splunk> a CISCO company

CUSTOMER STORY

World-Renowned Research Institution Reduces MTTD by 60%

Key Challenges

A university's campus IT security team faced challenges with fragmented dashboards, while its health system security analysts were unable to correlate logs across systems. Both needed to rapidly detect and respond to threats to keep students, faculty, patients, and IP safe.

Key Results

With Splunk, the university's campus and health security teams now view their environments from a single pane of glass — reducing MTTD by over 60% — to help safeguard everything from critical research to medical data.

Industry: Higher Education and Healthcare

Products: Splunk Enterprise Security (ES), Splunk Enterprise

Solutions: Security, Compliance, Platform

Capabilities: SIEM / Security Analytics, Investigation and Forensics, Risk-Based Alerting, Compliance Monitoring and Reporting, Infrastructure Monitoring and Troubleshooting, Incident Response and Automation

With tens of thousands depending on secure access to critical university systems, blind spots aren't an option.

Home to more than 40,000 students, faculty, and staff, this world-renowned academic institution includes dozens of departments and research centers, a leading medical school, and a preeminent health system. Its prestigious reputation made it a prime target for threat actors. The university and health system regularly confronted nation-state attacks and opportunistic actors who exploited weak credentials to gain access to critical IP, expose medical data, or disrupt operations and patient care.

Building an AI-centric strategy at scale requires having a solid foundation to manage massive amounts of data efficiently and keep systems resilient. Splunk underpins that foundation, supporting not only cybersecurity and compliance, but also IT infrastructure, network operations, and research monitoring.

Outcomes

60%+
reduction in MTTD

40%
reduction in ticket investigation times

Hundreds
of unmanaged endpoints secured

The university runs two parallel security operations teams, one protecting its academic and research environment, and another securing its medical school and health system. On the campus side, security insights were distributed across numerous dashboards, each built for a different use case. On the health system side, analysts were combing through raw logs, unable to cross-reference or correlate events. Without a unified view of their environments, blind spots emerged, and response times lagged, leaving the campus and hospitals vulnerable.

Splunk turned this complexity into clarity, enabling each security team to see across their environments. The university now has a solid data foundation to protect its students, patients, research, and critical operations.

Making the grade in security visibility

When the Senior IT Security Analyst joined the campus IT department, he found that while security dashboards existed, each was siloed and served only a narrow function, leaving the team without a comprehensive view of campus security.

That changed when the analyst built hierarchical security posture dashboards within Splunk Enterprise, starting at the university level and drilling down to units and hosts.

> Instead of chasing noise, we can prioritize based on actual risk.
>
> **SIEM Engineer**

The outcome was a complete view of the environment that let analysts spot vulnerabilities quickly and investigate with rich context. With Splunk Enterprise, the campus security team cut detection of high-risk security events by more than 60% and reduced ticket investigation times by 40%. This enabled the team to focus on high-level projects such as expanding posture dashboards and refining automated alerting. For IT leadership, leaderboard-style views highlighted remaining vulnerabilities and their average age, making it crystal clear that remediation was sluggish.

From out of sight to locked down tight

For the campus security team, this enhanced visualization also revealed a deeper problem. "Splunk exposed hundreds of systems that people didn't even realize they were responsible for," says the Senior IT Security Analyst. Bringing these forgotten assets to light closed security gaps that attackers could have exploited, reduced shadow IT, and gave the university a clearer baseline for compliance reporting. What once felt like scattered pieces is now a coherent program with accountability built in.

Splunk Enterprise also helped the team identify and remove stale accounts in AWS. By correlating AWS user data in Splunk, the campus security team set up automation to flag inactive accounts and send notices to their owners, eliminating hundreds of accounts that could have been hijacked after students left. Ultimately, Splunk enabled the security team to save precious time and resources. Instead of having to chase down account owners, investigations now move faster, reducing risk exposure.

The university health system gets a real-time pulse on risk

The health system's previous log tool ingested only a fraction of the organization's data and provided no way to manipulate logs or cross-reference sources. To fill the gaps, analysts had to rely on multiple disjointed tools, resulting in slow manual investigations that made hospitals and clinics vulnerable to threats. "Before, we'd have to check at least four systems to figure out why a machine wasn't allowed on the network," says a SIEM Engineer.

Now, with Splunk Enterprise Security (ES), analysts no longer bounce between disparate tools to find the data they need. Instead, they work from dashboards designed for their workflows. "With Splunk Enterprise Security, I just built one dashboard where you plug in a host name, IP, or MAC address, and it tells you what check that system failed," says the SIEM Engineer. It's a far cry from the old process, allowing analysts to resolve device issues faster and keep the health system's network more secure.

Risk-Based Alerting (RBA) became the health security team's most powerful tool. Instead of treating every alert as a standalone incident, it allows them to assign risk scores to users, devices, and systems, tracking those scores across multiple data sources. This correlation highlights patterns that would otherwise be hidden, giving the team insight into suspicious behavior and strengthening their overall security posture. "There's hardly ever a smoking gun if a good attacker is in your network," says the SIEM Engineer. "The best part of Splunk ES is that you can layer risk profiles onto alerts and calculate the overall risk in one view."

By consolidating alerts into risk scores, the security team also reduced false positives, keeping investigations focused on events that matter. "Now, instead of chasing noise, we can prioritize based on actual risk," says the SIEM Engineer.

Compliance reporting the university President can trust

When the university President required all campuses to achieve 100% endpoint detection and response (EDR) coverage, the health system's SIEM Engineer turned to Splunk ES. With the Splunk ES asset database as the single source of truth, the team can show exactly which devices are covered and which are not.

That accuracy not only satisfied university leadership, it gave the health system confidence in its own compliance posture, reducing the risk of costly penalties down the road.

> Splunk is the Cadillac of SIEMs.
>
> **SIEM Engineer**

Splunk also gave the health security team confidence to tackle more advanced initiatives. The SIEM Engineer credits his Splunk-Assigned Expert with helping him move beyond day-to-day monitoring to larger projects — from refining data models to converting a repository of detections into a custom Splunk app. "Having a dedicated expert really lets me take on projects I otherwise couldn't," he says. "I can rely on him as a sounding board, and he points out areas we can optimize further."

Building a resilient future for education and patient care

The journey is far from over. The university's health system security team plans to use Splunk Asset and Risk Intelligence (ARI) to fully understand their asset landscape, accelerate security investigations, and access out-of-the-box compliance metrics to identify compliance and risk controls.

Meanwhile, the campus security team aims to tighten inventory and compliance processes to prevent non-secure devices from connecting to the network. They also plan to expand their security posture dashboards and refine automated alerting.

The university is also one of Cisco's largest wireless customers and a key collaborator in Cisco scalability testing. Its full Cisco stack spans data center, campus, and wireless networking, with multiple Catalyst Center deployments addressing scalability challenges and one of the largest Identity Services Engine (ISE) rollouts in Cisco's portfolio.

"Splunk is the Cadillac of SIEMs," says the SIEM Engineer. His words reflect the vital role Splunk plays in campus and health security, ensuring this acclaimed university can continue to educate, innovate, and deliver patient care with confidence.