

Carrefour Responds to Security Threats 3x Faster With Splunk Cloud Platform

Key Challenges

Although Carrefour spent significant resources maintaining legacy infrastructure and detecting security events, it's sometimes complicated to provide the multi-channel experience customers expect.

Key Results

With Splunk Cloud Platform, Carrefour better protects its business and improves customer experience with actionable insights into system performance and faster security response times.



Industry: Retail

Solutions: Platform, Security

Products: [Splunk Cloud Platform](#), [Splunk Enterprise Security](#)

Today's superstore shoppers want a multi-channel experience.

The eighth-largest global retailer, Carrefour has superstores in Europe, South America and Asia. It knows customers expect the same convenience online as in-store, whether ordering via the mobile app or getting "click and collect" deliveries. To improve customer experience across its online shopping channels, Carrefour embraced a digitization strategy that includes taking advantage of cloud-based services.

With Splunk Cloud Platform, Carrefour now has the agility to focus on developing new features and services. Splunk Cloud Platform also simplifies security, so customers can shop safely. Using real-time insights from Splunk, Carrefour now responds three times faster to security threats and makes smarter decisions about preventing incidents.

A three-times faster response time to security events

Operating a complex infrastructure based on a legacy data center, Carrefour's Security Operations Center (SOC) team previously spent significant amounts of time and effort managing systems — rather than focusing on protecting the business from malware. By centralizing security analysis and integrating multiple data sources, Splunk Cloud Platform has significantly improved the SOC team's ability to respond to incidents in real time.

"Splunk Cloud Platform handles all of our logs, whether from our antivirus software or endpoint detection and response," says Romaric Ducloux, SOC analyst at Carrefour. "Splunk raises the alert, opens a ticket and contacts the on-call SOC analyst. It's the cornerstone of our security operations."

Using the cloud model means Splunk manages security operations and infrastructure, so Carrefour's SOC team has more time to focus on application management, threat analysis and security investigations. The team can now intervene during incidents before they cause damage to systems or affect customers. In the event of a breach, it gathers information about what went wrong so it can improve its systems in the future.

Outcomes

3x
faster threat response times

€10B
(\$10.45B) projected in e-commerce sales by 2026

More
team capacity for higher-value tasks

Now the team responds to incidents three times faster. “Splunk Cloud Platform allows us to refocus on our most important task: ensuring customers always have a safe shopping experience,” says Ducloux.

Innovation and resilience with Splunk

The Carrefour team appreciates how accessible Splunk Cloud is for the entire SOC team — including both technical experts and business analysts. Because the language used to investigate security events is both easy to learn while also providing powerful analytics, it helps the SOC team quickly mine deep intelligence about the tactics, techniques and tools used by cyber-attackers. This provides powerful protection against future incidents.

“We get so much value from Splunk,” says Ducloux. “It maximizes the insights we gain from analyzing detection use cases, rather than wasting time creating rules or struggling with a tool that’s too complicated.” And since business users now have full access to all the information happening at a systems and operational level during a security event, they can act independently to investigate and raise alerts across the organization.

To dig deeper into logs and data, the SOC team uses the Splunkbase app. It seamlessly integrates with multiple sources so Carrefour can carry out tasks, such as adopting SaaS proxies, with minimal effort. Now Carrefour is confident it can launch innovative new features and services for shoppers while maintaining resilient and efficient security operations.



We get so much value from Splunk. It maximizes the insights we gain from analyzing detection use cases, rather than wasting time creating rules or struggling with a tool that’s too complicated.”

Romarc Ducloux, SOC Analyst,
Carrefour



Splunk Cloud Platform is the cornerstone of our security operations.”

Romarc Ducloux, SOC Analyst,
Carrefour

Scaling to support €10bn in e-commerce sales

Carrefour has ambitious plans for the future, the retailer aims to triple its e-commerce sales to reach 10 billion euros (\$10.45 billion) by 2026 and to expand globally.

By providing the ability to easily scale to accommodate a global SOC spanning multiple countries, and to manage rising amounts of data and logs from new countries or markets, Splunk Cloud Platform gives Carrefour the insight and agility it needs to maintain a secure foundation on which to build an innovative future.

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