

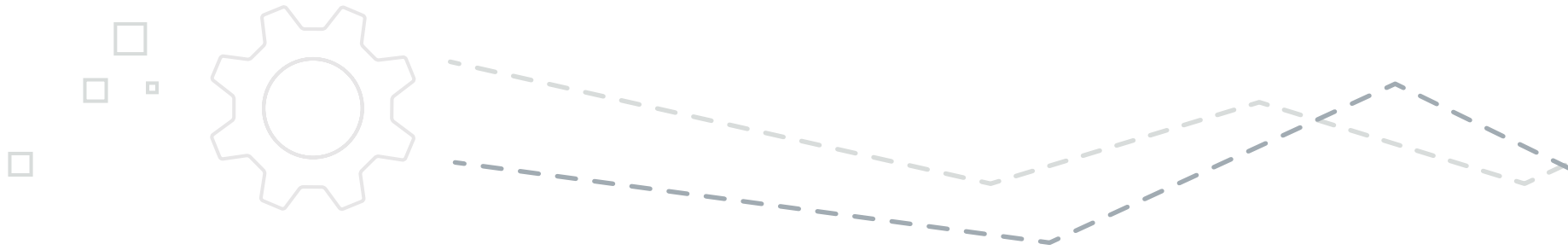
Ensuring Mission Success

How forward-thinking government agencies bring data to every action





Introduction.....	2
The Mission: Protect, Serve, Modernize	3
How Customers Are Harnessing Data	5
• The National Ignition Facility at Lawrence Livermore National Labs.....	5
• City of Gold Coast	5
• Jefferson County School District.....	5
• The U.S. Census Bureau.....	6
Mission-Focused Agencies	7
• The Bank of England.....	9
• City of Gold Coast	10
• City of Los Angeles.....	11
• Dubai Airports.....	12
• Fairfax County	13
• Hong Kong's Vessel Traffic Center	14
• Jefferson County Public Schools.....	15
• Leidos.....	16
• Maryland Lottery and Gaming Control Agency.....	17
• National Ignition Facility	18
• New York Regional Education Agencies	19
• NHS Choices.....	20
• Prince George's County.....	21
• Royal Flying Doctor Service.....	22
• Sacramento County Sheriff's Department.....	23
• SAIC	24
• Sandia National Labs	25
• State of Louisiana	26
• State of Michigan Department of Health and Human Services.....	27
• The U.S. Census Bureau.....	28
Achieving Mission Success Together	29



Digital technologies

promise to transform how government agencies can accomplish their mission to more effectively serve the public good. But exploring new digital avenues also creates new challenges. The public sector has to find new ways to work with data at scale, and to secure it in a world of heightened cybercrime and nation-state threats.

Agency IT environments are increasingly complex. Years of adopting new technologies while still supporting legacy infrastructure have created a heterogeneous landfill, strewn with disparate systems and applications. This makes it all the more difficult to achieve mission success, while failure can lead to everything from constituent dissatisfaction, increased oversight and regulatory inquiries to suboptimal outcomes and damage to agency reputation.

Whether protecting a nation or delivering citizen services, mission success requires efficient and informed decision-making. Agency leaders have to make more decisions than ever, faster than ever, and each decision in our modern, instantly connected world is increasingly critical — with an ever-shrinking margin of acceptable error.

Splunk is the Data-to-Everything Platform that delivers real-time insights, drives confident decisions and enables decisive actions at the speed the mission requires. It allows agencies to leverage and extract real value from their data, regardless of source, timescale or structure. This significantly enhances the potential for mission success while lowering total cost of ownership and increasing return on investment.

Digital technologies are becoming more sophisticated, constituent expectations are rising and data itself is becoming more complex. As a result, hundreds of public agencies — across local, state and national governments — are using the Splunk platform to handle every data challenge as they work to better protect our critical infrastructure, serve their constituents, modernize IT operations and meet mission objectives.

The Mission:

Protect, Serve, Modernize





For public sector agencies, success is not measured in terms of financial profit and loss. The mission is noble: to ensure the well-being and protection of the citizenry, promote and maintain peace and goodwill around the world, and ensure the efficient stewardship of public resources. To promote their varied missions, agencies have to ensure they deliver the best experiences through modern and efficient infrastructures while protecting these systems and data from harm.

Protect

Cybersecurity is one of the biggest challenges facing us today, given the increasing threats from nation-states and cyber criminals committed to inflicting maximum damage. At the same time, insider threats, both malicious and unintended, are rising. A strong security posture and a resilient operating environment are fundamental to agency mission success.

Serve

With each government agency's work tied directly to the benefit of the citizen, a large part of mission success is ensuring that the citizen experience is satisfying and the delivery process is efficient. Yet "good user experience" is a moving target, thanks to constantly improved consumer devices and applications that are steadily increasing expectations. Real-time insights delivered by the Splunk platform can ensure that services are timely and meet citizen needs.

Modernize

Agencies must fundamentally transform how they operate. Their evolution includes the pursuit of increased efficiency, enhanced security, improved processes and elevated citizen satisfaction. At the same time, agencies are charged to maintain accountability, transparency and compliance. The broad challenges of such transformative modernization extend across existing data centers, migration to the cloud, the deployment of shared services and much more. At the heart of every modernization is data.

Splunk helps public sector customers improve mission outcomes, make effective use of ever-limited funding, protect critical assets and drive modernization. Our single-platform, any-data approach lets agencies make the most of their investment by reducing mundane, repetitive tasks and empowering personnel at all levels to improve every decision and action through data.

Here is how some of our customers are harnessing data with Splunk to accomplish their missions.

Mission-Critical Success: The National Ignition Facility at Lawrence Livermore National Labs

The National Ignition Facility (NIF) is a unit within the Lawrence Livermore National Laboratory in Northern California. This premier facility is engaged in three core missions: stewardship of the U.S. nuclear stockpile through secure and reliable underground testing, experimentation in astrophysics to enhance the country's competitive advantage in scientific endeavors, and exploration of fusion ignition, which could potentially unlock a clean, carbon-free energy source. To support and promote these missions, scientists and engineers require a secure, reliable IT infrastructure.

"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," says Bruno Van Wonterghem, the facility's operations manager.

Splunk has helped NIF maximize systems uptime and improve the reliability of IT infrastructure — from enhancing performance of more than 66,000 IoT devices to ensuring precise operation of the world's largest laser.

"Scientists expect data to be accurate and delivered quickly; it's used for other experiments and to further their scientific career," says [NIF CTO Philip Adams](#). "As such, we have to ensure that we make decisions with the right data to effectively resolve any issues that could affect the next [experiment]."

Using Splunk, NIF has improved control systems reliability and maximized operations at the lab. Splunk has allowed scientists to double the number of laser experiments from 200 to 400 per year, maximizing ROI not merely on the Splunk platform, but across the facility's scientific work.

Gold-Medal Security: City of Gold Coast

When the **City of Gold Coast** hosted the 2018 Commonwealth Games, security became a heightened priority, among many other challenges of hosting more than 4,400 athletes from 71 nations, plus thousands more tourists and spectators. (More than a million tickets were sold to the various events.) All this meant the Australian city had to up its game, especially around security. The City of Gold Coast needed to coordinate with local, state and federal partners to mitigate cyber risks and to protect infrastructure and public safety throughout the city and sporting venues.

Splunk helped the city overcome the visibility challenges of running multiple security systems. "We lacked visibility across multiple environments," says Matthew Walker, an IT security advisor with the city. "We needed a solution that could consolidate and accommodate multiple environment types — from industrial control systems to traditional IT systems."

Splunk let Walker and his colleagues monitor different threat profiles and priorities across different environments on one holistic platform.

Smart Modernization: Jefferson County School District

Colorado's state-run **Jefferson County School District** (Jeffco) used Splunk to enable ambitious transformation initiatives that support technology-enhanced 21st-century learning. Delivering dependable wireless access across geographically distributed sites introduced operational complexity and heightened data security issues, requiring security across a complex environment of BYOD and district devices.

Jeffco delivered wireless uptime of 99.99% to 100,000 devices across 700 square miles, serving 86,000 students and 15,000 employees across 156 sites. With Splunk, Jeffco has enhanced reliability by reducing mean time to repair (MTTR) to half an hour or less.

The Splunk Data-to-Everything Platform helps Jeffco combat cyberbullying and safeguard against phishing attempts and other external threats. Advanced data capabilities also make schools more secure by enhancing physical security.

“Our biggest challenge was providing the flexibility for our teachers and students to create content and collaborate in innovative ways — while at the same time protecting information security in our distributed and complex environment,” says Chris Paschke, the district’s director of data privacy and security.

The district’s evolutionary vision is ambitious. Next steps include increasing security and logging around student grades and other data, as well as automating more processes and improving support and troubleshooting in the field.

Transformation of the Decade: The U.S. Census

The U.S. Census Bureau has a mission of amazing complexity: to serve as the nation’s leading provider of quality data about its people and economy.

Once every 10 years, the Census Bureau sets out to provide a complete, accurate count of the population and housing in the entire United States. That means counting every person, in every corner of our nation. As the 2020 census marks the country’s first digital census, the organization is using the Splunk platform to more effectively and efficiently complete its mission, which shapes public policy, distributes over \$675 billion in funding and literally redraws the political map for the next decade.

The 2020 census includes 35 operations and 52 systems, which span everything from HR and payroll to coordinating a nationwide effort that has to cover every household in the country, including urban apartment buildings, rural cabins, prisons and group homes in every state and U.S. territory. Yet thanks to digital transformation and improved data handling, this year’s operation has fewer systems than in 2010, which will improve performance, accuracy and efficiency while optimizing taxpayer dollars.

Splunk is enabling this massive data project, with a more complicated digital dimension than ever before, in numerous ways. Up front, Splunk helps the bureau coordinate address lists from multiple sources, use satellite data to reduce manual door-to-door efforts, and more efficiently and accurately consolidate field data as it comes in.

On the back end, Splunk makes recruiting, hiring and paying workers more efficient through automation and digital workflows. That solves a massive issue for an organization that has to hire and coordinate 6,000 door-to-door enumerators for the months-long effort.

Splunk serves as a key partner to the Census Bureau, providing multiple services from security to infrastructure and applications. The Data-to-Everything Platform increases efficiency and ensures data can be accessed in real time.

Earning and maintaining the public’s trust is a vital part of the Census Bureau’s mission. With highly sensitive data, and a tight timeline to complete a massive operation, the bureau’s security team relies on Splunk to proactively identify vulnerabilities, isolate and effectively respond to incidents, and adhere to proper data security policies. By using Splunk to accomplish key tasks like unifying data on a single platform, the Census Bureau is troubleshooting issues faster, gaining more visibility into systems, and protecting data from the time it’s collected to when it’s in transit and delivered to other systems.

Mission Focused



```
[cpu] done / done / password found / operation 129 227  
[cpu] negative / negative / [not found] / operation 2289 4  
[cpu] done / negative / error 003  
[cpu] error / error / restart  
[cpu] done / done / access / complete / operation 122 334  
[cpu] error  
[cpu] negative / analyzing / operation 552 390  
[cpu] preparation complete / code xxx000x0xx0x0
```



Splunk, the Data-to-Everything Platform, is helping public agencies bring data to every aspect of their work. From municipal governments, public education and healthcare to defense, transportation and cutting-edge scientific research, Splunk helps public sector agency leaders ensure mission success by driving confident decisions and decisive actions at speeds the missions demand through real-time, data-driven insights.

Unlike legacy data platforms and siloed monitoring tools, Splunk offers a cost-effective, extensible and massively scalable analytics platform that delivers enterprise-wide visibility across cloud, on-premises and hybrid system deployments, enabling agencies to reuse data to overcome challenges across discrete programs and mission objectives.

On the following pages, meet a select handful of the agencies whose missions we're proud to support.



The Bank of England Protects \$1 Trillion Every Day

Founded in 1694, the Bank of England is the central bank of the United Kingdom, facilitating transactions that amount to roughly \$1 trillion every day. The Bank of England's SOC — staffed by a team of 10 security analysts — is responsible for protecting the infrastructure that facilitates these transactions, processes one-third of the country's GDP and is used by 4,200 staff, across a network of 10,000 endpoints that cover servers and user devices. Seeking to evolve from a reactive to a proactive SOC, the Bank of England recognized the need for a new operating model — one where the technology fits the model, not the other way around.

BUSINESS IMPACT

- Develops analytics to quickly identify bespoke attack operations
- Reframed defense strategy, evolving from a reactive to a proactive SOC
- Enabled the SOC to recruit specialized talent for security analytics, rather than systems engineering, thanks to Splunk's ease of use

The bank's new strategy relies on Splunk for large-scale data mining, log analysis, threat intelligence matching and preventative controls. With Splunk's fast, iterative search development, analysts can develop a wide range of analytics that provide more flexibility and efficiency in detecting attacks. Implementing Splunk also allowed the SOC to reframe their defense strategy — targeting the adversary's operations across their MITRE ATT&CK framework, rather than the attack itself, with greater success.



City of Gold Coast Gains Real-Time Visibility for the Commonwealth Games

City of Gold Coast, the second largest local government in Australia, has 3,900 staffers and provides a range of services, activities and facilities for residents and visitors. Hosting the 2018 Commonwealth Games was an added impetus for the city to enhance its security operations and visibility across the organization. Since ensuring the safety of thousands of people is a key challenge faced by the host of any major sporting event, City of Gold Coast deployed Splunk to fortify its security posture.

BUSINESS IMPACT

- Consolidated monitoring and investigation for better efficiency and security
- Mitigated risk in a heightened threat environment
- Delivered real-time visibility into security events across diverse environments and systems

In deploying the Splunk platform, City of Gold Coast mitigated cyber risks and kept event attendees and the local community safe. With Splunk's help, the city established a core cybersecurity operations capability that would meet its current and future needs, beyond the games. The success of the service, cemented by Splunk's ability to monitor during the heightened threat period, has established confidence across the organization and made the city's security committee more prepared than ever before to handle threats.



“Splunk allowed us to leapfrog our security service maturity. With the service now stabilized and operational cadence established, we are ready for new use cases and new data sources in other areas of the organization.”

— Matthew Walker, Information Technology Security Advisor,
City of Gold Coast



City of Los Angeles Enables Real-Time Security Intelligence Across 40+ Agencies

To protect its digital infrastructure, the City of Los Angeles requires threat intelligence and situational awareness of its security posture. Previously, the city's more than 40 agencies had disparate security measures that complicated data analysis. Los Angeles turned to Splunk to assess citywide risks, gain visibility into suspicious activities and proactively mitigate threats.

BUSINESS IMPACT

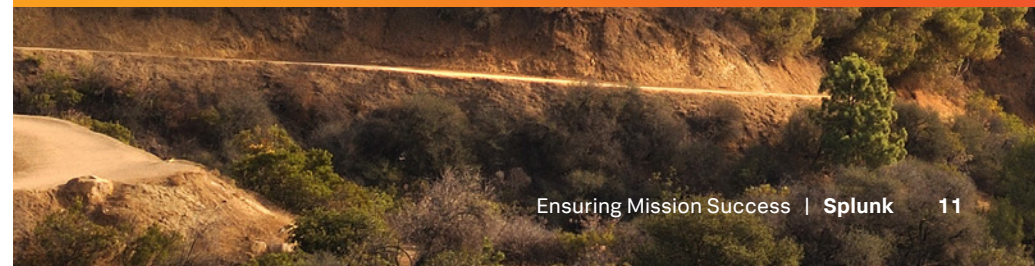
- Created an integrated citywide security operations center (SOC)
- Increased protection for digital assets, infrastructure and public services
- Enabled threat intelligence and real-time, 24/7 network surveillance across the city

The city now uses Splunk to ingest raw logs and other data from its more than 40 departments. Splunk then integrates this information into an integrated SOC where the team can analyze and visualize the data in easy-to-use dashboards. With this unified view, executives and analysts can monitor malware, identify top attackers and their targets, and have always-available situational awareness of security events to make the city a safer place for its citizens.



“With situational awareness, we know ourselves. But with threat intelligence, we know our enemy. We’re now operating an integrated threat intelligence program and our Splunk SIEM is one of the key solutions for a centralized information management platform that we deploy at our Integrated Security Operations Center (ISOC).”

— Timothy Lee, Chief Information Security Officer, City of Los Angeles



Use Cases

IT Operations
Security
Internet of Things

Dubai Airports Flies Into the Future With Splunk

Expecting to serve 100 million travelers annually — and to provide exceptional services to each of them — Dubai Airports turned to Splunk Enterprise. The airport meets its target to get 95 percent of passengers through security in five minutes or less by monitoring metal detectors to identify trends that keep queues moving efficiently. The IT team monitors all of its Wi-Fi access points in real time, detecting and dealing with congestion and rogue hotspots as they arise.

BUSINESS IMPACT

- Moves 95 percent of passengers through security in five minutes or less
- Provides the world's fastest airport Wi-Fi, with zero black spots
- Delivers consistent, high-quality customer experience

Each bag in Dubai Airports baggage system creates more than 200 data points, all of which are monitored in Splunk Enterprise to make sure bags reach their intended destinations. The airport is able to allocate resources effectively by combining baggage data with operations data to predict baggage load. Dubai Airports needed to increase airport capacity without any additional terminal space, infrastructure or runways. Using Splunk to uncover actionable data insights, the airport is doing just that.

WATCH THE VIDEO:

splunk.com/dubai-airport-video



“We are using Splunk to dramatically improve the travel experience for millions of people.”

— Michael Ibbitson, Executive Vice President,
Technology & Infrastructure, Dubai Airports



Use Cases

Compliance
Security

Fairfax County Protects Its Citizens' Data

Fairfax County, Virginia, located in the heart of the nation's capital, employs 12,000 people across more than 50 agencies and serves more than 1.1 million citizens. Its government is regarded as a leader in cybersecurity and IT, enabling the county to effectively serve and protect citizens. Since deploying Splunk Enterprise Security (ES) with Splunk Cloud as its security information and event management (SIEM) platform, Fairfax County has reduced security reporting from two weeks to real time.

BUSINESS IMPACT

- Proactively supports more than 50 county agencies and protects citizens' data
- Reduced security reporting from two weeks to real time
- Achieved significant cost savings by reducing data center hardware footprint

Fairfax County relies on the Splunk platform to monitor employee emails for phishing attempts and millions of daily threats on its endpoint systems. In addition to known threats, the county monitors and protects against dangerous malware while also defending its critical infrastructure, including supervisory control and data acquisition (SCADA) systems. Fairfax County is benefitting from its cloud service for operational intelligence in several ways, including elasticity, security and scalability — without the operational effort.

WATCH THE VIDEO:

splunk.com/fairfax-county



“Previously, reporting to leadership was difficult because everything was manual. My staff would spend countless hours, probably two weeks' worth of work, to get me a summary report of our cybersecurity stance. Now, with the Splunk platform, I have real-time access and can give an overall security posture to my leadership to let them know when we have issues.”

— Mike Dent, Chief Information Security Officer, Fairfax County, Virginia

Use Cases

Business Analytics
Internet of Things

Hong Kong's Vessel Traffic Center Gains Real-Time Port Operations Visibility

The Marine Department (MD) plays a vital role in achieving safe port operation within Hong Kong waters. Previously, while focusing on marine traffic on radar displays and other electronic systems, operators had to manually input vessel activity records and search through piles of paper to retrieve data, then pass the relevant documents to the next operator when vessels moved across the department's four sectors. To increase operational accuracy and efficiency, MD chose Splunk to revamp its whole system.

BUSINESS IMPACT

- Reduced vessel tracking from tens of minutes to seconds by operating manual procedures
- Facilitates operation through real-time, end-to-end visibility into marine traffic
- Enhanced public image with improved navigation safety and traffic efficiency

With Splunk, MD has created one of the world's first fully automatic vessel tracking systems. Splunk enables MD to collect, index and integrate big data in real time for traffic analysis. The operator then distributes navigational information and advises vessels through a high-frequency radio network to facilitate safe arrivals and departures. This end-to-end visibility enables everything from automatic vessel identification to statistical analysis. Now, operators can concentrate on vessel traffic and offer just-in-time advice to mariners, achieving more efficient and effective port operation.



“Splunk has impressed us with its exceptional flexibility and data processing capabilities. It helps us bridge the electronic system and Maritime Information Systems and provide deep insight into the data, giving us confidence to have a strong foundation between systems. The result is to achieve real efficiency in our daily operations.”

— Gordon Yuen, Information Technology Manager,
Marine Department of the Hong Kong Government



Jefferson County Public Schools Enables Secure 21st-Century Learning

Colorado's Jefferson County Public Schools is a K-12 district that requires technology to ensure a high-performing, flexible and secure learning and teaching environment. The five-member security team supports 86,000 students and 15,000 staff in 156 schools with firewalls, email gateways, investigations and other security defenses.

BUSINESS IMPACT

- **Delivers wireless uptime of 99.99% to 100,000 devices across 700 square miles**
- **Reduced mean time to repair (MTTR) to 30 minutes or less**
- **Supports complex distributed IT resources with small IT staff**

To prevent the district's physical security monitoring devices from outages, the team now relies on Splunk Enterprise to monitor error codes and proactively alert staff, who can repair systems before they crash. The Splunk platform also helps the district address cyberbullying issues by letting the team track system usage, user and device access.



“K-12 schools are always under tight budgets. With Splunk, two of us can manage our large network without pain.”

**— Michael Kent, Wireless Network Engineer,
Jefferson County School District, Colorado**



Use Cases

IT Operations Management
Log Management
Security

Leidos Taps Splunk for Better Event Management

As a Fortune 500 science and technology solutions leader, Leidos' 48-year history spans everything from supporting the U.S. space shuttle program to helping design an America's Cup yacht race winner. Today, Leidos is working to solve global challenges in defense, intelligence, health and other markets — and facing its own challenges to ensure its services are always available to customers. Since replacing its legacy event management solution with Splunk IT Service Intelligence (ITSI), the Leidos internal IT department has seen many benefits.

BUSINESS IMPACT

- Enables enterprise-wide infrastructure monitoring and event correlation
- Gained better visibility into IT and business processes
- Delivers easy-to-share dashboards to different audiences, from problem-solving techs to big-picture managers

Leidos needed a solution that could bring together functional silos and triage a flood of events spanning more than 120 IT services. The Splunk platform has broken down silos by enabling teams to see data across the service stack. By addressing a growing number of alert management issues, the Splunk platform also helped the company boil 3,500 to 5,000 daily alerts down to roughly 50 tickets for network and datacenter operations to act on.

WATCH THE VIDEO:

splunk.com/leidos



“My most important contribution at the end of the day is that we make a difference, that we provide a service that people find accurate and insightful. The fact that Splunk has all of the information means that people can get their answers quicker, and more accurately and efficiently.”

— Don Mahler, Director of Performance Management, Leidos



Use Cases

Security
Compliance
IT Operations
Business Analytics

Maryland Lottery and Gaming Control Agency

Bets on Splunk

Operating the state lottery and serving as regulator of the state's six casinos, the Maryland Lottery and Gaming Control Agency (MLGCA) oversees lottery and gaming activities that generate more than \$1 billion in annual contributions to the State of Maryland. Before Splunk, the agency spent several hours each week on manual processes— from meeting specific criteria regarding database security to documenting IT processes each week to meet audit requirements. The agency turned to Splunk, the Data-to-Everything Platform, to modernize its IT and security operations.

BUSINESS IMPACT

- Saved up to six hours every week on compliance by automating essential processes
- Improved anomaly detection to quickly identify and prevent security breaches
- Provides real-time compliance reporting for auditors, as well as security monitoring for the IT team and CIO

With Splunk, MLGCA has automated and modernized security operations, providing staff with visibility that's especially critical when dealing with the type of sensitive data that the agency collects. Splunk has also helped the agency reduce the time and effort spent on manual tasks, saving on average four to six hours weekly. By automating essential processes, the agency's IT staff can respond faster to events that might indicate a security breach, and more efficiently maintain and improve the MLGCA's overall security posture.



“How do you quantify the insight into some of these events that we proactively catch? Splunk is helping us to detect potential breaches before they turn into actual breaches that could cost the agency millions of dollars and become public relations nightmares.”

— Jeff Patchen, Chief Information Officer, Maryland Lottery and Gaming Control Agency



Use Cases

IT Operations
Application Monitoring
Infrastructure Monitoring
Predictive Analytics

Industrial Data
Internet of Things
Security Monitoring

National Ignition Facility Unlocks the Potential of Clean Energy and Safeguards the U.S. 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 (ITSI) now 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.

BUSINESS IMPACT

- Maximized system uptime and performance
- Improved control systems reliability, enabling the team to maintain the necessary systems to double the number of laser shot experiments from 200 to 400 annually
- Ensures the health of more than 66,000 Internet of Things (IoT) devices, in addition to the IT infrastructure

After bringing network, authentication and host data into Splunk to solve security challenges, the team aggregated this data with a variety of other sources to gain real-time visibility across the 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.

WATCH THE VIDEO:

splunk.com/nif-video



“Splunk ITSI enables the team to take a very complex machine and break it down into discrete components. Previously an AIOps approach would have taken a lot of resources to implement. This is the first time that we could simplify that technology for an IT user base and apply that to an infrastructure use case.”

— Philip Adams, CTO and Lead Architect, National Ignition Facility,
Lawrence Livermore National Laboratory

Use Cases

Application Delivery
Cloud Solutions
IT Operations
Log Management

New York Regional Education Agencies

Unify Data to Improve Operations and Accelerate Student Learning

Technology is a key component of K-12 educational instruction and school district operations, but keeping student data secure is a challenge. In New York state, a project called RIC One offers automated data integration and single sign-on for applications that students, teachers and administrators use to improve school operations and classroom instruction. RIC One turned to Splunk to improve central log management and application monitoring.

BUSINESS IMPACT

- Enhances overall educational experience with access to relevant applications at any time
- Ensures security of student and teacher data across districts
- Saves costs with a cloud solution that's easy to use and provision

RIC One relies on the Splunk platform for proactive log monitoring and to ensure that processes are running and succeeding every day. Splunk Cloud alerts the team if one of the processes fails, enabling them to resolve issues quickly. Splunk Cloud has also reduced the number of servers for the team to maintain and administer, allowing them to work on more strategic initiatives.



“I don’t think we could be operating without Splunk. If we had to manually go to these different places to find this information and do data correlations without the notifications, we wouldn’t be where we are. Splunk is so powerful that if you have all that information there, what you can do with it is just endless.”

— Staff Member, RIC One

Use Cases

IT Operations
Security
Fraud

NHS Choices Boosts Visibility to Deliver Critical Online Services

NHS Choices, the United Kingdom's biggest healthcare website, aims to be a "world-leading, multi-channel service for everyone engaging with the NHS and social care." In order to deliver the best possible service to its 48 million visitors every month, NHS Choices needed a solution to provide insight into the vast volume of log data produced by the website infrastructure.

BUSINESS IMPACT

- Improved ability to troubleshoot website issues
- Better management of website traffic
- More sophisticated reporting capabilities

As the online 'front door' for the National Health Service (NHS), NHS Choices had to ensure that the site is optimized to provide the best possible access to information to improve public health. Splunk helps NHS Choices monitor the large volumes of machine data generated with daily website visits, while allowing technology teams to quickly identify and address problems, effectively manage website traffic and enhance reporting within the organization. The Splunk platform is now also a key component of the monthly release cycle for the website, giving the team a real-time overview of the impact of updates as they're being implemented.



"Splunk allows us to continually improve the services we provide for the public at the same time as reducing our overall infrastructure costs."

— Andy Callow, Head of Technology Delivery, NHS Choices



Use Cases

Application Delivery
IT Operations
Security

Maryland's **Prince George's County** Mission-Ready With Splunk Platform

Home to NASA's Goddard Space Flight Center, the University of Maryland and nearly 1 million citizens, Prince George's County, Maryland, located outside of Washington, D.C., spans almost 500 square miles. The county's centralized Office of Information Technology (OIT), which supports all branches, agencies and government employees, faces many challenges when it comes to fulfilling its mission with limited resources and funding. The county relies on Splunk to monitor its extensive network, which consists of about 100 sites and 500 network devices.

BUSINESS IMPACT

- Improved government efficiency and transparency to better serve constituents
- Helped small IT team reduce time to identify and resolve IT issues from days or weeks to hours
- Transformed county operations by replacing data silos with a platform for IT operations, application monitoring and security

The county uses Splunk Enterprise for application monitoring, including an application that enables citizens and contractors to apply for and complete permits online. In addition to providing some of the county's senior managers and engineers with IT operations visibility, OIT staff members also rely on Splunk to help with cybersecurity. Moving forward, the county plans to grow its use of the Splunk platform to improve its security posture.

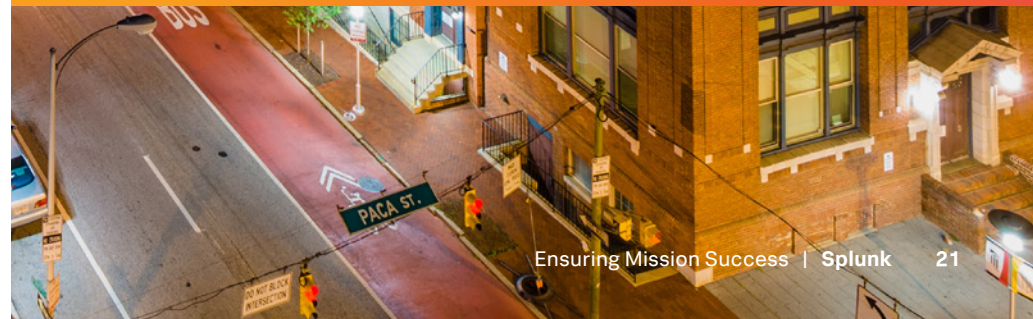
WATCH THE VIDEO:

splunk.com/prince-georges-county



“With Splunk, we’re able to have greater visibility across functional teams, to identify trends and potential problems in advance, and to solve issues more quickly by seeing a broader view of the problem.”

— Jayson Loveless, Enterprise Architect, OIT, Prince George's County



Saving Lives With Splunk and **Royal Flying Doctor Service**

The Royal Flying Doctor Service of Australia (RFDS) is one of the largest and most comprehensive aeromedical organizations in the world. This nonprofit organization provides emergency and primary healthcare services for those living in rural, remote areas of Australia — people who cannot access a hospital or general practice due to the vast distances of the Outback.

BUSINESS IMPACT

- **Centralized data analytics and monitoring to deliver critical care to 290,000 patients annually**
- **Enabled real-time alerts on the temperature of refrigerated vaccines and medicines, which has optimized medicine delivery and reduced waste**
- **Delivers detailed information to donors, communicating life-saving missions performed in their sponsored region**

RFDS's fleet of 63 aircraft — which makes them Australia's third-largest airline — produces large volumes of avionics and location data as it covers its "waiting room," which spans four-thousand square miles. Splunk dashboards provide real-time visibility into the status and movements of the fleet, equipping RFDS with the information it needs to efficiently deliver critical health services in circumstances where every second counts.



“Splunk is a critical part of our infrastructure that we use in delivering our critical health services. If somebody took Splunk away from me, I’d feel like I lost my right hand.”

— Adam Ind, IT Manager, Royal Flying Doctor Service



Use Cases

Business Analytics
Internet of Things

Sacramento County Sheriff's Department Powers Intelligence-Led Policing

The Sacramento County Sheriff's Department is responsible for law enforcement services for unincorporated areas of Sacramento County, California, and several incorporated cities within the county. The department implemented Intelligence-Led Policing (ILP), a strategy that depends on high-quality data analysis, and needed a way to harness data that existed in disparate, siloed systems.

BUSINESS IMPACT

- Provides holistic visualizations and real-time access to crime statistics and operational insight
- Helped cut reporting backlog by up to 50%
- Saves hundreds of hours per year in ad hoc report generation

Since the initial Splunk deployment, the department's applications team has created more than two dozen dashboards, many with multiple panels, including map-based views of weapons used by location and crime overviews showing crimes year-to-date, incidents by day of the week, race of victims and more.

The initial recipients of Splunk-based dashboards and reports were the Sheriff Department's top command, including the sheriff, the undersheriff, chiefs, captains, lieutenants and sergeants. Demand for additional dashboards and reports grew dramatically after the first deployment. For instance, requests for specific information on budgets and spending practices came from the County Board of Supervisors, which oversees the Sheriff's Department.



“The Splunk platform is critical to our Intelligence-Led Policing strategy. Our command group is now able to more clearly see trends in our crime statistics and take proactive action to address areas of concern and provide the best possible service to the public.”

— John Britto, Senior IT Analyst and Application Team Lead,
Technical Services Division, Sacramento County Sheriff's Department



Use Cases

Application Delivery
IT Operations
Security

SAIC Builds New World-Class Security Operations Center

Science Applications International Corp. (SAIC) is a leading technology integrator specializing in technical, engineering and enterprise information markets. With expertise in domains such as scientific research, program management and IT services, the company needed to build out a robust security operations center (SOC) and computer incident response team (CIRT) to defend against cyberattacks.

BUSINESS IMPACT

- Improved security posture and operational maturity
- Decreased time to detect and remediate incidents by over 80%
- Gained comprehensive visibility throughout the enterprise environment

Although it had most of the security tools it needed to build its SOC, SAIC lacked a SIEM solution to anchor its defenses. The company decided to rely on Splunk as the single security intelligence platform for all of its SIEM-like needs. With Splunk software, SAIC has been able to realize significant operational efficiencies and reduced labor costs across the 50-plus security personnel in the SOC and on the CIRT. Furthermore, data sharing in Splunk by various teams has led to greater ROI and improved overall IT efficiency.

WATCH THE VIDEO:
splunk.com/saic



“The template for effective security is visibility, analysis and action. Our Splunk system gives us comprehensive optics and deep, data-driven analytics, enabling us to take highly informed action to protect our assets.”

— Jonathan Jowers, Chief Information Officer, SAIC



Sandia National Labs Leverages HADES for Advanced Threat Intelligence

As an organization known for its scientific and engineering innovation, it comes as no surprise that Sandia National Laboratories, a multi-mission U.S. National Nuclear Security Administration (NNSA) research and development lab, has developed an advanced approach to addressing complex national security challenges. Sandia's High Fidelity Adaptive Deception and Emulation System (HADES) is a multi-faceted cyber-defense application that solves a fundamental deception challenge — fusing human-mediated and machine-assisted deception, live.

BUSINESS IMPACT

- Provides an automation-driven collaborative framework for fast and consistent threat identification and response
- Enables analysts to produce and share threat intelligence while interacting with attacks in real time
- Realizes the ability to deceive adversaries, profiling them incognito to expose their tactics — providing analysts with a significant competitive advantage

HADES uses the Splunk platform to arm analysts with end-to-end visibility. They can determine indicators of compromise (IOCs) to develop profiles of adversaries in real time. These profiles and IOCs can detect attacks in operational networks, minimizing and, in some cases, preventing damage. Thanks to Splunk, the team is able to stay one step ahead of attacks with a platform that shifts the cost to the adversary.



“We have such complex, non-homogenous data sources in HADES; we were already using the Splunk platform in other areas, so it made sense to leverage it for HADES to meet our needs.”

— Vincent Urias, Cybersecurity Research Strategist,
Sandia National Laboratories



State of Louisiana Saves Millions by Modernizing IT

The State of Louisiana recently consolidated all of its IT departments across 20 executive branch agencies, bringing 850 staffers into a modern, shared services model. The newly unified department has been tasked with cutting costs and enhancing service delivery to its core set of customers — state agencies and citizens. Since deploying Splunk, the state reports that agencies can focus on their business rather than spending time on IT maintenance and contracts.

BUSINESS IMPACT

- Saved \$70 million by accelerating modernization and legacy consolidation efforts
- Improves efficiencies and customer experiences with streamlined IT and centralized data management
- Drives business efficiencies and cost savings with a shared services model

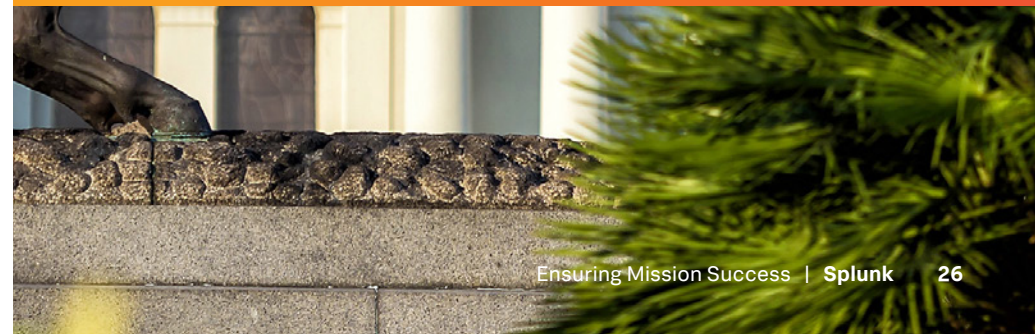
With Splunk, agencies now get an accurate read on their usage, such as the number of documents stored, the amount of storage consumed and the number of business rules run for analysis. The state is already planning the next step: customer dashboards to show not only that agencies' servers and applications are up and running but how much they cost — providing more transparency from the governor's office on down.

WATCH THE VIDEO:
splunk.com/state-of-louisiana



“Splunk is extremely efficient for us and makes the best use of taxpayer dollars. Not only does it save us money from having to do things manually with multiple systems, but it supports transparency. It gives us the ability to show people exactly how things are being used and why.”

— Derek Williams, Director of Data Center Operations, State of Louisiana



Use Cases

Application Delivery
Security

State of Michigan Department of Health and Human Services Delivers Superior Citizen Experience

The State of Michigan Department of Health and Human Services (MDHHS) is responsible for delivering services across healthcare, food assistance, child development and care, cash assistance and state emergency relief. To provide these services to more than 1.7 million citizens, MDHHS uses the integrated eligibility system called BRIDGES, which connects 52 different agencies and more than 10,000 users while processing over 12,000 transactions per minute.

BUSINESS IMPACT

- Achieved 20% improvement in addressing issues before they impact users
- Increased ability to meet SLAs by reducing MTTR by up to 35%
- Ensures passing compliance scorecards while reducing manual compliance efforts by 50%

After adopting Splunk, the Data-to-Everything Platform, MDHHS increased efficiencies across the business by gaining granular visibility into its BRIDGES application infrastructure. With the ability to pinpoint usage and analyze performance, combined with prediction capabilities and artificial intelligence, the agency now gains insights into issues well before users are impacted, helping improve the overall citizen experience.

Meeting compliance mandates is a core part of any government agency's objectives. With Splunk, MDHHS gained unprecedented visibility into their compliance posture in real time, enabling a passing scorecard, increasing audit efficiency and reducing staff's manual efforts by 50%.



“Our staff’s manual effort of providing and tracking PCI & audit compliance has been reduced by 50% by Splunk. This helps us to ensure a passing scorecard for audits.”

— Sanjay Srivastava, Division Director, Eligibility Area DTMB, State of Michigan



Use Cases

IT Operations
Infrastructure Monitoring
Application Monitoring
Security

Fraud
Business Analytics

The U.S. Census Bureau Goes Digital for the Country's Most Efficient Census

Every 10 years since 1790, the U.S. Census Bureau has set out to accomplish the country's largest civilian undertaking: getting an accurate count of each person living in the United States and its territories. As the country's first digital decennial census, the 2020 census will provide Americans with the option to respond online, in addition to by phone or mail. To navigate this new territory, the Census Bureau uses Splunk to take a data-forward approach to measuring America.

BUSINESS IMPACT

- Facilitating success for the 2020 census, which is the country's first digital decennial and the most efficient census ever planned
- Enabling executives to make better, more informed decisions through standardized dashboards and real-time insights
- Ensuring integrity, availability and security compliance for the bureau's complex infrastructure of 52 systems and 35 operations

Splunk's dashboards and data visualizations have become a critical part of daily workflows at the bureau, delivering real-time insights to inform how senior leadership and teams like security, IT and application approach questions, make decisions and turn data into action. With Splunk at the center of its SOC and NOC, the Census Bureau has improved uptime, and is proactively identifying vulnerabilities and troubleshooting issues faster for a more secure and reliable experience.





Achieving Mission Success **Together**

These are just a few examples of how Splunk has helped agencies across the globe protect their infrastructure, modernize operations and better serve their constituents.

For more information about how Splunk drives mission success, watch the .conf19 presentations to hear our customers tell their stories:

State of Michigan: splunk.com/stateofmichigan-conf19

City of Amsterdam: splunk.com/cityofamsterdam-conf19

FBI: splunk.com/fbi-conf19

Bank of England: splunk.com/bankofengland-conf19