

Slack Unlocks Data to Empower Collaboration

Key Challenges

Slack needed a best-in-class tool to gain better visibility and control over their security landscape — and when COVID-19 hit, this need became critical.

Key Results

With Splunk, Slack verifies security across all products and applications, operating in a zero trust network to ensure a secure experience for the more than 12 million daily active users who rely on its platform.



Industry: Technology

Solutions: Security, SIEM

Across the globe, more people are working from home than ever before.

A single pane of glass for all conversations, Slack creates an environment where remote workers can organize information and conversations around data. Every day, more than 12 million active users and 750,000 organizations rely on Slack to be their collaboration hub to bring people, information and tools together.

When the COVID-19 pandemic hit, Slack had to transition more than 1,600 employees to remote work while also continuing to provide a secure, enterprise-grade service to its booming user base.

With Splunk, Slack has seamlessly transitioned to remote work, operating under a zero trust network. The company verifies security with visibility into all activity occurring across its cloud services.

Uniquely Positioned for the Pandemic

Over its history, Slack has innovated its interface to provide an interactive experience for its users. “It’s designed to provide a virtual world that offers the best possible surrogate for the real-world interaction that we have with people,” says Larkin Ryder, director of product security at Slack.

When COVID-19 infections began to rise, the Slack platform proved ideal for remote work. “Everything about the way we’ve designed the interface of Slack — and the tools it provides and supports — is so that you can feel as close as you possibly can to the people you’re working with,” Ryder says. “You can have this organic conversation and discussion richly contextualized with information.”

Data-Driven Outcomes

12M+

daily active users and over 750,000 organizations with access to reliable, secure services

1,600+

Slack employees securely transitioned to remote work during the pandemic

Zero

trust network seamlessly operated with Splunk Cloud

Turning Data Into Action

Yet with a steep surge in demand during the pandemic, Slack needed to ensure that its security program was working effectively. As a result, the organization used Splunk's expertise to make enhancements — from launching new API integrations to functioning in a zero trust network.

"We want to be the organization that's always working with best-in-class tools like Splunk, which gives you a single view across your organization and provides all the analytics you need," Ryder says.

Slack integrated its analytics API with Splunk, making it easier for users to keep a finger on the pulse of their organization, especially during a pandemic. The API integration enabled customers to get information around topics and channels of messaging between people, allowing leadership to stay connected. All Slack's critical applications now send logging content into Splunk, bringing all data into one place offering insight into behavior patterns.

For instance, when a customer needed Slack's help to investigate a specific behavior pattern within the application, Slack immediately recommended that they turn to Splunk. "We were able to get our customer from a point where they knew very little about the behavior and usage of their Slack instance to leveraging Splunk for full visibility," Ryder says. "They were up and running in a matter of hours and could use Splunk and Slack together to take action on their data and protect their environment."



Splunk is a key part of Slack's ability to operate a zero trust network. Because Splunk gives us the visibility into all the activity that's happening across all of our cloud services."

Larkin Ryder, Director of Product Security, Slack



Splunk is how we verify that our security program is operating across our entire fleet and across our corporate applications the way we expect it to, the way we must to assure the integrity of our company."

Larkin Ryder, Director of Product Security, Slack

Running a Secure Ecosystem

Integration is key to managing complexity around Slack's security environment.

"If you can't integrate with Splunk, we can't use your service," Ryder says. "You have to be able to work with our best-in-class products ecosystem. And if you're going to be an island of data that requires people to spin up a whole area of expertise and have a separate team to manage, we just don't have time for that." This dedication to strong integrations has allowed Slack's customers, some of whom have tens of thousands of Slack teams, to visualize activity and connect the dots with applications and various rule sets in place.

Operating in a zero trust network — where users are authenticated and authorized — has strengthened Slack's security posture. "Splunk is a key part of Slack's ability to operate a zero trust network," Ryder says. "Because Splunk gives us the visibility into all the activity that's happening across all of our cloud services."

For Slack, staying secure has been essential as it continues to innovate and stays in lockstep with its customers. "Our employees do a great job of managing their power and control over our security systems, but of course the security engineer's adage is 'trust but verify,'" says Ryder. "Splunk is how we verify that our security program is operating across our entire fleet and across our corporate applications the way we expect it to, the way we must to assure the integrity of our company."

[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