

Aflac Adopts Splunk Platform for Analytics-Driven Security



Executive summary

Aflac is the leading provider of voluntary insurance in the U.S. Facing an increase in the volume and velocity of security threats, Aflac needed a new analytics-driven security approach to protect its customers, nearly 10,000 employees and brand reputation. The company adopted the Splunk platform to sit at the heart of its internal Threat Intelligence System (TIS). Since deploying Splunk Enterprise Security (ES) and Splunk User Behavior Analytics (UBA), Aflac has seen benefits, including:

- Two-week enterprise-ready implementation
- Blocking more than two million security threats in one six-month period
- Saving 40 hours monthly by replacing manual data collection and reporting, enabling teams to focus on proactive security monitoring and analysis

Why Splunk

As Aflac enters new markets and offers new services, the company needs to adapt its security program continuously to match a rapidly changing threat landscape that includes everything from spear-phishing to the proliferation of malware. Prior to adopting the Splunk platform, Aflac relied on a legacy security information and event management (SIEM) solution, but the company required a stronger threat intelligence platform to detect and respond to attacks adequately.

According to D.J. Goldsworthy, director of Security Operations and Threat Management for Aflac, “With our previous SIEM, you had to know the data exceedingly well before you could take action, whereas Splunk helps you know your data very quickly. Splunk made us much nimbler and enabled us to show value to all of our stakeholders quickly.”

Initially, Aflac stood up Splunk ES for threat hunting. “Our proof of concept, in essence, was using Splunk ES for our threat hunting use cases, and the time to value far exceeded our expectations,” Goldsworthy says. “We were able to do extraordinary things in a very short period of time to detect advanced threats. Ultimately, that was the decision point for us to make a much larger investment in Splunk ES and UBA across our different security use cases.”

Industry

- Financial Services

Splunk Use Cases

- Security
- Fraud

Challenges

- Needed a robust security platform to protect customers, 10,000 employees and brand reputation
- Wanted to eliminate manual data collection and reporting to focus on proactive security investigations

Business Impact

- Blocked more than two million security threats in one six-month period
- Orchestrated threat intelligence across 20 security technologies sitting within TIS
- Automated threat hunting and 90 percent of security metrics process in just two months
- More than 40 hours saved monthly
- TIS in place within five months, one month ahead of schedule

Data Sources

- Operating Systems
- Next-Gen Firewalls
- Intrusion Detection Systems
- Email Security
- Endpoint Security Agents
- DNS Firewall
- Web Application Firewalls
- Other various application and security solution logs

Splunk Products

- Splunk Enterprise Security
- Splunk User Behavior Analytics

Immediate return on investment

According to Goldsworthy, the time to implement the Splunk platform and get it enterprise-ready was short – just a couple of weeks. “That was quite surprising, given the volume of data sources we were bringing in and the number of use cases that we wanted to get in place,” Goldsworthy explains. “With Splunk, we saw immediate return on investment.”

Today with Splunk ES in Aflac’s security operations center (SOC), the company has saved time for numerous full-time employees. “We calculate that we save more than 40 hours a month in terms of doing reports that used to be manual that are now fully automated,” Goldsworthy says. “Splunk has made it very easy to ingest data from different sources and then present them in a way that is meaningful to stakeholders, such as our board or other leadership.”

Six teams composed of approximately 40 individuals rely on the Splunk platform to manage broad security use cases, including threat hunting, threat intelligence, security operations, incident response, application security, security administration and fraud.

“We implemented Splunk first for threat intelligence and then security operations, and realizing how versatile the solution is, we determined that that the logical next step for us was to apply that to fraud,” Goldsworthy says.

Automating threat intelligence

Aflac put its TIS in place within five months, finishing one month ahead of schedule. The system provides tactical and strategic functions, adding automation to create efficiencies in the daily threat data feed, saving time and reducing errors. The system automatically consumes indicators of compromise (IoCs) from more than 20 different threat intelligence sources and provides automated confidence scoring and risk profiling of each IoC. This enables Aflac to track thousands of IoCs and perform real-time correlation against network and system logs in its Splunk security analytics platform. Then, SOC analysts can rapidly

“We were able to do extraordinary things in a very short period of time to detect advanced threats. Ultimately, that was the decision point for us to make a much larger investment in Splunk ES and UBA across our different security use cases.”

D.J. Goldsworthy, Director of Security Operations and Threat Management
Aflac Incorporated

respond to potential incidents. Within one six-month period, Aflac was able to block more than two million security threats, with fewer than 12 false positives.

“From the perspective of an individual policyholder, I know they would want to know that we’re doing everything we can to help keep their information safe. We are paying close attention to how we manage our own information as well as how we manage their personal information, and that’s something that Splunk allows us to do,” says Ben Murphy, vice president of information security, Aflac.

Anomaly detection adds value

As businesses add contractors and others with privileged access to networks, it becomes very difficult to understand whether everyone is in compliance with all of the security policies and best practices or if there are any risks hidden in these activities. “Splunk UBA provided another rich layer of detection to Aflac’s security program, which is capable of identifying anything that happens outside of the normal behaviors we typically observe,” Goldsworthy says.

“From the perspective of an individual policyholder, I know they would want to know that we’re doing everything we can to help keep their information safe. We are paying close attention to how we manage our own information as well as how we manage their personal information, and that’s something that Splunk allows us to do.”

Ben Murphy, Vice President of Information Security
Aflac Incorporated

[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.



Learn more: www.splunk.com/asksales

www.splunk.com