of conforming with mandates as required, often by a government or regulatory agency. Examples of industry compliance mandates include HIPAA and DCOI.</p>
<p>Fraud</p> 	<p>A wrongful or criminal deception intended to result in financial or personal gain. Fraud often targets gaps in security.</p>
<p>Fraud Detection</p> 	<p>Implementing a process and actions that protect customers and enterprise information, assets, accounts and transactions through the real-time, near-real-time or batch analysis of activities by users and other defined entities.</p>
<p>Security</p> 	<p>The state of using tools and practices to protect against malicious intent to exploit and attack vulnerabilities to gain unauthorized access or use data.</p>

Splunk solutions can combat different types of fraud across banking, financial, healthcare and other industries. The Splunk App for Fraud Analytics (SFA) is a comprehensive fraud detection solution built on the existing frameworks of Splunk's industry leading Enterprise Security solution.

The Splunk App for Fraud Analytics includes customizable investigative dashboards to provide fraud teams easy access to targeted data to find fraud without typing SPL. SFA helps organizations achieve a faster time to value for their fraud protection endeavors and can optimize their investments and spending by utilizing their existing Splunk solutions.

Summary dashboards provide high-level overviews, trend analysis statistics and workflow based reports to get ahead of fraudsters. The Splunk platform can be configured to ingest structured, unstructured or proprietary data. Splunk software can easily onboard a variety of data sources, providing the ability to join distinct data sources together to gain insight into sequence-based transactions.

Splunk also offers the flexibility to integrate and export data to other systems via scripting, alert actions and dynamic forms or drilldowns. The ability to pull historical reports for compliance requirements and to assist in fraudulent investigations.

Unlock the Power of Machine Learning

As fraudsters continue to adapt and utilize new methods, it is important to leverage machine learning and data science algorithms to fight fraud. Detecting anomalies and outliers through machine learning, utilizing adaptive thresholds and other advanced techniques are the next wave in fraud detection and prevention. Use Splunk's [Machine Learning Toolkit](#) to examine outliers within your dataset for indicators of fraudulent activity.

Use Cases

Account Takeover

Account Takeovers happen when a cybercriminal takes fraudulent ownership of an online account through methods stolen passwords and usernames. There are various methods of gathering this password information, ranging from social engineering to phishing attacks. While historically motivations were usually financial, and the most impacted organizations were financial institutions, today, Account Takeover impacts any organization with a user-facing login.

New Accounts Fraud

New account fraud occurs when a cybercriminal or fraudster creates a new account, often historically with a financial institution, with the intent of committing fraud. Fraudsters are constantly adapting and failing to identify new accounts fraud can lead to significant losses.

With the Splunk App for Fraud Analytics, Fraud prevention teams can run correlation searches that detect anomalous or suspicious activity against user accounts and generate high fidelity alerts via the Risk Based Alerting Framework. Analysts can easily see all alerts, and notable events, in a single Fraud Incident Review dashboard that allows for easy investigations into notable events.

Ready to dig deeper into how machine data can improve fraud detection? See real-world examples and learn how much of an impact fraud has on our everyday lives in [our free "Guide to Fraud in the Real World."](#)