splunk> CASE STUDY

Surescripts Protects Doctors and Patients with Improved Fraud Detection and Security

surescripts
The Nation's E-Prescription Network

Executive summary

Founded in 2001, Surescripts operates the largest health information network in the United States, designed to connect a diverse and expansive community of care partners including pharmacies, providers, benefit managers and health information exchanges. With vast amounts of data flowing across its technology-neutral platform, Surescripts needed to maintain a close watch over fraudulent activity and wanted real-time visibility into its entire security posture for faster reporting and incident response. Since deploying Splunk Enterprise, Surescripts has seen benefits including:

- Improved fraud detection accuracy
- Immediate insights into security events
- Reduced incident response times

Why Splunk

Surescripts processes more than six billion transactions each year, including more than 700 million medication histories, one billion e-prescriptions and nearly ten million clinical messages. Prior to Splunk, identifying and analyzing fraudulent transactions was a tedious, time-consuming process for Surescripts' Information Security and Risk Management team. The team would receive unique alerts from each disparate platform, decipher each alert individually and then export the associated raw log data into Excel for analysis. Additionally, Surescripts was experiencing 24-hour latencies on investigations with its existing security information and event management (SIEM) system, which was too long of a delay.

Surescripts deployed Splunk Enterprise across its complicated infrastructure—consisting of multiple datacenters and extensive virtual and in-house hardware—for enterprise security and fraud management. "We realized our investment the minute we deployed the Splunk solution. Splunk software has empowered Surescripts to determine what is important—to take full control of all our data," says Paul Calatayud, Surescripts' chief information security officer (CISO).

Industry

- Healthcare

Splunk Use Cases

- Security
- Business analytics

Challenges

- Safeguarding huge volume of sensitive information
- Time-consuming manual process for identifying and analyzing fraudulent transactions
- 24-hour latencies on existing SIEM solution
- Lack of real-time visibility into processes

Business Impact

- Increased automation of daily fraud checks on billions of transactions
- Faster and improved fraud detection accuracy
- More in-depth real-time and historical data fraud analysis
- Immediate insights into security events
- Significantly reduced incident response times
- Ability to create customized, in-depth, intricate reports

Data Sources

- 3,000 data sources
- VPN, firewall and server logs
- Malware IDs
- Failed password attempts

Splunk Products

- Splunk Enterprise
- Splunk DB Connect
- Splunk for Palo Alto Networks
- Splunk on Splunk (S.o.S)
- Splunk Enterprise Security (planned)

Automating and improving real-time fraud detection

Since deploying Splunk Enterprise, Surescripts has streamlined processes and automated the analysis of fraudulent activity. All raw log event data now comes through the Splunk interface, significantly reducing the time needed to detect, analyze and mitigate fraud.

With Splunk software, Surescripts now sees patterns within the data that identify physicians who may be self-prescribing medications. Similarly, Surescripts can recognize legitimate doctors on the network writing valid prescriptions—and protect them from identity theft. More complex fraud queries in Splunk Enterprise have enabled Surescripts to introduce and monitor multiple "risk" variables, such as data about doctors prescribing restricted and commonly abused medications over a set time period in a particular location. Splunk provides historical trending for these variables so that Surescripts can identify pattern anomalies and determine whether a doctor's credentials have been compromised.

Replacing a legacy SIEM solution

After replacing its legacy SIEM solution with Splunk software, Surescripts gained immediate insights from its unstructured data. Calatayud explains, "Splunk allows you to look beyond your data into security areas, so you're getting an all-encompassing view. Our team's expertise becomes a key variable in the analysis of what is meaningful. That just can't be done with your typical SIEM."

"Not only are we achieving better response times, we're able to pivot and dig deeper whenever we find something of interest," says Steve Olson, manager of security services for Surescripts. "We're able to build velocities around patterns using Splunk's reporting engine to create intricately customized and in-depth reports. It is much easier to do that with Splunk software than the old SIEM. Moreover, reports that previously took 15 minutes to generate for each state are now generated automatically and instantaneously."

> **"We realized our investment the minute we deployed the Splunk solution. Splunk software has empowered Surescripts to determine what is important—to take full control of all our data. We've been able to expand our scope of fraud detection and improve alerting across our entire platform, enabling faster response to incidents."**
>
> Paul Calatayud, CISO
> Surescripts

In addition, Splunk DB Connect gives Surescripts access to data stored in relational databases. Previously, the team logged remotely into the production environment and the needed data wasn't always available due to dependency on upstream processes. "With DB Connect, as the data shows up, it's immediately imported. It makes our lives much easier," Olson explains.

Increased interoperability across entire infrastructure

The Surescripts network integrates with a variety of clinical, electronic prescribing and pharmacy management software systems. Interoperability is critical to these systems, especially in view of increasingly stringent federal regulations for the healthcare industry. Thanks to Splunk software, Surescripts now exchanges and interprets shared data across these internal platforms. This ensures that the electronic exchange of prescription information is carried out smoothly across Surescripts' entire infrastructure—while safeguarding patient privacy.

Currently, more than 200 individuals across Surescripts use the Splunk reporting interface, including IT, server, network, database and development staff. There are plans for the quality, products and formal business intelligence teams to use the Splunk solution as well. Calatayud concludes, "We're going to start to see Splunk software move from internal utilization to supporting all our products indirectly."