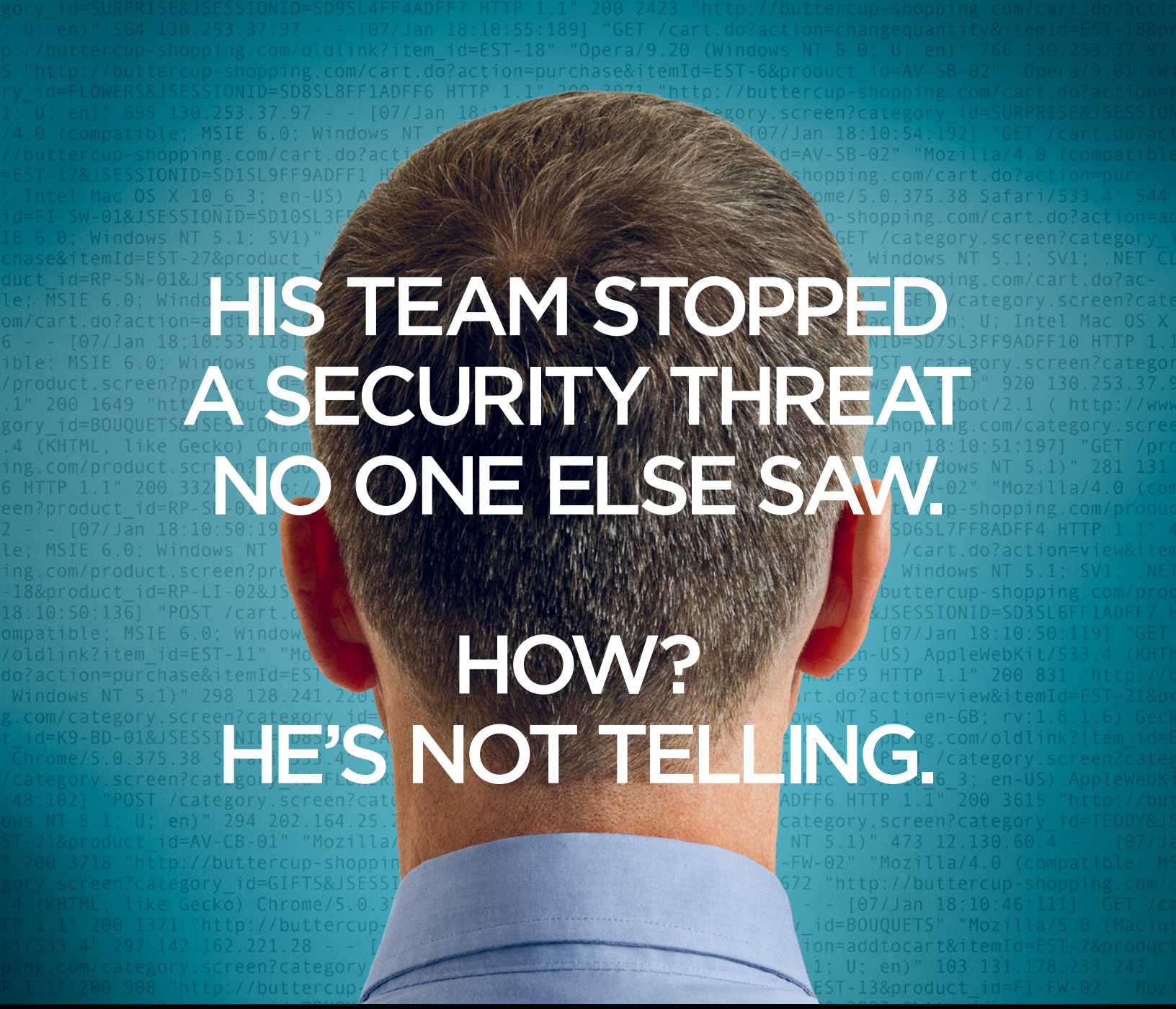
# ALL DATA, ALL USES:

## HOW DATA & OPERATIONAL INTELLIGENCE DRIVE PUBLIC SECTOR MISSION SUCCESS

splunk>




**Splunk® solutions give security teams visibility across the infrastructure so they can quickly detect and contain malicious activity before it becomes a breach. Government security experts use Splunk software and cloud services to protect their organizations, but only a few of them will talk about it.**

just ask | **What can you do with Splunk? Find out at splunk.com/justask-government**

splunk> listen to your data®

# FOREWORD

*By Kevin Davis*
*Vice President, Splunk*

Data is all around us, from our cell phones to the trains we ride on. Listening to our data can reveal valuable insights and a real-time understanding of what's happening across an IT system and infrastructure. But making use of all that data can be challenging.

Machine data – one of the most valuable aspects of big data – is generated by disparate sources in unstructured formats, making it difficult to fit into pre-defined schemas. The issue is more complicated for government agencies who are expected to deal with the same technological challenges as large-scale enterprise organizations, while operating with shrinking resources and budgets. They lack the necessary visibility across infrastructures, cloud components and connected devices. They're also tasked with providing better services to citizens, while protecting each citizen's data.

Public sector agencies can leverage the Splunk platform to protect, serve and grow an organization and its services, while maintaining the accountability, transparency and compliance requirements demanded of their organizations. The Splunk platform unlocks the value of machine data to provide Operational Intelligence—a new understanding of data that can help the agency drive fast, confident decisions through powerful, real-time insights.

The Splunk platform, a proven, extensible, and massively scalable data analytics platform helps government agencies achieve mission success by delivering Operational Intelligence with three key pillars:

→ **Protect** – Reduce the attack vectors and impact of cyberthreats

→ **Serve** – Improve citizen experience through operational excellence

→ **Grow** – Ensure agility and scale for consistent, satisfying service delivery

This GovLoop guide, in collaboration with Splunk, will explore the challenges facing the public sector and how big data can help solve some of these problems. It will also explain how Splunk can support all public sector agency missions from cybersecurity to compliance and more by leveraging machine data.

---

**CONTENTS**

# EXECUTIVE SUMMARY

Operational Intelligence means turning massive amounts of machine data into valuable insights — no matter what type of data you're collecting. Operational Intelligence can give you real-time understanding of what's happening across your IT systems and technology infrastructure so you can make informed decisions.

On August 31, 1854, a cholera outbreak struck London's Soho district. By September 10, the neighborhood had reported more than 500 deaths. Curious about how the outbreak was spreading so quickly, John Snow, often credited as one of the founders of epidemiology, began what would now be considered rudimentary data collection methods.

Snow gathered information on fatalities and sick residents and then mapped the location of the data. Through his analysis, he deduced that the source of the outbreak was a contaminated water pump, and he convinced officials to replace it. Soon after, the outbreak stopped and life returned to normal for London citizens. By clustering the data, Snow was able to visualize the outbreak and help officials make an informed decision, saving lives.

Today, we have surpassed Snow's basic — yet at the time, effective — data analysis techniques, and our society now creates more data than Snow could have ever imagined. As an example, an IDC research report highlights the growth in data:

- From 2005 to 2020, the digital universe will grow from 130 exabytes to 40,000 exabytes, or 40 trillion gigabytes.
- From now until 2020, the digital universe will double every two years.
- The investment in spending on IT hardware, software, services, telecommunications and staff to work with this data will grow by 40 percent between 2012 and 2020.
- By 2020, as much as 33 percent of the digital universe will contain information that might be valuable if analyzed.

This growth in data represents a remarkable opportunity for government. As public sector professionals, your mission is to learn how to capitalize on your high value and authoritative data. You are responsible for learning what skills, tools and information technology you need to transform your agency.

But realizing the full value of intelligence locked in massive amounts of unstructured data means looking beyond traditional data management and database technologies — and the public sector is not always fully equipped to do that. Government agencies are creating more data than ever before, yet they often fail to capitalize on all of the information they're collecting. A recent Forrester Research study found that organizations are analyzing only 12 percent of their data.

So how can this change? The answer lies in better Operational Intelligence. Operational Intelligence means turning massive amounts of machine data into valuable insights — no matter what type of data you're collecting. Operational Intelligence can give you real-time understanding of what's happening across your IT systems and technology infrastructure so you can make informed decisions. You collect your data once and then put it to work across multiple use cases, reducing redundancies and creating better insight and decision-making.

To further explore this potential, GovLoop and Splunk, which offers the leading platform for Operational Intelligence, have partnered to create this guide. Within, we will provide an overview of how big data is reshaping government, discuss the challenges agencies face in extracting value from this information and offer ways to work around common big data roadblocks. We will also highlight how Splunk is helping government organizations leverage their data in new and innovative ways.

Now is the time for agencies to capitalize on their data. Let's get started.

*From 2005 to 2020, the digital universe will grow from 130 exabytes to 40,000 exabytes, or 40 trillion gigabytes.*

# THE CHALLENGES FACING OPERATIONAL INTELLIGENCE IN THE PUBLIC SECTOR

To fully understand the challenges the public sector faces in using data for Operational Intelligence, you must first understand the definitions of two important aspects: **big data and machine data.**

## BIG DATA

Conversationally, big data refers to datasets so large and complex that they become awkward to work with using on-hand database management tools. Public sector officials are well aware of the value of these massive datasets. In a recent survey, 83 percent of federal IT officials said big data could save 10 percent ($380 billion) or more from the federal budget, or about $1,200 per American, and 75 percent believed that real-time big data is helping government improve the quality of citizens' lives.

## MACHINE DATA

Machine data is any data created by machines as an artifact of running systems or applications, leading to a type of big data domain that contains a definitive record of all the activity and behaviors of customers, users, transactions, applications, servers, networks and mobile devices. And it's more than just logs. It includes configurations, data from application programming interfaces, message queues, change events, the output of diagnostic commands, call detail records and sensor data from industrial systems and more.

This machine generated data holds critical information on user behavior, security risks, capacity consumption, service levels, fraudulent activity, customer experience and much more. That's why it's the fastest growing and most complex and valuable segment of big data.

Machine data comes in an array of unpredictable formats, and traditional monitoring and analysis tools were not designed for the variety, velocity, volume or variability of this data. A new approach is needed to quickly diagnose service problems, detect sophisticated security threats, understand the health and performance of remote equipment, and demonstrate compliance through this class of data.

## Government Roadblocks to Using Operational Intelligence

As we noted earlier, Operational Intelligence means turning massive amounts of this big data and machine data into valuable insights, in addition to getting a real-time understanding of what's happening across your IT systems and technology infrastructure so you can make informed decisions. An example? Just look at government defense and intelligence agencies, which are tasked with collecting, analyzing and storing massive amounts of data to detect and correlate patterns of activity related to security threats. They also need systems that can handle extremely granular role-based access controls so that only those who "need to know" have access to the right data at the right time.

And it's not surprising to discover that making use of machine data is hard for government agenices. Data is generated by disparate sources in unstructured formats. That makes it difficult to fit into pre-defined schemas. Traditional business intelligence, data warehouse or analytics solutions are simply not engineered for this class of high volume, dynamic and unstructured data.

On top of these preexisting challenges to using machine data, government agencies at every level also confront difficult mandates. Security teams need to safeguard public assets and sensitive information from cyberthreats. IT operations teams need visibility into and insights from their IT infrastructures to deliver services more effectively. Agencies must analyze all of the data these services generate to improve operations, protect sensitive information and ensure public satisfaction. And they must achieve these objectives with shrinking budgets.

Finally, in addition to these stringent requirements, public sector IT teams face many of the same operating challenges as their large scale enterprise counterparts. Each manages highly diverse and distributed technology footprints, uses a combination of custom and packaged applications, moves some workloads into private or public clouds, and looks for ways to gain more insights from the big data generated by these systems and infrastructure, plus other external sources.

But obstacles abound. Their systems are siloed, their internal teams don't naturally interoperate and often their priorities don't align. To make matters more complex, these organizations' chief information officers and chief information security officers are responsible for delivering better service to constituents faster by consolidating resources and tools, exploring cost saving technologies, and adopting strict security guidelines associated with infrastructure and user monitoring, top secret data, personal privacy and critical infrastructure protection.

Delivering successful missions with siloed teams who manage siloed technology stacks is nearly impossible. It becomes even more problematic when you add in trying to innovate with the massive amounts of data that the public sector now creates and collects daily.

So although public sector officials are more aware than ever before, numerous roadblocks prevent them from being able to make the data driven decisions that can improve life for citizens across all areas, from cybersecurity to national defense.

**That's where Splunk comes in.**

## PAIN POINTS TO DERIVING VALUE FROM BIG DATA

**A lack of visibility across infrastructure and/or cloud components**

**Siloed people and tools**

**Disparate products that don't integrate well**

**Lack of skilled resources**

**Big data promise is fleeting due to limited insights from data lakes**

**A lack of visibility across connected devices**

**Rigid and hard-to-use analytics tools**

**Vendor lock-in — forced use of agency approved technologies**

# SPLUNK & THE THREE PILLARS OF THE PUBLIC SECTOR

Legacy monitoring solutions are inflexible, siloed and not designed for the cloud. Traditional data platforms connect to rigid relational database systems, which are unsuited for scale or ad hoc investigations. And big data solutions require extensive programming at a time when data science skills and value are elusive.

Splunk helps you unlock the hidden value from your machine data. And with the ability to bring in insights from your other tools, you get value from the full spectrum of your data, not just a subset. With it, you can collect, index, search, analyze and visualize all your data in one place. Splunk provides a unified way to organize and extract real-time insights from massive amounts of machine data from virtually any source.

For public sector CIOs and CISOs who need complete visibility to ensure mission success, Splunk provides a real-time data platform that enables Operational Intelligence. Unlike legacy data platforms and separated monitoring tools, Splunk provides a single, massively scalable platform that collects data once and delivers the visibility to support multiple, discrete use cases.

The Splunk platform does not rely on a database or schema on the backend — two of the key limiting aspects of monitoring and analytics software. The platform provides data driven intelligence for security, IT operations, analytics and more. It includes a rich ecosystem of apps that allow you to retire multiple legacy tools for greater value, cost savings and simplicity. With the Splunk platform, government agencies can work smarter and faster, and address key security and IT operations needs.

This potential for big data analytics to serve all areas of government becomes clear when you break down how government needs to use Operational Intelligence to support three main public sector mission pillars: protect, serve and grow.

## PROTECT

Government agencies face many challenges, but few have grown more recently, and more quickly, than cybersecurity threats. Our national security and way of life depend on safe, secure and robust cyber defense.

The unfortunate reality is, however, that even with world class technology, eliminating cyberattacks and breaches continues to be an uphill battle.

To increase resiliency against cyber and other threats, government agencies must improve visibility to understand events happening on their networks. Just as businesses review large amounts of customer data to watch for patterns that allow them to better understand customer buying behavior, government IT security professionals need to monitor and analyze relevant data sources to gain new insights that will help them identify and respond to potential threats quickly.

This can be done with Operational Intelligence via Splunk's platform.

The Splunk platform, with security solutions for security information and event management (SIEM) and user behavior analytics, provides advanced offerings for security analytics. Leveraging this scalable platform, Splunk User Behavior Analytics (UBA) applies unsupervised and supervised machine learning to detect anomalies, breaches and identify advanced attacks (attacks without signatures). Integrated with UBA, the Splunk Enterprise Security solution provides the real-time monitoring of known threats and incident response capabilities to confirm, pinpoint and take action on threats. From national security to homeland security to local law enforcement and public safety, the Splunk Platform offers agencies the operational insight into cybersecurity threats that they need.

## SERVE

Delivering better service to citizens and government employees is critical to every mission and program. These are relatively basic things that citizens have come to expect from government: roads, bridges, air traffic control, automobile registration, education, food regulation and research, and much more. In fact, the public sector's success depends on its ability to provide the populace with easy access to resources and services, and it's built complex infrastructures around them and the public's ability to retrieve them. It is imperative that all levels of government be able to quickly, effectively and efficiently deliver these services to their citizens to fulfill their serve mission pillar.

Operational Intelligence and data play a part in the delivery of these services. The Splunk platform can be positioned as the monitoring and analytics foundation that supports the key tenets of each of these most basic but necessary services: optimizing resource use, consolidating infrastructure, sharing IT resources and providing communications frameworks associated with each mission. A key to mission success is data centric monitoring and analytics. The Splunk platform, with the IT Service Intelligence (ITSI) solution, provides breakthrough visibility into the health and key performance indicators of IT services. This solution helps overcome and potentially replace traditional IT silos and delivers a central, unified view of critical IT services. It uses advanced analytics driven by machine learning to highlight anomalies, detect root cause and pinpoint areas of impact.

## GROW

A broad range of programs is in place that help the government evolve and grow — indeed, growth is a part of the government's mission. But this doesn't necessarily mean creating "big government." Rather, it means creating a more scalable and agile government.

Some programs help the government grow by subtraction. Programs that mandate government transparency, efficiency, accountability and public and private sector innovation help the government grow in new and better ways. Some of the supporting initiatives include open data, the National Spatial Data Infrastructure, data center consolidation and green energy. Each supports delivering a better — not necessarily bigger — government.

The Splunk platform includes a large suite of mathematical, statistical and visualization capabilities to evaluate and model the machine data streaming through the platform. As agencies consider opportunities to find efficiencies and provide better service, the ability to apply these advances analytics against time-series data could mean the difference between understanding and defining a response and not even realizing there was an opportunity to innovate and grow.

This capability applies to every use case we have described, from the emerging DevOps practice to cybersecurity and agile IT operations.

# SPLUNK INDUSTRY SPOTLIGHT: THE ART OF THE POSSIBLE

*An interview with Adilson Jardim, Vice President for Sales Engineering in Splunk's Public Sector division.*

Machine generated data is one of the fastest growing and complex areas of big data. It's also one of the most valuable, containing a definitive record of all user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more.

More than ever before, the public sector faces a vast quantity of machine generated data. But until now, agencies weren't able to extract value and meaning from that data. It sat untapped, unrealized and unhelpful to agencies and the citizens they serve.

Enter Splunk. Splunk is the engine for machine generated data, making data easy to collect, store, search and report on. All kinds of data, once too diverse or expensive to gather, is now actionable.

To learn more about the capabilities possible with Splunk's solutions, GovLoop sat down with Adilson Jardim, area vice president for sales engineering in Splunk's Public Sector division. Jardim discussed the concepts of collecting data once and using it multiple times, and envisioning a world where Operational Intelligence enables agency officials to dream big and do more.

"First and foremost, how we help the public sector is understanding that there is a vast majority of machine generated data, that agencies struggled to extract value and meaning from," Jardim said. "With our technology, agencies are able to evaluate within the context of their operational environments, within the context of their business and mission, what this mission data means, and what value it holds."

For example, when unauthorized access happens inside an agency or somebody touches a network, most of that information is held in data that's generated in system or network logs. Splunk can capture and index that information and present it back to their users in a temporal view. This enables them to understand their environment outside the packaged applications and custom applications that they've written to run their mission.

"Holistically, what we're doing is adding a new lens to the operational environments of our customers and helping them solve problems or understand the environments that they're operating," Jardim said. "We can give visibility into that data, and we're able to add and enrich the data to provide analytics and visibility into business processes that was missing."

As Jardim pointed out, that has been a perpetual problem for public sector customers who have needed to adopt many technologies to keep pace with technological development and emerging agency needs.

"At this point, you may not be entirely sure what's in your environment," he said. "There's so much to keep up with. Splunk helps by providing visibility to all of the information generate by the systems and applications allowing customers to assess operating rhythms, security threats and even user patterns. Things like data center consolidation or optimization efficiencies are very hard to achieve when you're struggling to enumerate the problem to begin with. Federal initiatives like CDM are fashioned around this exact need to enumerate and secure the IT infrastructure in as reliable a way as possible. Splunk helps you to do that."

*This sort of visibility, insight, & information leads into what Splunk refers to as the* ***art of the possible*** *—*

*the capabilities to turn pure, huge amounts of data into real-life visualizations & impact.*

"When you think of machine data, you probably have this image of lots of bytes and streaming data, a lot of text," Jardim said. "When we talk about this, we're talking about textual data." But Jardim suggested you put abstract data in a real-life instance – for example, the machine data that is generated during the act of registering students at a high school or university. With the advent of mobile technologies and IP enabled access, users are able to interact with this registration in a multitude of ways, making it increasingly difficult to understand the user experience during the registration process.

But if you can ultimately aggregate, present and visualize the experience in real time, you can then use predictive abilities on it — meaning you know when you might need to add another server to your process or create efficiencies around registration. This then means that more students can select the classes they want, and complete registration more efficiently.

"That's just one example of where we see when we turn this business problems into solutions with the art of the possible of this data and with this enrichment of operational visibility," Jardim said. This can be applied to any number of scenarios that public sector agencies deal with every day.

"When we start to look at the business process, and not just the operational side, not just system logs and cyber logs, but actually looking at how we enhance and improve a process for these agencies, then we start to see cost savings, we start to see efficiency, and better citizen services," Jardim concluded. "That's really what we define as the art of the possible with what Splunk can do."

# HOW DATA SUPPORTS ALL PUBLIC SECTOR MISSIONS

We hope it's clear to you by now that Operational Intelligence supports public sector missions at all levels and interests. No matter the area or the agency, Operational Intelligence can turn machine data into new insights that can be used to provide better services to citizens while protecting private data.

Additionally, within the public sector mission pillars of grow, serve and protect, there is a unique set of mission areas where Operational Intelligence and data analysis can help. In this section, we'll focus on the following five areas and explain how Operational Intelligence can support each:

- CYBERSECURITY
- DATA CENTER CONSOLIDATION
- GEOSPATIAL DATA ENRICHMENT
- COMPLIANCE
- THE INTERNET OF THINGS

# CYBERSECURITY

## The current situation:

**This mission is identified as one of the most serious economic and national security challenges we face as a nation. Threats come from many adversaries: nation states, criminal enterprise sponsored cybercrime, malicious insiders, hacktivists and hackers. Sixty-one percent of experts in technology and policy predict a major cyberattack causing widespread harm will occur by 2025, according to a Pew Research Center report.**

## How Operational Intelligence helps:

**Splunk's platform collects and visualizes data so you can streamline traditionally resource intensive tasks such as troubleshooting, root cause analysis, compliance and identifying security incidents.**

## Splunk in action:

Splunk helps dozens of agencies combat cyberthreats. Here's how the Nevada Department of Transportation (NDOT) uses it.

Since 1917, NDOT has maintained, planned, constructed and operated the state's highway system. Situated in Carson City, the division employs more than 2,000 professionals and is responsible for more than 5,400 miles of highway and more than 1,000 bridges. Additionally, NDOT administers the state's 511 system, which enables citizens to report and access information on delays, road closures and construction. NDOT also runs a statewide camera system that gives real-time feeds so people can check traffic levels before traveling.

As a result, the department has huge amounts of critical data that it must protect. When an NDOT security official recently became worried that data was not properly protected, the department took preventive steps. First, the division audited its system by attempting to hack into its own data to obtain documents. This allowed officials to assess network vulnerabilities and security gaps. And once they got in, they found that understanding how the attack had occurred was a tedious process. The team had to sift through system logs, relying on a mistake prone manual process. They realized they were losing precious time should a real cyberattack occur and that they needed an automated system to better combat attacks.

NDOT turned to Splunk to aggregate data from disparate sources across the network's infrastructure. The team downloaded Splunk Enterprise for a trial and built two Splunk dashboards to present log data. The first dashboard captures logs from the department's web and file transfer protocol services, tracking cyber incidents. Another dashboard collects data from servers, switches, routers and firewalls throughout a network, informing managers about abnormal events on a network, such as crashes, timeouts and errors. With this new system, NDOT immediately gained visibility into its network. Splunk took away and automated the laborious tasks, saving NDOT time and resources.

# DATA CENTER CONSOLIDATION

### The current situation:

**The current inventory of data center facilities that the federal government manages is untenable. There are too many, they are underused and many are insecure as a result. By shutting down, consolidating and optimizing these data centers, the government expects to save taxpayers billions of dollars and minimize risk exposure.**

### How Operational Intelligence helps:

**Splunk helps agencies identify the machine data of their existing systems, letting them see how often those systems are used and if they should be consolidated going forward.**

# GEOSPATIAL DATA ENRICHMENT

### The current situation:

**Government, industry and individual citizens rely on information linked to location for planning, investment and management activities. But because geospatial information involves a significant investment of resources, many government agencies need to coordinate their efforts to reduce costs, improve the quality of services and increase efficiency.**

### How Operational Intelligence helps:

**Splunk's Geospatial Platform focuses on web applications that facilitate participatory information sharing, interoperability, user centered design and collaboration on the Internet. It also promotes improved coordination and more effective use of geospatial information.**

### Splunk in action:

United States Postal Service Click n Ship – Fraud – Splunk provides geospatial tracking of incoming IP addresses allowing quicker resolution to international fraudulent shipping, by mapping out place of order origination and associated IP addresses. This has helped to deter fraudulent activity and avoid cost.

# COMPLIANCE

## The current situation:

**Reporting on security and privacy controls that span a wide variety of technologies – boundary protection, access controls, configuration and vulnerability scanning tools, application logs and machine data – to measure and demonstrate control compliance is difficult and costly. Each technology generates data in different formats and locations and each auditor request involves a different manual procedure to gather evidence.**

## How Operational Intelligence helps:

**With Splunk's Operational Intelligence, you can search, alert and report on machine data from virtually any source and meet compliance requirements such as audit trail collection, reporting and file integrity monitoring with a single solution.**

## Splunk in action:

The U.S. government is seeing a rise in cyberattacks. One path toward better government cybersecurity? Continuous monitoring of your controls — a way to automate the assessment of your security posture, provide a roadmap for your organization to comply with cybersecurity standards and enable you to pass even the most rigorous audits with greatly reduced effort on aggregating, mapping and prioritizing critical security data required for audit and compliance support.

Meeting and demonstrating compliance is the start to a more secure agency. Theft or loss of confidential information has sparked numerous legislative requirements and standards-based protocols from the National Institute of Standards and Technology. These security controls and data protection requirements impact agencies at the national, state and local levels and all departments concerned with national security.

Splunk, working with the cybersecurity software firm Qmulos, provides cybersecurity and compliance solutions and services for several federal agencies. Their platforms work together to use audit logs and configurations from operating systems, host based agents, applications and network appliances to demonstrate compliance with common frameworks such as the NIST Risk Management Framework (RMF) and the related security and privacy controls detailed in NIST Special Publication 800-53 revision 4 and the Intelligence Community Standard for Enterprise Audit, ICS 500-27.

"Splunk is critical to security and compliance for the federal sector and really all sectors said Matt Coose, Chief Executive Officer of Qmulos. "When we look to solve compliance for federal agencies or the intelligence sector, the problem is basically trying to figure out how to bring data sources of nearly infinite variety together and coalescing that in near-real time to figure out how well you're implementing required controls and ultimately defending your networks."

Splunk and Qmulos do this by combining near real-time monitoring of agencies' systems' machine data with the context and workflows of an IT Governance, Risk and Compliance (IT GRC) tool, making it a complete compliance monitoring and reporting solution based on the NIST Risk Management Framework. Unlike other IT GRC tools, which are just databases that help organize policies, paperwork and status notes, Qmulos Enterprise Compliance adds near real-time measurement of your systems' actual compliance state.

"Splunk's platform is great at ingesting machine data from a variety of sources and different formats," Coose said. "So as a platform, we feel like their Operational Intelligence combined with our domain expertise is absolutely the right answer to solve cyber compliance issues."

# THE INTERNET OF THINGS

## The current situation:

**Every public sector agency and organization has an array of devices, appliances, vehicles, wearable material and sensor-laden components in their environments that connect to the internet and/or one another. But the signals these devices generate are not being used to their full potential. This is primarily because of the cost and complexity of collecting, storing and analyzing these types of data.**

## How Operational Intelligence helps:

**You'll be able to capture and index disparate data from IoT sources and visually display the information in configurable dashboards, in addition to detect patterns and trends by viewing IoT data in real time, over specified time periods or overlaid on maps.**

## Splunk in action:

When you think of the U.S. Air Force, you might think about fighter jets, airstrips, missile sites or military satellites. But what you might not know is the Air Force is also focused on another area: reducing energy costs.

At the 724-square-mile Eglin Air Force Base in Florida, managers turned to an IoT strategy to meet several legislative mandates to reduce energy consumption. They launched a strategic energy master plan to identify cost cutting opportunities, using Splunk as their platform to gather machine data from more than 20,000 sensors deployed in more than 100 buildings to analyze energy usage and costs.

The Eglin Energy Management System uses Splunk-enhanced solutions to provide dashboards that will help base maintenance staff assess building performance and energy efficiency, generate automated energy usage reports, compare current energy usage with historical data, and enable the deployment of load shedding and load shifting to take advantage of favorable electric rates.

For example, by correlating both historical and real-time energy use and pricing data with occupancy and environmental data from heating, ventilation and air conditioning (HVAC) systems, Eglin might find significant opportunities for load shedding, identifying times it can shut off select HVAC systems during high energy cost periods.

When awarded in 2013, the project was expected to save about $2.5 million annually, with a payback period of less than three years.

"We've always allowed customers to see what was happening in the three-dimensional space that their facilities occupy," said a program manager of the strategic plan. "But it was just a real-time view and lacked historical perspective. By using Splunk software to capture and index data, we now enable customers to compare averages and see trends in usage."

# CONCLUSION

At its core, the government's ability to harness data's value is, for the most part, not actually an information or a technology issue. Agencies have access to massive amounts of data. The critical success factor is getting agency leaders to increase their investment in analytics. A comprehensive analytics solution is the only way agencies can transform data into actionable intelligence.

This requires a bit of imagination. You could refer to it, as we have in this guide, as the "art of the possible." By now, you know all of the possibilities that proper data analysis and Operational Intelligence can bring your agency. But can you think even bigger? Can you think beyond what currently is to what might be?

Take a step back and envision a world where you could:

- → **Apply** statistical models and pattern analysis to unstructured data to understand patterns of activity.
- → **Ask** new questions of your unstructured data to gain new insights and efficiencies.
- → **Help** reduce the crime rate in specific locations through hotspot maps.
- → **Detect** patterns and anomalies across terabytes of raw data in real time without specialized skills, up front data normalizations or fixed schemas.
- → **Monitor** and detect outbreaks of diseases such as the West Nile Virus.
- → **Reveal** the impact and sources of ozone in a city.
- → **Collect,** analyze and store data to discover threats that could compromise our national security.
- → **Turn** petabytes of machine generated data into new insights that can be used to provide services to citizens.

All this and more can become a reality when you deploy the right data analytics solution. Realizing the full value of intelligence locked in massive amounts of unstructured data means looking beyond traditional data management and database technologies. It means being able to collect massive amounts of data once and use it many times in many use cases.

Only Splunk provides a proven, integrated and massively scalable data platform providing public sector organizations the Operational Intelligence they need. With Splunk, these organizations can collect data once and use it often to power multiple use cases that support strategic public sector missions: cybersecurity, data center operations and consolidation, compliance, geospatial intelligence, and connected devices.

By using Splunk's solutions for better Operational Intelligence, you will enable yourself and your agency to see the forest and the trees. The big, the small, the patterns, the specific incidents can all be revealed in queries and visualizations that apply the proper context.

Ultimately, what differentiates Splunk is that, at its core, the company wants to power public sector agencies and officials to make data driven decisions, improve day-to-day operations, and deliver on their goals, missions and objectives. Splunk works with you to get a strategy in place, craft the right reporting and drive successful outcomes that ultimately enable you to live in a world where the art of the possible is simply a reality.

# ABOUT & ACKNOWLEDGMENTS

Thanks to Splunk for their support of this valuable resource for public-sector professionals.

## About Splunk

Splunk Inc. provides the leading platform for Operational Intelligence. Splunk® software searches, monitors, analyzes and visualizes machine-generated big data from websites, applications, servers, networks, sensors and mobile devices. More than 8,400 organizations use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, improve service performance and reduce costs.

## Author

Catherine Andrews, Director of Content

## Designer

Kaitlyn Baker, Graphic Designer

## Photo Credit

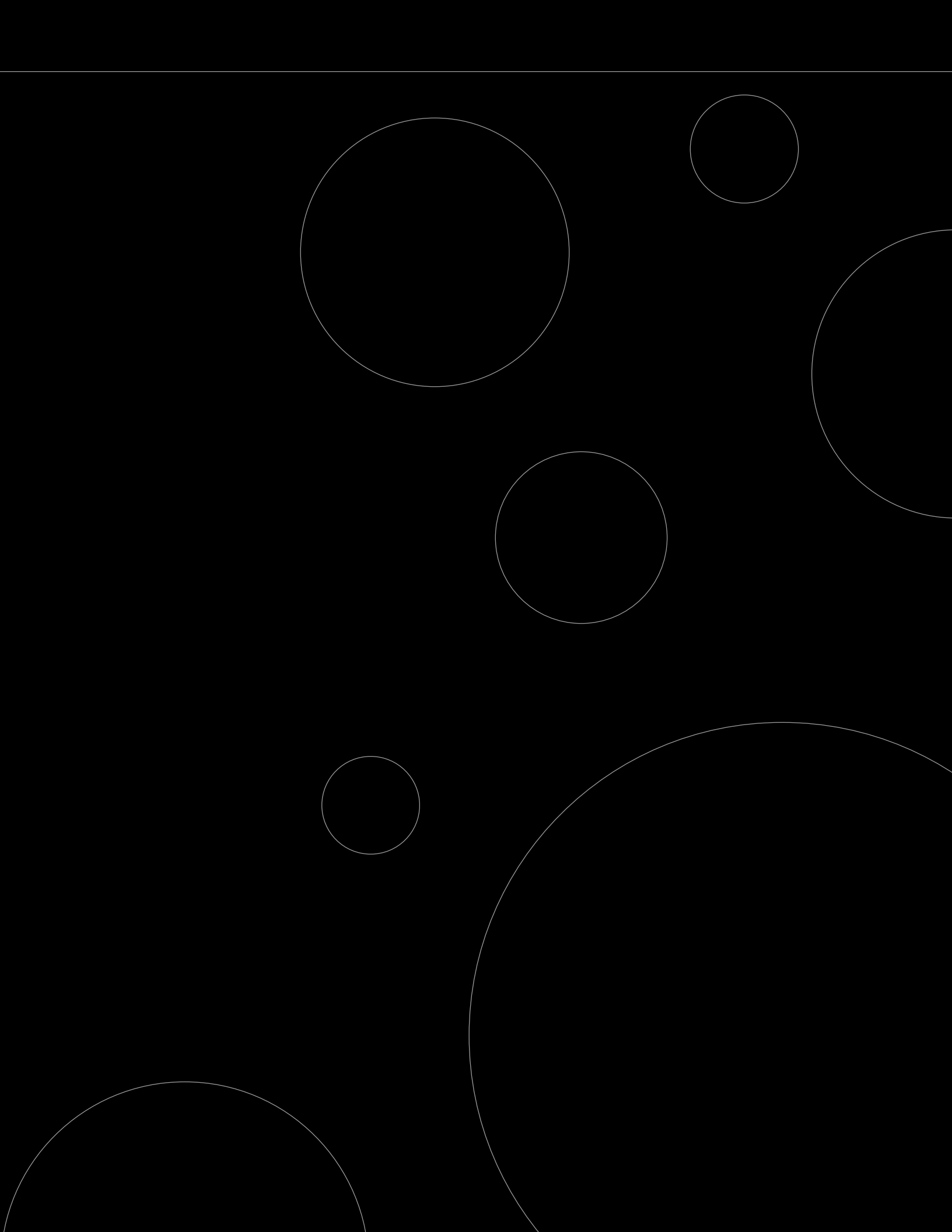
*All photos licensed for use under Creative Commons 2.0 (CC-BY-2.0)* : Alan Stark, Angela N., U.S. Air Force, Zach Welty

## About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop



1152 15th St. NW, Suite 800
Washington, DC 20005

(202) 407-7421
F: (202) 407-7501

www.govloop.com
@govloop