

splunk>

# INNOVATORS IN ACTION

A Collection of Inspiring Customer Stories



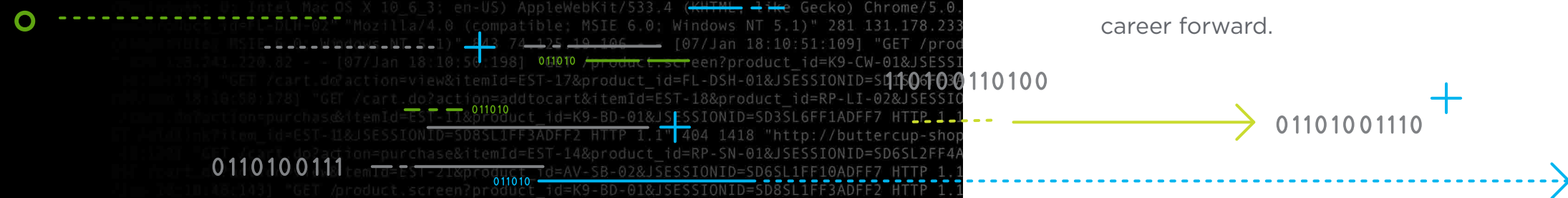
Forward-leaning organizations around the globe and across industries — from financial services to manufacturing to healthcare, the public sector and beyond — are turning mountains of machine data into answers.

**They're achieving their goals with individual ingenuity and by harnessing the power of their**

**machine data, in the cloud, on-premises and in hybrid environments.** And they're gaining valuable insights across multiple use cases, including IT, security, IoT and business analytics. These organizations are driving business transformation to deliver better customer experiences, reduce downtime, increase profitability and improve security.

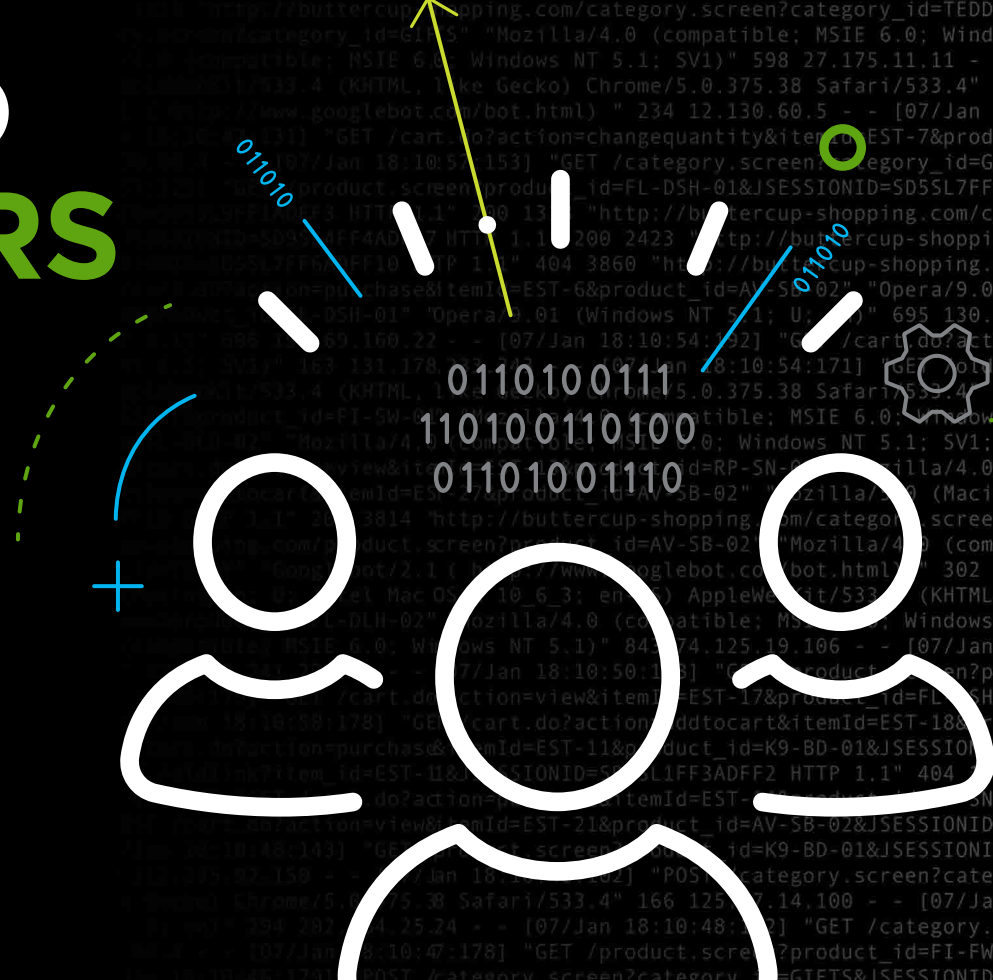
**Splunk customers are doing some amazing things.** A global manufacturing company is leveraging real-time factory-floor data to break production records and reduce energy usage. A pharmaceutical company is on track to achieve its goal to discover new treatments for 100 genetic diseases by 2025 using an innovative combination of biology, automation and machine learning. And at the world's busiest airport, 95 percent of passengers are getting through passenger security in five minutes or less, while enjoying fast and secure airport Wi-Fi and benefiting from sparkling-clean washrooms — all powered by machine data monitoring and alerting with Splunk.








**You're an innovator.** Whether your role is in IT, cybersecurity, systems, architecture or business management, in a SOC, NOC, marketing department or the C-suite, Splunk can help you wade through mass quantities of data to improve organizational management and agility and help you move your career forward.









FEATURED CUSTOMERS



	<b>COMMUNICATIONS.....</b>	<b>6</b>
	CenturyLink.....	7
	<b>ENERGY .....</b>	<b>8</b>
	TransAlta .....	9
	<b>MANUFACTURING.....</b>	<b>10</b>
	Shaw Industries Group, Inc.....	11
	<b>RETAIL.....</b>	<b>12</b>
	Ferguson.....	13
	Travis Perkins PLC.....	14
	Global Fashion Accessories Retailer.....	16
	OTTO.....	17
	Heartland Automotive Services, Inc. ....	18
	<b>EDUCATION.....</b>	<b>20</b>
	New York Regional Education Agencies.....	21
	University of San Francisco.....	22
	University of Nevada, Las Vegas.....	24
	<b>HEALTHCARE.....</b>	<b>26</b>
	NRC Health.....	27
	Recursion Pharmaceuticals.....	28
	Global Biopharmaceutical Company.....	30
	<b>TRAVEL AND TRANSPORTATION.....</b>	<b>32</b>
	DB Cargo.....	33
	Dubai Airports.....	34
	Hyatt Hotels Corporation.....	35
	MTR Corporation Ltd.....	36

	<b>ONLINE SERVICES .....</b>	<b>38</b>
	SMSGlobal.....	39
	TrueCar.....	40
	BrightEdge .....	41
	Rokt.....	42
	PEXA (Property Exchange Australia) .....	44
	Networld Technology Ltd. ....	45
	SONIFI Solutions, Inc.....	46
	<b>FINANCIAL SERVICES .....</b>	<b>48</b>
	ENGIE Global Markets.....	49
	NAPAS.....	50
	The Japan Net Bank, Ltd.....	51
	TransUnion.....	52
	<b>PUBLIC SECTOR .....</b>	<b>54</b>
	InfoTeK.....	55
	City and County of San Francisco.....	56
	Maryland’s Prince George’s County .....	57
	Fairfax County, Virginia.....	58
	State of Louisiana .....	60
	Sandia National Laboratories .....	61
	Maryland Lottery and Gaming Control Agency .....	62
	<b>TECHNOLOGY .....</b>	<b>64</b>
	PagerDuty .....	65
	Econocom.....	66
	Digital Services Provider.....	67
	Leidos .....	68
	iZettle.....	70
	Intelliflo .....	71
	Micron Technology .....	72

INDUSTRY  
COMMUNICATIONS

- INDUSTRY
  - Communications
- SPLUNK USE CASES
  - IT Operations
  - Business Analytics

Second largest U.S. communications provider to global enterprise customers

CENTURYLINK. FROM SWITCHBOARDS TO DASHBOARDS: COMMUNICATIONS LEADER FINDS NEW SOLUTIONS

CenturyLink has grown from a rural telephone carrier to a consumer, business and enterprise broadband, security, IT services and cloud provider across the U.S. and around the world. Along the way, it has faced challenges. With Splunk Enterprise and Splunk IT Service Intelligence, CenturyLink has achieved fast time to value and return on investment, and experienced steep decreases in mean-time-to-identify and mean-time-to-resolution.

CenturyLink puts a heavy focus on customer experience, and Splunk helps ensure our end users are always satisfied with their service team interactions. Splunk Enterprise and Splunk IT Service Intelligence give us real-time, executive-level visibility into the health of our IT applications. This ensures that our representatives can get the information that matters most to each customer at all times. Splunk has helped us raise the bar in customer service by improving time to resolution, resource optimization and executive-level communication.”

Manager, Systems Engineering Group, CenturyLink



INDUSTRY

ENERGY

INDUSTRY

Energy

SPLUNK USE CASES

Security

IT Operations

DevOps

Power generation and wholesale marketing company operating in Canada, the U.S. and Australia

TRANSALTA TEAMS WITH SPLUNK FOR SECURITY AND OPERATIONAL INTELLIGENCE

TransAlta had been using a competing integrated security information and event management (SIEM) tool, but the company's talented team of certified SIEM professionals struggled to build actionable dashboards, reports and alerts, perform advanced correlations and complete security investigations fast enough. TransAlta deployed Splunk Enterprise and Splunk Enterprise Security (ES) as its SIEM platform.

BUSINESS IMPACT

- ➔ User investigation time reduced from days to minutes
- ➔ On-time delivery of new energy trading platform
- ➔ Cost savings of up to \$1 million
- ➔ Fast time to value with no training required

After implementing the Splunk platform, TransAlta gained immediate value for IT security, IT operations and DevOps — all without any training. The company was productive with advanced security use cases such as event correlation across multiple sources with data enrichment in three to four months, something it was never able to accomplish with its legacy SIEM. According to TransAlta's senior IT security specialist, "Previously, confidential user investigation took us days or longer, and now it takes us minutes." And the company has saved up to \$1 million by bringing storage logs into Splunk Enterprise and using prediction algorithms to forecast storage growth across all data domains.

"With Splunk ES, we experienced quick time to value. It was very easy to get up to speed on it. What I dreamed of in the past that was never possible, Splunk makes possible. Now, if somebody has a question, I say, 'just give me a minute.'"

Senior IT Security Specialist, TransAlta



INDUSTRY  
MANUFACTURING



INDUSTRY

Manufacturing

SPLUNK USE CASES

Industrial Data and IoT

Leading flooring solutions provider

SHAW INDUSTRIES BREAKS  
PRODUCTION RECORDS  
WITH SPLUNK IOT

With annual sales nearing \$6 billion, Shaw Industries Group, Inc. supplies carpet, hardwood, tile and stone, and laminate flooring products and synthetic turf to residential and commercial markets around the world. To retain its competitive position, Shaw Industries implemented Splunk Enterprise for industrial internet of things-based, real-time factory floor analytics. Data from systems and industrial sensors provides new business insights, improving production performance and spurring friendly competition among plant workers.

BUSINESS IMPACT

- Improved work order lead times
- Increased sample panel production output significantly
- Reduced energy usage at one facility, resulting in significant cost savings

Initially, Shaw Industries adopted the Splunk platform to provide visibility into a new post-consumer recycling facility. Given the ease of ingesting plant data and correlating disparate industrial data streams, additional Shaw manufacturing plants began implementing their own Splunk instances, resulting in a corporate initiative spanning 37 manufacturing facilities. Today, approximately 300 managers and engineers are trained to write Splunk searches

for their machine and enterprise data. Plant managers and production managers consume Splunk dashboards for key business insights.

This past week, we broke the record for the panels produced, so Splunk is helping to change the way we do business.”

Department Manager, Samples Division,  
Shaw Industries Group, Inc.



## INDUSTRY RETAIL

INDUSTRY  
Retail/Wholesale  
and Distribution

SPLUNK USE CASES  
Business Analytics  
Security

\$13.8 billion in revenue and the largest U.S.  
distributor of plumbing supplies

## FERGUSON ENHANCES CUSTOMER SERVICE, PROFITS WITH SPLUNK CLOUD

Ferguson operates in a dynamic marketplace where buyers range from small plumbers to billion-dollar refineries, and new housing trends affect product demand. In this climate, sales teams must anticipate customer needs and react quickly to changes in behavior. Predictive analytics initiatives recently uncovered large amounts of valuable sales data, but the customer experience team struggled to get actionable information to regional teams, so it deployed Splunk Cloud.

### BUSINESS IMPACT

- Better alignment of organizational resources with customer needs
- Increased sales efficiency through quick adoption and ease of use
- Reduced reporting from one month to real time

Once the company moved forward with Splunk Cloud, it discovered a broad scope of consolidated customer data, segmented into categories based on need. Before adopting the Splunk platform, data was laboriously parsed and sent to regional teams, and there was a risk of sensitive material falling into the wrong hands. Reports with exhaustive numbers have now been replaced with dashboards that associates find more actionable. With less security risk and easier access to data, Ferguson is gaining a better understanding of the variables that drive customer success and business results.

“

I was blown away with the instant access to intelligent visual reports, the broad scope of use cases, and the embedded security in Splunk Cloud...

We've been able to astonish everyone, and they're saying the same thing. 'When can I bring my data into Splunk?'"

Customer Experience and Marketing Analyst, Ferguson



WATCH THE VIDEO:  
[splunk.com/ferguson](https://splunk.com/ferguson)



British builders' merchant and home improvement retailer with 2,000 outlets and 28,000 employees



## TRAVIS PERKINS PLC ADOPTS ANALYTICS-DRIVEN SIEM TO ENABLE HYBRID CLOUD TRANSITION

When Travis Perkins PLC's existing security information and event management (SIEM) solution couldn't provide the necessary security insights across a hybrid environment, it selected Splunk Cloud, Splunk Enterprise and Splunk Enterprise Security (ES) as its SIEM. With Splunk ES, Travis Perkins PLC now calculates risk scores on different threat activities based on previously correlated data or alerts from the company's existing security solutions.

“

Replacing our previous SIEM with Splunk Enterprise Security has dramatically improved our ability to effectively monitor and secure our complex hybrid environment. At the same time, using Splunk Cloud has helped ensure we have the flexibility we need to respond to the evolving threat landscape.”

Head of Information Security, Travis Perkins PLC



WATCH THE VIDEO:

[splunk.com/travis-perkins](https://splunk.com/travis-perkins)

### BUSINESS IMPACT

- Enabled a lean SOC, with all IT operations staff empowered as cyberattack “first responders”
- Intrinsic risk score-based correlation has improved the ability to detect and respond to significant threats
- Security incident investigation time reduced from three weeks to three hours

Travis Perkins PLC plans to extend the capabilities of its lean security operations center (SOC) with additional insights driven by the Splunk platform's growing machine learning capabilities. Travis Perkins PLC will look to use machine learning to improve the quality of its existing alerting, reducing the number of false positives. Machine learning capabilities such as pattern recognition and anomaly detection will further enhance the effectiveness of the lean SOC model while providing the highest level of protection across the business.





INDUSTRY  
Retail



Retailer manufactures and sells fashion accessories to consumers and acts as a wholesaler to more than 90 locations worldwide

## GLOBAL FASHION ACCESSORIES RETAILER SPEEDS THREAT IDENTIFICATION, PREVENTS ATTACKS WITH SPLUNK SIEM IN THE CLOUD

A strong security posture for retail companies is more critical than ever, with ransomware, distributed denial-of-service (DDoS) attacks and security breaches affecting major companies — and their customers across the globe — with growing frequency. When one leading global fashion accessories retailer was bogged down with an inefficient alerting system and unable to prevent security incidents proactively, it turned to Splunk Cloud with Splunk Enterprise Security (ES).

### BUSINESS IMPACT

- Drastically reduced security incident investigation times
- Prevented ransomware attacks by identifying threats quickly
- Freed up of analysts' time to proactively prevent issues before they arise

Lacking a security information and event management (SIEM) system, email alerts served as an inefficient system to monitor the company's security posture. Analysts manually investigated every security event, but correlations were not done. This was both a time drain and not scalable as the company grew. To ensure the company was protected, the team needed to equip itself with the right tools.

When the company was deciding on a SIEM, Splunk Cloud with Splunk ES stood out above the competition for its high performance, functionality and value. With Splunk software in place, the company is now able to adequately address growing security concerns, like potential ransomware or DDoS attacks.



With our old system, it could take anywhere from a couple of hours to a couple of days for a typical investigation. Now, with Splunk Cloud, it's only about 20 minutes."

Senior SOC Analyst,  
Global Fashion Accessories Retailer

"The Splunk solution gives us real-time visibility into complex business processes. This allows us to simply and quickly identify, analyze and fix problems such as failures, work processes and delays. Furthermore, Splunk Enterprise helps us with achieving our KPIs through identifying the actual system stability and performance. Splunk is indispensable in our daily work.

Department Manager, Customer Care Center  
Software Development, OTTO IT



INDUSTRY  
Retail



Leading German retail company and one of the biggest web retailers in Europe

## REAL-TIME OPERATIONAL INTELLIGENCE KEEPS OTTO GROUP RUNNING 24/7

OTTO is a member of the Otto Group, a worldwide-operating retail and services group comprised of over 120 companies in more than 20 countries. OTTO needed a real-time monitoring solution that could provide operational and digital intelligence across its complex infrastructure, and it deployed Splunk Enterprise.

### BUSINESS IMPACT

- Enhanced customer experience across multiple channels
- Increased operational efficiency
- Improved speed and quality of new software deployment

OTTO operates a multichannel retail model, giving customers the flexibility to order online, via telephone or catalog in a seamless and frictionless way. Supporting this critical business objective is a complex, multitiered, heterogeneous infrastructure. Some of the most critical systems at OTTO are its customer relationship management (CRM) call center application and the central order processing system.

Group Technology Partner (GTP), the Otto Group's IT service provider, initially deployed Splunk Enterprise to achieve a consolidated monitoring approach and gain insight across its transactional infrastructure. Splunk software was initially used as part of the monitoring system for production use, and it has expanded to the development and quality assurance (QA) testing environments.



Largest U.S. franchisee of quick lube retail service stores



## HEARTLAND AUTOMOTIVE PROTECTS BRAND REPUTATION, SECURES DATA WITH SPLUNK PLATFORM

Known for its signature oil change, Heartland Automotive Services, Inc., dba Jiffy Lube, needed a cybersecurity platform to protect its brand and its most important resource — its data. Heartland Automotive deployed Splunk Enterprise Security (ES) and Splunk User Behavior Analytics (UBA) as its integrated security information and event management (SIEM) platform.



Splunk's licensing was 25 percent less expensive than alternative solutions. The TCO comparison only supported, or further reinforced, our decision to choose Splunk...

Data is our most critical asset, and as a retailer the ability to have a platform to help protect our brand is everything."

Head of IT and Information Security, Heartland Automotive Services

WATCH THE VIDEO:

[splunk.com/heartland-automotive](https://splunk.com/heartland-automotive)

### BUSINESS IMPACT

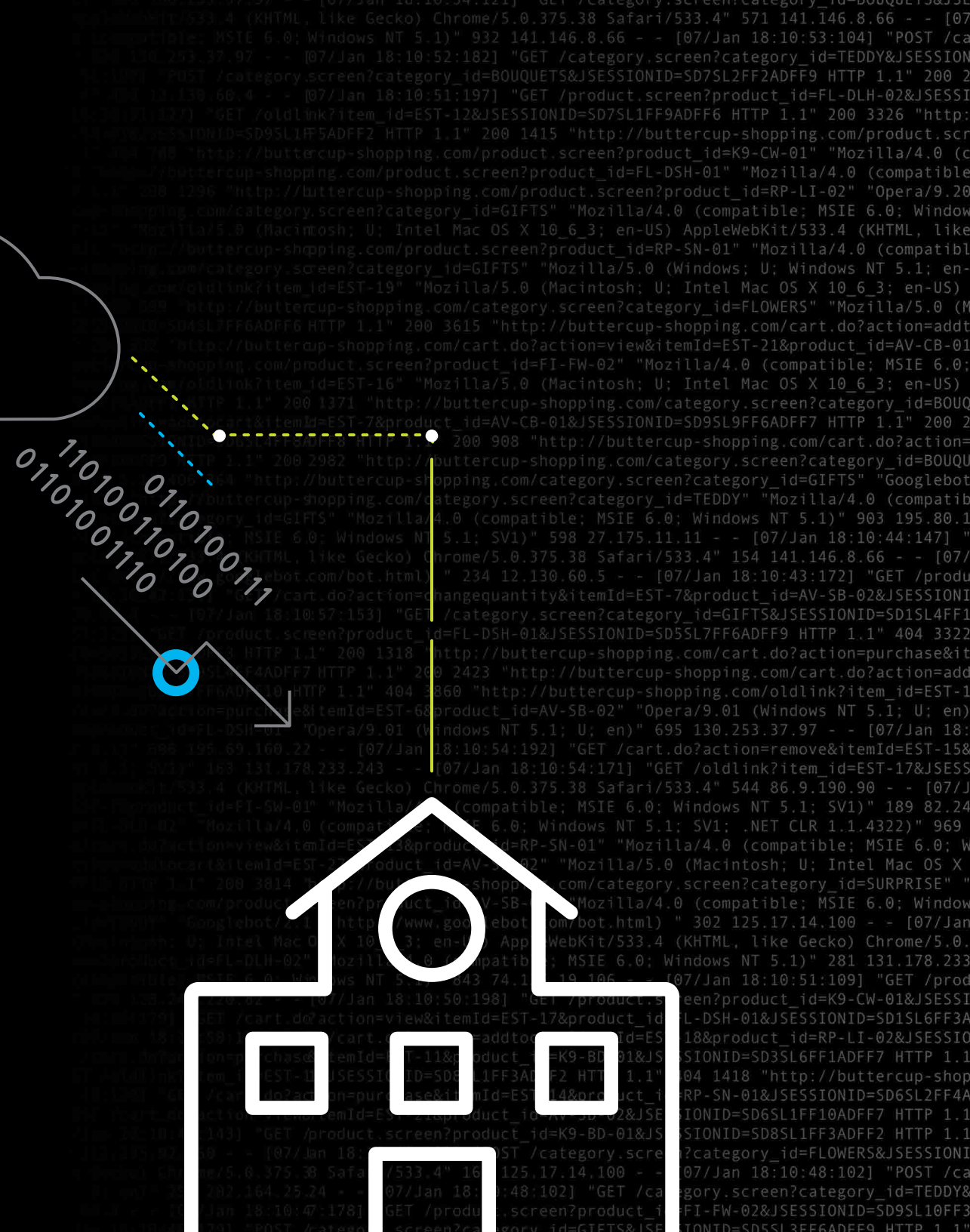
- Realized time to value by implementing a SIEM and insider threat protection solution in only three weeks
- Gained platform to drive innovation with 25 percent less TCO
- Established real-time security investigations and insider threat protection



As organizations face an increasing number of sophisticated zero-day attacks, they need a more dynamic way of identifying issues. Splunk User Behavior Analytics (UBA) brought the power of machine learning into the environment, enabling the team to monitor patterns of behavior built into the solution and respond quickly. With UBA, Heartland Automotive is eliminating blind spots that can be addressed by machine learning.



## INDUSTRY EDUCATION



“

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



INDUSTRY  
Education

SPLUNK USE CASES  
IT Operations

A partnership between the Boards of Cooperative Educational Services with school districts to provide shared educational programs and services

## NEW YORK REGIONAL EDUCATION AGENCIES UNIFY DATA TO IMPROVE OPERATIONS AND ACCELERATE STUDENT LEARNING

With 12 Regional Information Centers (RICs) across New York State collaborating on the RIC One project, the infrastructure and operations team needed to collect log data to monitor the many components that make up the technology stack. The team relies on several open-source tools and chose Splunk Cloud as a central log management solution, since the components of the stack are deployed, in part, to both Amazon Web Services (AWS) and local infrastructures in RICs throughout the state. A key benefit of Splunk Cloud was that it required fewer servers to maintain and administer.

### BUSINESS IMPACT

- Enhances overall educational experience with simplified access to relevant applications at any time
- Easier user and application management reduces IT burden
- Ensures security of student and teacher data across districts

RIC One relies on Splunk Cloud for proactive log monitoring and ensuring that processes are running and succeeding every day. Splunk Cloud alerts the team if one of the processes fails, so they can resolve issues quickly. The team also relies on the Splunk App for AWS for critical insights into its AWS account and Splunk Enterprise to safeguard students' personally identifiable information.

Jesuit university founded in 1855



## UNIVERSITY OF SAN FRANCISCO PROMOTES EFFICIENCY, INCREASES TRANSPARENCY WITH SPLUNK CLOUD SIEM

Like other universities, University of San Francisco (USF) faces many challenges — from making payroll on time to maintaining accreditation and ensuring IT and security systems are in place to educate 10,000 students and support 2,500 faculty and staff. After evaluating several options, USF invested in Splunk Cloud as its new security information and event management (SIEM) solution.

“

We evaluated a handful of SIEM solutions and created a matrix to compare them against one another. There were several similar features and opportunities among them, but there were also big differences. Splunk’s turnkey cloud offering and hybrid option makes it magnitudes better than any of the others.”

ISC Director and Information Security Officer,  
University of San Francisco

### BUSINESS IMPACT

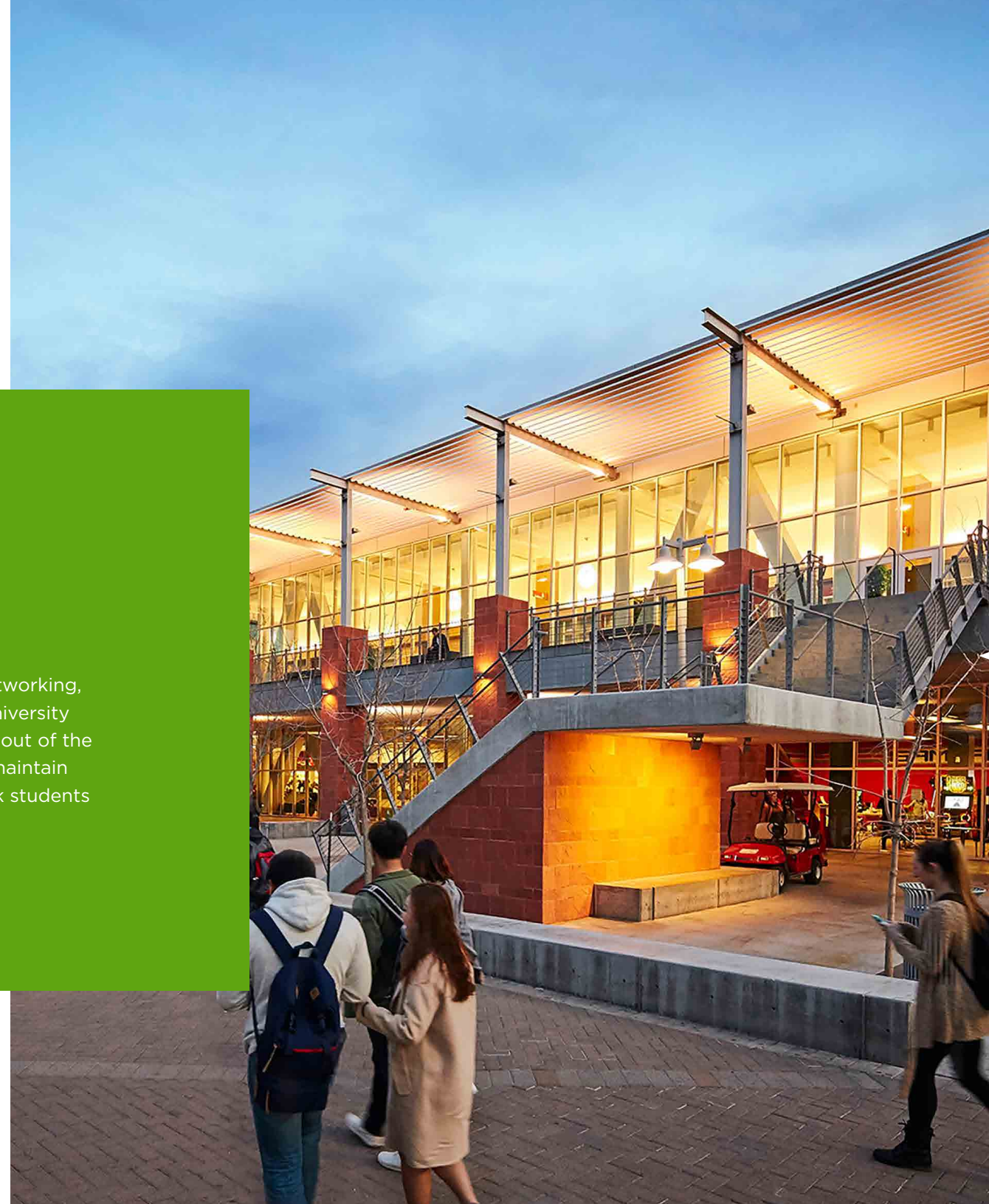
- Improved security posture and ensured payment card industry (PCI) compliance
- Reduced phishing investigations from days to minutes
- Promoted transparency among university executives and staff

Previously, staff were concerned about the university’s security posture and its ability to protect against and prevent phishing attempts and security breaches. Additionally, USF required a solution that could ensure PCI requirements were met, and that would promote security operations transparency among university executives and staff.

Prior to adopting Splunk Cloud, the manual process of investigating a phishing email would span from hours to days. Now, the Splunk platform enables USF to generate a list of all who need to be contacted, enabling investigations to take place within minutes. And, the use of Splunk Cloud to automate processes ensures that USF is PCI compliant.



Premier research university serving  
29,000 students



## UNLV LEARNING ANALYTICS RESEARCH BOOSTS ACHIEVEMENT

At the University of Nevada, Las Vegas (UNLV), the IT department provides networking, datacenter and application support for students, faculty and staff. When the university adopted Splunk Enterprise it was able to solve IT infrastructure problems right out of the box, and it now depends on the solution for fast IT problem resolution and to maintain maximum system uptime. Now, UNLV has repurposed its data to identify at-risk students and improve academic outcomes.

Typically, for a class like Introduction to Anatomy and Physiology, one-half of the students fail to get the grade they need to move on to the next course. By building prediction models into Splunk Enterprise, the university was able to provide proactive feedback to students who had a possibility of getting a C grade or lower in the class. One-third of the students who received feedback within the first four weeks of class ended up earning an A or a B in the class.

Splunk Enterprise also indexes the university's campus alarm system data, enabling folks in the facilities department to understand what is going on in real time when they are testing the system.

WATCH THE VIDEO:  
[splunk.com/UNLV](https://splunk.com/UNLV)

### BUSINESS IMPACT

- Fast IT troubleshooting, reducing resolution times and maximizing system uptime
- Increasing student academic success outcomes by at least one-third
- Ensuring optimal emergency preparedness while increasing campus safety



UNLV uses the Splunk Machine Learning Toolkit to continue to improve our overall approach to predictive research.”

Professor, UNLV



INDUSTRY

HEALTHCARE

INDUSTRY

Healthcare

SPLUNK USE CASES

Security

One of the nation's largest healthcare performance improvement firms, supporting more than 7,200 organizations

NRC HEALTH'S TONY REINKE:  
IT'S MORE THAN JUST PROFESSIONAL

After talking about the challenges he faces as a father of three, SplunkTrust member and security engineer Tony Reinke shares what it's like being the face of Splunk for Nebraska, and how his Splunk user group has evolved into a tight band of supportive, data-loving friends.

WATCH THE VIDEO:  
[splunk.com/nrc-health](https://splunk.com/nrc-health)

Watch the video to learn how SplunkTrust ninja Tony Reinke balances fatherhood and corporate security at NRC Health as part of the SplunkTrust.

SplunkTrust members are dedicated and helpful members of the Splunk community. They assist other members, demonstrate the power of Splunk's products and services, and help identify future product needs.

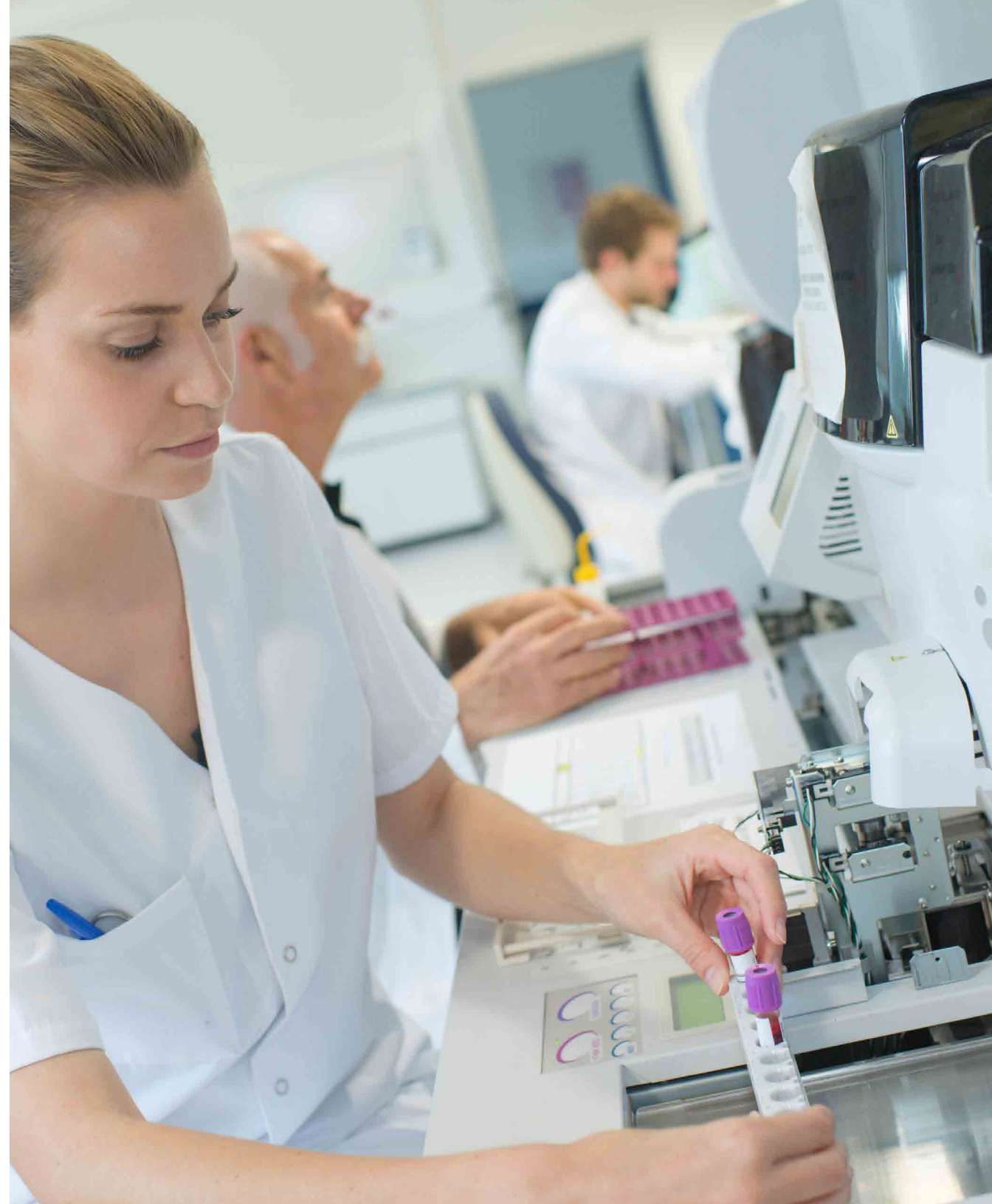




Biotech company that combines artificial intelligence, experimental biology and automation to discover drugs at scale

## RECURSION PHARMA TARGETS 100 GENETIC DISEASES WITH SPLUNK AND MACHINE LEARNING

In the past, Salt Lake City-based Recursion Pharmaceuticals found it difficult to manage large amounts of time-series data collected from computer-controlled instruments and video footage generated from cameras in the laboratory. The initial data management strategy hardly matched the firm's aggressive high-volume ambitions — its laboratory's microscopes currently produce on the order of 700,000 TIFF files each week, representing an 800 percent increase in productivity over 10 months. While the company considered open-source alternatives, the director of high-throughput science (HTS) operations saw the pivotal role that Splunk Enterprise could fill as Recursion ramped up its capabilities.



“

If you combine the amount of data we are collecting with the speed and scale at which we work, it would be impossible to do it all manually. Splunk is more than just a resource for our team, it's a requirement.”

Director of HTS Operations, Recursion Pharmaceuticals



WATCH THE VIDEO:  
[splunk.com/recursion-pharma](https://splunk.com/recursion-pharma)

### BUSINESS IMPACT

- Time to value in three days, with complex laboratory adoption complete in only three months
- Visibility into all parts of the production process informs disease-targeting experiments
- Massive scale while managing data volume of 700,000 TIFF files weekly

The Splunk platform helps monitor and diagnose issues in real time with complex lab instruments, catching anomalies in automated operations, letting the high-throughput science team build dashboards to measure quality over time. It also serves as a data management platform that feeds machine data back to the data scientists who work with Splunk add-ons such as Splunk DB Connect, enabling the team to share discovered knowledge.



## BIOPHARMA LEADER GETS AHEAD OF SECURITY THREATS WITH ANALYTICS-DRIVEN SIEM IN THE CLOUD

With data silos located worldwide, a global biopharmaceutical leader realized it needed a security information and event management (SIEM) solution. To better protect its customers and intellectual property against cyberthreats and breaches, particularly given today's ever-changing security threat landscape, the company adopted Splunk Cloud with Splunk Enterprise Security (ES) for security and compliance.

### BUSINESS IMPACT

- An estimated 30 percent lower cost of ownership compared to on-premises alternatives
- A dramatic reduction in security investigation and resolution times
- Protection against threats, breaches and malware; ensuring regulatory compliance

Given that the company manages highly sensitive consumer and proprietary intellectual property data, it needed a solution that would provide visibility into any possible threats in its IT environment as soon as possible. The company was satisfied with the immediate availability of Splunk Cloud with Splunk Enterprise Security as its SIEM, and the security team began asking questions and getting answers from its data right away. The Splunk analytics-driven SIEM takes in log information from all areas of the company — including infrastructure, applications and devices — to detect security incidents and manage those events, which simply could not be done adequately with its legacy SIEM. Overall, security investigation and resolution times have been reduced from up to months to hours or even minutes.

In addition to relying on Splunk Cloud for security and compliance, the company is also beginning to use Splunk Cloud to monitor its IT operations, and plans are underway to identify additional ways to leverage insights from the data and help the business moving forward.



# INDUSTRY TRAVEL AND TRANSPORTATION

INDUSTRY  
✈ Travel and Transportation

SPLUNK USE CASES  
☁ Internet of Things

Europe's largest rail freight operator

## REAL-TIME FLEET ANALYTICS AND SMART ASSET MAINTENANCE AT DB CARGO

DB Cargo is Europe's largest railway operator managing one of the largest fleets of locomotives. To improve the service quality of this asset-heavy business, with some assets up to 25 years old and the infrastructure supporting them also aging, the organization embarked on an effort to digitize the fleet. "We needed a solution that could handle large volumes of diverse data in real time, which made Splunk Enterprise an obvious choice," says the company's vice president of asset digitization. The company now uses the Splunk platform to provide real-time insights across fleet control, engineering, maintenance and operations.

### BUSINESS IMPACT

- ➔ Single real-time view of locomotive fleet health and performance provides transparency
- ➔ Improved locomotive availability and reduced downtime enhances customer service and lowers maintenance costs
- ➔ Locomotive data insights have enabled a move toward condition monitoring

Previously, when issues arose, technical hotline engineers provided remote support to drivers based on phone calls and a locomotive manual. Today, the staff analyze real-time, continuous sensor values and GPS information in the Splunk platform to detect issues when they occur. Now when there's an issue, real-time data from the locomotive helps the team identify the root cause of the problem and determine how best to resolve it, enabling DB Cargo to keep locomotives in service longer and reduce maintenance costs.



Splunk Enterprise helps us improve reliability and availability of our assets so that we can keep locomotives in service longer than before. This enables us to deliver a better service to our customers, which ultimately makes us more competitive."

Vice President Asset Digitization, DB Cargo



WATCH THE VIDEO:  
[splunk.com/db-cargo](https://splunk.com/db-cargo)

INDUSTRY  
✈ Travel and Transportation

SPLUNK USE CASES  
🔍 IT Operations  
🛡 Security  
🌐 Internet of Things

The world's busiest airport

## DUBAI AIRPORTS FLIES INTO THE FUTURE WITH SPLUNK

With 90 million travelers passing through it each year, Dubai Airports is the world's busiest airport and passenger numbers are still growing. To deliver the additional capacity this requires, the airport deployed Splunk Enterprise to drive efficiencies.

### BUSINESS IMPACT

- 95 percent of passengers through security in five minutes or less
- Better customer experience
- New insights to drive future plans

The airport meets its target to get 95 percent of passengers through security in five minutes or less. Dubai Airports monitors metal detectors to identify trends that help keep the queue moving efficiently — insights are also shared with police and security teams to help improve service and security.

With up to 20,000 people connected to its free Wi-Fi at any one time, the IT team uses Splunk Enterprise to detect areas of congestion and rogue Wi-Fi hotspots. Dubai Airports has the largest baggage system in the world — each bag creates more than 200 data points, all of which are monitored in Splunk Enterprise to make sure it reaches its intended destination. Baggage data is also combined with airport operations data to predict baggage load, enabling the airport to allocate resources accordingly.

WATCH THE VIDEO:  
[splunk.com/dubai-airports](https://splunk.com/dubai-airports)



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

Executive Vice President, Technology & Infrastructure, Dubai Airports

INDUSTRY  
✈ Travel and Transportation

SPLUNK USE CASES  
📱 Application Delivery  
📊 Business Analytics  
🔍 IT Operations

Global hospitality company with more than 700 properties in over 50 countries

## HYATT REDUCES MTTR AND GIVES DEVELOPERS MORE TIME TO INNOVATE

Hyatt Hotels Corporation is driven by its purpose “to care for people so they can be their best.” Ensuring hotel guests have a seamless and enjoyable experience is a key part of this purpose. To provide this type of experience Hyatt needed a centralized solution to monitor and troubleshoot server issues and improve application delivery, so it deployed Splunk Enterprise and the Machine Learning Toolkit.

### BUSINESS IMPACT

- Faster issue resolution with real-time visibility across the entire business
- Increased developer productivity
- Improved customer experience

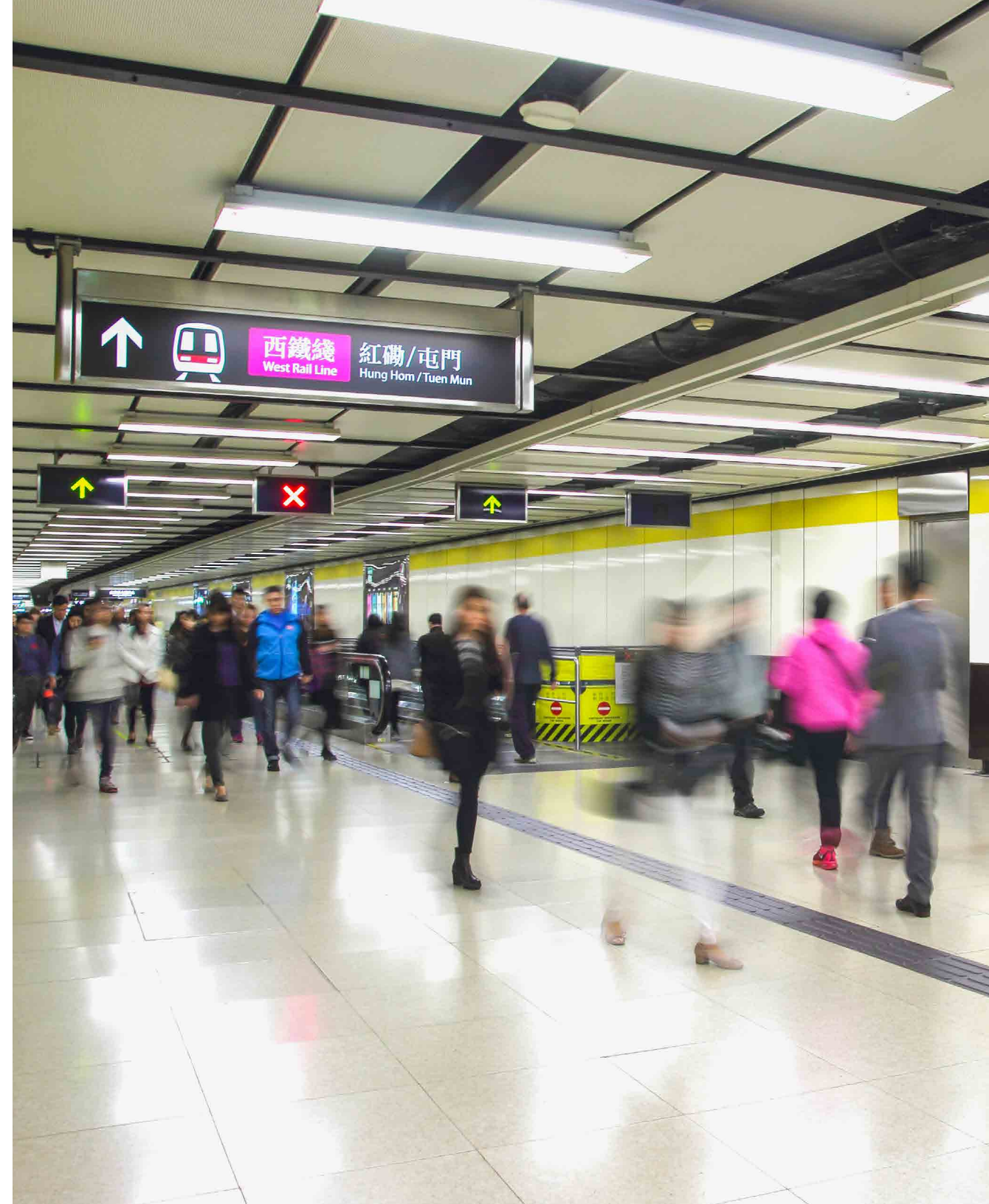
Previously, the online check-in experience was not as reliable, due to a time-consuming troubleshooting process. Prior to using the Splunk platform, developers had to log into an individual server and run a search tool to figure out what was happening, which could take hours. And there was no way for them to determine if an issue was local to one server, or occurring across multiple servers. With Splunk Enterprise and the Machine Learning Toolkit, the application development manager and his developer team are able to troubleshoot server issues quickly. Results have been positive — issues are solved faster. And, moving forward, predictive analytics will provide further insight into hotel room occupancy and more.



Splunk allows our developers to focus on developing instead of wasting their time looking for the issues. If they can find the issue faster, then they can go back to the development.”

Application Development Manager, Strategic Systems and Innovation,  
Hyatt Hotels Corp.





## MTR GOES THE EXTRA MILE WITH SOLUTION PROVIDING AUTOMATED REAL-TIME VISIBILITY

Responsible for about 5.8 million passenger trips on a normal weekday, Hong Kong's MTR Corporation Ltd. decided to upgrade its system to automate daily IT security management and threat detection, with a special focus on tracking corporate network access. In 2017, MTR started replacing its old security information and event management (SIEM) system with Splunk Enterprise, Splunk Enterprise Security and Splunk IT Service Intelligence monitoring and analytics solution.

“

A turnkey analytics platform, Splunk offers us a rapid entry to actionable threat intelligence, giving us the visibility into potential risks in our production environment and a tool to monitor, investigate and report on them.”

**Head of Information Technology,** MTR Corporation Ltd.

### BUSINESS IMPACT

- Real-time visibility into IT operations
- Enhanced operational efficiency and productivity; improved resource utilization
- Ultrafast threat tracking in minutes

Splunk Enterprise matches searches on all data sources in the MTR information system to analyze potential threats. Data from the Active Directory, privileged account management system and other sources are well integrated, and user login information is matched to approved user records, enabling automatic user tracking and identification. Splunk Enterprise has converted manual investigations into simple, proactive and automated searches, facilitating real-time security monitoring through internal risks and threats analyses.

Splunk Enterprise detects high-risk activity, access and events, providing actionable insights in minutes. It alerts the team about threats so they can search historical event data to determine the scope, intent and severity. By freeing up valuable time and resources, Splunk Enterprise enables MTR's IT teams to focus on value-added business activities.



INDUSTRY

# ONLINE SERVICES

- INDUSTRY
- Online Services
- SPLUNK USE CASES
- Security
  - Compliance
  - Business Analytics

Provider of customizable web messaging solutions

## SMSGLOBAL GAINS REAL-TIME VISIBILITY INTO CUSTOMER NEEDS AND SYSTEM HEALTH

Australia-based SMSGlobal provides customizable web messaging solutions for small businesses as well as the world's best-known brands, banks, governments and airlines to engage internal and external stakeholders. As the market adapted to the increased use of mobile text messages, the company identified an immediate need to add more advanced features to its offerings. It also needed to boost its security posture and ensure compliance, so it adopted Splunk Enterprise and Splunk Enterprise Security.

- BUSINESS IMPACT
- Real-time reporting and operational intelligence
  - Optimized compliance management
  - Automated threat intelligence

With the Splunk platform, compliance reporting that was a painstaking task requiring 10 people and days to complete now is a simple job that takes only one administrator seconds. Scheduled searches and automated reporting make it easy to provide compliance analysts and auditors with needed information. SMSGlobal also uses Splunk software to harness machine data to determine everything from operational health to infrastructure security posture. The company can now easily create action rules to identify anomalies and protect critical infrastructure from cyberthreats.

“Splunk Enterprise is a fantastic solution that transforms machine data into accessible, usable and actionable business insights in real time, enabling us to realize fast time to value. It took us by surprise by offering out-of-the-box functionality that enables us to turn big data into revenues.

Co-founder and Chief Operating Officer, SMSGlobal







INDUSTRY  
Online Services

SPLUNK USE CASES  
Security  
Application Delivery

Digital automotive marketplace provider

## TRUECAR DRIVES LOG MANAGEMENT, APPLICATION DELIVERY AND SECURITY SUCCESS WITH SPLUNK CLOUD AND AMAZON WEB SERVICES

TrueCar, a digital automotive marketplace, provides comprehensive automotive pricing transparency. While migrating its technology infrastructure to the cloud, the company required a log management and infrastructure monitoring solution that could scale and support cross-functional searching and reporting to manage and troubleshoot its complex IT environment. TrueCar had set up ELK (Elastic Stack) “because it was an open-source tool we could run in our environment. Our infrastructure team spent many hours maintaining ELK. By moving to Splunk Cloud running on Amazon Web Services (AWS), we were able to free up our infrastructure team’s time to tackle other problems,” says the company’s technology platform senior vice president.

### BUSINESS IMPACT

- Immediate value from deploying Splunk Cloud in one day and gaining real-time insights
- Accelerating software and product development
- Providing additional visibility into AWS billing

The team integrated Splunk Cloud into its tool set, quickly relying on it for monitoring all core infrastructure and application delivery across the organization. From there, a lot of reporting moved into Splunk Cloud. The infrastructure team created dashboards to provide visibility into AWS billing, to better control costs and allocate resources effectively throughout TrueCar’s cloud migration without needing to manage infrastructure. Splunk Cloud adoption happened very rapidly — TrueCar’s security team created several valuable dashboards to monitor and prevent malicious exploits and soon after, other teams repurposed the same data sources for important business insights.

“

Splunk Cloud just works, and it’s one of the things that people rely on day to day.”

Senior Vice President, Technology Platform,  
TrueCar

INDUSTRY  
Online Services

SPLUNK USE CASES  
Security and Fraud

Search engine optimization and content marketing performance company

## BRIGHTEDGE BOOSTS SECURITY WITH SPLUNK CLOUD

“As a cloud-first company without a large IT department, we use pretty much all of the best-of-breed SaaS products, from NetSuite as a financial system to BambooHR for human resources,” says the head of information security at BrightEdge. After evaluating tools including Loggly and Sumo Logic, BrightEdge realized that Splunk Cloud, “is not just a SIEM system; it’s a platform with an app for almost everything that I need,” he says. Splunk Cloud was up and running within a day, giving visibility into logs and correlation with multiple data sources that BrightEdge’s previous solution couldn’t offer.

### BUSINESS IMPACT

- Immediate impact, time and headcount savings compared to generic log management
- Discovered unauthorized access attempts and malware
- Smorgasbord of apps and add-ons for integration with other workflows

BrightEdge relies on Salesforce.com for customer relationship management, and the Splunk App for Salesforce to gain insight into the CRM platform’s adoption, usage and security. When a BrightEdge employee compromised her access, Splunk Cloud detected it immediately, the team responded quickly, and no data was lost. Splunk Cloud also detected that two end-user computing devices in the office were vulnerable to threats. “The endpoint security software we had at the time didn’t detect the malware, so we immediately replaced it. Without Splunk Cloud we probably wouldn’t have known,” concludes the company’s head of information security.

“Now I can do a security investigation in less than an hour. I can’t believe what Splunk Cloud can do; it’s achieving the impossible.

Head of Information Security,  
BrightEdge

”

INDUSTRY  
Online Services

SPLUNK USE CASES  
Business Analytics  
IT Operations

Martech company that connects  
brands and e-commerce sites  
with customers

## ROKT EMBRACES ADVANCED ANALYTICS TO IMPROVE PREDICTABILITY AND SERVICE

As Rokt's business began to experience significant growth, it needed a better way to manage its diversifying range of logs to increase efficiency and productivity, and it adopted Splunk Enterprise. Initially used for log management, Splunk Enterprise now serves as a multipurpose business platform enabling Rokt to embrace advanced analytics to improve predictability and service, which has since exceeded expectations.



“

By delivering end-to-end visibility across our IT infrastructure, Splunk provides unprecedented benefits for both technical and business users.”

Lead Engineer (DevOps), Rokt

### BUSINESS IMPACT

- Enhanced business efficiency due to real-time, proactive log management
- Improved productivity with full visibility into IT environment, user behavior and DevOps testing
- Real-time operational insights through predictive analytics

Rokt's engineers rely on Splunk Enterprise to proactively monitor the operational health of critical IT and business services, prioritize problem resolutions and enable analytics-driven IT on-premises and in the cloud. Splunk Enterprise also enables business users to trace consumer behaviors through real-time visibility and historical analytics on user-friendly dashboards. By monitoring online interconnections with e-commerce partners in real time, the team can now take immediate corrective actions before technical problems arise.

Rokt's DevOps team has also derived maximum benefits from Splunk software. From application development, testing to production monitoring, Splunk offers real-time insights across all stages of the delivery lifecycle, which enables the team to seamlessly move from concept to production and achieve more efficient application delivery.



INDUSTRY  
Online Services

SPLUNK USE CASES  
IT Operations  
Security  
Compliance

Australia's first online property exchange network

## OPERATIONAL VISIBILITY ENABLES PEXA TO DRIVE DIGITAL TRANSFORMATION AT AUSTRALIAN PROPERTY EXCHANGE NETWORK

PEXA (Property Exchange Australia) assists members of its network — such as lawyers, conveyancers, financial institutions and property developers — to lodge documents with land registries and complete financial settlements electronically. To better manage regulatory complexities, its growing product portfolio, and the volume of interactions with a diverse network, PEXA deployed Splunk Enterprise for enhanced IT operations and security visibility across its business.

### BUSINESS IMPACT

- Greater operational visibility into system health
- Real-time alerts provide faster insight into potential disruptions for proactive resolution
- Uncompromised customer experience

Splunk dashboards provide visibility into every aspect of the applications PEXA brings to market. The Splunk App for AWS provides a consolidated view into the company's AWS environment across multiple accounts, which was previously a challenge. PEXA can now bring all the data into a single pane of glass and monitor movement across the entire IT infrastructure in real time. Splunk software also helps improve customer experience internally and externally. Dashboards linked to operational data from third-party sources ensure there's no disruption to the end-user experience. With Splunk Enterprise, the operations team can automate compliance reporting, such as availability reports and tracking certificate expiration, as well as key metrics including response times, transaction totals and API usage to internal and external stakeholders.

“

The greatest value we get from Splunk is the ability to keep the health of PEXA's system in check. The real-time alerts we get range from security and machine-related issues to operational triggers, which are integrated into our day-to-day communications via email, SMS and other alerting tools.”

Head of DevOps, PEXA

INDUSTRY  
Online Services

SPLUNK USE CASES  
Business Analytics

Provider of online communities for millions of global users

## NETWORLD GAINS REAL-TIME BUSINESS INSIGHT INTO WEB DATA FOR FAST DECISION-MAKING

With more than 130,000 products for sale by local merchants, the team at Networld Technology Ltd.'s Price.com.hk needed to monitor and identify top products, categories and merchants for business management purposes. With Splunk Enterprise, Networld replaced manual reporting with powerful dashboards that show overall business trends of various retail brands in a real-time, user-friendly graphical interface that tracks overall site performance. The Price.com.hk team was able to deploy Splunk Enterprise quickly, ingest database and web-log data, build its first dashboard and gain actionable visibility into its data in only five weeks.

### BUSINESS IMPACT

- Real-time business analytics increased operations efficiency
- Seamless IT system and website monitoring improved performance
- Real-time revenue analysis generated new business opportunities

Splunk Enterprise also helps the team that handles Networld's discussion forum, Discuss.com.hk, by generating real-time threads treemap queries. By clicking on a certain part of a treemap, users can immediately explore content generation and traffic details of a subforum, such as the number of new threads generated and related hot topics being covered. With those insights, timely and targeted promotions can easily be planned and carried out.

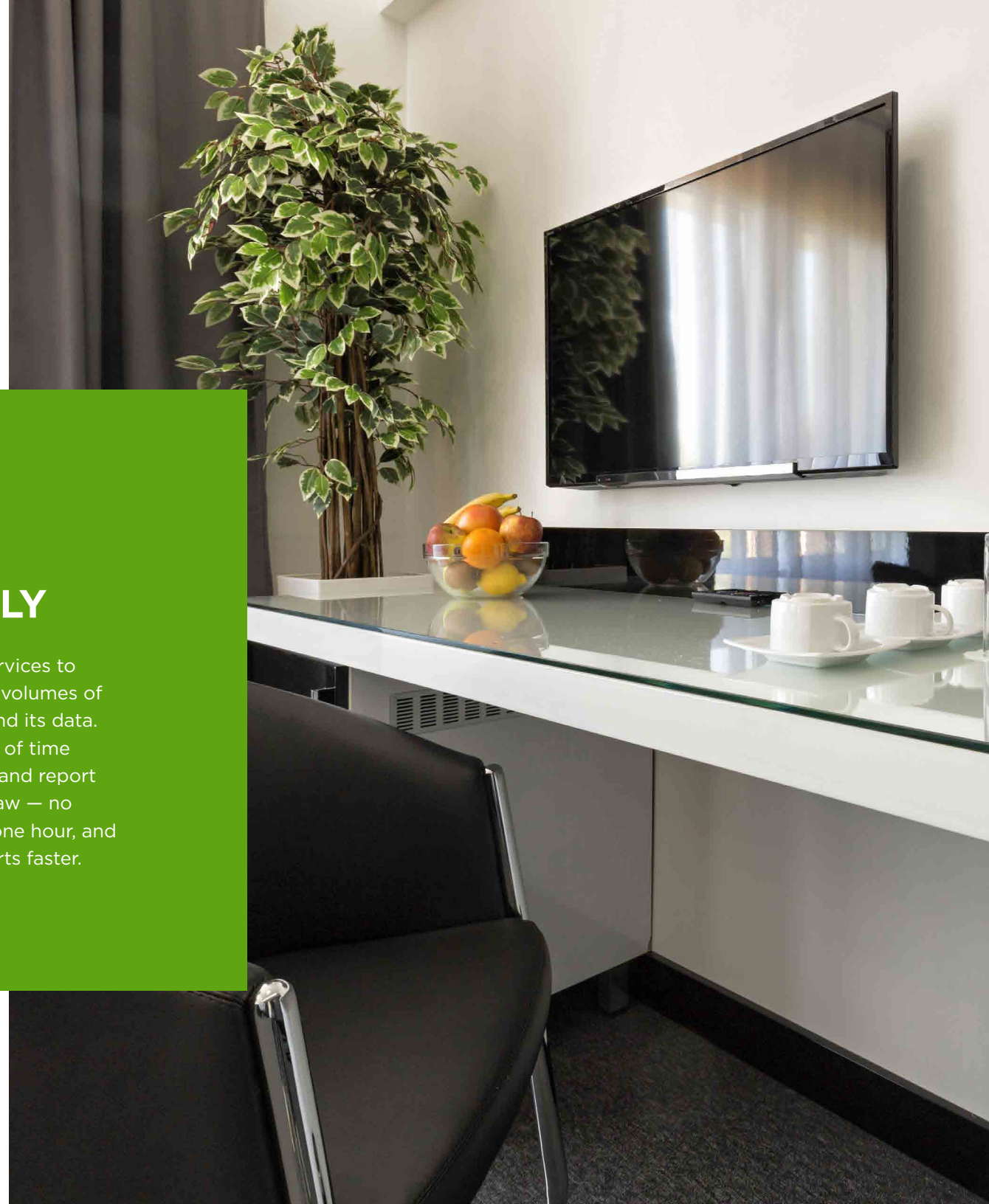
“We never imagined that we could create dashboards this easily. It only took us five weeks to begin aggregating, searching and understanding our data and building dashboards to gain actionable visibility. Splunk makes a real difference in our business intelligence and paves the road for our next business endeavors.

Head of Data Science team, Networld Technology Ltd.

”

## SONIFI SOLUTIONS, INC. CREATES SEAMLESS REPORTING, SAVES THOUSANDS OF DOLLARS ANNUALLY

SONIFI Solutions, Inc. provides interactive television, streaming and internet services to more than one million hotel rooms and 500 million people annually. With large volumes of data in multiple places, the company struggled to quickly access and understand its data. Additionally, SONIFI spent weeks to generate reports, with significant amounts of time dedicated to developing tables to first structure the raw data, and then to test and report on this data. With Splunk Enterprise, the team can now ingest this same data raw — no tables or structure required. This ability cuts data query time from one day to one hour, and the time savings enables engineers to detect bugs and generate accurate reports faster.



“

We were cross-referencing multiple databases, building massive spreadsheets, which was very manual and tedious. Splunk put all of that information into a visual format that’s usable, empowering us to make better decisions. Previously, what had taken us days, we’re now able to do in hours, if not minutes.”

Vice President, Product Management and User Experience, SONIFI Solutions, Inc.

WATCH THE VIDEO:  
[splunk.com/sonifi](https://splunk.com/sonifi)

### BUSINESS IMPACT

- Saved \$85,000 annually by centralizing reporting and streamlining processes
- Saved \$100,000 per month by correlating viewing habits with billing data and detecting questionable cancellations
- Reduced reporting time from days to minutes



The company has also adopted Splunk Enterprise to provide insight into its billing decisions, allowing the company to save \$100,000 monthly. Currently, SONIFI uses the Splunk platform to correlate customers’ viewing habits with billing data, detect questionable cancellations and implement preventative processes.



INDUSTRY

FINANCIAL SERVICES

INDUSTRY

- Financial Services
- Energy

SPLUNK USE CASES

- IT Operations

Energy trading platform at the heart of ENGIE, a global energy player in gas, power and energy services

SPLUNK ENSURES PERFORMANCE OF KEY TRADING APPLICATION AT ENGIE GLOBAL MARKETS

ENGIE Global Markets (EGM) needed a centralized, real-time view of the health of its critical trading application to speed troubleshooting and ensure performance. Before deploying the Splunk platform, the development and infrastructure teams used their own siloed monitoring tools, which required a lot of back and forth to resolve issues. After deploying Splunk Enterprise and Splunk IT Service Intelligence (ITSI), the collaboration between the teams improved and incident resolution time was reduced.

BUSINESS IMPACT

- Holistic view of health of key business services
- Better cross-functional collaboration enables faster mean time to resolution
- Adaptive thresholds in Splunk ITSI help find and fix issues before they become real problems

Deploying Splunk ITSI has made it easier for EGM to correlate data across the IT stack to improve incident management and resolution. With the swimlane visualizations in Splunk ITSI, EGM can collaborate across technology functions to also see how lower-level services are impacting top-layer services. Moving forward, EGM plans to use the Splunk Machine Learning Toolkit to deliver further IT operations and business insights.

“When there’s an issue, Splunk ITSI shows us where to look so we can solve the issue. With machine learning in Splunk ITSI, we don’t have to create thresholds manually to measure the performance of each server. We can adapt them dynamically to account for expected performance variances. This eliminates the cost of frequent configuration and tuning and frees our team to focus on triage on actual incidents before they impact end-user experience.

Head of Infrastructure, ENGIE Global Markets







- INDUSTRY**  
Financial Services
- SPLUNK USE CASES**  
Application Monitoring  
Business Analytics

Intermediary payment gateway to manage interbank transactions across Vietnam

## NAPAS ENSURES SEAMLESS OPERATIONS WITH REAL-TIME BUSINESS VISIBILITY AND INTELLIGENCE

Currently handling over one million transactions daily and hundreds of millions of online transactions every year, NAPAS must monitor the health and ensure 24/7 availability of all of its business applications. To optimize business performance, NAPAS needed a sophisticated monitoring solution to simplify application management, achieve total IT infrastructure monitoring transparency and enable instant access to critical data. As a solution, NAPAS deployed Splunk Enterprise.

### BUSINESS IMPACT

- Enhanced productivity with full visibility into daily operations
- Heightened customer satisfaction when issue resolution decreased from hours to minutes
- Simplified business operations due to an automatic, seamless compliance process

Splunk Enterprise enables NAPAS to generate real-time, end-to-end insights into machine data across its entire infrastructure, providing deep visibility into faults, events, capacity, configurations and the security of servers and network elements. NAPAS can now collect, store, index, search, correlate, visualize, analyze and report on any machine-generated data in real time to identify and resolve operational issues.

Standardizing on the Splunk platform also takes the guesswork out of issue resolution, supporting NAPAS to get in front of an issue before an incident happens, rather than responding to it after the fact. With just a few clicks, the operations team now gets holistic views of system health, application availability and performance.

What also impresses NAPAS is the scalability of Splunk Enterprise. This flexible, adaptable platform enables us to embrace strategic opportunities to support broader business objectives, including fraud monitoring and business analytics.”

Chief Information Officer, NAPAS



- INDUSTRY**  
Financial Services
- SPLUNK USE CASES**  
Security and Fraud

Japan's first internet-only bank

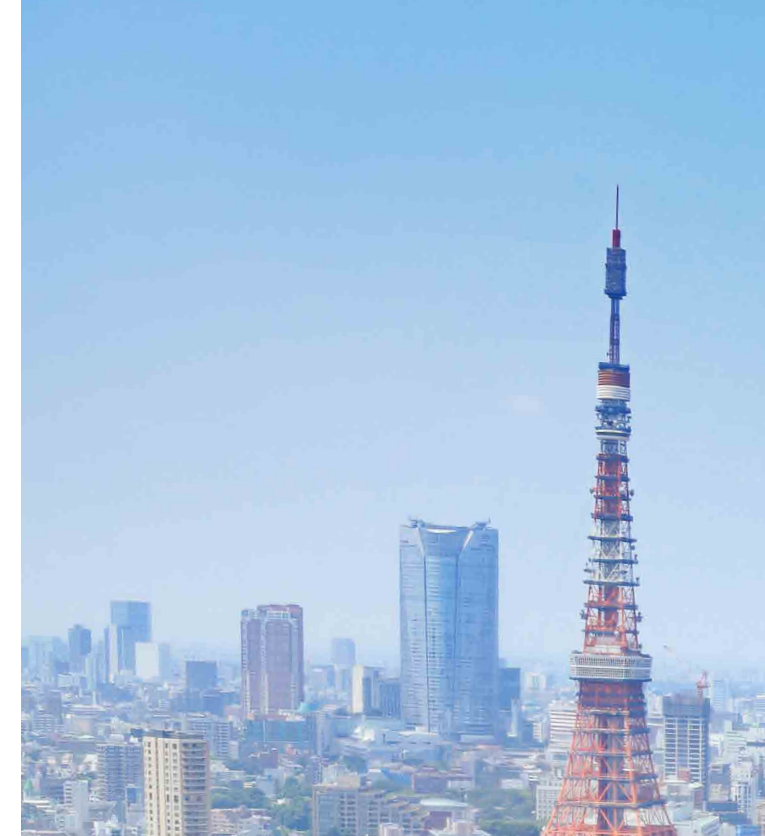
## JNB, JAPAN'S ONLINE BANKING PIONEER, GAINS REAL-TIME VISIBILITY INTO CYBERSECURITY RISKS

With a banking model conducted entirely online, The Japan Net Bank, Ltd. (JNB) needed an intelligent platform to collect, analyze and deliver real-time insights from its data to improve its cyber defense strategies. Previously, the IT Supervision Department spent many hours digging out firewall and proxy logs from the office automation environment and analyzing web access logs to spot unauthorized accesses. The bank also required high accuracy in monitoring transaction logs to safeguard against spoofing and illegal fund transfers. To capture, analyze and act upon the untapped value of data generated from daily operations, JNB deployed Splunk Enterprise.

### BUSINESS IMPACT

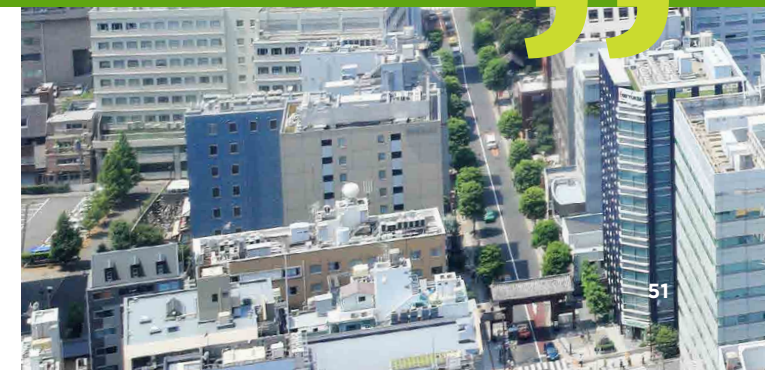
- Accelerated cyberattack analysis, from up to one day to a few minutes
- Prevented illegal money transfers
- Gained new opportunities for enhancing cybersecurity

The bank now has real-time data access and completing an investigation is a multi-minute exercise. Captured logs can be searched on demand with only a few clicks, and with Splunk Enterprise, the team can create consolidated reports and dashboards to view enterprise-wide security risk in a single pane of glass. And, Splunk Enterprise automatically sends real-time alert emails to JNB's computer security incident response team upon detection of any signs of phishing attacks, enabling the team to successfully identify more than 20 spoof websites in a single year.



“The Splunk solution enables JNB to lead the way in cybersecurity and become a role model in Japan's banking industry.

Assistant Manager, IT Planning Department,  
Cyber Security Office / JNB-CSIRT, The Japan Net Bank, Ltd.





INDUSTRY  
Financial Services

SPLUNK USE CASES  
IT Operations

Provider of consumer reports, risk scores, analytical services and more for over one billion consumers and business customers

## TRANSUNION INVESTS IN SPLUNK SOLUTIONS FOR ENTERPRISE MONITORING, MACHINE LEARNING

With a global presence in more than 30 countries and territories, TransUnion helps businesses manage risk while also helping consumers manage their credit, personal information and identity. To improve performance monitoring for external customer traffic and customer volume transactions, the company deployed Splunk Enterprise, Splunk IT Service Intelligence (ITSI) and the Splunk Machine Learning Toolkit for enterprise IT monitoring and machine learning-powered analytics.



“

We use Splunk for a wide variety of use cases from alerting to root cause analysis, reporting, audit and security. Nothing else on the market provides the ability to query such massive amounts of data and quickly pinpoint complex technical issues.”

Senior Monitoring and Operations Architect, TransUnion

### BUSINESS IMPACT

- Provide reliable transactions and meet customer SLAs
- Discover incident root causes in minutes instead of hours
- Reduce the number of false alerts

TransUnion experiences variable traffic cycles on its website, with higher transaction volumes at certain times of the day and week. With automation and machine learning algorithms in place, the company has a new way to monitor these traffic cycles and transactions. With Splunk ITSI, the engineering team visualizes and combines machine data from multiple applications to create an end-to-end transaction flow not available in commercial APM solutions.

TransUnion analysts recently looked to Splunk dashboards when troubleshooting traffic for a large banking customer. With accrued knowledge of expected traffic at specific times of day, traffic that fell outside that data was considered an anomaly and generated an alert. And, TransUnion’s enterprise monitoring department will soon use accelerated data models to populate summary indexes to increase speed further.

INDUSTRY

PUBLIC SECTOR



- INDUSTRY
  - Public Sector
- SPLUNK USE CASES
  - Security
  - IT Operations

Leading cybersecurity, software and systems engineering firm

INFOTEK AND SPLUNK DELIVER SECURITY INTELLIGENCE PLATFORM FOR PUBLIC SECTOR CUSTOMER

Many organizations depend on security information and event management (SIEM) software to monitor, investigate and respond to security threats. But at one U.S. government agency, its legacy SIEM software from HP ArcSight failed to live up to expectations, so the agency replaced it with Splunk Enterprise and Splunk Enterprise Security (ES).

BUSINESS IMPACT

- Deploying in one weekend and stopping an attack the next day
- Achieving a 75 percent cost reduction to support its SIEM
- Reducing number of tools required, including log aggregators and endpoint solutions

InfoTeK deployed Splunk software over one weekend for the customer, and the software proved its value starting the next day. The IT team was able to search security events and immediately thwarted an attack vector.

The agency’s operational savings are significant. By moving to the Splunk platform, it has dramatically reduced the number of tools that IT staff need to manage, and it reduced the number of servers required to support the SIEM. Before, the agency needed two security engineers to manage ArcSight, and now only one engineer is needed — and he only spends one-half of his time managing the Splunk platform.

“Something that used to take hours, days or even weeks with other products or jumping between multiple tools can be done in seconds, minutes or hours with Splunk. We were able to provide a ROI before the product was even fully purchased because the customer successfully stopped a threat that would have required a complete rebuild of the network.”

Senior Incident Handler and Security Engineer, InfoTeK



WATCH THE VIDEO:  
[splunk.com/infotek](https://splunk.com/infotek)



INDUSTRY  
Public Sector

SPLUNK USE CASES  
Security

Sixty departments, 35,000 employees  
and more than 865,000 residents

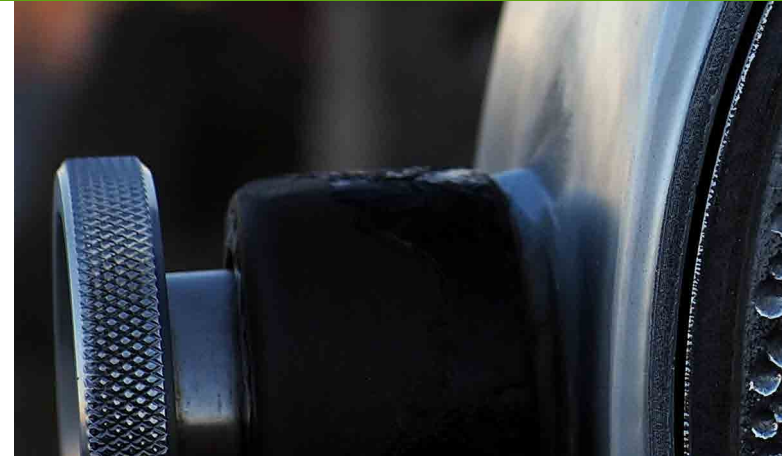
## CITY OF SAN FRANCISCO WOMEN IN TECH: SF'S NINA D'AMATO

San Francisco's chief of staff for the department of technology, Nina D'Amato, talks about service, leadership and creating a culture of diversity that allows people to thrive.



WATCH THE VIDEO:  
[splunk.com/city-county-san-francisco](https://splunk.com/city-county-san-francisco)

Watch the video to learn about Nina D'Amato's career, what makes the San Francisco Bay Area so special, and her advice for women in technology.



INDUSTRY  
Public Sector

SPLUNK USE CASES  
IT Operations  
Application Delivery  
Security

Home to NASA's Goddard Space  
Flight Center, the University of Maryland  
and nearly one million citizens

## MARYLAND'S PRINCE GEORGE'S COUNTY MISSION-READY WITH SPLUNK PLATFORM

Prince George's County, Maryland's centralized Office of Information Technology (OIT) provides infrastructure and core IT services to support the goals of diverse countywide agencies. Siloed data sets made it challenging for the small IT team to get visibility into issues. By implementing Splunk Enterprise, the team gained visibility across functional teams to solve issues more quickly.

### 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

Splunk Enterprise monitors the network to ensure that services are available and agencies can serve county citizens. The county also relies on Splunk Enterprise for application monitoring, including an application that enables citizens and contractors to complete permits online.

The county plans to grow its use of the Splunk platform to improve its security posture and quickly investigate potential threats or vulnerabilities to take action on those events proactively. The OIT has faced recent cyberthreats and needs to ensure data integrity, availability of service and that the service is used as intended.

“

We look at Splunk Enterprise as a solution to get a better understanding of all data including system health, public safety and transportation data, to solve problems, help our agencies fulfill their missions and make government more efficient.”

Enterprise Architect, Prince George's County OIT



WATCH THE VIDEO:  
[splunk.com/prince-georges-county](https://splunk.com/prince-georges-county)

Employs 12,000 people across  
50-plus agencies and serves more  
than 1.1 million citizens



## FAIRFAX COUNTY PROTECTS CITIZEN DATA USING SPLUNK ENTERPRISE SECURITY IN THE CLOUD

Located in the heart of the nation's capital, Fairfax County, Virginia, is regarded as a leader in many areas when it comes to cybersecurity and IT, enabling it to serve the needs and protect the data of its IT-savvy and high profile citizens. Fairfax County deployed Splunk Enterprise Security (ES) with Splunk Cloud as its security information and event management (SIEM) platform.

According to Fairfax County's chief information security officer (CISO), 210 IT professionals support more than 50 county agencies, each with unique business and security requirements. Some agencies, such as the Health Department, are governed by regulations like HIPAA, while others must comply with payment card industry (PCI) regulations. Ultimately, the county requires reliable and secure access to data so it can make the best decisions to support county citizens.

Today, 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.

WATCH THE VIDEO:  
[splunk.com/fairfax-county](https://splunk.com/fairfax-county)

### BUSINESS IMPACT

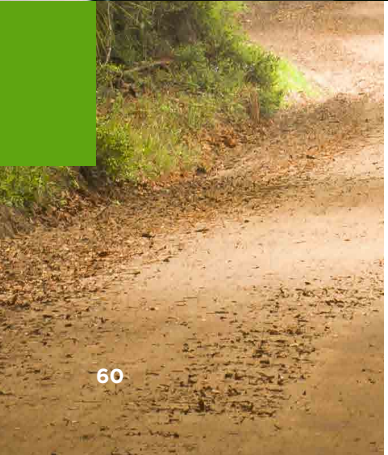
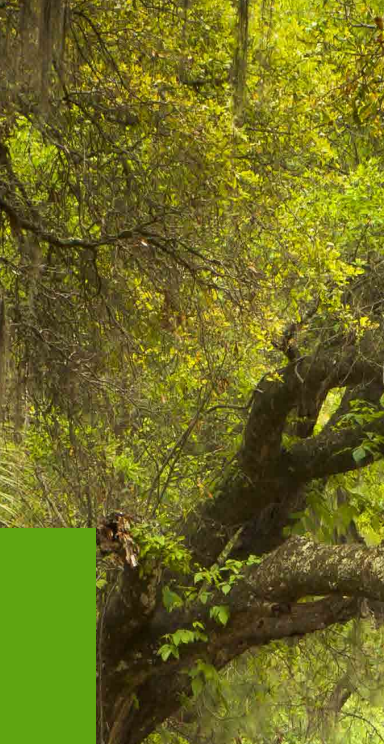
- Proactively supporting more than 50 county agencies and protecting citizens' data
- Reducing security reporting from two weeks to real time
- Increasing focus on strategic initiatives by leveraging cloud services



My top priority is to protect the citizens' data. Making sure that these citizens can trust the government they have with the data that they have entrusted us with is our mission.”

CISO, Fairfax County, Va.





INDUSTRY  
Public Sector

SPLUNK USE CASES  
IT Operations

State of Louisiana IT departments include 20 executive branch agencies and 850 staffers

## STATE OF LOUISIANA IMPROVES CITIZEN EXPERIENCE, SAVES \$70 MILLION IN IT CONSOLIDATION

The newly unified State of Louisiana IT department has been tasked with legacy consolidation and modernization efforts to improve efficiencies, cut costs and enhance service delivery to its core set of customers — the state agencies and citizens. According to the state’s director of data center operations, the Splunk platform was “by far the most robust for us to handle petabytes of data.”

### BUSINESS IMPACT

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



It is rare to find a single product that has a meaningful impact across our entire state government, but that’s exactly what Splunk does. Splunk is extremely efficient and helps us make the best use of taxpayer dollars. Not only does Splunk save us money by freeing us from doing things manually with multiple systems, but it also enables transparency. Splunk gives the ability to show people exactly how things are being used and why.”

Director of Data Center Operations, State of Louisiana

WATCH THE VIDEO:  
[splunk.com/state-of-louisiana](https://splunk.com/state-of-louisiana)

INDUSTRY  
Public Sector

SPLUNK USE CASES  
Security

Multi-mission U.S. National Nuclear Security Administration (NNSA) research and development lab

## SANDIA NATIONAL LABORATORIES 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 has developed an advanced approach to address complex national security challenges. Sandia’s High Fidelity Adaptive Deception and Emulation System (HADES) is a multi-faceted cyber-defense application.

### BUSINESS IMPACT

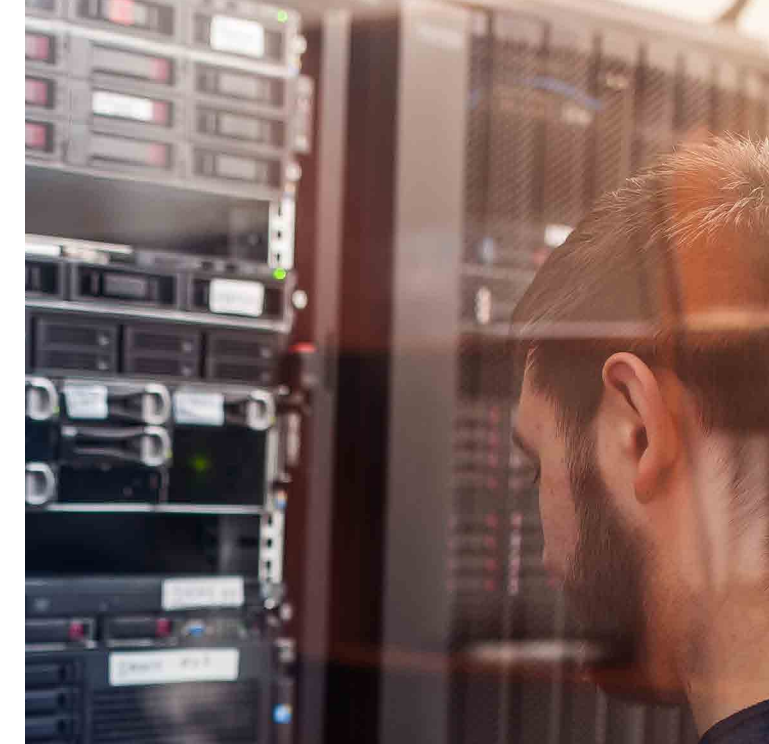
- Provides an automation-driven collaborative framework for fast and consistent threat identification and response
- Enables analysts to produce and share threat intelligence while interacting with attacks in real time
- Realizes the ability to deceive adversaries, profiling them incognito to expose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

HADES uses the Splunk platform to develop profiles of adversaries, and even detect lateral movement that could take over additional systems. This knowledge helps analysts prepare defenses based on adversarial tactics. The team is able to stay one step ahead of attacks and disrupt the cost cycle with a solution 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.”

Cybersecurity Research Strategist, Sandia National Laboratories





#### INDUSTRY

Public Sector



Security



Compliance



IT Operations



Business Analytics

Operates the state lottery and serves as the regulator of six casinos

## MARYLAND LOTTERY AND GAMING CONTROL AGENCY BETS ON SPLUNK

Public sector IT leaders face the challenge of ensuring secure operations while meeting significant compliance mandates with limited budgets and staff. 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. The agency deployed Splunk Enterprise as part of an effort to modernize its IT operations and has saved up to six hours a week on compliance tasks, improved its security posture and more.



“

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.”

CIO, Maryland Lottery and Gaming Control Agency

#### BUSINESS IMPACT

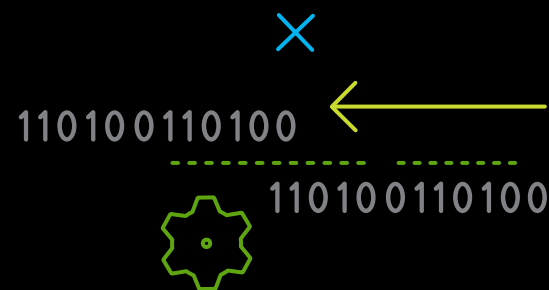
- Real-time, self-service compliance reporting for auditors
- Improved security monitoring for the IT team and Chief Information Officer
- Improved anomaly detection to quickly identify and prevent security breaches

In Maryland, every prospective casino employee must pass a background investigation prior to receiving a gaming license. These investigations require access to federal and state criminal records, and the MLGCA must meet specific criteria regarding the security of the database used in this licensing process.

The agency also needs to document IT processes to meet audit requirements pertaining to systems, firewalls and network devices. Splunk Enterprise provides staff with visibility that is especially critical when dealing with sensitive data that the agency needs to collect, and it also helps protect against internal misuse.



# INDUSTRY TECHNOLOGY

[illegible]

INDUSTRY  
Technology

## SPLUNK USE CASES

- Security
- IT Operations
- Business Analytics

Enterprise incident resolution service

## PAGERDUTY ENSURES END-TO-END VISIBILITY WITH SPLUNK CLOUD AND AMAZON WEB SERVICES

Customers turn to PagerDuty to manage and resolve their IT incidents quickly and efficiently. When the cloud-native company needed a solution to meet its operational analysis and triage needs, it adopted Splunk Cloud and AWS to ensure high availability of its services and scalability to meet customer demand.

## BUSINESS IMPACT

- Ensured customer satisfaction and highly available cloud services
- Gained 30 percent cost savings over prior service
- Reduced IT and security incident resolution time — from tens of minutes to single digit minutes or seconds

Prior to adopting Splunk Cloud, PagerDuty relied on a logging solution that could not scale as the company began indexing hundreds of gigabytes of logs daily. What's more, the team found it difficult to get actionable information out of its data to make decisions and solve problems quickly.

Today, PagerDuty has AWS and Splunk Cloud as its platform for operational visibility and triage across the business — from IT operations monitoring to security and compliance. With Splunk Cloud, engineering teams have a solution for monitoring and alerting, and then they can dig deeper into the source of issues and resolve them quickly. The company also uses the Splunk App for AWS, which provides visibility — from a security and compliance standpoint — and an audit trail of all of the activity in its AWS account.

“My accounting team was absolutely ecstatic when I told them, ‘We’re going to get the best solution, and by the way, it’s 30 percent cheaper compared to what we are currently using.’”

**Director of Infrastructure Engineering, PagerDuty**



INDUSTRY  
Technology

SPLUNK USE CASES  
IT Operations

10,000 employees in 19 countries  
and revenue of 2.5 billion euros

## EVENT ANALYTICS HELPS ECONOCOM DELIVER BETTER SERVICES TO CUSTOMERS

Econocom designs, finances and oversees digital transformation solutions for companies. Previously, Econocom teams lacked the ability to apply analytics across multiple data sources to accelerate incident investigation, visualize data with business-service context and apply capacity planning, so it implemented Splunk IT Service Intelligence (ITSI).

### BUSINESS IMPACT

- Improved service delivered to customers through quicker response to events
- Unified view of all events from dozens of legacy monitoring and event management solutions
- Reduced number of false positives resulting in 60 percent event reduction

Event analytics in Splunk ITSI helps Econocom to better prioritize and react more quickly to customers’ infrastructure events, ultimately providing a better service. Splunk ITSI also allows Econocom to exclude events considered false positives from the event management process, reducing total event volume by 60 percent. Having a reduced number of events to process, a single interface and the streamlined event analytics framework in Splunk ITSI allows Econocom operators to process events eight minutes more quickly, on average. This has led to a 15 percent improvement in the company’s SLA performance.

“Thanks to the integrated machine learning in Splunk ITSI, we now have a reduced number of events to process and the streamlined event analytics framework allows us to process events eight minutes more quickly, on average. This has led to a 15 percent improvement in SLA performance.”

Technical Director, Infrastructure Management Services, Econocom

INDUSTRY  
Technology

SPLUNK USE CASES  
Security  
Compliance

Innovative global digital services provider

## DIGITAL SERVICES PROVIDER IMPROVES SECURITY POSTURE WITH SPLUNK ENTERPRISE SECURITY

When a global digital services provider faced security and compliance challenges, it was concerned that failure to address issues quickly could have a negative impact on the bottom line. The company had relied on a managed security services provider (MSSP) that was not providing the robust security coverage required, so it decided to bring security monitoring in-house with Splunk Enterprise Security (ES) as its security information and event management (SIEM) solution.

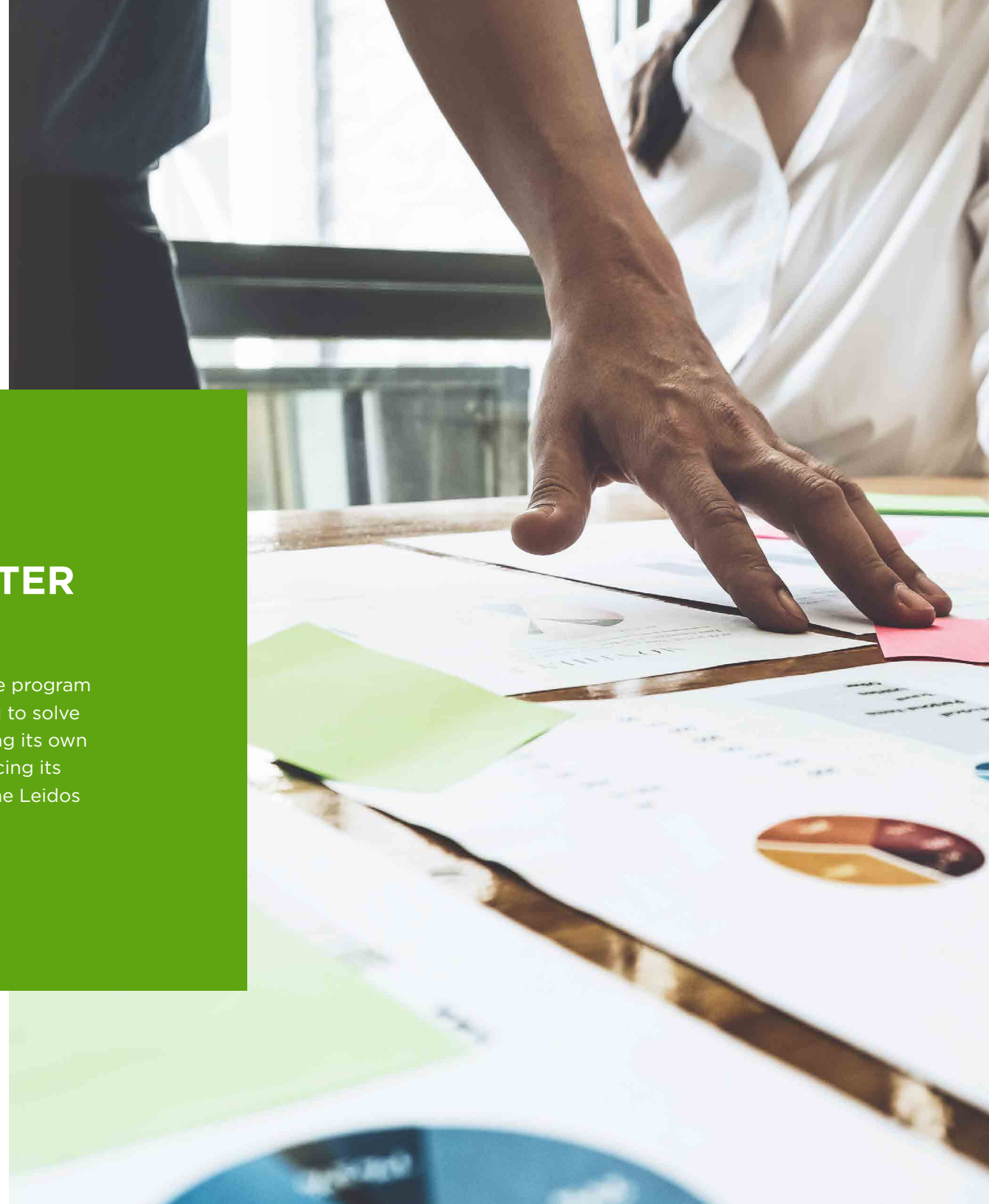
### BUSINESS IMPACT

- Improved security posture through an increase in reporting frequency from daily to real time
- Achieved SOC 2 Type II compliance, demonstrating the company’s commitment to keeping customer data safe
- Freed up engineering resources to focus on higher-level hunting and policy recommendations

The company issued an RFP to vendors in the Gartner SIEM Magic Quadrant, including Splunk, HP, IBM and LogRhythm, before narrowing its selection to Splunk and LogRhythm. The value and credibility of Splunk’s implementation services delivery, its ability to address multiple use cases beyond security, its Splunkbase apps ecosystem, and the ability of Splunk ES to scale were deciding factors in the company’s decision.

With Splunk ES, the digital services provider has the analytics it needs to monitor and respond to security incidents. The company also relies on the threat intelligence framework, a mechanism for consuming and managing threat feeds, detecting threats and alerting — one of five frameworks that organizations can integrate into Splunk ES.





## LEIDOS TAPS SPLUNK ITSI FOR BETTER EVENT MANAGEMENT

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 benefits.

“

I've not seen a product that does this. This is the first time I've been truly able to do heterogeneous, up-and-down-the-stack monitoring of my IT environment because Splunk has all the data and allows me to search it all in the same way.”

Director of Performance Management, Leidos

WATCH THE VIDEO:  
[splunk.com/leidos](https://splunk.com/leidos)

### BUSINESS IMPACT

- Real-time enterprise-wide infrastructure monitoring
- Robust solution to tear down IT silos and correlate events
- Dashboards for different audiences, from problem-solving techs to big-picture managers



Leidos started with a small Splunk Enterprise license to collect logs from routers and switches. The next natural step was alert management. Leidos had been using another solution for more than 15 years, which was not only outdated but bare-bones, with a complicated back-end rules language. The company wanted a modern product with out-of-the-box correlation and a rules engine to differentiate critical from minor events. The answer was Splunk ITSI. Today, ITSI is helping the company boil 3,500 to 5,000 daily alerts down to roughly 50 tickets for network and datacenter operations to act on.

INDUSTRY  
Technology

SPLUNK USE CASES  
IT Operations  
Security  
Fraud  
Application Delivery

International mobile payments company  
founded in Sweden in 2010

## IZETTLER TACKLES COMPLIANCE REQUIREMENTS, IMPROVES PRODUCT DELIVERY

iZettle enables merchants to quickly and easily accept consumer card payments through an app and accompanying chip card reader. To ensure compliance with the payment card industry data security standard (PCI-DSS), iZettle adopted Splunk Enterprise as its centralized platform for security events, and to improve application delivery.

### BUSINESS IMPACT

- Ensured iZettle was PCI compliant within five weeks
- Enhanced ability to meet current and future compliance requirements
- Improved insider threat detection capabilities

iZettle operates in a highly regulated market. For example, PCI-DSS is a compulsory industry regulation that requires 90 days of online log retention and one year of log archiving for any organization that handles credit cards. iZettle initially reviewed the open-source options available for a centralized logging solution for security events. However, it quickly became clear that the Splunk platform would provide faster time to value than the alternatives, and iZettle was able to demonstrate its improved capabilities to auditors within five weeks.

Once iZettle began using the Splunk platform for compliance purposes, it quickly recognized that the same data could offer value across both product development and wider security use cases.



As iZettle has grown over the past four years, so has our use of Splunk Enterprise. It has become integral to the business not just for compliance, but ensuring that customers have a positive and secure experience using our services.”

Head of DevOps & Infrastructure, iZettle

INDUSTRY  
Technology

SPLUNK USE CASES  
Application Delivery  
IT Operations  
Business Analytics

Provides solutions to the U.K. financial  
advisor market, with over 19,000 users  
managing over £300 billion in assets

## INTELLIFLO ENABLES NEXT-GENERATION FINANCIAL ADVICE WITH SPLUNK ENTERPRISE

Intelliflo provides web-based software and support to the financial services industry, enabling clients to streamline the way they deliver wealth management advice to their customers. Intelliflo wanted to improve access and visibility to data across its software infrastructure, enabling it to understand and improve the client experience, and it deployed Splunk Enterprise.

### BUSINESS IMPACT

- Enhanced software development process
- Better ability to manage client turnover
- Faster mean time to resolution with access to real-time data on user activity and problems

Intelliflo needs to ensure reliable solution delivery to its clients. Prior to Splunk Enterprise, the company used multiple tools to troubleshoot software issues, with access to machine data spread across disparate tools and siloed solutions with little integration.

Intelliflo required a holistic view over all of its machine data. With Splunk Enterprise, Intelliflo now has centralized access to all company machine data, enabling real-time software troubleshooting for clients, complete operational visibility over all product usage and an improved capacity for product development and performance management.

Splunk Enterprise also supports the entire Intelliflo software development process. The Intelliflo product set is evolving at a far quicker pace than would have been possible previously, helping the business to stay at the forefront of innovation.



Splunk Enterprise is a window into our business analytics and allows us to see our data in real time, helping us to more accurately shape business priorities and software development pipeline. We are at the point where our management team is debating major business decisions using Splunk dashboards.”

CEO, Intelliflo



WATCH THE VIDEO:  
[splunk.com/intelliflo](https://splunk.com/intelliflo)



## ANALYTICS-DRIVEN APPROACH TRANSFORMS IT OPERATIONS AT MICRON TECHNOLOGY

As a global leader in advanced semiconductor systems and with a broad memory solutions portfolio, Micron Technology, Inc. strives for high service quality that is critical to ensure a great customer experience and keep the competition at bay. To maintain its competitive position in the industry, Micron deployed Splunk IT Service Intelligence (ITSI) to innovate its IT operations strategy.



“

If we do happen to wind up in a major incident, Splunk ITSI is the first place we go. We always ask ourselves the question, ‘Did ITSI help us figure out where the problem was?’ Every time the answer has been, ‘Yes.’”

IT Director, Micron Technology

### BUSINESS IMPACT

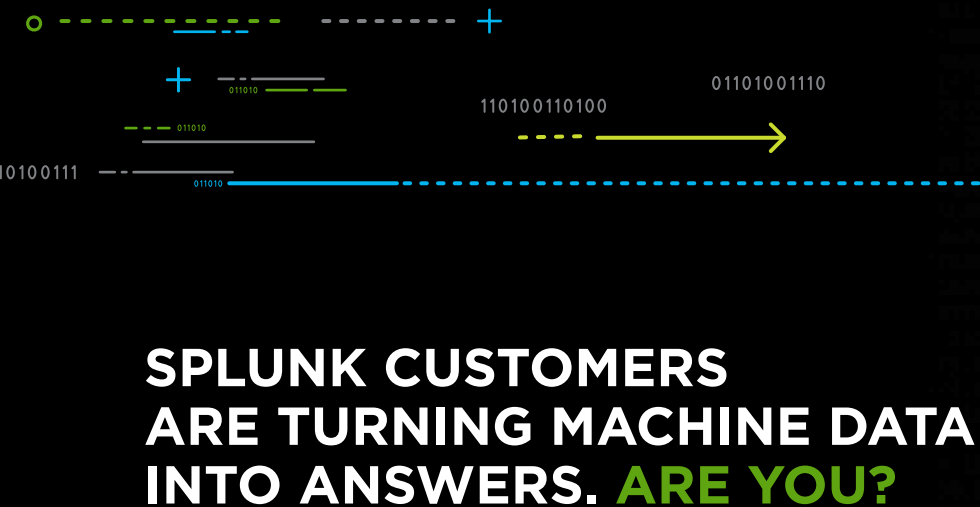
- Reduced business-impacting IT incidents by more than 50 percent
- Slashed mean-time-to-resolve major IT incidents by 32 percent
- Reduced the number of major IT incidents by 23 percent

Today, Micron Technology relies on Splunk ITSI for everything from event management alerting and incident management to problem and change management. The solution is helping Micron not only gain much needed real-time visibility but also save time and reduce the impact of IT incidents on its business.

In addition, Splunk ITSI has expedited the manufacturing IT team’s ability to build dashboards that provide a macro view of the environment. According to Micron’s IT director, “Splunk ITSI enables us to break down the walls of those silos such that the expertise of the entire organization can be used to help each other out.”







# SPLUNK CUSTOMERS ARE TURNING MACHINE DATA INTO ANSWERS. **ARE YOU?**

Machine data has the power to drive new, powerful and unique business insights. By accessing and analyzing massive amounts of data in real time it can propel your career and your business forward, making your company more productive, competitive and secure.

If you would like to learn more about Splunk customer success, please visit [splunk.com/customers](http://splunk.com/customers) and try Splunk today [splunk.com/download](http://splunk.com/download).

**splunk**> listen to your data®