

DATA SECRETS REVEALED

A Collection of Security Customer Stories

IT'S NOT
MAGIC.
IT'S SPLUNK.™



4
2 5 7
8



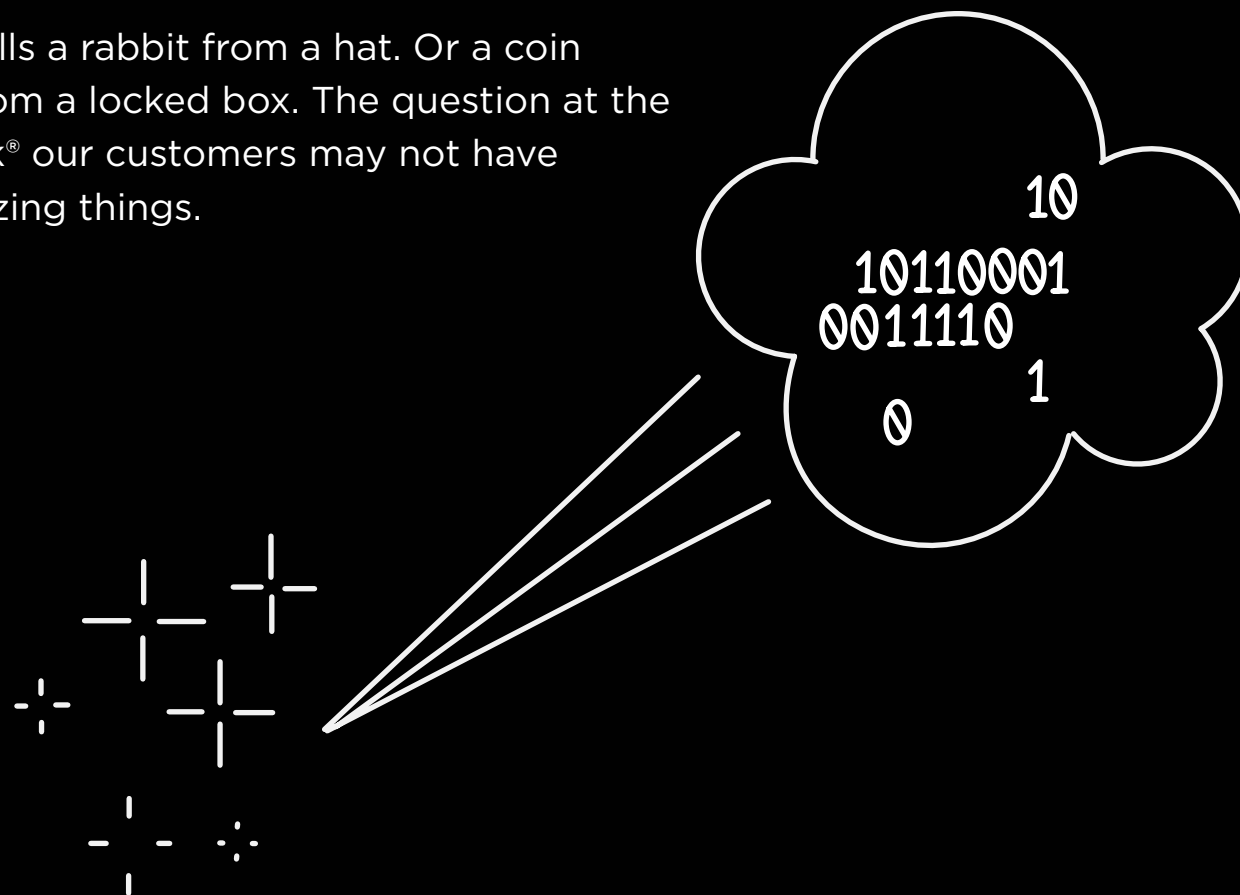
splunk>



HOW DID THEY DO THAT?

We've all seen the magic trick where the magician pulls a rabbit from a hat. Or a coin from someone's ear. Or makes someone disappear from a locked box. The question at the end is always, "How did they do that?" Here at Splunk® our customers may not have rabbits, coins or magic boxes, but they do some amazing things.

Let us show you how.



The Key Element Is Data.

Today, businesses and organizations are generating a tremendous volume of data every day. This abundance of data creates unique challenges and opportunities. Disparate systems, siloed infrastructures and increasing volumes of data can make it difficult, costly and time-consuming to manage IT environments. At the same time, ensuring the security and integrity of data is vital for organizations in protecting sensitive business and customer information, meeting compliance regulations and ensuring uninterrupted business operations.
















That's not all. In industrial settings, gaining real-time insights from data generated by industrial control systems, applications, sensors and connected devices can be challenging. But with the right solutions, organizations can reduce costs, optimize operations, increase uptime and availability of critical industrial and IT assets, better protect from security threats, and make faster decisions to respond to new business opportunities.

How? By Turning Data Into Answers.

Forward-thinking organizations are discovering the value of machine data to deliver better customer experiences, improve products, provide data security, increase operational efficiency, optimize marketing and enhance business processes. That's where you come in. You're an innovator, and you know that it's possible to manage your IT systems, protect your data effectively and efficiently, and derive actionable insights from all of your data in one place. At Splunk, customers like you—from enterprise architects to business analysts, IT directors and CISOs—are turning mountains of machine data into new, unique, valuable and real-time business and operational answers. No hats, rabbits or coins required.

**IT'S NOT
MAGIC.
IT'S SPLUNK.™**

FEATURED SECURITY CUSTOMERS

	DISCOVERY COMMUNICATIONS.....	6
	EQUINIX.....	7
	OHIOHEALTH	8
	INTERMEDIA	9
	DUKE UNIVERSITY	10
	FEDERAL DEPARTMENT	11
	POSTFINANCE	12
	CITY OF LOS ANGELES.....	13
	LUXURY RETAILER.....	14
	MBDA GERMANY	15
	GLOBAL RETAILER.....	16
	UNIVERSITY OF ADELAIDE.....	17
	AMAYA GAMING	18
	GLOBAL ENERGY COMPANY	19
	CHILDREN'S DISCOVERY MUSEUM OF SAN JOSE	20

SECURITY

In an era when businesses and organizations are generating a tremendous volume of data every day, ensuring the security and integrity of that data is paramount. Data security is vital for organizations in protecting sensitive business and customer information, meeting compliance regulations and ensuring uninterrupted business operations.

With the right solutions, organizations can protect their data effectively and efficiently, no matter how much data and where it is—at rest or in motion. A secured infrastructure equates to greater operational efficiencies, better insight and higher customer satisfaction.

At Splunk, our customers are turning mountains of machine data into business and security insights. Find out more: splunk.com/customers

IT'S NOT
MAGIC.
IT'S SPLUNK.™





MEDIA AND ENTERTAINMENT

DISCOVERY COMMUNICATIONS

SPLUNK USE CASES:
SECURITY
IT OPERATIONS

"We needed a versatile SIEM platform that could consume the security contextual data from across our environment, out of the box. Splunk Enterprise Security has given us real-time visibility into everything from malicious exploits like advanced persistent threats and phishing attacks to administrative rights, access authentication and anomalies."

Manager of Platform Operations, Discovery Communications

Discovery Communications Gains Full Operational Visibility Into Security Posture and Critical Services

For 30 years, Discovery Communications has been dedicated to satisfying curiosity and entertaining viewers with high-quality content through its global television brands. The company needed to ensure compliance, bolster its security posture and to give staff—from administrators to C-level leadership—full operational visibility into the health of its online services, and is using Splunk Enterprise to do so.

BUSINESS IMPACT

- Eliminated legacy platform and improved awareness, detection and investigation of internal and external threats
- Enhanced reliability
- Improved operational and cost efficiencies with automated remediation

Discovery initially deployed Splunk Enterprise to aggregate logs for compliance verification, which the software platform did effectively. More recently, Discovery deployed Splunk Enterprise Security (ES) to replace a legacy security information and event management (SIEM) solution and to improve forensic investigations. And, finally, the Splunk IT Service Intelligence (ITSI) solution was added to provide service-centric health reporting to various constituencies within the company.

DISCOVERY COMMUNICATIONS REACHES 3 BILLION CUMULATIVE VIEWERS IN MORE THAN 220 COUNTRIES AND TERRITORIES.

"From day one, Splunk Cloud has given us actionable, data-driven intelligence. With Splunk Enterprise Security in the cloud, we're getting comprehensive SIEM functionality, the economics and simplicity of software as a service, and outstanding availability and security. As more employees use the Splunk platform, we're sure to find important new use cases beyond securing our infrastructure."

Chief Information Security Officer, Equinix

TECHNOLOGY
EQUINIX
SPLUNK USE CASES:
SECURITY

Innovative Cloud-Based SIEM Deployment Delivers Actionable Security Intelligence for Equinix

Security is of paramount importance at Equinix, as thousands of companies worldwide rely on its datacenters and interconnection services. To gain a unified view across its security infrastructure, Equinix needed a cloud solution with centralized visibility and security information and event management (SIEM) functionality that could be implemented easily, quickly and without significant operational effort. It uses Splunk Cloud and Splunk Enterprise Security (ES) as its SIEM platform.

BUSINESS IMPACT

- Full operational visibility
- 50 percent TCO savings compared to an on-premises based legacy SIEM deployment
- Achieved 30 percent faster response to security incidents

With Splunk ES and Splunk Cloud, the security team can now reduce the 30 billion raw security events to about 24,000 indicators of compromise and then to 20 actionable alerts, thus providing actionable security intelligence. With all the data aggregated within the Splunk platform, the security team can cross-reference data between systems, enabling them to research, investigate and respond to incidents 30 percent faster than before.

EQUINIX CONNECTS THE WORLD'S LEADING BUSINESSES TO THEIR CUSTOMERS, EMPLOYEES AND PARTNERS IN 44 MARKETS ACROSS FIVE CONTINENTS.



“Our security information and event management (SIEM) was just a SIEM, whereas Splunk is a data analytics platform with SIEM capability. Particularly when we have to dig through logs or look at internet usage reports, it’s just much faster to do it with Splunk Enterprise. We can ask any question and, with the right data, we can provide an answer with Splunk software.”

Manager, Infrastructure Technologies, OhioHealth



HEALTHCARE
OHIOHEALTH

SPLUNK USE CASES:
SECURITY
IT OPERATIONS



OhioHealth Accelerates Incident Investigations With Real-Time Data Analytics

OhioHealth relies on a networked environment to provide seamless and secure access to patient medical records, telemedicine and other healthcare services. OhioHealth wanted a solution that would work across data silos to consolidate security tools, build an industry-leading security program and provide an easy means of communicating potential risks to the organization. OhioHealth’s security operations team deployed Splunk Enterprise to do so.

BUSINESS IMPACT

- Accelerated incident investigations
- Savings of about \$5,000 per phishing session
- Avoidance of up to \$30,000 in annual maintenance for Active Directory audit software

Once logs and other data began to flow into Splunk Enterprise, the team used the solution to better protect its infrastructure and ensure regulatory compliance to HIPAA and other requirements. Splunk software has helped accelerate incident investigations, enhance event correlation and provide automated, real-time data analytics.

The OhioHealth networking group sends log data from all routers and switches to be indexed in Splunk Enterprise. The group was immediately rewarded with far deeper insight into network operations, and it plans to feature the Splunk solution as part of its next-generation network operations center.

**OHIOHEALTH HAS
11 HOSPITALS,
MORE THAN 50
AMBULATORY
SITES, HOSPICE,
HOME-HEALTH,
MEDICAL EQUIPMENT
AND OTHER HEALTH
SERVICES SPANNING
A 47-COUNTY AREA.**

Intermedia Builds an Instant Security Operations Center and Speeds Business Processes

Intermedia’s competitive advantage is delivering enterprise-grade security, 99.999 percent uptime and prompt 24/7 phone support. To meet these goals, the company sought security and Operational Intelligence by collecting and analyzing logs from its datacenters, security devices and endpoints. Splunk Cloud anchors Intermedia’s first security operations center (SOC).

BUSINESS IMPACT

- Stronger security through incisive, enterprise-wide intelligence
- Real-time insights and KPIs into its services delivery
- Cost savings through efficiencies and reduced staffing

Intermedia’s security team displays real-time data in dashboards and sets alerts for questionable events. It accelerates investigations by rapidly querying all data to analyze and scope issues and to determine appropriate courses of action. Splunk Cloud allows administrators to correlate logs from across the enterprise with threat intelligence feeds to contextualize vulnerabilities, build threat profiles and prioritize alerts.

Mindful of the value of data-driven intelligence, the company continues to expand its use cases for Splunk analytics into all facets of its business, enhancing its competitiveness by efficiently meeting its customers’ needs.

INTERMEDIA
IS A ONE-STOP
SHOP FOR CLOUD
BUSINESS
APPLICATIONS.

CLOUD SERVICES
INTERMEDIA
SPLUNK USE CASES:
SECURITY
IT OPERATIONS

“Splunk Cloud gave us a near-instant SOC that delivers comprehensive yet cost-effective security intelligence. I don’t know of another solution providing all-inclusive, data-driven analytics that can allow us to do so much, faster and with less staffing. We’re prepared for the future because there’s nothing we can’t do with our Splunk platform.”

Vice President of Security and Privacy, Intermedia

“We wanted a solution that was not simply a security product. We wanted something that could meet the unique needs of our systems team, our network team, application owners and identity management group. And that’s what we got with Splunk Enterprise.”

Chief Information Security Officer, Duke University



HIGHER EDUCATION
DUKE UNIVERSITY
SPLUNK USE CASES:
SECURITY

Duke University Gains Powerful Security Insights and Fraud Protection

The Duke University IT Security Office was faced with data and usage challenges, including not having a security information and event management (SIEM) solution. Splunk Enterprise was easy to deploy and use, and also flexible enough to meet a wide range of needs across the university.

BUSINESS IMPACT

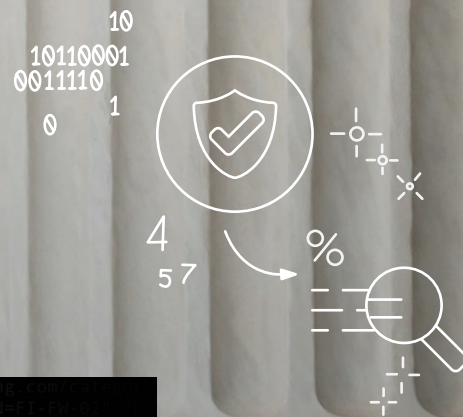
- ➔ Incident investigation and remediation reduced from hours to minutes for enhanced security posture
- ➔ Improved collaboration among formerly siloed departmental IT operations
- ➔ Prevented phishing attacks and payroll fraud

Splunk Enterprise has enabled Duke to move from a reactive to a proactive approach to security, helped automate threat identification and remediation, centralized log management and analysis, streamlined performance monitoring, and made reporting more accessible and quantitative. The Splunk platform also plays a key role in real-time threat analysis and alerting.

The university now also uses Splunk’s geoIP mapping capabilities to distinguish between Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. Early identification of DDoS attacks is critical in combating the ongoing attack and preventing future events.

DUKE UNIVERSITY,
A PRIVATE RESEARCH
INSTITUTION, SERVES
NEARLY 15,000
UNDERGRAD AND
GRADUATE STUDENTS.





US Government Cabinet-Level Department Reduces Costs, Improves Security Posture With Splunk Platform

Citizens expect government agencies to not only spend taxpayer dollars wisely but also make every effort to ensure resilient operations to deliver services effectively. One large U.S. cabinet-level department previously had HP ArcSight, a slow and expensive security information and event management (SIEM) tool that did not stand up to the needs of the agency. Since replacing it with Splunk Enterprise for security and compliance the department has seen benefits.

FEDERAL DEPARTMENT MADE UP OF APPROXIMATELY 40 AGENCIES, UPWARD OF 200,000 HOSTS AND 130,000 USERS.

BUSINESS IMPACT

- Reduced security investigation time from hours to minutes
- Improved security detection, response and remediation
- Proactive security stance and faster incident response

Previously, team members focused on responding to and remediating security incidents after receiving an alert from one of its tools. Now, staff have more time to hunt, and intuitive searches are rewarding because they complete quickly and reveal important insights. For instance, Splunk Enterprise has helped identify and reduce waste, fraud and abuse incidents.



PUBLIC SECTOR

FEDERAL DEPARTMENT

SPLUNK USE CASES:
SECURITY
COMPLIANCE

"Splunk has helped my department save \$900,000 in maintenance this year, which paid for my whole team."

Splunk Architect and Consultant, Federal Department

“Our use of the Splunk platform has grown dramatically and it is now an integral part of our IT operations, providing insights in areas from e-commerce to security and fraud. Ultimately, with Splunk Enterprise, we have improved the protection we offer our customers.”

Head of IT Infrastructure, PostFinance



FINANCIAL SERVICES

POSTFINANCE

SPLUNK USE CASES:

SECURITY AND FRAUD

APPLICATION DELIVERY

PostFinance Delivers Improved Fraud Detection and Enhances Customer Experience

PostFinance provides a full range of financial products to both consumers and merchants, with an established position as the No. 1 payments provider in Switzerland. The bank deployed Splunk Enterprise to improve visibility into its payments processing and online banking services to be more proactive in addressing threats and protecting customers from potentially fraudulent activity.



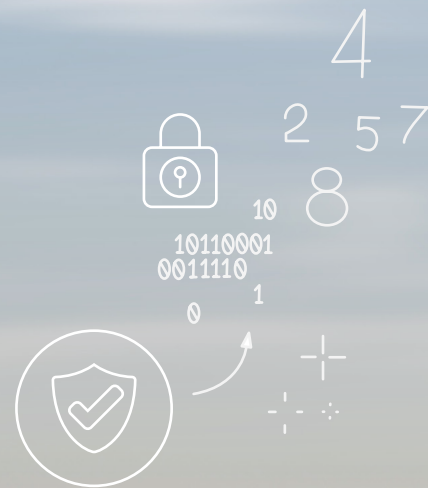
Watch the video: splunk.com/post-finance

POSTFINANCE
IS ONE OF
SWITZERLAND'S
LEADING FINANCIAL
INSTITUTIONS,
WITH JUST UNDER
3 MILLION
CUSTOMERS.

BUSINESS IMPACT

- Streamlined fraud detection across online and in-store transactions
- Real-time Operational Intelligence across its online banking platform
- Better overall visibility into its payments architecture

Splunk Enterprise is used by the fraud management team at PostFinance to provide insight into the online shopping solution used by 11,000 merchants in Switzerland. It monitors the technology at each stage of the buying process, providing useful data for the team to analyze.



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

To protect its digital infrastructure, the City of Los Angeles requires situational awareness of its security posture and threat intelligence for its departments and stakeholders. It sought a scalable SaaS security information and event management (SIEM) solution to identify, prioritize and mitigate threats, gain visibility into suspicious activities and assess citywide risks. After considering available solutions, Los Angeles chose Splunk Cloud and Splunk Enterprise Security (ES).

BUSINESS IMPACT

- Creation of citywide security operations center (SOC)
- Real-time threat intelligence
- Reduced operational costs

Splunk Cloud provides Los Angeles with holistic views of its security posture. Splunk forwarders send raw logs and other data from the city's departments to Splunk Cloud, where they are normalized and returned to the integrated SOC, and then analyzed and visualized in Splunk dashboards. Using pre-built, easily customizable dashboards in Splunk ES, executives and analysts have always-available, real-time situational awareness of security events across the city's networking infrastructure.

**LOS ANGELES HAS
35,000 EMPLOYEES
AND OVER 100,000
ENDPOINTS
GENERATING 14
MILLION SECURITY
EVENTS DAILY.**



PUBLIC SECTOR

CITY OF LOS ANGELES

SPLUNK USE CASES:
SECURITY

"By deploying the Splunk SIEM solution, we enhance our detection and response capabilities to protect the city's critical assets from all manner of cyberthreats and intrusions. By utilizing a cloud solution, our security team can focus on security events rather than deploying and maintaining infrastructure."

Chief Information Security Officer, City of Los Angeles

“There is no other vendor that would have come into our enterprise and helped us to the degree that Splunk did. Most of the others would have just waited around for us to fix our issues, twiddling their thumbs and doing nothing. Splunk was fantastic, a partner, not just a vendor.”

Security Manager, Luxury Retailer



RETAIL

LUXURY RETAILER

SPLUNK USE CASES:

SECURITY

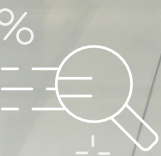
COMPLIANCE

FRAUD

IT OPERATIONS

APPLICATION DELIVERY

10
10110001
0011110
0
1



Luxury Retailer Replaces Legacy SIEM With Analytics-Driven SIEM

Retail companies face many challenges when it comes to protecting their businesses and their customers—from securing online accounts and point-of-sale (POS) systems, to eliminating malware and other vulnerabilities. When one luxury retailer grew concerned about security breaches negatively affecting its customers and brand reputation, it replaced its security information and event management (SIEM) solution with an advanced and reputable alternative—Splunk Enterprise Security (ES).

BUSINESS IMPACT

- Fast implementation: replaced underperforming SIEM in only six weeks
- Added capabilities to prevent security breaches, mitigate fraud and ensure Payment Card Industry (PCI) compliance
- Gained ability to protect customer data and company reputation

Soon after adopting Splunk ES, the company cleaned up its legacy data misconfigurations and captured the data necessary for PCI and security compliance. In addition to its legacy data, the company now has brought more useful and valuable data into Splunk ES to deliver an analytics-driven security operations center.

SPLUNK ENTERPRISE SECURITY REPLACED HP ARCSIGHT, WHICH THE RETAILER HAD RELIED ON FOR 10 YEARS.



MBDA Germany Drives Security Intelligence With Splunk Enterprise Security

MBDA Germany is part of the European MBDA Group, a world leader in missiles and missile systems. The company needed to gain visibility into the security-relevant data across the organization, and selected a solution from the “leader” quadrant in the Gartner Magic Quadrant for Security Intelligence and Event Management (SIEM) solutions, Splunk Enterprise and Splunk Enterprise Security (ES).

BUSINESS IMPACT

- Reduced time to investigate security incidents
- Improved identification and classification of security attacks
- Enhanced overall security posture

MBDA Germany’s main goal of using Splunk Enterprise and Splunk ES is to quickly identify and investigate security threats and attacks. Since deploying Splunk ES, the time to analyze Computer Emergency Response Team (CERT) messages has been reduced from an average of 372 minutes to just 15.

Since deploying the Splunk platform as its security intelligence solution, MBDA Germany has been able to identify a greater number of attacks, many of which would previously have gone undetected.

MBDA GERMANY IS THE LEADING GUIDED MISSILE AND AIR DEFENSE SYSTEMS COMPANY IN GERMANY.

“Splunk dramatically reduces security risks at MBDA Germany. The software helps us to work much more efficiently, gain visibility across our entire network, react more quickly to security breaches and use insights from our data analysis to inform our future security strategy.”

Head of IT and Project Manager, Information Technology, MBDA Germany

Global Retailer Detects Online Fraud With Greater Visibility and Insight

To safeguard its online business, a global retailer needed a single security platform that could quickly detect new fraud techniques, index all fraud and security-relevant machine data, and more quickly present the information to internal teams to identify, investigate and prevent fraud. The company turned to Splunk Enterprise, which it was already using for operational and application management.

BUSINESS IMPACT

- Reduced financial losses from fraud and chargebacks
- Reduced labor costs from fraud investigations
- Reduced security vulnerabilities and improved security posture

With Splunk software, all relevant machine data from the retailer’s e-commerce business is now in a single location for fast searching, correlations and reporting. Investigations now can be completed as rapidly as five to 10 minutes or less.

With the Splunk platform, the retailer’s security and loss prevention teams now have additional context and data integrated into their legacy portal for fraud investigations that can be shared by multiple teams.

A U.S.-BASED DEPARTMENT STORE CHAIN WHOSE ONLINE BUSINESS FEATURES MORE THAN 100 WEBSITES.



RETAIL GLOBAL RETAILER

SPLUNK USE CASES:
SECURITY
FRAUD
APPLICATION DELIVERY
IT OPERATIONS

“Our Splunk solution proves over and over that Operational Intelligence can combat malicious exploits like fraud on e-commerce sites. Fraudsters and cybercriminals may be getting savvier, but with the analytics enabled by our Splunk software, so are we.”

Lead Application Security Engineer, Leading Global Retailer

“Previously, it could take hours to extract and analyze logs to identify security issues—now it can be measured in minutes. Splunk has given us the highest degree of certainty in meeting our immediate and future security needs.”

Information Security Specialist, Information Technology Services,
University of Adelaide

HIGHER EDUCATION
UNIVERSITY OF
ADELAIDE

SPLUNK USE CASES:
SECURITY
IT OPERATIONS
BUSINESS ANALYTICS
INTERNET OF THINGS

University of Adelaide Gains Operational Visibility, Enhances Incident Detection and Resolution

As the University of Adelaide’s large and disparate IT network expands, security remains a significant priority. Its Information Technology Services Group deployed Splunk Enterprise to collect, analyze and secure the university’s growing machine data volume and provide better overall visibility into security log data.

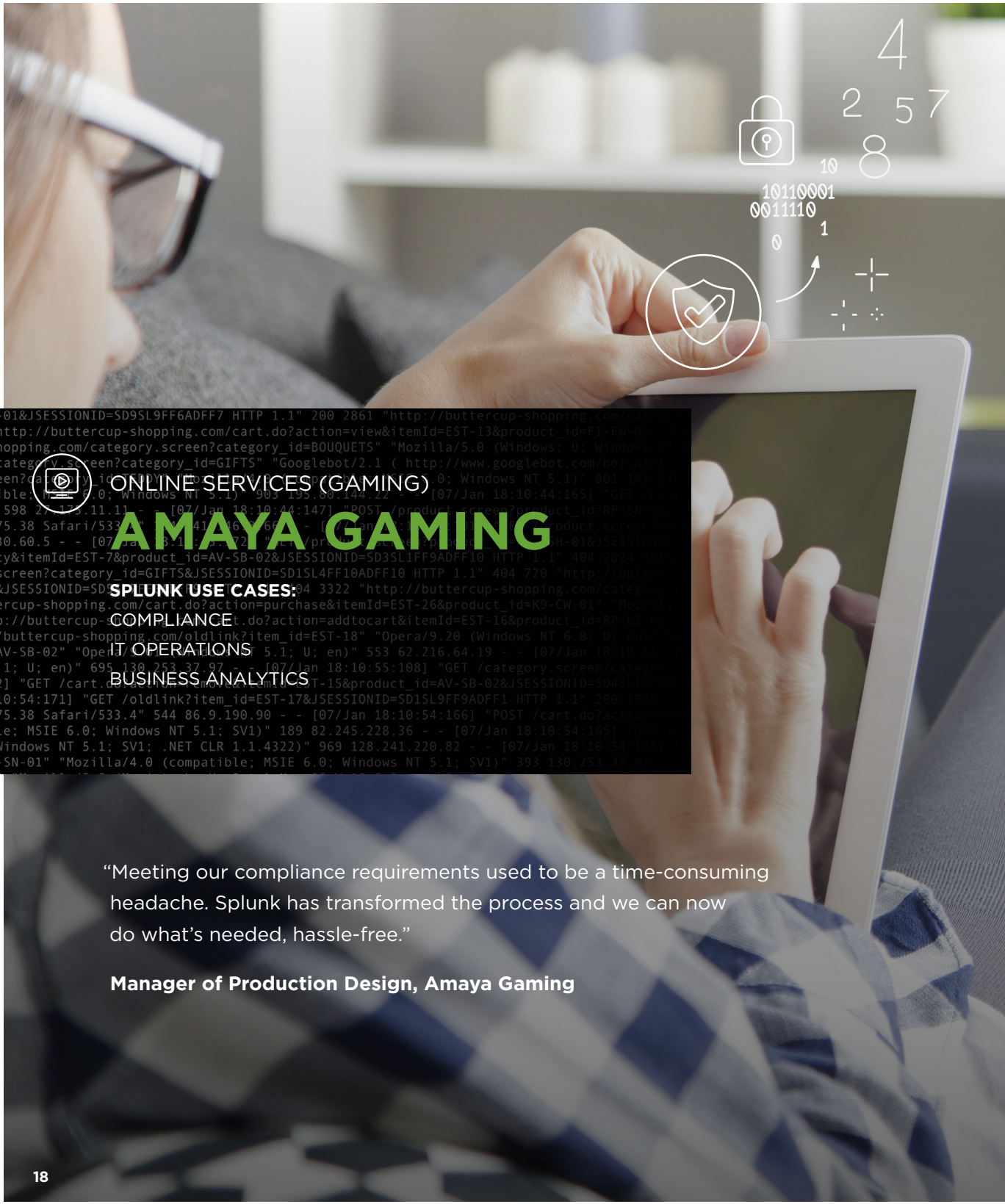
BUSINESS IMPACT

- Hundreds of hours saved in security analyst time annually
- Ensures uptime and service continuity by mitigating security threats
- Faster threat mitigation

An immediate goal of the deployment was to reduce the number of security-related events, in addition to efficiently identifying the initial problem, correlating the associated data and remediating the issue before it became a significant threat. Splunk software now provides enhanced incident detection at the university through numerous security-related searches across all data log sets.

Although it was initially deployed at the University of Adelaide as a security solution to help identify vulnerabilities across the university’s network and continues to provide invaluable insights, the Splunk platform’s wider potential for real-time Operational Intelligence has been proven.

UNIVERSITY OF
ADELAIDE IS
AUSTRALIA’S THIRD
OLDEST UNIVERSITY,
WITH A STRONG
REPUTATION FOR
RESEARCH AND
TEACHING EXCELLENCE
AND PRODUCING
GRADUATES THAT
MAKE AN IMPACT
ON THE WORLD.



Amaya Gaming Experiences Smarter Development and Reduces Compliance Headache

Amaya Gaming was faced with a fragmented infrastructure, making it difficult to consolidate information from more than 80 applications. In addition, Amaya needed to conform to strict compliance requirements that prohibited the developer team from accessing production sites. Splunk Enterprise has enabled Amaya to streamline several time-consuming and potentially costly processes—from meeting compliance requirements to troubleshooting incidents and errors.

BUSINESS IMPACT

- Elimination of compliance challenges
- Critical insights into development and performance
- Improved DevOps collaboration

In 2012, Amaya Gaming acquired Ogame, a B2B online poker network. Ogame was already using Splunk software to proactively optimize its online gaming services. Amaya began to use the platform for Operational Intelligence to support its production sites, sending the machine data produced by all of its applications into Splunk Enterprise. The company also uses Splunk Enterprise to index, search and analyze the data from as much third-party infrastructure as possible.

Thanks to the Splunk platform, Amaya has improved the availability of its services. By analyzing data, seeing trends, visualizing operations data and spotting errors, the company continues to ensure a high-quality customer experience.

A LEADING PROVIDER OF TECHNOLOGY-BASED PRODUCTS AND SERVICES IN THE GLOBAL GAMING AND INTERACTIVE ENTERTAINMENT INDUSTRIES.

“Meeting our compliance requirements used to be a time-consuming headache. Splunk has transformed the process and we can now do what’s needed, hassle-free.”

Manager of Production Design, Amaya Gaming

“We discovered that we could accomplish the same tasks as four different applications with a single instance of Splunk Enterprise. The TCO of Splunk is approximately 400 percent less. We are very pleased with our investment and the capabilities of Splunk software.”

**Supervisor, SCADA Infrastructure and Cybersecurity,
Global Energy Company**



ENERGY
**GLOBAL ENERGY
COMPANY**

**SPLUNK USE CASES:
SECURITY
INTERNET OF THINGS**



Supporting SCADA Systems to Secure Pipeline

One energy company has approximately 50,000 miles of pipeline across the United States, controlled by complex supervisory control and data acquisition (SCADA) systems and embedded industrial devices. It needed to improve reliability and security of systems deployed within SCADA and adopted Splunk software to increase operational and security visibility.

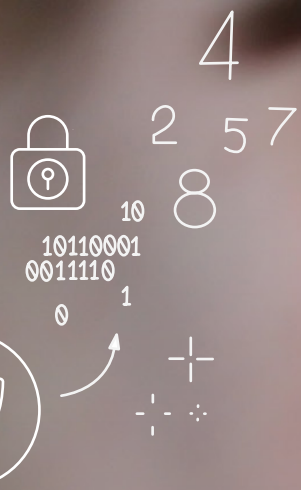
BUSINESS IMPACT

- Increased operational and security visibility
- Improved system availability and increased pipeline visibility
- Reduced security investigation time

In terms of security, Windows security, Intrusion Detection System (IDS) and vulnerability scan logs are helpful in providing important visibility into vulnerabilities so that staff can proactively remedy them. If there is a security issue affecting multiple endpoints, Splunk Enterprise helps accomplish the security investigation in about one hour, down significantly from as many as 12 hours required in the past.

With Splunk Enterprise, the company has dramatically reduced time to investigate incidents, increased SCADA system stability and overall pipeline visibility, and expanded its reporting and alerting capabilities to proactively warn users about control system stability.

**LEADING ENERGY
COMPANY PROVIDES
MIDSTREAM ENERGY
SERVICES TO
PRODUCERS AND
CONSUMERS OF
NATURAL GAS, NGLS,
CRUDE OIL, REFINED
PRODUCTS AND
PETROCHEMICALS.**



Children's Discovery Museum of San Jose Adopts Splunk 'Operational Idea Factory'

Since its inception, the Children's Discovery Museum (CDM) has welcomed millions of visitors and has offered new exhibits each year that respond to children's diverse educational needs. As a nonprofit, CDM faced challenges running its IT and security operations with limited staff and budget. Then it deployed Splunk Enterprise.



Watch the video: splunk.com/childrens-discovery

BUSINESS IMPACT

- Increasing protection from fraud and malicious security threats
- Reducing spam by 98 percent
- Enhanced cybersecurity and always-on operations

Nonprofit organizations face many of the same challenges as their private sector peers. Security—especially messaging security—including guarding against unsolicited and fraudulent email, are critical priorities. Cybercriminals test vulnerabilities and are willing to attack any organization, even a children's museum.

As CDM began to learn more about how Splunk Enterprise processed and stored data, it began to experiment. The museum had a significant spam problem, and by looking at expressions and functions inside of Splunk software, it was able to reduce spam by about 98 percent after only a couple of weeks.

NONPROFIT CHILDREN'S DISCOVERY MUSEUM OF SAN JOSE

SPLUNK USE CASES: SECURITY AND FRAUD IT OPERATIONS

"Splunk's technology is like an 'operational idea factory' that continuously gives us new ideas about how to do more with less and to identify and cut unnecessary costs."

Visiting Principal Engineer, Children's Discovery Museum

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

The massive amounts of data generated by multiple systems and disparate networks can be overwhelming. But when you can access and analyze data in real time it can propel your business forward, making your company more productive, competitive and secure. Learn more about how security teams investigate, respond and adapt to threats with **analytics-driven** security. It's Not Magic. It's Splunk.™

If you would like to learn more about Splunk customer success, please visit splunk.com/customers.

We'd also love for you to share your story with us at tellusyourstory@splunk.com.



IT'S NOT
MAGIC.
IT'S SPLUNK.™

For more magical moments, visit splunk.com

splunk> listen to your data