splunk> a CISCO company

A Use Case Guide

Splunk for the Public Sector

“

Visibility is our first priority. If I can’t see it, I can’t do anything about it. Splunk is key to our gaining this visibility without compromising student privacy.

Katrina Biscay, Assistant Vice President
and Chief Information Security Officer,
University of Cincinnati

Contents

The highest of stakes

A parent in California just swiped their EBT card at Ralphs. The cashier bags their perishables with a smile. An automated dispensary cabinet in a New York hospital refuses entry to a pharmacy technician. They've been using it far more than their peers. A quiet calm accompanies each of these events — and that's a good thing.

Because if downtime brings down the grocery store's payment systems at the only time a parent can make it to the store, their family can go without dinner. If a hospital doesn't know how many controlled substances are being diverted, it can't possibly do its part to fight the opioid crisis.

It's no longer possible to separate an organization from the digital systems it relies upon. This means that disruptions aren't just expensive. Downtime, security breaches, or fraud could threaten public safety.

That's why today's public sector leaders are investing in digital resilience. When issues are resolved even faster — or avoided altogether — and teams have the time and tools to be proactive, mission success is immediate and lasting. Sensitive data is protected. Tax dollars are saved. Lives are saved. And sometimes, some really cool breakthroughs in nuclear fusion happen.

Critical concerns across the sector

Public sector leaders support multiple missions, including defense, education, and delivering vital healthcare services. To succeed, they have to navigate a world of modern threats and technologies.

With each passing year, the sophistication of cyberattacks increases — making robust cybersecurity measures and proactive threat detection paramount to safeguarding national security and maintaining the integrity of critical systems.

Cybersecurity is also critical for fighting fraud. Each day, a new story breaks on how a bad actor has committed fraud against a government agency or entity, an educational institution, or an individual. (Maybe that individual has even been you.) Fraud happens when cybersecurity fails, and it's far from a victimless crime.

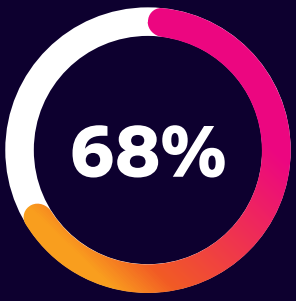
In addition, agencies and organizations across the sector are facing evolving compliance regulations, new concerns around AI, and how to turn buckets and buckets of data (that's the technical term) into actionable insights that keep our nation's most critical systems secure and reliable.

Mission possible with Splunk

While the end goal might be clear, it can be difficult to know where to start. That's why we've created this **use case guide** to show you just some of the ways in which Security and IT teams across the public sector rely on Splunk to help achieve mission success.

Splunk is proud to support a wide range of public sector organizations and their powerful missions, including:

of the 50 largest cities



of the 25 largest counties

---

3 branches of government

50 states

15 Cabinet-level departments

1 territory

450 higher education institutions

Use case 1

Data optimization

Why it matters

Federal IT leaders face multiple priorities, from modernization to risk management to citizen experience improvements. And it all starts with gaining foundational visibility across your environments. It's an adage by now for a reason — you can't secure what you can't see. Being resilient hinges on your ability to have visibility and contextual insights so you can effectively investigate and respond to security incidents across your on-prem, hybrid, and multicloud environments.

Challenges

Cybersecurity is increasingly a data problem: Security log volume is growing, and logs are getting more complex. Events over the past years, like a surge in remote work, digital transformations, and the ever-changing threat landscape, have required organizations to make investments that often create more data — making it even more difficult to secure it all. The result: Security analysts are plagued with managing tradeoffs in value and cost.

At the same time, OMB M-21-31 is driving the need to optimize data value, with requirements around event logging and maturity, centralized access, and developing automated hunt and incident response playbooks. What's needed is a cost-effective approach regarding the sheer volume of data to log — an approach that also ensures teams aren't creating new silos and sacrificing centralized visibility and the comprehensive incident response and automation that the mandate also calls for.

> **Splunk delivers visibility into what is happening across complex agency operating environments.**
>
> IT Systems Analyst, State and Local Government

Splunk's approach

The Splunk platform enables teams to index and search large volumes of data from various sources and work with any data structure or time scale to create a comprehensive view of all transactions and activities. With Splunk you're able to:

- Normalize your data to match a common standard and remove security data silos with Splunk Common Information Model and OCSF.
- Collect and configure data ingestion from a variety of cloud data sources with **Splunk Data Manager**.
- Organize data based on its business value — from critical to compliant — to optimize search performance and egress costs.
- Build and manage pipelines — from the edge to cloud — to filter, mask, enrich, and transform slices of data you want.
- Control the volume and flow of data with an eye on costs.
- Manage and store data flexibly, the way you need — in Splunk for analytics or a cost-effective Amazon S3 object.

Learn more about Splunk's solutions for federal civilian agencies:
https://www.splunk.com/en_us/solutions/industries/public-sector/federal-civilian-agencies.html

Source: TechValidate

Use case 2

Security monitoring

Why it matters

Cyber defense is at the heart of national security. This includes ensuring the confidentiality, integrity, and availability of information systems. When agencies can ingest data from any source, they gain end-to-end visibility across on-prem, hybrid, and cloud environments for real-time security monitoring. With the ability to make data-centric decisions, agencies can meet increasing cybersecurity mandates and intensifying cyberattacks head-on.

Challenges

One of the most pressing issues facing the sector is the increasing frequency and sophistication of cyberattacks. Federal agencies reported[1] over 32,000 IT security incidents in fiscal year 2023 alone, an increase of 9.9% from the previous year, highlighting the persistent threats from both external actors and internal weaknesses. These attacks often target critical infrastructure and sensitive data, posing significant risks to national security.

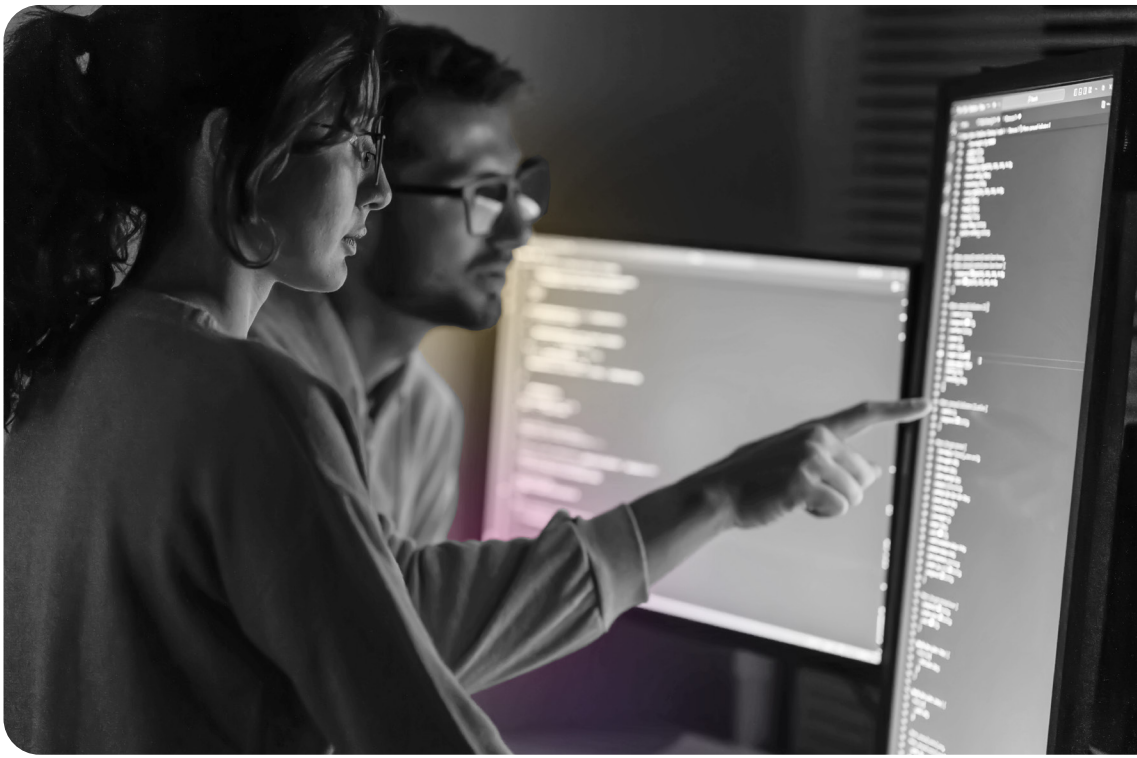
Another challenge is the shortage of skilled cybersecurity professionals within federal agencies, which makes it difficult to implement and maintain effective security measures. On top of this, agencies must navigate complex regulatory requirements while facing budget constraints that limit their ability to invest in advanced security solutions to protect across the complexity and scale of their operations.

1 https://www.whitehouse.gov/wp-content/uploads/2024/06/FY23-FISMA-Report.pdf

How Splunk helps

Splunk Cloud Platform, which can support sensitive information at the FedRAMP High and IL5 levels, makes it easier for agencies to investigate, monitor, analyze, and act on security threats. It also supports the "Cross-Cutting Capabilities" identified in CISA's Zero Trust Maturity Model, such as Visibility and Analytics, Automation and Orchestration, and Governance. In addition, **Splunk Enterprise Security** is the market-leading SIEM and security analytics solution trusted by SOCs around the globe, giving SecOps teams a deep understanding of users and identities throughout the organization.

Another critical capability is Splunk's support for the Continuous Diagnostics and Mitigation (CDM) program, which helps federal agencies achieve real-time visibility and automated reporting across all phases of their security programs. In addition, Splunk's Government Logging Modernization Program helps agencies meet requirements of cyber incident response as outlined in the Biden administration's executive order on cybersecurity and guidance included in OMB M-21-31.



Case study

Sandia Labs detects and counters supply chain attacks with the HECATE platform

With more than 200 reported software supply chain attacks over the last 10 years, Sandia Labs wanted to help organizations reduce risks when installing new software. With Splunk, Sandia developed the HECATE platform to help automate the identification of supply chain risks and investigate suspect behaviors before there's a breach.

Provided the ability to **automatically scan patch updates** prior to production

Gave organizations a consistent method to **uncover software subversion** through supply chain risk management, source code analysis, and open-source intelligence

Reduced time of analysis from **days to minutes**

Our adversaries have weaponized compliance and fundamentally broken the trust relationships in software. New tools and techniques are needed to evaluate software before entering our networks.

Vince Urias and Will Stout, Research and Development, Sandia National Laboratories

Use case 3

Align IT and organization with service monitoring

Why it matters

With a unified view across security and IT teams, all stakeholders can more easily see the health of the services across their environment and troubleshoot potential issues faster. Also, they're able to continuously identify, report, and improve on key performance metrics and forecast potential incidents before they occur.

Challenges

Tech stacks and interdependencies are only becoming more complex, making visibility and connecting the dots even harder. Traditional monitoring tools don't allow for flexibility and can be limited to analyzing infrastructure health and application performance issues, which don't translate to a language that all stakeholders and tech buyers can understand.

Tool sprawl is another major issue contributing to increased operational cost — which gets in the way of spending on the modernization projects and personnel that the sector desperately needs. With no centralized location to see all the data, much less surface relationships between applications and infrastructure and how these relationships affect services, it's hard for teams to prioritize incidents based on their real or potential impact when issues do occur.

How Splunk helps

Splunk IT Service Intelligence (ITSI) provides out-of-the-box, easily customizable dashboards with a live view of service performance relevant to IT and non-IT stakeholders. With Splunk ITSI, ITOps teams can align with other stakeholders across and outside of the organization on common KPIs, metrics, and visibility. And with glass tables in ITSI, leaders can see the real-time health of business SLAs and SLOs and connect that health back to the underlying services, KPIs, and entities that support them — including third-party, homegrown, and commercial off-the-shelf applications. This means that stakeholders can quickly see what's important for them — whether that means hospital bed vacancy or laser voltage.

To help prevent issues, Splunk ITSI can give ITOps teams early warning before an incident occurs. A mature approach to preventing outages, the degradation of service health can be predicted up to 30 minutes in advance. This gives ITOps teams extra time to prevent issues before they occur in the first place.

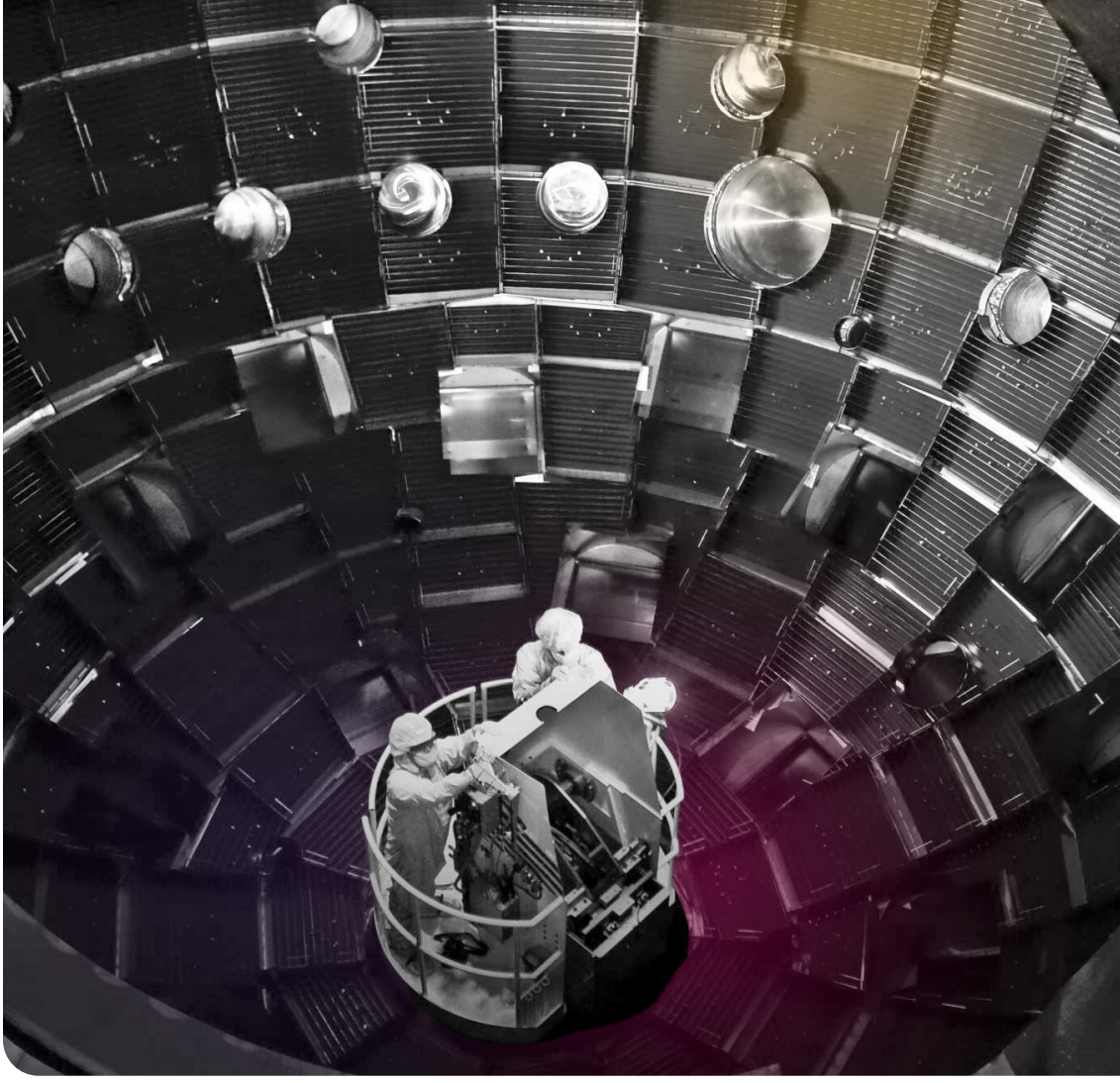
Case study

The National Ignition Facility unlocks the potential of clean energy and safeguards the US nuclear stockpile

The National Ignition Facility (NIF), located at California's Lawrence Livermore National Laboratory, is the world's largest laser. To support the NIF's core missions, including nuclear stockpile stewardship and scientific discovery, scientists and engineers require a secure, reliable IT infrastructure. Splunk Enterprise and Splunk IT Service Intelligence sit at the heart of the NIF's control system, which manages more than 66,000 control points to power NIF's massive laser facility. The lab's engineers can now take action on events based on everything from application data to sensor data like laser voltage, temperature, and pressure.

Data is really critical to our rate of learning and the progress we make on the complex questions we're trying to understand at NIF.

Bruno Van Wonterghem, Operations Manager, National Ignition Facility



66K+ IoT devices in addition to IT infrastructure monitored by Splunk

Doubled laser shots to 400 annually without compromising uptime or data integrity

Achieved nuclear fusion breakthrough with a blast of 192 lasers to further advance the goal of clean, unlimited energy

Use case 4

Threat hunting

Why it matters

With actionable data often found on multiple mediums, including illicit marketplaces, forums, blogs, social media, and more, it can be tricky to get access to it — not to mention the risk that accessing data sources on the deep and dark web brings. When organizations can bring together threat intelligence sources from across the internet, teams can uncover new threats, accelerate threat hunting, and improve their organization's — and nation's — security posture.

Challenges

Once an adversary has gotten into an environment, it's very, very difficult to toss them out. According to Splunk's State of Security[2] report, the average dwell time is nine weeks. A lot of havoc can be (and has been) wreaked in that amount of time. It's simply not possible to conduct investigations and threat hunting across the entire attack surface with a single tool, and when our adversaries are ever-more focused and persistent, security teams might not be able to surface insights — especially during day-to-day correlation activity.

How Splunk helps

With the **Splunk platform** and **Splunk Enterprise Security**, security teams can conduct threat hunting across the entire attack surface and from a single tool. When data is easily collected, normalized, accessed, and analyzed, this provides valuable clues for threat hunters to chase down threats.

Also, with **Splunk User Behavior Analytics** (UBA), teams can identify unknown threats with machine learning. With UBA, teams can automatically analyze, enrich, and validate alerts, eliminate false positives, group related events into incidents, and prioritize them by organizational risk to facilitate rapid and effective investigations and threat-hunting activities.

2 "State of Security 2024: The Race to Harness AI," Splunk, April 30, 2024, https://www.splunk.com/en_us/form/state-of-security.html

Case study

Townsville City Council protects its community with cybersecurity

Serving 200,000 citizens, Townsville City Council (TCC) is the largest regional council in Queensland, Australia. TCC is committed to fostering sustainable growth through driving economic diversity and generating an enriching lifestyle.

While cybersecurity is of top importance to TCC, security issues were being handled manually, which did not offer full threat visibility and impacted residents' trust. TCC engaged a new managed cybersecurity service from RIOT Solutions — powered by the Splunk platform — to adopt a more holistic approach to cybersecurity and tackle ever-changing needs and threats.

With Splunk applied across all security operations, RIOT Solutions empowers TCC to accurately identify suspicious activities, infrastructure misconfigurations, and exploitable vulnerabilities while prioritizing security alerts according to risk level. Critical threats now never go unnoticed and are always escalated — quickly. Previously, it could take up to 50 minutes to explore a security issue. With Splunk, the team is now able to address concerns about 85% faster.

~85%
faster threat hunting

65%
savings in SIEM operating costs

Improved **customer experience**

Use case 5

Troubleshooting mission-critical apps and infrastructure

Why it matters

When ITOps teams can centralize logs and gain visibility across siloed log data sources, they can quickly troubleshoot problems in mission-critical apps and infrastructure and detect and resolve incidents quickly and effectively to keep digital systems up and running. When downtime adds up to staggering amounts in losses — over $190 million for the public sector alone[3], observability emerges as a critical capability for maintaining network and application availability.

Challenges

Among the greatest challenges facing the sector — although certainly not unique to the sector — are siloed teams and tools, along with staff attrition and talent gaps. More tools, more data, and more alerts — combined with limited visibility across complex environments — hinder cross-functional collaboration across teams and agencies. This creates data silos, leading to lack of visibility, lengthy time to detection and resolution, and time wasted when resources and personnel are already spread too thin.

3 "The Hidden Costs of Downtime," Splunk, October 1, 2024, https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html

How Splunk helps

The ongoing digital transformation in the government sector demands a comprehensive approach that considers the entire system architecture. Splunk assists federal agencies in achieving their observability goals by providing comprehensive visibility and actionable insights to help detect anomalies and respond to incidents swiftly.

Machine learning is embedded into the Splunk platform in both **Splunk Enterprise** and **Splunk Cloud Platform**, allowing users to detect anomalies, generate forecasts, make predictions, and cluster data into groups. This proactive approach is crucial for federal agencies that need to maintain high levels of security and availability.

Case study

The University of Illinois advances student success through a data-first approach

Before Splunk, data at the University of Illinois Urbana-Champaign was siloed and inaccessible to most staff, hindering efforts to improve the student experience. When COVID-19 hit, the university faced new challenges: to quickly transition to online learning and then navigate how to safely bring students back to campus. With Splunk, Illinois has improved classroom learning and student satisfaction — and, in the fall of 2020, the university used a data-first approach to testing and contact tracing[4] to resume in-person learning while protecting the campus community, even conducting over 1.5 million tests across campus for a safe transition to in-person learning.

> **In this emergency situation, Splunk became the tool we relied on to automatically get out information quickly, whether it was sending testing data or alerts.**

Nick Vance, Manager of Data and Technology, University of Illinois

4 "University of Illinois Urbana-Champaign Scales COVID-19 Saliva Tests, Safely Brings Students Back to Campus," Splunk, March 9, 2021, https://www.splunk.com/en_us/blog/customers/university-of-illinois-scales-covid-19-saliva-tests-safely-brings-students-back-to-campus.html

Bringing the future forward

The Splunk you love is now even better. Supercharged by Cisco, Splunk delivers unparalleled visibility and insights across the entire digital footprint. It's a new day for your data, and the possibilities — and use cases — are endless. But don't just take our word for it …

We have everything in a single system, and we know everything that's being addressed. We have a record of what happened and what the analyst has done, which has been a generational leap for us.

Jason Mihalow, Senior Cloud Cyber Security Architect, McGraw Hill

What I've learned through our partnership with Splunk is that you may not know the answer right away. But when you have really good partners who are there to listen to your goals and provide solutions, the world's your oyster.

Simone Williams, Director of Programs, LCWINS

Splunk has very good customer service and has a 'Yes, we can see about getting this capability going for you' response to my requests.

Erik Mason, IT Manager, Department of Defense

Splunk Cloud has achieved FedRAMP High authorization

In reaching the highest level of FedRAMP authorization, Splunk Cloud offers the entire spectrum of security standards necessary for all government agencies to modernize their strategies and adopt the cloud. Federal agencies and their partners can leverage Splunk Cloud Platform with FedRAMP High to help manage the government's sensitive data and enhance security posture.

"Obtaining FedRAMP High authorization was a significant milestone for our organization as it demonstrates our unwavering dedication to the highest standards of security in the federal space," said Bill Rowan, VP of Public Sector at Splunk. "With our proven track record of delivering innovative and effective security solutions, combined with our commitment to continuous improvement and collaboration, we are the preferred choice for public sector organizations. This accomplishment further reinforces our position with public sector customers and strengthens our contributions to our nation's cybersecurity mission."

In June 2023, Splunk also attained StateRAMP authorization for the Splunk Cloud Platform at a moderate level, and in August 2022, it obtained its IL5 for the Splunk Cloud Platform. In August 2024, Splunk SOAR achieved FedRAMP authorization at a moderate level.

For additional information related to the Splunk FedRAMP package, please visit the FedRAMP Marketplace:
https://marketplace.fedramp.gov/products

Security, IT, and DevOps teams require the very best solutions so they can detect and resolve incidents faster and work cross-functionally as needed to ensure cyber resilience. Discover how Splunk drives resilience for organizations across the public sector.

Visit our industry solution page:
www.splunk.com/public-sector

24.splunk-for-the-public-sector.print-book.digital-rgb

splunk> a CISCO company