splunk>
a CISCO company

CUSTOMER STORY

Splunk ARI Gives Security Operations 40% Time Savings on Daily Checks

Key Challenges

To keep data from over 120 million medical visits safe — and stay compliant with strict security standards — one company needed to easily correlate identity actions with assets across its network.

Key Results

With Splunk Asset and Risk Intelligence (ARI), the SOC now has a comprehensive asset and identity view, allowing them to build out a more proactive practice — mitigating both security and compliance risk.

Industry: Healthcare

Products: Splunk Asset and Risk Intelligence (ARI); Splunk Enterprise Security (ES)

Solutions: Security

Capabilities: Investigation and Forensics, SIEM / Security Analytics, Infrastructure Monitoring and Troubleshooting, Service Monitoring and Insights, Incident Response and Automation

When you serve over 21,000 healthcare professionals and their patients, digital resilience is vital.

From routine appointments to major procedures, this company processes over 120 million medical visits each year, ensuring hospitals and clinics receive payment efficiently so they can continue to save lives in their communities. Since the company deals with highly sensitive patient data, it's a prime target for hackers. That's why security — and meeting rigorous compliance frameworks — is its top priority.

So when the revenue payments provider realized it was unable to get a comprehensive asset and identity view with its current tooling — putting its security and compliance postures at risk — the Security Operations Center (SOC) got to work manually pulling data from various sources. Because of the company's strict internal security configuration standards, devices in the network are checked in to antivirus and verified daily. "This whole process could take up to 5 hours because the data was spread across different tools," says its Director of Information Security. The hours spent each day running these standard checks left little room for the SOC to focus on other, critical tasks — such as building out more proactive security measures. "In the past, we didn't have a regularly updated, current state of devices, making the process even more daunting. If we don't know a device exists, how can we tell if there's a security or compliance gap?" admits the Director of Information Security.

There had to be a better way. The good news? There was.

Outcomes

40%
less time spent on daily security checks

800+
devices identified for critical security patching

120 million
medical visits processed annually

Time saved is never wasted

With Splunk Asset and Risk Intelligence (ARI), the SOC easily correlates identity actions with assets in its network — all from one place. ARI serves as a single source of truth (the "who," "what," "where," "when," "why," and "how") during investigations, mitigating compliance risk.

"ARI is a great forensic tool," says the Director of Information Security. "You see all the IP addresses every time a device connects to the VPN without having to beat up your SIEM, or create a bunch of custom searches to find the information you need."

Oh, and those routine security checks? They now take 40% less time to complete — some only lasting five minutes. With that time saved, the SOC can now address gaps in its robust decommission process, tackle network-device configuration errors more efficiently, and optimize ARI even further to create more value for the organization as a whole.

> ARI takes our digital resilience to the next level.
>
> **Director of Information Security,**
> Healthcare Software Company

ARI has helped the SOC find outliers in its network. Leveraging it as a vulnerability management tool, they found a handful of devices that weren't patching, allowing them to catch security gaps before it's too late. "For the first time, we're able to execute a proactive defense to mitigate risk," says the Director of Information Security.

In addition, prior to implementing ARI, communication between the SOC and the Network Operations Center (NOC) was less than ideal. "We always had difficulty communicating the best way to tell each other when there was a new device that used our file integrity monitoring software — details like when the last time we saw it checked in and the last time the logs came in," admits the Director of Information Security. But ARI solved that with a lot less work and searching.

"We now have better processes in place to not only improve communication between the SOC and NOC, but also get better, faster responses, making sure we always meet the high internal standards we have set."

> Even though we've applied ARI to many use cases already, we're still in the infancy of using it for what we know it's capable of.
>
> **Director of Information Security,**
> Healthcare Software Company

Zeroing in on vulnerabilities in the network

When two zero-day vulnerabilities came out suddenly, the Director of Information Security dug into the problem with conventional vulnerability management tools — only to realize they couldn't help determine whether or not the company was at risk.

Luckily for him, ARI was on hand to save the day. Within minutes, he quickly correlated configuration data across four different sources, identifying over 800 devices that required critical security patching. "With ARI, we're able to have a comprehensive view of assets and identities across our whole network — online and offline."

Thanks to his quick thinking, the crisis was quickly averted. "With standard vulnerability tools, you only get part of the story. With ARI, you get the whole thing," he says. "More importantly, it allowed us to have a direct, positive impact on the business because we were able to remediate those vulnerable devices. And that's an awesome feeling."

Increased visibility and proactive security continue

Looking ahead, the revenue payments provider plans to continue consolidating several of its current tools into ARI. It also plans to use ARI to cut down on false positive vulnerabilities. “The funny thing is,” admits the Director of Information Security, “even though we’ve applied ARI to many use cases already, we’re still in the infancy of using it for what we know it’s capable of.”

As Splunk Enterprise Security (ES) users for almost a decade, the company’s choice to implement ARI was an easy one, given its seamless integration into ES. Using tools like ARI, the company is finding new ways to continue building upon its high security configuration standards to protect its customers and their patients from data breaches — so they can focus on saving lives.

“The road ahead will show us more we can do, giving us better visibility and awareness, and allowing us to be even more proactive,” says the Director of Information Security. But according to him, the biggest win would be leveraging ARI from an IT perspective, enabling those teams to be more proactive as well. “IT infrastructure could use ARI for the data centers, and the desktop team can use it on their new builds — or even their main maintenance items,” he says. “ARI takes our digital resilience to the next level.”

> With ARI, we’re able to have a comprehensive view of assets and identities across our whole network — online and offline.
>
> **Director of Information Security,**
> Healthcare Software 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.

splunk> a CISCO company

Learn more: www.splunk.com/asksales

www.splunk.com