

Minnesota Judicial Courts Boost Productivity and See \$1M ROI Through Automation

Key Challenges

Minnesota Judicial Courts lacked a single interface through which to analyze data across their ecosystem, while security analysts spent too much time on repetitive, manual tasks.

Key Results

The court system uses Splunk as its single, unified platform to respond to security alerts. With automation from Splunk SOAR, analysts can offload manual tasks, focus on alerts that matter and reduce cost of operations.



MINNESOTA
JUDICIAL
BRANCH

Industry: Public Sector

Solutions: Security

Delivering swift, secure justice is no easy feat.

To provide justice through a system that assures equal access and fair, timely case resolution, the Minnesota Judicial Courts must be reliable, responsive, free from discrimination and well managed. That's a lot to achieve — and success requires delivering services within a secure environment.

To do this, the Minnesota Judicial Courts turned to Splunk Enterprise Security (ES) and Splunk SOAR to safeguard their systems, thwart threats and better deliver on their mission to serve justice.

Better data management, faster root cause identification

Gretchen White, chief information security officer (CISO) for the Minnesota Judicial Courts, leads both a risk management and security operations team responsible for protecting the entire unified courts system of 100 locations, 3,500 users and almost 9,000 assets.

Prior to implementing Splunk, the branch was missing a single way to analyze data across their ecosystem. But with Splunk ES, Minnesota Judicial Courts now ingest and analyze data from multiple sources used for day-to-day operational views. This capability allows the team to present data in a format that's not only usable and valuable for IT, but for colleagues outside of IT and security as well.

“When we have a plaguing problem, we use Splunk ES to correlate data and identify early precursors to an issue,” says White. “Splunk helps us get to the root cause quicker.”

Data-Driven Outcomes

\$1 million
ROI in 2020

13.6
full-time employee equivalent freed up to accomplish more strategic tasks

0 minutes
of dwell time between phishing alerts

Automation saves time and improves security posture

Splunk ES is now at the core of how Minnesota Judicial Courts ingest data and perform queries. Seeing marked success, Gretchen and team turned to Splunk SOAR for an even faster way to review, investigate and act on their data.

“In the beginning, automation seemed like a nice-to-have,” says White. “We were really focused on setting standards, gathering data and identifying security pain points for the branch. But as we started to get a volume of incidents that we just could not handle manually, automation was no longer optional. It became a priority for us.”

With Splunk SOAR, Minnesota Judicial Courts can review and investigate processes much faster while freeing up analyst time to focus on critical tasks. “I had a lot of very smart people doing very general security review steps,” says White. “Splunk SOAR allows those smart people to focus on continuously improving our security posture, which is where I want them to be.”

By querying data in Splunk ES, then putting it into Splunk SOAR, Minnesota Judicial Courts present all information in reports or dashboards, which saves the team from endlessly scrolling through security data for pertinent information and improves collaboration.

Splunk SOAR does the work of 13 full-time employees

One of Minnesota Judicial Courts top use cases for automation is phishing investigations. “We were getting inundated with phishing,” says White. “We didn’t have an automated process to triage, determine the validity of the phish or pull it from the environment, which required the work of a full-time analyst. This alone justified Splunk SOAR.”

By automating responses to phishing attacks in 2020, Minnesota Judicial Courts saw a return on investment (ROI) of \$1 million. They also report that through phishing response automation alone, Splunk SOAR completed the workload equivalent of 13.6 full-time employees. Because of this, White says, “You can get your return on investment just from automating one scenario, then supporting your team to expand beyond there.”



I had a lot of very smart people doing very general security review steps. Splunk SOAR allows those smart people to focus on continuously improving our security posture, which is where I want them to be.”

Gretchen White, CISO, Minnesota Judicial Courts

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