SPLUNK® FOR FRAUD DETECTION

Protect your customers and reputation and avoid fraud-related costs

- **Patterns of fraud** are often found in unstructured machine data, requiring a big data solution
- **Traditional anti-fraud tools** struggle with machine data for a variety of reasons
- **Splunk Enterprise** is the leading big data platform to harness machine data to reduce fraud

Fraud Detection and Prevention is a Big Data Challenge

Fraud detection and prevention has become a global problem, impacting organizations of all sizes, across all industries. Fraudsters are becoming increasingly sophisticated and successful, especially as commerce and financial transactions move online, where it's easier for fraudsters to evade detection, use stolen credit card information, impersonate individuals and take over online accounts. Furthermore, internal fraud committed by sophisticated employees is difficult to spot. The result is significant fraud-related costs to organizations. When customers are defrauded, the costs can include financial reimbursement of fraud victims, as well as long-term negative impact to company reputation and customer loyalty.

Fraud detection and prevention is a big data challenge. As business moves online, the evidence or patterns of internal or external fraud often lie in the massive amounts of unstructured machine data, often log files, generated within your business applications, IT infrastructure and security systems. This fraud relevant machine 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 and alert on fraud in real time and act to prevent it before it adversely impacts the bottom line.

What Do the Patterns of Fraud Look Like?

Patterns of fraud vary and evolve, just as the behaviors of a cybercriminal are constantly changing. There is no magic "silver bullet" to detect fraud, and detection methods will vary for each organization and each industry. This means that anti-fraud teams need a flexible solution that can search and visualize all fraud relevant data in ways specific to their organization. See Figure 1 for a few examples of fraud across different industries and what related fraud patterns might look like.

Vertical	Fraud Type	Fraud Pattern
Financial Services	Account takeover	Abnormally high velocity or $ of transactions
Healthcare	Physician billing	Physician billing for drugs outside their expertise area
E-tailing	Account takeover	Many accounts accessed from IP or user agent string
Telecom	Roaming abuse	Excessive roaming on partner network by unlimited use customers
Online Education	Student loan fraud	Student who has taken out loans has IP in "high-risk country" and student absent from classes

Figure 1: Fraud patterns vary across industries and organizations.

Limitations of Traditional Anti-Fraud Tools

Traditional anti-fraud detection technologies are rigid and optimized for structured data collection, and their architectures do not easily support the variety or velocity of unstructured machine data. They're limited in the data types they can ingest and often suffer from scale limitations, leading to challenges with massive amounts of data and being able to return results quickly. Because these solutions generally impose data normalization and a data schema, users are limited in the types of questions they can ask, the investigations they can perform and the ways the data can be visualized.

While traditional solutions are effective for selective data analysis, they only provide a narrow window into the full fraud process, such as only looking for front-end web fraud or backend credit card fraud. This siloed view limits the solution's ability to meet the needs of anti-fraud teams.

In addition, these solutions often are expensive, difficult and time consuming to deploy, configure and maintain, and are dependent on extensive services and customization. Each solution typically involves multiple products and data stores, extensive custom development, rigid ETL processes, several user interfaces and specialized resources to build searches and reports.

Enter Splunk

As fraudster behaviors evolve, the solutions that are used to detect fraud must also evolve. Splunk Enterprise is a machine data platform that's increasingly used for anti-fraud purposes. Splunk Enterprise was designed to handle massive amounts of unstructured data on the order of dozens of terabytes a day, and lets organizations index all fraud-relevant machine data across their IT infrastructure—this is the data that often has the fingerprints of fraud. This also includes data from point fraud tools, enabling antifraud teams to break down the siloed views from individual tools and incorporate other fraud-related data (see Figure 2). The data can be further enriched with lookups from structured external sources, such as Active Directory, asset management databases or third-party feeds to provide additional context.

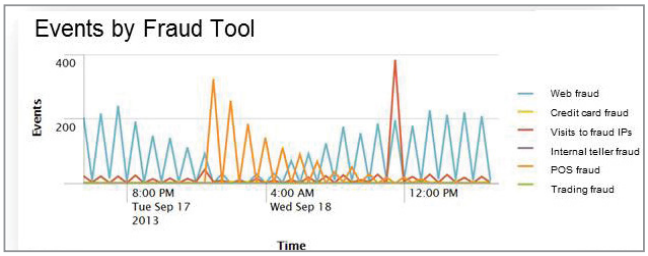

Figure 2: Splunk software breaks down traditional fraud silos.

Splunk Enterprise allows anti-fraud teams to quickly search, correlate, visualize and alert on fraud-relevant data, so these teams can quickly adapt to changing fraud techniques and address a wide range of team needs. As an integrated solution, Splunk Enterprise uses a common data store and user interface, offering a fast time-to-value, ability to easily index data and an intuitive user interface for searching and reporting.

Meeting Anti-Fraud Team Needs

Fraud Monitoring and Detection

Real-time searches and correlations performed in Splunk software can connect disparate events across different data sets to identify fraud as it happens. Splunk Enterprise can create baselines or risk profiles of normal activity and then apply statistical analysis to detect outliers and anomalies that may indicate fraudulent activity (see Figure 3). These anomalies can be detected in both real-time and over a prior period. Real-time alerts can be set to notify anti-fraud teams to take immediate action or initiate actions in other applications to block the activity before it impacts the bottom line.

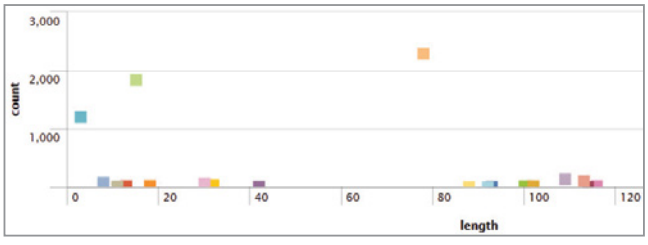

Figure 3: Use statistical analysis to detect outliers and anomalies

Fraud Investigations

Splunk software lets users quickly search and pivot through current or historical data to research possible fraud and to understand the "who, what, where, when and why" around a possibly fraudulent action. If fraud is found, the user can see if the fraud pattern exists elsewhere in the data, as it could potentially be part of a larger fraud ring. Users can then turn the pattern into a real-time search and alert for immediate notification if the fraud re-appears.

Fraud Analytics and Reporting

Flexible, advanced reporting and visualizations support any user or role and makes it easy to analyze, measure and manage fraud risk. Visualizations can include historical reports, projections, order reviewer dashboards, executive/auditor dashboards, GeoIP maps and more.

Enhance Existing Anti-Fraud Tools

Most organizations deploy multiple fraud solutions to combat fraud. In these instances, Splunk Enterprise can index and consolidate the event data from these siloed tools. Splunk software can then consolidate the fraud scores from each tool for a specific web session, transaction, IP or user account to come up with a single, aggregate fraud score. Splunk can also generate consolidated reports containing event information from multiple point fraud tools, allowing organizations to view their enterprise-wide risk posture on a single pane of glass. The Splunk platform helps organizations get more value out of their existing fraud tools.

Supporting Additional Use Cases: Cybersecurity and Compliance

The machine data collected in Splunk software can be used to support other use cases, including cybersecurity and regulatory/internal compliance. Cybersecurity use cases include the detection and prevention of advanced cyberthreats; if successful, these threats could compromise customer data and lead to fraud and account takeovers. Splunk Enterprise is also broadly used for non-fraud/security use cases, such as IT operations, application management and business analytics. Customers who deploy Splunk software for multiple use cases enjoy a compelling ROI and improved interdepartmental collaboration.