Profiles in Resilience

How forward-thinking public sector organizations are building cyber resilience

splunk>

Table of Contents

SOLUTIONS KEY

- IT
- Security

Preparing for Every Pitch

Imagine you're stepping up to the plate. You're stabilizing your stance, adjusting your grip, preparing to swing at the unexpected that'll come hurtling toward you from the pitcher's mound.

As public sector leaders, how many times over the past few years have you felt like this — unsure of what the next moment will bring? Curveballs of cyberattacks, heightened geopolitical tensions and a war in Ukraine. Fastballs of a global pandemic and remote work. Change-ups of intensifying citizen expectations and evolving compliance regulations.

These challenges have come hard and fast — and to adapt at a moment's notice, resilience has never been more vital.

When Splunk and researchers at Meritalk surveyed more than 300 government cybersecurity professionals, 91% said their organization needs a mature, overarching strategy for cyber resilience. Yet 82% of these organizations still defined cyber resilience as basic compliance and risk management.

Cyber resilience has evolved far beyond the concept of security to encompass a wider range of goals and needs, as evidenced by the National Institute of Standards and Technology's new definition: "Cyber resilience is the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks and compromises."

With wild pitches being thrown our way seemingly every second, these abilities are no longer a nice-to-have. They're essential.

91%

of public sector security pros say their organization needs a mature, overarching strategy for cyber resilience.

82%

still define cyber resilience as basic compliance and risk management.

The right tools for the perfect swing

So in a world of threats that could devastate our ability to achieve our missions, how do you prepare for the unexpected? The answer is to invest in the capabilities needed for cyber resilience — which means taking a multipronged approach that includes security, availability and performance.

From Cal Poly thwarting more than a million threats a day to Lawrence Livermore Labs preventing downtime for uninterrupted scientific experiments, future-minded organizations are defending against evolving threats while withstanding system disruptions and delivering a more reliable experience.

And they're using Splunk's unified security and observability platform to deliver. By relying on the Splunk platform for visibility into every aspect of their complex environments, public sector organizations are detecting and countering supply chain attacks (Sandia National Labs), achieving regulatory compliance (University of Cincinnati) and ensuring a safe, reliable learning environment for students — whether remote or in person (NYC Department of Education).

Across these profiles in resilience, you'll see how institutions are continuing to adapt and advance their mission objectives — from making historical strides toward clean energy (National Ignition Facility) and fighting human trafficking (Global Emancipation Network), to furthering gender parity in national security (Leadership Council for Women in National Security) and helping citizens pay for food and shelter (California Statewide Automated Welfare System).

We're working toward a more resilient future where every public sector organization can adapt quickly to the next curveball, evolve with changing expectations and make their missions possible. Let's step up to the plate together.

— Juliana Vida, Splunk's Group Vice President, Chief Strategy Advisor (Public Sector), Former Deputy CIO for the U.S. Navy

WHAT IS MISSION SUCCESS?

Making historical strides toward clean energy

— National Ignition Facility

Fighting human trafficking

— Global Emancipation Network

Furthering gender parity in national security

— Leadership Council for Women in National Security

Helping citizens pay for food and shelter

— California Statewide Automated Welfare System

Resilience in Action

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

3 branches of U.S. government

10+ Cabinet-level agencies

4 U.S. military services

48 of the 50 largest U.S. cities

900+ higher education institutions

On the following pages, meet a select handful of organizations that are using Splunk to improve resilience and deliver better outcomes for citizens.

Bank of England Protects $1 Trillion a Day

Key Challenges

The Bank of England needed to evolve from a reactive to a proactive SOC and recognized the need for a new operating model — one in which the technology fits the model, not the other way around.

Key Results

The Splunk platform has been critical in helping the Bank of England execute on large-scale data mining, log analysis, threat intelligence matching and preventative controls.

Founded in 1694, the Bank of England is the central bank of the United Kingdom, facilitating transactions that amount to one-third of the country's GDP. The bank's SOC — staffed by a team of 10 security analysts — is responsible for protecting the infrastructure that enables these transactions. With Splunk's fast, iterative search development, analysts now 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.

Outcomes

$1 trillion in transactions protected every day with secured infrastructure

10,000 endpoints covering servers and user devices **secured** with analytics that quickly identify bespoke attack operations

1/3 of the country's GDP secured by a proactive defense strategy

Solutions
Security

> I know the number of threats against the university is higher and the complexity greater than ever before. But I also know that we're protecting the university at a level we've never had before."

— Bill Britton, Chief Information Officer, Cal Poly

Outcomes

1M+ threats thwarted each day

<5 minutes to respond to incidents

2-4 students per quarter given **real-world cybersecurity experience**

Cal Poly Drives Resilience While Training Tomorrow's Security Leaders

Key Challenges

To better protect its campus and data, Cal Poly needed a unified security platform to give them visibility into the university's complex, hybrid infrastructure while also centering students' learning.

Key Results

With Splunk, Cal Poly gained the visibility it needed to strengthen its security posture, which has increased resilience and provided students with more real-world learning opportunities.

California Polytechnic State University (Cal Poly) students learn by doing — and in Cal Poly's SOC, which is tasked with providing around-the-clock protection from cyber threats, students provide tier-one incident response. But as the university began to migrate to the cloud, its security environment became exponentially more complex. With Splunk Cloud Platform and Splunk Enterprise Security (ES), SOC team members have eyes into the university's distributed systems so they can quickly detect and defend against security incidents. This heightened visibility helps the team provide 24/7 protection while offering students critical skills that will serve them well long after they graduate.

$30M annual savings for California taxpayers

Tens of millions of dollars in benefits **distributed each month**

1T+ of logs managed and analyzed **each day**

CalSAWS Meets Californians' Diverse Needs With a Strong Foundation of Security and Resilience

Key Challenges

CalSAWS needed to ensure highly secure, uninterrupted delivery of benefits to Californians who depend on the system for state and federal aid.

Key Results

With Accenture and Splunk, CalSAWS now has a robust SIEM infrastructure that helps protect resident data and privacy, shield the system from cyberattacks and proactively identify IT issues.

Millions of California residents depend on public assistance to pay for essential items and services — from food to housing to medical care. Built on AWS, the California Statewide Automated Welfare System (CalSAWS) replaces three disparate legacy systems with a single cloud-based platform to make it easier for people to access the social safety net. To ensure this platform provided uninterrupted delivery of benefits to constituents, IT services partner Accenture integrated Splunk Cloud Platform, Splunk Enterprise and Splunk Enterprise Security with their offerings. The resulting system more efficiently collects data and generates real-time, actionable insights to improve productivity, lower costs and reduce security risks.

Solutions

IT

Security

Derbyshire Fire & Rescue

Saves Money and Lives by Maximizing Data

Key Challenges

Without a centralized log monitoring solution, the service's small IT team had poor visibility across system management, software updates and security threats.

Key Results

With the Splunk platform, the IT team improved security response and reduced cyber risk with better insights into the service's security posture, faster troubleshooting and enhanced collaboration.

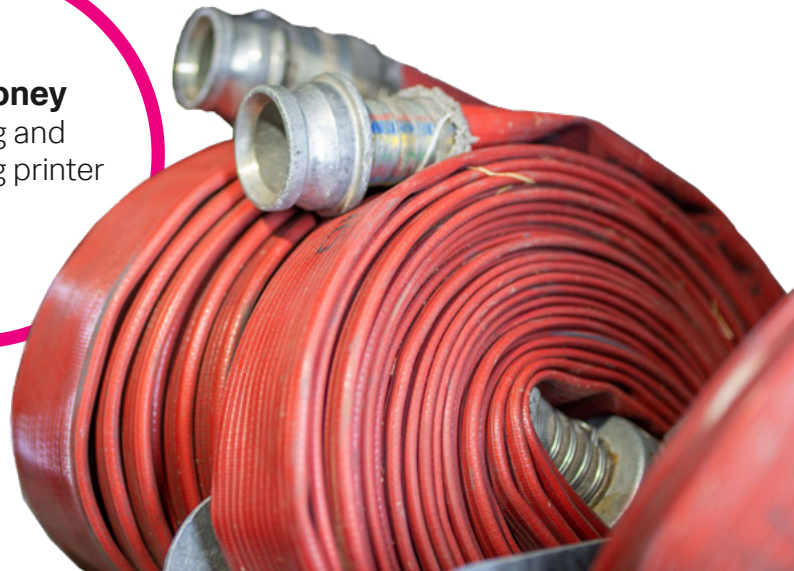
Derbyshire Fire and Rescue Service (DFRS) is tasked with protecting more than a million people. Yet to deliver safety for citizens, the service must first ensure security for its 31 fire stations and two data centers, which were at risk of cyberattacks. With Splunk's dashboards, the busy, hard-working DFRS team has an easy-to-access visual overview of system health. Previously, security incidents may have gone unnoticed, with engineers having to manually trawl through log files to look for anomalies when something suspicious was identified. With the Splunk platform, DFRS has improved worker productivity while also avoiding security disasters by blocking intrusions before any damage occurs.

Blocked security intrusion before damage occurred

Quickly spotted and repaired system maintenance issues

Saved money by tracking and addressing printer misuse

> "Thanks to Splunk, we get vital information at a glance. It's helped us make better, more informed decisions."
>
> — Pete Garyga, ICT Security and Project Team Manager, Derbyshire Fire & Rescue Service



Solutions

IT

“GEN would not be where it is today without Splunk. The support has been fantastic; the product is wonderful. Splunk has been as much a stakeholder in the success of GEN as we have ourselves.”

— Sherrie Caltagirone, Founder and Executive Director, Global Emancipation Network

Outcomes

Days to process and analyze massive volumes of data, cut **down from years**

Millions of data points from more than 22,000 massage businesses analyzed

55K+ schools across Northern Ireland, England and Wales analyzed, accelerating child abuse investigations

Global Emancipation Network
Fights Human Trafficking With Data

Key Challenges

Human trafficking affects an estimated 45 million people per year, but the data needed to trace perpetrators of this crime is poorly defined, siloed and hard to access.

Key Results

Splunk has been the bedrock of GEN’s mission, supplying the mission with software licenses, training, support and education through the Splunk for Good program.

Global Emancipation Network (GEN) and Splunk partnered to develop an analytics platform, dubbed Minerva, that analyzes unstructured, siloed data to uncover the people behind global human trafficking operations. Splunk helps sift through data from hundreds of sources to make connections between usernames, email addresses, phone numbers, texts and images that would be difficult or impossible manually. Through GEN and Splunk for Good, Minerva is available free to national and international government and law enforcement agencies, NGOs, academia and the private sector to help identify and stop human trafficking.

Solutions

IT

LCWINS Advances Gender Parity in National Security With Splunk Pledge

Key Challenges

The lean team at LCWINS was relying on Google Sheets to manage its data, which resulted in a platform that was not user friendly and hindered the organization's growth.

Key Results

Through Splunk Pledge, LCWINS gained necessary expertise and custom-built technology to increase efficiency, broaden its community of women and further its mission of gender parity in national security.

The Leadership Council for Women in National Security (LCWINS) seeks to advance gender parity in America's national security leadership. Already managing a database of 900 candidates, LCWINS needed a way to scale their organization and impact, but was limited by a reliance on Google Sheets. Splunk selected LCWINS as a recipient of the Splunk Pledge, an initiative that provides software licenses and training to organizations around the world. LCWINS team members now have the tools and expert support they need to grow and empower their community of women committed to serving their country in national security.

Faster, tailored candidate **search** — **from an entire day** to about **15 minutes**

Small team empowered to use data to achieve strategic goals

More opportunities for women in national security

> "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

McGraw Hill Counters Threats Faster With Splunk SOAR

Key Challenges

McGraw Hill manually responded to thousands of malicious emails every day, slowing mean time to resolution (MTTR) and increasing the risk of cyberattacks.

Key Results

Splunk SOAR automated the company's response to threats, accelerating response times, centralizing investigations, boosting productivity and increasing ROI.

With a small team and siloed security tools, learning sciences company McGraw Hill lacked a centralized platform to monitor malicious emails and prevent phishing attacks. Enter Splunk SOAR, which helped the company consolidate its 10 different security tools and automate its response to cyber threats. This shift sparked faster incident response times, and the centralized security operations center (SOC) saves McGraw Hill valuable time when training new analysts who join the team.

Outcomes

Within six months, McGraw Hill:

Automated 22 months' worth of **manual security tasks**

Completed the **workload equivalent of 10 full-time employees** with a small team

Resolved 9,439 security events via automated response

"We have everything in a single system, and we know everything's been 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

Solutions

IT

Security

National Ignition Facility

Unlocks the Potential of Clean Energy and Safeguards the U.S. Nuclear Stockpile

Key Challenges

NIF needed a secure way to safeguard data and prevent facility downtime, ensuring facility availability so scientists can conduct experiments.

Key Results

With Splunk, the team solved security challenges and gained visibility into all its disparate data for more resilient systems and increased uptime, helping the lab achieve breakthroughs in nuclear fusion and clean energy.

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

Outcomes

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

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

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

Solutions

IT

Security

The New York City Department of Education Fuels Remote Learning

Key Challenges

The largest school district in the United States needed to make remote learning work for over a million students when the pandemic hit in early 2020.

Key Results

With the Splunk platform, students and employees transitioned smoothly to remote learning and work, helping New York City kids stay connected and receive an excellent education — even from home.

As the largest school district in the United States, the New York City Department of Education serves a staggering 1.1 million students. As the world transitioned to remote learning, the department quickly recognized the need to adapt — fast. As their IT, security and business intelligence teams quickly set up critical infrastructure and digital learning systems, they used the Splunk platform to collaborate and identify bandwidth bottlenecks to ensure hundreds of thousands of employees and students kept learning in the new remote environment.

Secure, reliable remote learning for hundreds of thousands of students and employees

Ability to **adapt fast to meet evolving needs**

More resilient systems and infrastructure, thanks to proactive resolution of bandwidth bottlenecks

Solutions

IT

Security

> There is a cost avoidance benefit by identifying security issues and incidents early, and quickly, that meant things like when WannaCry was hitting the NHS we could quickly identify where there were issues and remove the offending device from the network to prevent it from spreading further."

— Morgan Rees, Technical Delivery Manager, Orbis

Outcomes

Eliminated siloes and **unified security visibility across 550 sites**

Secured information governance and compliance requirements that are critical to operating in the public sector

Improved customer service through **faster response times** to faults and incidents

Local UK Councils

Collaborate Over Security and IT Operations to Improve Operational Efficiencies

Key Challenges

To better deliver local government services, Orbis needed to replace its antiquated legacy systems with one platform that retains separate data ownership while offering full visibility across the partnership.

Key Results

With Splunk, Orbis has created a single view of data across the three councils, improving collaboration and accelerating issue resolution while maintaining information governance.

Orbis has a big job on its hands. Created to streamline back-office services across three local authorities in South East England, Orbis delivers finance, IT, procurement and HR services to over 20,000 users. Combining such a vast infrastructure meant a standardized security information and event management (SIEM) solution was essential to improve efficiencies and security. Splunk has been a key part of Surrey County Council's infrastructure upgrade and modernization, which kick-started the SIEM replacement process. By using Splunk Enterprise and Splunk Enterprise Security, Orbis has gained greater efficiency of services at scale and improved operational visibility.

Sandia Labs Detects and Counters Supply Chain Attacks With the HECATE Platform

Key Challenges

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.

Key Results

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.

Rather than attacking an organization directly, software supply chain attacks target the vendors of apps and other software that an organization uses. To help organizations identify and counter these attacks, Sandia National Laboratories developed the HECATE platform, which sits on Splunk technology. Creating an immersive environment to install, execute and observe software, this one-of-a-kind analysis solution automatically identifies software supply chain risks through everything from static and dynamic analysis to scalability and automation. By checking and cleansing software for breaches or intrusions before it's installed, HECATE helps leaders across industry, government and academia verify trust and reduce the risks that come with installing commercial and open-source software in their networks.

Data-Driven Outcomes

Provided 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 & Development, Sandia National Laboratories

University of Cincinnati

Ensures Regulatory Compliance and Protects Student Health

6 lives potentially saved through quick emergency response

Reduced time to incident response, containment and recovery

48K+ students protected

Key Challenges

Without full visibility into its distributed environment, the university's SOC team struggled to keep up with the size and scale of security alerts that threatened the safety of its community.

Key Results

Now with all logs and investigations in Splunk Cloud Platform, the university team can quickly address and remediate issues — supporting regulatory compliance and, crucially, the university's suicide prevention work.

Security is of the utmost concern for this Carnegie Mellon Research 1 institution — not only around compliance for its highly sensitive DoD research, but also in the organization's efforts to prevent suicide and ensure public safety. To that end, the SOC team wanted to expand the footprint of security within the university and streamline risk management. Now with Splunk Cloud Platform, the university's security team has deep visibility into its entire environment, quickly investigating and addressing threats to its security posture as well as to the health and safety of its students. The university's quick, compassionate and data-centric response to suicide threats connected local police with six students who had threatened self-harm — potentially saving those students' lives.

> "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

Solutions

IT

Security

The University of Illinois

Advances Student Success Through a Data-First Approach

Key Challenges

Before Splunk, data was siloed and inaccessible to most staff, which hindered efforts to improve the student experience. When COVID-19 hit, the university faced new challenges: to quickly transition to online learning then navigate how to safely bring students back to campus.

Key Results

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 to resume in-person learning while protecting the campus community.

At University of Illinois Urbana Champaign (Illinois), data is an integral part of every decision. The Student Success Initiative, for example, helps improve student success by using insights from the Splunk platform to provide academic care to at-risk students. When the pandemic hit, this data-centric approach helped Illinois increase resilience and act fast. With the help of the Splunk platform, the university smoothly shifted to remote learning — and by fall of 2020, was ready to transition back to in-person learning.

Using data to curb the spread of COVID-19, Illinois relied on the Splunk platform to keep its campus community informed with automatic alerts about who tested positive. Real-time data equated to speed, allowing the housing department to quickly move residents with the virus into isolation. By scaling proactive testing, the university significantly reduced COVID-19 cases to less than 1% — even in times when cases were spiking across the state.

> “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

Conducted **over 1.5 million tests** across campus for a safe transition to in-person learning

Slashed COVID-19 cases to less than 1%, even during a state-wide surge in cases

Optimized athletes’ health and performance by using fatigue levels during practice to inform training plans

Raising More Voices

Hear from more leaders across the public sector — including the Department of Defense and other federal agencies, state and local governments, and educational institutions — as they share why they choose Splunk to advance their missions.

"Splunk has enabled us to combat threats with actionable intelligence and advanced analytics that scale with our needs."

— Chief Security Officer, Medium Enterprise Aerospace & Defense Company

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 delivers visibility into what is happening across complex agency operating environments.”

— IT Systems Analyst, State & Local Government

Splunk is fantastic and makes threat hunting much easier than some of the other options available.”

— Security Officer, Federal Government

We save time triaging our most repetitive, basic security tasks by using automated security workflows; and, we have reduced our mean time to respond to security incidents.”

— Engineer, Federal Government

Splunk enables us to automate our process and significantly reduce the time required for compliance-related activities.”

— IT Specialist, Federal Government

Source: TechValidate

Discover how Splunk drives resilience for organizations across the public sector.

Learn More

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.

23-26110-Splunk-Profiles-in-Resilience-EB-105

splunk>