CASE STUDY

Heartland Automotive Protects Brand Reputation, Secures Data With Splunk Platform

Heartland Automotive Services
America's Largest Jiffy Lube® Franchisee

Industry

- Retail
- Automotive Services

Splunk Use Cases

- Security
- Compliance

Challenges

- Lacked a platform for real-time security investigations and insider threat protection
- Security investigations involved manual processes and took hours
- Needed platform to protect brand and drive innovation

Business Impact

- Achieved time to value in three weeks
- Gained platform to drive innovation with 25% less TCO
- Reduced security investigations from hours to real time
- Gained insider threat protection
- Established PCI compliance

Data Sources

- Network routers
- Network switches
- Microsoft SQL Server
- Amazon Web Services, CloudTrail

Splunk Products

- Splunk Enterprise Security
- Splunk User Behavior Analytics

Executive summary

Known for its signature oil change, Heartland Automotive Services, Inc., dba Jiffy Lube, is the largest franchisee of quick lube retail service stores in the U.S. Heartland Automotive needed a cybersecurity platform to protect its brand and its most important resource—its data. Since deploying Splunk Enterprise Security (ES) and Splunk User Behavior Analytics (UBA) as its integrated security information and event management (SIEM) platform, Heartland Automotive has seen benefits including:

- Realized time to value by implementing a SIEM and insider threat protection solution in only three weeks
- Gained platform to drive innovation with 25% less TCO
- Established real-time security investigations and insider threat protection

Why Splunk

Heartland Automotive owns and operates nearly one-quarter of the U.S. Jiffy Lube stores—approximately 531 locations across 26 states. The private equity-owned company is one of 200 Jiffy Lube franchisees. "While most franchisees are operations with 10 locations or fewer, given Heartland Automotive's scale we are often in the unique position to provide thought leadership, not only within the Jiffy Lube brand but across the industry," says Chidi Alams, head of IT and Information Security, Heartland Automotive Services.

Alams is responsible for IT and cybersecurity, and he also collaborates with the chief marketing officer and operational leaders to align with business needs and surface innovation opportunites. Prior to adopting Splunk software, Heartland Automotive did not have a cybersecurity program or a Security Operations Center (SOC). Instead, systems administrators manually checked events using the company's Kaseya log management tool and responded to security incidents reactively. Overall, Heartland Automotive lacked the technology and security personnel resources needed to adequately protect its brand.

Alams notes that Heartland Automotive was lucky to have avoided significant malware and ransomware events. However, the IT team found that security events were difficult to address and mean time to resolution was a problem. For example, addressing malware infections should have taken 30 minutes or less, but instead took several hours on average. The company also lacked adequate security analysis and forensic capabilities.

Alams had maintained a Splunk instance and used Splunk Enterprise at another company previously, but he assessed Heartland Automotive's cyber and operational needs to avoid a blind spot born of product familiarity. "Splunk ES checked all the boxes and then some. The seamless integration with UBA was a differentiator," Alams says. "With Splunk I have a centralized platform to address security and insider threats. If we can, we choose a platform over a technology solution so we can solve many problems and extend it to other business use cases and requirements."

> **"Data is our most critical asset, and as a retailer the ability to have a platform to help protect our brand is everything."**
>
> Chidi Alams
>
> Head of IT and Information Security, Heartland Automotive Services

Alams appreciates the flexibility of a platform that enables the company to meet business needs and drive innovation at a lower cost. "Splunk's licensing was 25 percent less expensive than alternative solutions," Alams says. "The TCO comparison only supported, or further reinforced, our decision to choose Splunk."

Fast, seamless SIEM implementation

SIEM implementations are often complex, as large organizations have many data sources and it may require weeks to configure alerts. According to Alams, the Splunk professional services team made the entire process of identifying the company's data sources, fleshing out the SIEM design and configuring alerts seamless.

"Fast time to value is everything—we were able to implement a SIEM and insider threat detection solution in three weeks in what would normally take three months," Alams says. "The chief financial officer and other members of our senior leadership team have been impressed with time to value—to see it one day and almost be implemented the next—increased their confidence in us to deliver quickly."

Innovation platform for security and beyond

Heartland Automotive's new security program includes a SOC, security policies and procedures, and PCI compliance. With the Splunk platform, Heartland Automotive now has end-to-end visibility into its security posture and potential threats to the enterprise. The team can see a full breakdown of critical daily events to prioritize management and resolve issues quickly.

One important alert informed Alams' team that tens of thousands of DNS inquiries were generated at corporate headquarters by a few domains. The team was able to quickly triangulate the threat and take a device off the network to avoid data exfiltration that could have harmed not only the bottom line, but more importantly, the brand. "Data is our most critical asset, and as a retailer the ability to have a platform to help protect our brand is everything," Alams says.

UBA delivers machine learning

Organizations face more sophisticated zero day attacks and they need a more dynamic way of identifying issues. According to Alams, UBA brought the power of machine learning into the environment, enabling his team to monitor patterns of behavior built into the solution and respond quickly. With UBA, Heartland Automotive is eliminating blind spots that can be addressed by machine learning. "With Splunk Enterprise Security and UBA, we have one platform for cyberthreats and Operational Intelligence through which to drive innovation," Alams says.

> **"Splunk's licensing was 25 percent less expensive than alternative solutions. The TCO comparison only supported, or further reinforced, our decision to choose Splunk."**
>
> Chidi Alams
>
> Head of IT and Information Security, Heartland Automotive Services

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