splunk> a CISCO company

CASE STUDY

Progressive Protects Customers and Revenue with Splunk

Key Challenges

Progressive Insurance needed to expand its visibility into security, IT, and engineering environments, prevent costly outages and safeguard its customers' ability to access critical information during an emergency.

Key Results

With full-fidelity security and observability, Progressive advanced its monitoring capabilities to detect threats faster and quickly resolve service delays and downtime.

PROGRESSIVE®

Industry: Financial Services

Solutions: Security, Observability

Product: Splunk Cloud Platform, Splunk Observability Cloud, Splunk Enterprise Security

Progressive Insurance is on the front lines of any crisis.

Serving more than 30 million policies globally, the insurer is often the first phone call customers make after a car accident, house fire, or natural disaster. Customers rely on Progressive to help them get back on their feet in those critical moments. For Progressive, being the calm in the eye of the storm is a daily reality.

"It's a relationship. Customers trust us to be there at the worst moment in their life. So if your property gets damaged, your home, your car, or you're in a significant event, oftentimes one of the first people you talk to is on the insurance side." - Jon Moore, Domain Architect, Progressive Insurance.

Progressive insures everything from automobiles and homes to RVs and motorcycles. When a home or possessions are damaged or destroyed, Progressive steps up to the plate. But with millions of dollars on the line daily, split-second transaction delays can mean exponential financial losses.

Edge failures and latency were costing Progressive real dollars. Its existing tools couldn't identify all of the request failures. They needed a solution specifically designed for cloud platforms. Progressive turned to Splunk Observability Suite and Splunk Enterprise Security to expand visibility across security, IT and engineering to prevent costly outages, ensuring customers could access critical information—and a helping hand—when they needed it most.

Outcomes

- **$120 billion** in market capitalization protected
- **Reduced noise** in SOC significantly with risk-based alerting
- **8 million traces** and **50 million spans** effortlessly captured without impact on compute performance

Cutting through the noise and putting out fires

Expanded visibility and a holistic view of Progressive's IT environment is especially critical when keeping organizations safe from attack. Like many security operations centers (SOC), Progressive's SOC was inundated with security alerts, which overwhelmed analysts and caused alert fatigue.

Now, risk-based alerting (RBA) in Splunk Enterprise Security allows the Progressive team to quickly cut through the noise and prioritize the most serious threats, reduce alert volumes, and detect security events at exactly the right time. "Too early, you're going to get a whole bunch of noise. Too late, all the bad things have already happened," says Dru Streicher, DevOps lead engineer at Progressive. "

What RBA allows you to do is to say it's okay to have noise. Because eventually, we're going to prioritize the noise and get the signals out of all of those breadcrumbs."

It also provides granular data visibility, enabling the team to correlate and contextualize numerous factors around every event. Instead of judging a single incident, they're able to create a narrative around their entire risk environment.

"Put it all together and tell us a story. Security should always be a story. If you're not telling a story with security, you're completely doing it wrong. With RBA, we can stitch together a bunch of events to form the story of risk to our environment," says Streicher.

Being progressive on observability

Progressive manages an incredible amount of data, and the insurer needs unified visibility into all of it. Continuity is key. A thirty-second processing delay can rob customers of critical information they need while costing the company millions of dollars in lost time and revenue.

In the wake of a disaster or accident, Progressive's Claims application processes are a lifeline — the company handles roughly 15 million web requests each day, protecting over $120 billion in market capitalization. Splunk APM's full-fidelity tracing captured each of the app's 8 million traces — adding up to 50 million spans — while having little to no impact on compute performance. On this huge volume of data, Splunk's impact is just a 10-millisecond page response, with less than 1% on both CPU and memory processing.

When you have a company the size of Progressive, approaching 65 billion in annual revenues, with 10 minutes, one hour, two hours of outage, there are real dollars there," says Moore. "So if we can show that monitoring was able to pick up prior to a service disruption, we're able to show that the investments we make in the monitoring tool are giving the business value."

Jon Moore, Domain Architect, Progressive Insurance

And while being a modern insurance provider means relying on data and technology, it is still very much rooted in human empathy, and supporting people in their greatest times of need. "Our goal is to get you in and out of that claims process as quickly as possible so you can get back to your life, get that car payment ready to go for the claims process, get back to your job, and put this behind you," says Kyle Sickels, Progressive's claims monitoring capability leader.

The claims organization improved their understanding of the user experience with real user monitoring (RUM) in Splunk Observability Cloud which allows them to identify and prioritize when and where to work on a web app. Meanwhile, Splunk Observability Cloud provides real-time insights to help spot and resolve anomalies, successfully preventing disruptions, latency, and other critical issues.

Splunk's application performance monitoring (APM) capability is also essential for maximizing revenue. It provides critical business continuity so Progressive can deliver vital services smoothly with no interruptions. Today, the team uses APM to determine the application error rate, which errors are occurring or if those errors are new, and the overall health of the applications. For business leaders, APM helps measure the quality at which they're delivering those applications.

"When you have a company the size of Progressive, approaching $65 billion in annual revenue, with 10 minutes, one hour, two hours of outage, there are real dollars there," says Jon Moore, domain architect at Progressive. "So if we can show that monitoring was able to pick up prior to a service disruption, we're able to show that the investments we make in the monitoring tool are giving the business value."

Driving toward new horizons with Splunk

Looking ahead, Progressive plans to expand its deployment of Splunk Observability Cloud, exploring various applications for OpenTelemetry and infrastructure and synthetic monitoring for ease of use and effectiveness.

24-679723-Progressive-CS-102