splunk> a CISCO company

CUSTOMER STORY

U.S. State Unifies Security and Compliance, Cuts Audit Findings by 1,200

Key Challenges

A U.S. state's IT teams were juggling legacy systems, fragmented security tools, and manual workflows that made it difficult to detect threats, protect citizen data, and meet strict compliance requirements.

Key Results

With Splunk, the state eliminated 1,200+ IRS compliance issues, reduced false positives, and cut response times, modernizing security operations and laying the groundwork for statewide cyber defense.

Industry: Public Sector

Products: Enterprise Security, SOAR, ITSI

Solutions: Security, Observability

Capabilities: SIEM / Security Analytics, Unified Security Operations, Automation and Orchestration, Security Incident Response

Tackling legacy systems and security challenges

This state's central IT agency manages all IT resources and technology assets in the executive branch of the government. "Data is the state's number one asset," says its Secretary and CIO tasked with modernizing IT operations to enhance service delivery and safeguard citizens' data. "If we get the data right and keep it secure, every service we deliver to our citizens can be better and more trusted."

As the state's technology needs grew, it faced significant challenges in standardizing security controls, navigating legacy systems, and ensuring data privacy for sensitive citizen information. "Legacy systems and processes are like a nesting doll of problems," says its Information Security Analyst III and team supervisor. "You fix one layer, and three more appear."

Previously, the state's application teams operated in silos, using disconnected systems and inconsistent security workflows. The agency needed a robust solution to monitor security events, reduce operational complexity, and maintain compliance across various state departments.

Under the leadership of the Secretary and CIO, the state adopted Splunk's security and observability solutions. Since then, it has streamlined its monitoring and compliance processes, reduced security incidents, and significantly improved incident response times across state agencies.

Outcomes

- **1,200+ IRS compliance issues eliminated** in one audit cycle through a Splunk-built compliance dashboard.
- **Significantly faster detection and response**, with most issues resolved in minutes instead of hours.
- **Reduced alert noise**, allowing analysts to focus on real threats rather than false positives.

Optimizing security, compliance, and incident response with Splunk

To address its growing IT security and compliance challenges, the state adopted Splunk as a comprehensive solution for real-time monitoring, incident response, and data analysis across its entire digital infrastructure. It integrated Splunk Enterprise Security, SOAR, and ITSI solutions to provide a centralized view of security events and improve operational efficiency.

The state had previously struggled with monitoring legacy systems, manual security workflows, and a decentralized approach to data analysis. These hurdles made it difficult to ensure data privacy, particularly for sensitive citizen information such as personally identifiable information (PII) and federal tax information (FTI). Splunk's ability to ingest data from various sources, normalize it, and analyze it at scale allowed the state to achieve holistic visibility into its IT environment and strengthen its security posture. It also enabled the state to consolidate three separate Splunk instances and other SIEM tools into one unified platform, eliminating the need to dig through multiple disconnected systems.

> Data is the state's number one asset. If we get the data right and keep it secure, every service we deliver to our citizens can be better and more trusted.
>
> **Secretary and CIO**

This work also laid the foundation for the broader "State Theory" vision: protecting all agencies and municipalities as one cohesive entity rather than as isolated teams with separate security postures. Splunk Enterprise Security gave the state a consolidated, real-time view of alerts so that threats could be identified and addressed quickly. SOAR automated routine response workflows, cutting down on the time security teams spent triaging alerts. ITSI added deeper insights into IT performance, helping teams identify trends, optimize resources, and reduce downtime before issues affected citizens.

By combining these tools, the state established a comprehensive security and observability foundation. It is now better equipped to respond to incidents quickly, manage data access effectively, and maintain compliance with strict state and federal regulations. These gains have modernized operations and improved the resilience of its digital services.

"Splunk became our central brain," says the Information Security Analyst. "If we need to see something, it has to be in Splunk; otherwise, it's not truly secured."

> Splunk became our central brain. If we need to see something, it has to be in Splunk; otherwise, it's not truly secured.
>
> **Information Security Analyst**

The role of AI and automation

The state views AI and automation as critical to its long-term security strategy but is adopting them deliberately, remaining cautious about how these systems process and store sensitive citizen data.

Even so, the state is already using machine learning features in Splunk Enterprise Security to identify anomalies and surface threats faster. These capabilities help reduce noise and allow the team to focus on high-priority issues. "The pace of threats means we can't afford to investigate everything manually," says the Information Security Analyst. "We need automation that we trust."

Looking ahead, the state sees significant potential in pairing Splunk SOAR with AI-driven workflows. Automated playbooks could quickly answer complex security questions, for example, identifying which assets are vulnerable to a newly disclosed threat, without lengthy manual investigations.

Reducing risk and raising efficiency statewide

The benefits of Splunk were immediate and measurable. The state reduced IRS compliance findings by more than 1,200 issues in its most recent audit cycle. A Splunk-built IRS compliance dashboard gave executives and compliance teams full visibility into required security controls, making it far easier to track and close gaps before auditors arrived.

The security team also cut alert noise dramatically. Before Splunk, analysts were spending hours chasing down false positives across multiple systems. "With Splunk dashboards, we can spot issues almost instantly," says the Information Security Analyst. "I can run a query in under two minutes, confirm whether it's real, and often avoid opening an incident entirely. That speed has changed how we work."

> The pace of threats means we can't afford to investigate everything manually. We need automation that we trust.
>
> **Information Security Analyst**

"It's also changed the stress level for the team," the Information Security Analyst III and team supervisor adds. "We're not chasing false alarms all day anymore; we can focus on real threats and proactive work."

Now Splunk's correlation searches and tuned "notables," developed in partnership with managed services provider New Harbor, surface only the alerts that matter. Analysts can focus on real threats, which has significantly improved response times and reduced pressure on the team.

Splunk's dashboards and search capabilities have also transformed day-to-day operations. Previously, help desk staff often had to escalate user lockout issues to multiple teams, a process that could take hours.

"Now they can solve that in minutes without escalating at all," the Information Security Analyst says. "It's good for users and a huge time-saver for IT."

Analysts can run queries and see results almost instantly, enabling them to confirm or dismiss potential issues quickly and avoid unnecessary incidents, freeing up time for more proactive work.

The state also leverages Cisco's switching and wireless solutions to provide reliable, secure connectivity. With Cisco's advanced switching technology, the state ensures high-performance network traffic management and seamless data flow. Meanwhile, Cisco's wireless infrastructure delivers secure, scalable Wi-Fi access, supporting more efficient operations, and enabling digital government services statewide.

Building on a strong foundation

The state is already planning to build on its success with Splunk. The team aims to expand its use of Splunk SOAR to automate more security workflows and free up staff for higher-value initiatives. It also plans to extend its unified security model statewide, aligning municipalities and agencies under the "State Theory" approach for stronger, more consistent cyber defense.

These efforts will further strengthen the state's ability to safeguard citizen data, meet strict compliance requirements, and deliver resilient digital services to the public.

"We've matured rapidly, but we're just getting started," says the Secretary and CIO. "The goal is to raise the baseline for every agency and town in the state."

With Splunk at the core, the state is moving confidently toward a future where every municipality benefits from consistent protections, faster response, and greater visibility. A more resilient, unified digital government isn't just a vision; it's the next phase.