splunk>

CASE STUDY

Splunk's Security Teams Reveal How We Protect Customers and Our Own Environment

Key Challenges

Protecting Splunk and our customers is our highest priority, which means our security teams must be agile, flexible and resilient to stay ahead of the ever-evolving cyber threat landscape.

Key Results

With the Splunk platform at the heart of our SOC, teams have the visibility and insights they need to combat threats, protect our complex environment and equip customers with valuable tools to bolster their own security.

Industry: Technology

Solutions: Security, Platform

Splunk knows a thing or two about the security challenges our customers encounter — because we face them too.

Increasingly sophisticated cyber threats that relentlessly pose a threat to our 7,500 Splunkers. Rising volumes of distributed data that make end-to-end security harder than ever. A cloud transformation that expanded our attack surface.

As a high-growth company with global scale, Splunk has seen all these challenges and more — just like our customers. But in relying on the Splunk platform for granular visibility into our complex environment, security teams have remained resilient throughout these challenges, combating threats, protecting our customers and ensuring systems and Splunkers stay secure around the clock. With the Splunk platform, teams across security, IT and DevOps are all on the same page, ensuring holistic visibility into our global infrastructure and helping Splunk remain resilient in the face of persistent threats.

Separating the noise from the real threats

Splunk's Threat Response team is tasked with being ready to respond to a security event at a moment's notice — working quickly to ensure the integrity of the company's security posture. But in an environment where hundreds of alerts are triggered weekly, it's a challenge to separate the real bad news from the noise.

With Splunk SOAR, our team optimizes threat response by reducing manual operations — while also keeping costs down in the process. With playbooks to run repeated searches and automate enrichment workflows, team members can focus on critical, strategic projects, not time-consuming, repetitive tasks. "Since appending details to the search is all done automatically, Splunk SOAR playbooks save analysts from having to hunt around for additional information or jump to another console," says Matthew Bellezza, senior manager of monitoring operations at Splunk. "This means we can keep SOC efficiency up while keeping costs down even as the business scales."

Data-Driven Outcomes

30%
faster MTTR on average across security use cases

1st
to market with prescriptive guidance on Log4Shell

Improved
visibility across a distributed ecosystem

These efficiencies increased by reducing the mean time to resolve an incident by as high as 30% across all use cases — and improved MTTR by as much as 84% on a single use case. "The speed and depth of analysis is hands down best with Splunk, which makes it the clear first choice for security teams," says detection engineering senior manager Jonathan Heckinger. "That was true back when I was a Splunk customer, and it's true today for our Splunk SOC to keep customers and Splunkers protected."

The speed and depth of analysis is hands down best with the Splunk platform, which makes it the clear first choice for security teams. That was true back when I was a Splunk customer, and it's true today for our Splunk SOC to keep customers and Splunkers protected."

Jonathan Heckinger, Senior Manager, Detection Engineering, Splunk

First on the scene for Log4Shell

The sun doesn't set on security. Splunk ensures 24/7/365 security to protect our $3 billion business and our customers' organizations from a constant barrage of threats. Enter Log4Shell, which splashed onto the scene in late 2021. The zero-day vulnerability in the popular Java logging library allows bad actors to perform remote code execution undetected — critically threatening countless applications worldwide. Splunk didn't just remediate our own vulnerabilities — we immediately rolled up our sleeves to show our customers how to do the same.

In around 12 hours, the Splunk security threat research team used Splunk Enterprise Security to quickly isolate potentially vulnerable assets, initiate incident response procedures and mitigate the vulnerability. Determined to share critical messaging about Log4Shell, the team then developed a first-to-market response playbook for customers and the broader public. The Cybersecurity and Infrastructure Security Agency recognized Splunk as the first cybersecurity company to issue prescriptive guidance on Log4Shell — with 13 detections and nine playbooks, to be exact.

Our data-agnostic platform helped us make informed decisions when it mattered, and helped us live up to our values — taking care of our customers by acting quickly and equipping them with tools to protect themselves from headline-making threats.

Delivering on our promise to our customers — and ourselves

Thanks to our technology and amazing village of Splunkers and customers, Splunk has experienced historic growth at scale, including 15 acquisitions in the last 10 years. Add to that our own cloud transformation efforts, and we have a complex technology ecosystem — every inch of which needs to be ironclad at all times. To deliver a secure environment for customers in over 130 countries, we use Splunk Cloud Platform to visualize and proactively close any gaps in security coverage that might impact our customers' business — as well as our own.

With Splunk Cloud Platform, the detection engineering team can measure end-to-end visibility across our environment, visualize missing or incomplete data and collaborate with leadership to continuously improve our security posture. This is key to helping Splunk and our customers remain resilient, regardless of what new threats may be on the horizon.

23-71455-Splunk on Splunk for Security-CS-SS-103