CASE STUDY

Global Retailer Detects Online Fraud with Greater Visibility and Insight

Retail

Executive summary

A U.S.-based department store chain operates globally and sells clothing, tools, appliances, automotive supplies and other products via brick-and-mortar stores, mail-order catalogs, and increasingly, online. The company was facing online fraud ranging from customer account takeovers to abuse of new account activation incentives. Its security team was tasked with supporting the online anti-fraud efforts, but was unable to aggregate, correlate or reveal data quickly from multiple systems and sources. Since deploying Splunk Enterprise, the retailer has seen benefits including:

- Reduced financial losses from fraud and chargebacks
- Reduced labor costs from fraud investigations
- Reduced security vulnerabilities and an improved security posture

Why Splunk

With an online business featuring more than 100 websites, the retailer faced a variety of online fraud threats. The fraud investigation workflow process involved multiple teams and a manual process of gathering relevant log files and then searching through the logs. The process was tedious, often requiring multiple people to work on the issue for hours. Worse, correlating information across different log types was difficult and sometimes log data was overwritten, limiting investigations.

To safeguard its global online business, the retailer needed a single security platform that could quickly detect new fraud techniques, index all fraud and security-relevant machine data, and more quickly present the information to internal teams to identify, investigate and prevent fraud. Traditional security information and event management (SIEM) products couldn't ingest the data sources the retailer needed to index and were focused on fixed rules that couldn't catch creative fraudsters. The company turned to Splunk Enterprise, which it was already using for operational and application management.

Industry

- Retail

Splunk Use Cases

- Security and fraud
- Application delivery
- IT operations

Challenges

- Unable to aggregate, correlate and reveal data quickly
- Manual, time-consuming fraud investigation workflow process involving multiple teams
- Difficulty correlating across different log types
- Existing anti-fraud tools unable to keep up with creative fraudsters

Business Impact

- Reduced financial losses from fraud and chargebacks
- Reduced labor costs from fraud investigations
- Real-time detection of fraud and cyberattacks
- Reduced security vulnerabilities and an improved security posture

Data Sources

- RSA Silver Tail
- Accertify
- Fox IT threat intelligence feed
- Firewalls
- Akamai Web Application Firewall and content delivery network
- OSSEC
- Riverbed Cascade network monitoring
- Custom tools and applications

Splunk Products

- Splunk Enterprise

Rapid investigation and detection of fraud

With Splunk software, all relevant machine data from the retailer's e-commerce business is now in a single location for fast searching, correlations and reporting. Rather than manually searching through logs, teams can quickly research alerts by entering data such as a suspicious IP address on the security portal and then have the Splunk solution show all the behavior associated with that address.

Investigations now can be completed as rapidly as five to 10 minutes or less—just 0.2 worker-hours—and are not hampered by missing log data. The result is substantially quicker identification and blocking of fraud before it undermines the bottom line or tarnishes the company's reputation, as well as reduced labor costs associated with fraud investigations.

Large-scale investigations and IP lookups

Splunk Enterprise has proven particularly useful for large-scale fraud investigations, detecting fraud rings and advanced correlations. For example, the retailer might see a transaction with an overseas IP address, a shipping address in New York and a billing address in California, and can then immediately alert its fraud team.

With Splunk Enterprise, the retailer can also automate lookups against all the IPs connecting to its websites to quickly spot possible site traffic related to fraud. All IP addresses in Splunk Enterprise are crosschecked against both a list of known bad IPs from Fox IT as well as a custom blacklist of IPs previously involved in fraud against the retailer. Splunk has also proven helpful in identifying fraudsters trying to hide their true location, such as overseas fraudsters who use proxies with U.S. IP addresses to appear as though they are domestic users.

> **"Our Splunk solution proves over and over that Operational Intelligence can combat malicious exploits like fraud on e-commerce sites. Fraudsters and cybercriminals may be getting savvier, but with the analytics enabled by our Splunk software, so are we."**
>
> Lead Application Security Engineer
> Leading global retailer

Prevent customer account takeovers and safeguard incentive programs

Splunk can also help identify account takeovers where a fraudster has obtained the online store credentials of legitimate customers via phishing or malware. The retailer can spot these account takeovers by looking for patterns such as a single IP or URL referrer string accessing an excessive number of customer accounts, or a single IP address attempting to log in using hundreds of different credentials. Using Splunk Enterprise, administrators are also able to detect fraudulent attempts to open and exploit multiple loyalty accounts with the sole intent of obtaining "account opening" financial incentives.

Safeguarding data across the enterprise

With the Splunk platform, the retailer's security and loss prevention teams now have additional context and data integrated into their legacy portal for fraud investigations that can be shared by multiple teams. Splunk Enterprise provides consolidated fraud reporting across multiple fraud tools to help break down the data silos that typically exist between point tools to show a broader, enterprise-wide view of fraud. Splunk dashboards show trending of fraud events, critical alerts from other fraud tools and spikes in alerts. The security team also uses Splunk software to detect and defeat cyber attackers attempting to break into the network to compromise customer information, which can lead to downstream fraud.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com