splunk>
turn data into doing

Splunk's Top 3 Public Sector Highlights of 2021

A year in review to help prepare for what's ahead

Government agencies, Fortune 100 companies and more are using Splunk to turn data into doing. In 2021, Splunk developed new ways data can help organizations of all kinds, including those in the public sector, to be more secure, resilient and innovative.

From the future of cybersecurity, to the uses of observability in digital services, to the increasing importance of a strong data platform, like Splunk, in a time of accelerated digital transformation, 2021 was full of important updates to help you prepare for what's coming next.

Splunk created a new program to help federal agencies meet evolving cybersecurity requirements, achieved IL5 authorization and rolled out new product updates to help you achieve mission success.

Does 2021 already seem like a blur? No problem. We've got Splunk's top three public sector highlights of 2021 for you.

1. How data can help your agency meet the latest cybersecurity requirements
2. How government agencies stay secure, compliant and efficient by turning data into doing
3. New product features and updates to help you be a data hero

How data can help your agency meet the latest cybersecurity requirements

Digital transformation has many benefits for the public sector, and during the pandemic, it has become imperative. With digital transformation comes expanded cyberattack surfaces and threats, and new government cybersecurity requirements. Splunk helps agencies meet those ever-evolving mandates and in 2021, we made two important announcements for public sector cybersecurity.

Accelerate compliance, improve cybersecurity resilience and lower costs

Splunk is committed to supporting federal agencies by answering President Biden's call to strengthen cyber capabilities across the federal government — both in the near and long term.

Splunk unveiled a new Government Logging Modernization Program designed to help U.S. government agencies meet the Biden Administration's executive order on cybersecurity. Leveraging this program and Splunk Cloud, agencies can directly map to this mandate.

The program's packages and pricing are tailored specifically to help federal agencies accelerate compliance and improve cybersecurity resilience, while also lowering costs. With expanded storage options, security teams can speed up investigation and remediation through enterprise log retention. The program also includes a comprehensive Splunk Cloud FedRAMP migration assessment, and customized services to help agencies rapidly modernize their logging program and meet the requirements outlined in OMB's maturity framework for event log management.

Leverage Splunk Cloud for U.S. DoD IL5

Cloud computing and technology allow the U.S. Department of Defense (DoD) to consolidate infrastructure, leverage commodity IT functions and eliminate functional redundancies while improving operations. To take advantage of the benefits of the cloud, Federal agencies must use cloud products and providers that are U.S. DoD authorized.

Building on the recent FedRAMP Moderate authorization, Splunk Cloud Platform achieved the U.S. Department of Defense Provisional Authorization at Impact Level 5 (IL5), which allows access to national security systems and higher-sensitivity, controlled unclassified information (CUI).

U.S. government agencies can use the Splunk Cloud Platform to meet the specific challenges they face when using cloud computing to address a variety of data analytics and AI use cases — with confidence, and at mission speeds.

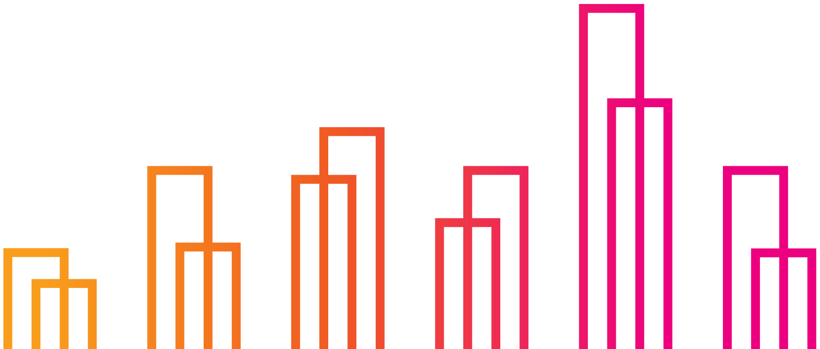
How government agencies stay secure, compliant and efficient by turning data into doing

At .conf21, Splunk's annual user conference, government agency experts took a deep dive into how they use Splunk to keep their organizations secure and efficient, improve the lives of citizens, and solve enormous compliance challenges. Click here to watch use case highlights for free.

One example highlighted was The Ministry of Energy of the State of Israel, which uses Splunk Enterprise with machine learning to better **protect its critical infrastructure and operational technology (OT)** — prime targets for cyberattacks that threaten national security. The agency implemented an advanced security strategy to protect all the power plants in the country and now has a comprehensive view of the nationwide security posture in energy supply. They use Splunk to monitor all of their decentralized security information event management (SIEM) solution and events from power plant operations, with the added edge of machine learning. This is just one example of how Splunk's Machine Learning Toolkit enables public sector agencies to iterate faster on use cases and see immediate outcomes in their security operations.

Spunk also helps government agencies use data to **solve complex compliance challenges in FedRAMP/ FISMA environments**. The U.S. Navy is solving enormous compliance visibility and assessment challenges by automing subjectivity out of inspections and improving cyber hygiene by using Splunk to collect, report and visualize data — at enterprise scale.

State agencies are using data to **detect fraud and improve the lives of citizens**. The State of New Jersey used Splunk to detect unemployment insurance fraud during the pandemic and saved its citizens billions of dollars. And a California agency unified operational silos and improved the lives of its citizens by consolidating all of their monitoring tools into one, Splunk Infrastructure Monitoring.



New product features and updates to help you be a data hero

In 2021, Splunk also rolled out several new product features and updates to help data heroes like you do their jobs even better.

In cybersecurity, you can now integrate and automate intelligence into every stage of the incident response process, as well as across an entire ecosystem of teams, tools, peers and partners. To bring our rapidly growing intelligence marketplace to users everywhere, Splunk Intelligence Management (formerly known as TruSTAR) is now available to all Splunk Enterprise Security (ES) customers. And new enhancements to the security orchestration, automation and response (SOAR) solution, Splunk SOAR, help security teams eliminate tedious work and resolve security incidents in record time.

Your critical digital services depend on a variety of applications and services — both legacy on-premise and cloud-native. With Splunk IT Service Intelligence (ITSI) content packs, managing it all just got easier. Content packs are available for free on Splunkbase and provide out-of-the-box content to jumpstart your IT monitoring. Splunk Service Intelligence for SAP is now also available to help you bridge infrastructure data with SAP data, and gain in-depth visibility into the health and performance of SAP-related business services. Splunk added many other significant content packs, such as one for Microsoft365 and one for third-party app performance management (APM), and launched the Splunk App for Content Packs — your one-stop shop for pre-packaged content for IT monitoring.

Splunk's commitment to innovation doesn't stop there. In the past year alone, Splunk has closed four acquisitions and delivered 43 major releases, as well as hundreds of enhancements across the product portfolio.

Ready to learn how to bring data to every mission?