splunk> a CISCO company

SERVICES SOLUTION GUIDE

Advanced Loyalty Fraud Detection and Protection

Detect. Prevent. Protect your Loyalty Program.

Empowering businesses to safeguard your assets and reputation with precision and efficiency, our Splunk App for Fraud delivers actionable insights, real-time monitoring, and proactive risk mitigation strategies, ensuring integrity, trust, and resilience in the face of evolving fraudulent threats. This offering enables our customers to install and configure the Splunk App for Fraud Analytics while delivering on one or multiple of the following use cases (unusual point redemption patterns, refund abuse, inconsistent customer behavior, abnormal point transfers or inactive accounts suddenly active).

Leverage the Splunk fraud app for advanced use cases

Identify complex loyalty fraud use cases

Gain valuable insights to align customer behavior and program performance

Address these challenges with the Splunk App for Fraud

- **Inefficient Manual Processes**: The Splunk App for Fraud automates data collection, correlation, and analysis, reducing the need for manual intervention and streamlining fraud detection workflows.
- **Difficulty in Detecting Sophisticated Threats**: The Splunk App for Fraud leverages advanced analytics and machine learning capabilities to identify complex patterns and anomalies indicative of fraudulent activity, enhancing detection accuracy and effectiveness.
- **Fragmented Data Sources**: Organizations often struggle to consolidate and analyze data from disparate sources, hindering their ability to detect fraud across multiple channels and systems. The Splunk App for Fraud integrates data from various sources, including transaction logs, network traffic, and user behavior, providing a comprehensive view of fraud-related activities and enabling organizations to identify cross-channel fraud patterns.
- **Limited Scalability and Flexibility**: As organizations grow and evolve, their fraud detection needs may change, requiring scalable and adaptable solutions. The Splunk App for Fraud offers scalability and flexibility, allowing organizations to expand your fraud detection capabilities as needed and adapt to changing fraud trends and business requirements.

Why Advanced Loyalty Fraud Detection and Protection?

Key Features & Benefits		
Search-time Detection	●	The Splunk App for Fraud enables search-time monitoring and detection of fraudulent activities across various data sources. This allows organizations to identify and respond to fraudulent behavior as it occurs, minimizing financial losses and reputational damage.
Integration with Existing Systems	●	Splunk integrates seamlessly with existing IT infrastructure and security tools, allowing organizations to leverage your investments in technology. This enables unified visibility and correlation of data across different systems, enhancing fraud detection capabilities.
Scalability and Flexibility	●	The Splunk platform is highly scalable and flexible, capable of handling large volumes of data and adapting to evolving fraud detection requirements. Organizations can easily scale your fraud analytics capabilities as your data volume and complexity grow, ensuring continuous protection against fraud.
Improved Operational Efficiency	●	Splunk streamlines fraud detection workflows and reduces the need for manual intervention, improving operational efficiency. This allows organizations to allocate resources more effectively and focus on investigating genuine fraud cases, rather than false positives.
Enhanced Fraud Prevention	●	Beyond detection, the Splunk App for Fraud enables proactive fraud prevention by identifying emerging threats and vulnerabilities. By analyzing historical data and identifying patterns indicative of potential fraud, organizations can implement preventive measures to mitigate future risks.
Enablement of Advanced Data Analytics	●	Enhanced detection accuracy leads to more effective identification of fraudulent activities, reducing financial losses and minimizing reputational damage.
Customizable Dashboards and Reports	●	Customizable visualizations empower stakeholders to gain a deeper understanding of fraud patterns and make informed decisions based on real-time data.
Unusual point redemption patterns, refund abuse, inconsistent customer behavior, abnormal point transferred or inactive accounts suddenly active	●	Enhanced security, protecting customer assets, preserving trust, reducing financial losses and enhancing customer experience.
Threat Intelligence Integration	●	Access to real-time threat intelligence helps organizations stay ahead of evolving fraud trends and proactively defend against new and emerging threats.

What We'll Do and Deliver

- Install and Configure Splunk App for Fraud on Enterprise Security search head
- Normalization of up to 2 data sources per use case to the applicable fraud data model(s). This task will include setting up necessary macros and lookups to align with the data models in scope
- Enabling of all applicable correlation searches related to the Splunk App for Fraud Analytics, which encompasses configuring risk rules and risk notables that correspond with the enabled data models
- If multiple use cases are required, multiple quantities of this offering should be ordered as one engagement will enable one of the following use cases:
  - **Unusual Point Redemption Patterns -** atypical or suspicious behaviors observed in the redemption of loyalty points within a rewards program. These patterns may indicate fraudulent activity or misuse of the loyalty program.
  - **Refund Abuse -** the practice of exploiting a retailer's return or refund policies to obtain undue financial benefits or products. It is a form of fraud where customers manipulate the system, often repeatedly, to gain refunds, replacements, or store credits in a dishonest manner
  - **Inconsistent Customer Behavior -** actions or patterns displayed by a customer that deviate significantly from their typical or expected behavior. In the context of fraud detection and risk management, such inconsistencies can be red flags indicating potential fraudulent activity or account compromise.
  - **Abnormal Point Transfers -** fraudulent activity where loyalty points are transferred between accounts in ways that deviate significantly from normal behavior patterns. Such activity is often a sign of account takeover, collusion between accounts, or other malicious attempts to exploit a loyalty program.
  - **Inactive Accounts Suddenly Active -** refers to the suspicious or fraudulent activity that occurs when accounts that have been dormant or inactive for an extended period suddenly show a spike in activity. This behavior is often a red flag for potential fraud, particularly if the activity involves high-value transactions or other atypical behavior

Resilience, let's build it together

Splunk Customer Success provides end-to-end success capabilities at every step of your resilience journey to accelerate time to value, optimize your solutions and discover new capabilities. We offer professional services, education and training, success management and technical support, surrounding you with the expertise, guidance and self-service success resources needed to drive the right outcomes for your business. For more information contact us at sales@splunk.com.

[1] Outcomes shown were realized by actual Splunk customers and not every customer will realize similar outcomes. Realization of these outcomes are dependent on many factors including state of the customers' environment, skill level of customer personnel, Splunk product(s) being used and many other factors. The figures in this table are used to show examples of the types of outcomes customers can realize and is it not a guarantee for all customers.

Terms and Conditions

This Solution Guide is for informational purposes only. The services described in this datasheet are governed by the applicable fully signed ordering document and any incorporated terms and conditions.

Contact us: splunk.com/asksales

splunk.com