BANKING ANALYTICS AND DATA INSIGHTS

Customer Success on the Frontlines

The financial services industry faces many challenges, from security and financial crime to credit and debit card fraud, payment card industry (PCI) compliance and more.

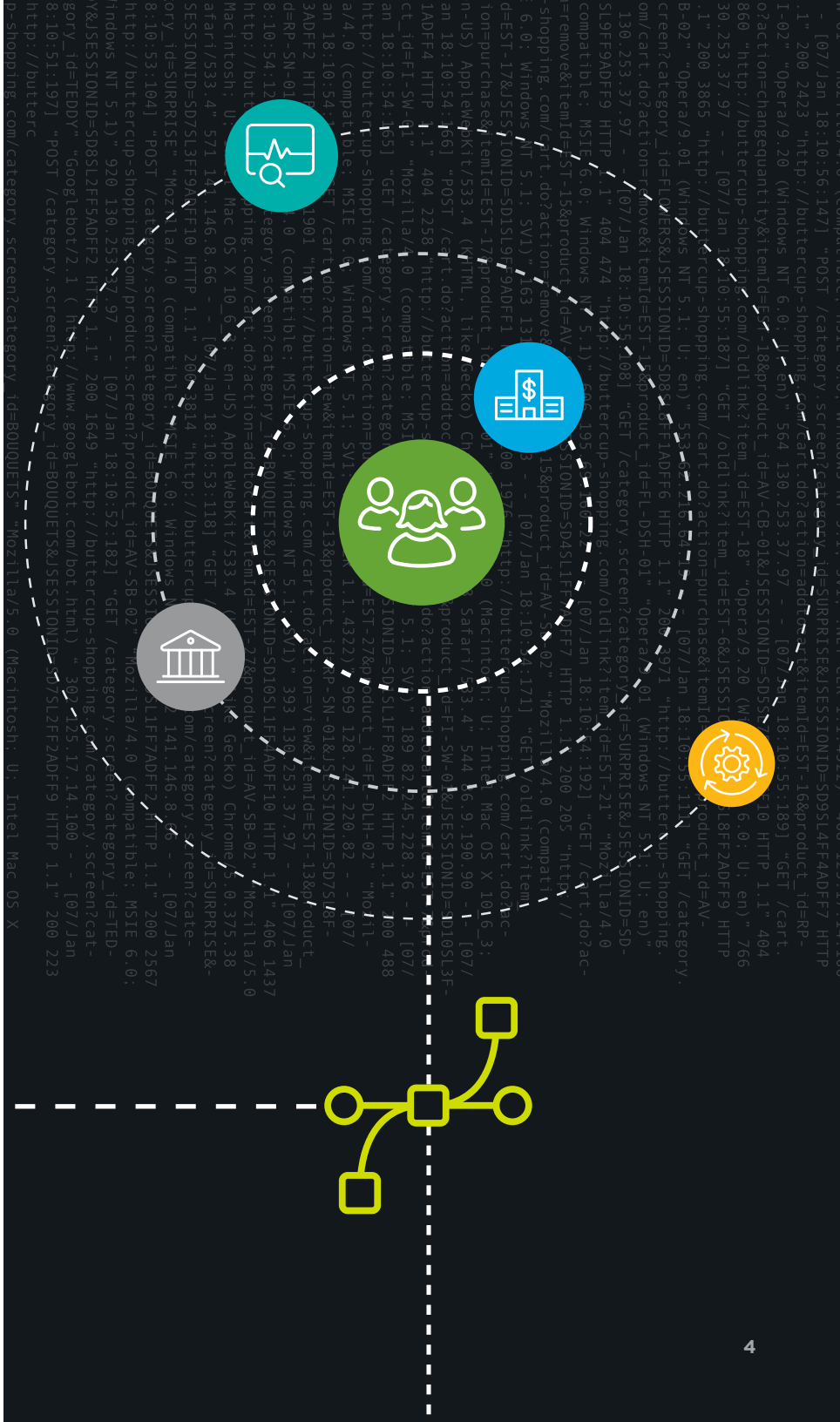
More so than many other industries, financial services customers require the real-time ability to correlate across huge volumes and varieties of data to take immediate action.

This e-book illustrates some of the challenges that financial services customers are solving with Splunk solutions. The uses are broad and vary considerably, and this is just the tip of the iceberg since Splunk is continuously pushed to new limits by customers' creativity.

With Splunk, customers are achieving their goals with individual ingenuity and by harnessing the power of their machine data, in the cloud, on-premises and hybrid environments. And they're gaining valuable insights across multiple use cases, including IT, security, fraud and application analytics. Organizations are driving business transformation to deliver better customer experiences, increase profitability, minimize risk and improve security.

You're an innovator. Whether your role is in DevOps, IT, cybersecurity, fraud, financial crime, and you work on a trading desk, in the 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.

TABLE OF CONTENTS



Aflac Adopts Splunk Platform for Analytics-Driven Security

Executive summary

Aflac is the leading provider of voluntary insurance in the U.S. Facing an increase in the volume and velocity of security threats, Aflac needed a new analytics-driven security approach to protect its customers, nearly 10,000 employees and brand reputation. The company adopted the Splunk platform to sit at the heart of its internal Threat Intelligence System (TIS). Since deploying Splunk Enterprise Security (ES) and Splunk User Behavior Analytics (UBA), Aflac has seen benefits, including:

- Two-week enterprise-ready implementation
- Blocking more than two million security threats in one six-month period
- Saving 40 hours monthly by replacing manual data collection and reporting, enabling teams to focus on proactive security monitoring and analysis

Why Splunk

As Aflac enters new markets and offers new services, the company needs to adapt its security program continuously to match a rapidly changing threat landscape that includes everything from spear-phishing to the proliferation of malware. Prior to adopting the Splunk platform, Aflac relied on a legacy security information and event management (SIEM) solution, but the company required a stronger threat intelligence platform to detect and respond to attacks adequately.

According to D.J. Goldsworthy, director of Security Operations and Threat Management for Aflac, "With our previous SIEM, you had to know the data exceedingly well before you could take action, whereas Splunk helps you know your data very quickly. Splunk made us much nimbler and enabled us to show value to all of our stakeholders quickly."

Industry

- Financial services

Splunk Use Cases

- Security
- Fraud

Challenges

- Needed a robust security platform to protect customers, 10,000 employees and brand reputation
- Wanted to eliminate manual data collection and reporting to focus on proactive security investigations

Business Impact

- Blocked more than two million security threats in one six-month period
- Orchestrated threat intelligence across 20 security technologies sitting within TIS
- Automated threat hunting and 90 percent of security metrics process in just two months
- More than 40 hours saved monthly
- TIS in place within five months, one month ahead of schedule

Data Sources

- Operating systems
- Next-gen firewalls
- Intrusion detection systems
- Email security
- Endpoint security agents
- DNS firewall
- Web application firewalls
- Other various application and security solution logs

Splunk Products

- Splunk Enterprise Security
- Splunk User Behavior Analytics

Initially, Aflac stood up Splunk ES for threat hunting. "Our proof of concept, in essence, was using Splunk ES for our threat hunting use cases, and the time to value far exceeded our expectations," Goldsworthy says. "We were able to do extraordinary things in a very short period of time to detect advanced threats. Ultimately, that was the decision point for us to make a much larger investment in Splunk ES and UBA across our different security use cases."

Immediate return on investment

According to Goldsworthy, the time to implement the Splunk platform and get it enterprise-ready was short – just a couple of weeks. "That was quite surprising, given the volume of data sources we were bringing in and the number of use cases that we wanted to get in place," Goldsworthy explains. "With Splunk, we saw immediate return on investment."

Today with Splunk ES in Aflac's security operations center (SOC), the company has saved time for numerous full-time employees. "We calculate that we save more than 40 hours a month in terms of doing reports that used to be manual that are now fully automated," Goldsworthy says. "Splunk has made it very easy to ingest data from different sources and then present them in a way that is meaningful to stakeholders, such as our board or other leadership."

Six teams composed of approximately 40 individuals rely on the Splunk platform to manage broad security use cases, including threat hunting, threat intelligence, security operations, incident response, application security, security administration and fraud.

"We implemented Splunk first for threat intelligence and then security operations, and realizing how versatile the solution is, we determined that that the logical next step for us was to apply that to fraud," Goldsworthy says.

Automating threat intelligence

Aflac put its TIS in place within five months, finishing one month ahead of schedule. The system provides tactical and strategic functions, adding automation to create efficiencies in the daily threat data feed, saving time and reducing errors. The system

"We were able to do extraordinary things in a very short period of time to detect advanced threats. Ultimately, that was the decision point for us to make a much larger investment in Splunk ES and UBA across our different security use cases."

D.J. Goldsworthy, Director of Security Operations and Threat Management
Aflac Incorporated

automatically consumes indicators of compromise (IoCs) from more than 20 different threat intelligence sources and provides automated confidence scoring and risk profiling of each IoC. This enables Aflac to track thousands of IoCs and perform real-time correlation against network and system logs in its Splunk security analytics platform. Then, SOC analysts can rapidly respond to potential incidents. Within one six-month period, Aflac was able to block more than two million security threats, with fewer than 12 false positives.

"From the perspective of an individual policyholder, I know they would want to know that we're doing everything we can to help keep their information safe. We are paying close attention to how we manage our own information as well as how we manage their personal information, and that's something that Splunk allows us to do," says Ben Murphy, vice president of information security, Aflac.

Anomaly detection adds value

As businesses add contractors and others with privileged access to networks, it becomes very difficult to understand whether everyone is in compliance with all of the security policies and best practices or if there are any risks hidden in these activities. "Splunk UBA provided another rich layer of detection to Aflac's security program, which is capable of identifying anything that happens outside of the normal behaviors we typically observe," Goldsworthy says.

Blackstone

Automating Malware Investigation at One of the World's Leading Investment Firms

Executive summary

As one of the world's leading investment firms with more than 21 offices spanning the globe, it's not uncommon for the security team at Blackstone to see as many as 30 to 40 malware alerts in a single day. Blackstone's Incident Response team investigates each malware alert as if a compromise has already occurred, a process that requires 30 to 45 minutes to address each alert fully if done manually. Considering the volume of alerts and the potential for inconsistency in any manual process, Blackstone knew there had to be a better way. Since deploying Splunk Phantom, Blackstone has seen benefits including:

- Processing malware email alerts in about 40 seconds versus 30 minutes or more
- Ensuring a repeatable and auditable process for investigating malware alerts

Why Splunk Phantom

Despite Blackstone's expertise in scripting and automation, developing this capability across a large set of security vendors became difficult to maintain. As each vendor changed the API for its product, the automation scripts had to change as well. To address this challenge, Blackstone began the search for a commercially available solution that could tie together its existing security products to reduce the response and remediation gap caused by limited resources, a widening attack surface and a complex technology infrastructure. Blackstone selected Phantom as its security orchestration, automation and response platform.

Industry

- Financial services

Splunk Use Cases

- Security orchestration, automation and response (SOAR)

Challenges

- Difficulty maintaining automation scripts across large number of security vendors
- Needed to tie together existing security products to reduce the response and remediation gap

Business Impact

- Dramatically reduce time to investigate malware alerts
- Drive accuracy and consistency in the incident response process
- Incident response automation enables the team to investigate issues faster

Splunk Products

- Splunk Phantom Enterprise Edition

Security automation and orchestration with Phantom

Using Phantom's Python-based Apps and Playbooks, Blackstone is now able to execute actions quickly, ensuring a repeatable and auditable process for investigating malware alerts. A Phantom Playbook is triggered when an email malware alert is received. Due to the lack of context in these alerts, Phantom's first order of business is to query Blackstone's security information and event management (SIEM) solution for all recipients, then Active Directory to collect context from the profiles of all affected users – business group, title and location. Next, Phantom orchestrates a "hunt file" action in Carbon Black and queries iSightPartners' threat intelligence database before concluding with a file reputation check on VirusTotal and an assessment by Cylance's Infinity model. This information is immediately presented back to the security team in a quick-analysis format for review and action.

Starting with a well-defined manual process is essential for automation, and has allowed Blackstone to quickly implement Phantom Playbooks. Once the Blackstone team was familiar with Phantom's platform, they were able to write Playbooks in a matter of hours. Blackstone already has a roadmap for additional use cases such as automating time-consuming operational tasks and addressing additional incident response scenarios. As a next step, Blackstone plans to create remediation Playbooks, which would allow analysts to take immediate action based on the initial Playbook result. Such actions could include additional investigation tasks, notifying users, or even isolating hosts, which would be integrated with multi-factor authentication to ensure the action is properly authorized.

Fast and accurate resolution of malware alerts

With Phantom, Blackstone has been able to dramatically reduce the time required to investigate malware alerts. By the team's estimate, the time needed to complete the manual process ranged from 30 to 45 minutes. The same process, automated with a Phantom Playbook, completes in less than one minute, freeing the team to focus on analysis and resolution.

"Automation with Splunk Phantom enables us to process malware email alerts in about 40 seconds versus 30 minutes or more."

Adam Fletcher, CISO
Blackstone

Equally important, Phantom drives accuracy and consistency in the incident response process. In the past, as alert volume increased, analysts tended to become overwhelmed with information, potentially causing them to overlook key indicators. Similarly, experienced analysts might have been tempted to make "gut calls" based on previous incidents and incomplete information. With a Phantom Playbook, the same data is gathered for every alert, and every alert is investigated and memorialized the same way, every time.

As the first community-powered security automation and orchestration platform, Phantom gives Blackstone the flexibility to address its dynamic network. The Python-based Apps and Playbooks are easy to develop, and the Blackstone team shares those responsibilities across different integrations. The Phantom platform then ensures that both the Apps and the Playbooks integrate seamlessly with one another.

Automating incident response with Phantom has resulted in a number of improvements at Blackstone, ultimately allowing the team to spend less time performing tedious, repetitive tasks, investigate issues faster and drive consistency to ensure a fast, accurate result.

FINRA Protects American Investors With Splunk Cloud and AWS

Executive summary

FINRA — the Financial Industry Regulatory Authority — regulates one critical part of the securities industry — brokerage firms doing business with the public in the United States. FINRA processes and analyzes massive amounts of data, and one challenge is to protect that data against new and unexpected threats. FINRA's security information and event management (SIEM) solution, despite high costs, was providing limited functionality. Migrating to Splunk Cloud, Splunk Enterprise Security (ES) and Amazon Web Services (AWS) has provided FINRA with benefits including:

- The ability to ingest data from 170 different applications and run ad hoc queries
- Flexible scaling in a pay-per-use model matching cost to demand
- Unprecedented transparency into every aspect of the computing environment

Why Splunk

Every day in the United States, as many as 100 billion securities market financial transactions take place, involving billions of investors' dollars. A Congressionally authorized not-for-profit organization, FINRA oversees market integrity.

"We bring in tons of data, every order, quote and transaction in almost every equities and options market in the United States, and we look for abnormalities," says Gary Mikula, senior director of cyber and information security at FINRA. "There were so many other logs we wanted, like badge information and different access logs, and our SIEM couldn't ingest that data. Secondly, it didn't provide a flexible user interface allowing us to query the data how we wanted."

Industry

- Financial services

Splunk Use Cases

- IT operations
- Security
- Log management

Challenges

- Needed central logging and ad hoc querying capabilities for massive amounts of data from many different types of logs

Business Impact

- Ingest massive amounts of data from diverse access logs
- Run ad hoc queries with central logging, dashboard access
- Visibility into most U.S. stock and options market transactions
- Gain cost and operational efficiencies with Splunk on AWS
- Protect investors from fraud, foster market transparency

Data Sources

- Amazon Kinesis Data Firehose
- Amazon CloudWatch
- AWS CloudTrail
- AWS IAM
- AWS RDS
- AWS Config
- Amazon Simple Storage Service (S3)
- Amazon Elastic MapReduce (EMR)
- Windows and Linux syslog data
- Firewalls
- VPN
- Proxies
- 170 enterprise applications

Splunk Products

- Splunk Cloud
- Splunk Enterprise Security
- Splunk App for AWS

Searching for a better solution, FINRA considered several SIEMs. The products could generate alerts, but they didn't significantly improve data ingestion or analysis. Then Mikula attended SplunkLive! in Washington, D.C., and found what he was looking for — a means to capture, index and correlate big data from all of FINRA's desired sources in real time, and customize queries through flexible dashboards.

"The competitors were playing catch-up to the capabilities that were already in Splunk," Mikula says. "We didn't want to play that game."

All-in on cloud

Already impressed by the capabilities of Splunk Enterprise and Splunk Enterprise Security (ES), FINRA learned that Splunk Cloud had just come on the market and decided to become its first big customer. The pay-per-use cloud model lets FINRA match its computing costs to demand fluctuations. And instead of spending months building out an environment, FINRA leveraged the mature data-collection agents within Splunk to start consuming data within days of signing the contract. Today, Splunk ingests logs from 170 different applications and AWS Services, including Amazon Simple Storage Service (S3), Amazon CloudWatch, AWS Config and AWS CloudTrail. "No SIEM could match this," Mikula says.

Powerhouse design

Magnifying the power of FINRA's Splunk Cloud solution is integration with Amazon Web Services. AWS Lambda lets FINRA run code without provisioning or managing servers, paying only for the compute time consumed. Amazon Kinesis Data Firehose, a fully managed service, delivers real-time streaming data to Splunk. Mikula calls Amazon Kinesis Data Firehose an ideal solution for creating subscriptions filters to reliably, securely, quickly and cost-efficiently move AWS logs into the Splunk solution for analysis. This capability benefits developers and network staff as well as security specialists, bridging silos.

"It's made a partnership between our security and operations teams," Mikula says. "We have a common goal of wanting the same logs. Now we have a single place to ingest and consume them."

"We are putting our crown jewels — our ability to take every transaction every day on almost every U.S. stock and options market and analyze that data in the cloud — and we are using Splunk to assure that it is secure. Splunk and AWS together give us an unparalleled ability to protect investors."

Gary Mikula, Senior Director, Cyber and Information Security
FINRA

Such efficiencies keep FINRA ahead of evolving threats by enabling teams to analyze data flexibly. FINRA is one of the biggest users of Amazon's EMR Hadoop framework; deploying the Splunk agent onto this platform-as-a-service provides information that allows FINRA to optimize resource allocations. What's more, FINRA sunset a dedicated third-party billing tool and replaced it with its own process for ingesting the data into Splunk. With Splunk Cloud, FINRA has better analytics and reporting, which has led to better project tracking of AWS Services and reduced costs. "We are more effectively managing our cloud costs using our Splunk solution and at less than five percent of the dedicated tools price tag," Mikula adds.

In addition to its commitment to cloud computing, FINRA embraces open source software development, sponsoring multiple open source projects in big data, DevOps and quality assurance. Mikula's team even built a tool to collect AWS CloudTrail logs and ingest them into Splunk.

Pursuing such innovations as serverless computing in the cloud, FINRA finds that it must track logs more than ever. "You can never know what the next threat will be and what questions we'll want to ask our data. Splunk allows us to easily collect all the data we want and query it ad hoc," Mikula says. "What's more, the insights from Splunk allow us to use more AWS services. We are putting our crown jewels — our ability to take every transaction every day on almost every U.S. stock and options market and analyze that data in the cloud — and we are using Splunk to assure that it is secure. Splunk and AWS together give us an unparalleled ability to protect investors."

ING Bank Śląski S.A. Enables Real-Time Business Decisions With Greater Customer Insight

Executive summary

ING Bank Śląski S.A., a member of the ING Group, aims to develop and strengthen its position in the Polish banking sector by providing integrated financial services while remaining a customer-oriented bank. This strategy relies on a number of factors, including cooperation with the ING Group, the use of modern technology, expansion of distribution channels and providing top quality service. The bank wanted to gain real-time visibility into its operations and performance, while enhancing its business analytics. Since deploying Splunk Enterprise, ING Bank Śląski S.A. has seen many benefits, including:

- Greater application availability
- Faster troubleshooting
- Improved insight into customer behavior

Why Splunk

Customers of ING Bank Śląski S.A. have access to the bank's services 24 hours a day, seven days a week. The bank also offers an online banking service, ING BankOnLine, which provides direct and fast access to ING accounts over the Internet, for both individual clients and businesses. ING Bank Śląski S.A.'s IT unit is responsible for providing IT services for the entire bank, which includes maintaining over 200 business applications, of which 20 are mission critical. The IT department needed real-time insight into application performance in order to spot any potential issues to keep these applications running 24/7, with a minimum 99 percent uptime. ING Bank Śląski S.A. chose Splunk Enterprise for its fast time to value and agile analytics and reporting functionality.

Industry

- Financial services

Splunk Use Cases

- Application delivery
- Business analytics
- IT operations

Challenges

- Providing seamless IT services for an entire organization
- Maintain 200 business applications, including 20 mission critical
- Needed real-time insight into application performance

Business Impact

- Increased availability of key applications through improved troubleshooting
- More accurate and efficient forecasting of IT systems capacity
- Greater insight into customer behavior through real-time monitoring of their online journey
- Ability to make better business decisions in real time

Data Sources

- Web application logs
- Mobile application logs

Splunk Products

- Splunk Enterprise

Seamless monitoring and troubleshooting lead to improved uptime

Splunk Enterprise is now used at ING Bank Śląski S.A. by the IT team for application management, which includes monitoring systems for any failures that could result in the unavailability of key business applications. If something goes wrong, Splunk software automatically sends out an alert to notify the appropriate authority and activate the necessary support. Thanks to this improved troubleshooting, the IT team has real-time insight into application performance and can proactively address any potential issues. In addition, the IT team is using Splunk software to monitor the status of all the IT systems and forecast occupancy disk resources.

Making business decisions in real time

The business unit at ING Bank Śląski S.A. also uses Splunk Enterprise, but for business analytics and customer insight. By indexing logs from web and mobile applications, the bank can now see—in real time—which pages within the ING BankOnLine service customers are visiting. This data can also be exported in a range of formats, from Excel spreadsheets to interactive dashboards. The business unit uses this insight to make business decisions, such as tailored product offerings and other marketing activities.

"Splunk Enterprise provides answers incredibly fast and we make business decisions based on the insights it provides."

Software Administration Expert
ING Bank Śląski S.A.

Japan's Online Banking Pioneer Gains Real-Time Visibility Into Cybersecurity Risks

Executive summary

The Japan Net Bank, Ltd. (JNB), Japan's first internet-only bank, offers convenient, around-the-clock online banking services. To follow the common practice in Japan's financial services industry, JNB has joined the Financial Services Information Sharing and Analysis Center Japan (Financials ISAC Japan), a global financial industry resource for cyber and physical threat intelligence analysis and sharing. Since adopting Splunk Enterprise to derive real-time, actionable cybersecurity intelligence from operational data, JNB has seen the following benefits:

- Cyberattack management decreased from hours to minutes
- Prevention of illegal money transfers
- Identified opportunities for new security measures

Why Splunk

Unlike bricks-and-mortar banks, JNB runs a unique banking model that is conducted entirely online. Therefore, cybersecurity is absolutely critical for its business. Previously, the bank's IT Supervision Department found it challenging to manage security risks. The 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, and it needed to share information with Financials ISAC Japan.

Industry

- Financial services

Splunk Use Cases

- Security and fraud

Challenges

- Inefficient log management in the office automation environment
- Labor-intensive and time-consuming risk management processes
- Ineffective analysis of web access logs in detecting unauthorized accesses

Business Impact

- Accelerated analysis of cyberattacks from one-half to one day to a few minutes
- Prevented illegal money transfers
- Gained new opportunities for enhancing cybersecurity

Data Sources

- In-house office automation environment
- Firewall
- Access logs
- Next-generation firewall
- Filtering logs
- Proxy
- Internet banking
- Customer transaction logs
- Request header
- Response header
- Geographical IP address information
- Response time
- WAF detection information

Splunk Products

- Splunk Enterprise

JNB decided to establish an intelligent platform to collect, analyze and deliver real-time insights from machine-generated big data to improve its cyber defense strategies. Among all of the alternatives considered, JNB found that Splunk Enterprise was the best option.

Hours of manual processing reduced to minutes

Splunk Enterprise makes it easy to capture, analyze and act upon the untapped value of the big data generated from JNB's daily operations. Previously taking one-half day or a full day to complete a search or security investigation, the bank now has real-time access to data and completing an investigation is a multi-minute exercise. Captured logs can be searched on demand with only a few keyboard clicks, and with the cybersecurity information shared from Financials ISAC Japan, IT supervisors can easily investigate every case to spot security vulnerabilities in the online banking system before they adversely impact the bottom line.

Splunk Enterprise provides an analytics-driven security solution that enables real-time security monitoring, advanced threat detection, forensics and incident management. It enables JNB to access operational and security intelligence in different views to accommodate specific needs. JNB can easily create consolidated reports and dashboards to view enterprise-wide security risk in a single pane of glass.

Prevention of illegal money transfers

With the Splunk analytics platform in place, JNB was able to implement a new cybersecurity measure that provides all online bank users with a free-of-charge, one-time password. In addition, Splunk Enterprise automatically sends real-time alert emails to JNB's Computer Security Incident Response Team upon detection of any signs of phishing attacks. This has improved the team's capabilities and enabled them to successfully identify more than 20 spoof websites in a single year, achieving a new level of security. JNB has also set up the Security Operations Center to go the extra mile in combatting cyberattacks.

"Visibility is critical to boosting cybersecurity. Splunk Enterprise eases our life in managing various types of logs and reports and allows us to acquire different viewpoints of our online banking business. It has created a brand-new chapter in the cybersecurity history of JNB."

Kenji Ninomiya, Senior Manager, IT Planning Department / JNB-CSIRT
The Japan Net Bank, Ltd.

Opening up new cybersecurity possibilities

"The Splunk solution enables JNB to lead the way in cybersecurity and become a role model in Japan's banking industry," says Kaz Ozawa, assistant manager, IT Planning Department, Cyber Security Office / JNB-CSIRT, The Japan Net Bank, Ltd. The company is also planning to extend powerful Splunk analytics to a broader range of applications, including the detection of unauthorized accounts and financial crimes, monitoring of illegal deposits and withdrawals, as well as machine learning-based detection of illegal money transfers.

"Visibility is critical to boosting cybersecurity," says Kenji Ninomiya, senior manager, IT Planning Department / JNB-CSIRT, The Japan Net Bank, Ltd. "Splunk Enterprise eases our life in managing various types of logs and reports and allows us to acquire different viewpoints of our online banking business. It has created a brand-new chapter in the cybersecurity history of JNB."

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

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

ORRSTOWNBANK

Orrstown Bank Invests in Splunk® Cloud for Security and Business Intelligence

Executive summary

With more than $1.2 billion in assets, Orrstown Financial Services, Inc. and its wholly-owned subsidiary, Orrstown Bank, provide a full range of financial services through 22 locations throughout Pennsylvania and Maryland. With a need to comply with demanding security regulations, Orrstown Bank wanted a security solution that could provide visibility into its complex hybrid IT infrastructure, identify and resolve threats, and provide required uptime and compliance. Since deploying Splunk Cloud, the bank has seen benefits including:

- Improved operational efficiency and customer satisfaction
- Estimated 50 percent reduction in fraud losses
- Enhanced security posture

Why Splunk

Initially, Orrstown Bank relied on a security services provider that delivered basic security information and event management (SIEM) functionality around the bank's security devices. Unfortunately, the security service could not offer enough intelligence for the bank's security team to rapidly identify incidents or respond to requests from regulators.

"Our security provider is a one-size-fits-all solution designed for community banks, which did not give us long-term trending and analytics," says Andrew Linn, SVP, chief information security officer, Orrstown Bank. "We needed to augment its monitoring to properly defend the bank against threats and fraud. We wanted greater visibility to detect both internal and external threats and to collect forensic evidence to understand and neutralize them. But our business is banking, not running a datacenter, so we want as little on-premises infrastructure as possible."

Industry

- Financial services

Splunk Use Cases

- Security and fraud
- Business analytics
- IT operations

Challenges

- Protect the bank and its customers from the growing threat of debit and credit card fraud
- Needed to identify and respond to internal and external security threats
- Obtain the maximum value for IT spend by using as much cloud-based or off-site services as possible
- Consolidate operational and security analytics into one platform

Business Impact

- Faster detection of potential fraud, malware or anomalous behavior
- Estimated 50 percent reduction in fraud losses and improved operational efficiency
- Bolstered security posture thanks to cost-effective SIEM functionality
- Business value gained from improved security, performance and financial oversight of ATMs
- Able to meet regulatory compliance mandates
- Enhanced customer experience

Data Sources

- ATM devices
- Debit card transaction history
- Perimeter firewalls and VPN servers
- Internet proxy
- IDS/IPS systems and routers
- On-premises and AWS servers
- Microsoft Azure, web servers and Active Directory

Splunk Products

- Splunk Cloud

Prior to Orrstown, Linn and his colleagues had worked for some of the world's largest financial institutions and were familiar with Splunk Enterprise. Splunk Cloud, which delivers all the functionality of Splunk Enterprise as a cloud service, eliminated the need for an onsite deployment. Another important factor was Splunk Cloud's 100 percent uptime SLA and its SOC2 Type II certification.

"Rather than buy a dedicated SIEM solution and numerous monitoring solutions, we deployed the Splunk Cloud platform, which slashed our administrative overhead," says Linn. "We're aggregating data from over 60 sources, mostly on-premises servers and security systems, and are constantly discovering new use cases for Splunk software."

Centralized visibility into security and business processes

Splunk Cloud took just two weeks to deploy at Orrstown Bank and is providing the bank with real-time, centralized visibility into its security, network and business operations. Administrators and security specialists now use the platform to establish baseline performance metrics to assess the health of systems, proactively monitor and receive alerts, and quickly investigate and resolve any issues. "Rather than pore over thousands of lines of transactions, we use Splunk Cloud dashboards to visualize patterns and trends," says Linn. "We can observe login anomalies, detect questionable activities and behaviors, and promptly take measures to remediate them."

Fraud reduction yields far-reaching benefits

Orrstown has experienced an increase of more than 400 percent in debit card fraud over the past three years. To combat this, the bank integrates an anomaly detection solution in its Splunk Cloud deployment. This joint solution rapidly identifies the first instance of fraud and then prevents subsequent fraudulent transactions. The solution uses statistical modeling to discover abnormal activities, incorporating transaction characteristics such as the location, amount, time of transaction, as well as the risk profile of the vendor.

"We initially applied Splunk Cloud for security use cases, but we're developing more and more business-focused use cases where we use the visibility and analytics provided by the Splunk platform to improve our operations and customer satisfaction. We're enjoying security, IT and business value from a single, cost-effective solution."

Andrew Linn, SVP, CISO
Orrstown Bank

The combination of these dimensions determines a risk score for each transaction. Based on the severity of the score, Orrstown is able to take appropriate action, such as disabling the debit card or issuing a proactive customer notification. By incorporating anomaly detection into Splunk Cloud, the bank estimates it cut debit card fraud losses by over 50 percent.

Security intelligence improves ATM operations

With Splunk Cloud, Orrstown gains real-time fraud and business analytics across its network of ATMs. The bank indexes data from the ATMs and displays the information in Splunk dashboards, providing near real-time insight into potentially fraudulent activities.

Thanks to Splunk Cloud, the bank also derives business intelligence from its ATMs. By baselining the flow of money in and out of each ATM, for instance, it ensures the devices are neither under nor over-provisioned, efficiently making funds available to customers.

Linn concludes, "These innovative Splunk use cases allow us to further monetize our ATM system. We initially applied Splunk Cloud for security use cases, but we're developing more and more business-focused use cases where we use the visibility and analytics provided by the Splunk platform to improve our operations and customer satisfaction. We're enjoying security, IT and business value from a single, cost-effective solution."

PostFinance Delivers Improved Fraud Detection and Enhances Customer Experience

Executive summary

PostFinance is the third largest retail bank in Switzerland with just under three million customers. It provides a full range of financial products to both consumers and merchants with an established position as the number one payments provider in Switzerland. The bank needed 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. Since deploying Splunk Enterprise, PostFinance has seen benefits including:

- Improved debit card fraud detection
- Real-time Operational Intelligence across its online banking platform
- Better overall visibility into its payments architecture

Why Splunk

Protecting its customers' financial assets and personal data from criminal elements is a top priority for PostFinance. With a large quantity of machine data generated and stored due to government regulation, the bank recognized that this resource could be used to drive greater value, with particular focus on fraud prevention and security.

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. Around 50 automated fraud

Industry

- Financial services

Splunk Use Cases

- Security and fraud
- Application delivery

Challenges

- Absence of operational visibility across the online shopping solution
- Need to build an in-house fraud security solution for PostFinance debit cards
- Changing security landscape required an improved ability to respond to potential phishing attacks

Business Impact

- Streamlined fraud detection across online and in-store transactions
- Introduction of operational visibility enables the security team to quickly identify and respond to phishing attacks and other online threats
- Improved ability for product management teams to respond to merchant needs

Data Sources

- E-commerce applications
- Web server logs
- Middleware logs
- DB logs (Oracle and MSSQL)
- Online banking logs
- Network devices and appliances
- Reverse proxies
- Unix, Solaris and Windows Server

Splunk Products

- Splunk Enterprise

searches feed data into a dashboard that enables the fraud management team to track activity, as well as allowing for ad hoc searches and reporting according to the team's needs.

The Splunk platform also monitors the company's online banking portal, which is used by 1.6 million customers. When the online security team is alerted to a potential attack, they mimic the actions of a customer to get more information. Each attack stage is monitored through Splunk Enterprise, providing details such as the pattern for fraudulent activity and whether further action is needed.

Insights shine a light on debit card fraud

PostFinance had to develop its own security and fraud detection system to protect customers using debit cards within the bank's payments processing solution. PostFinance relies on Splunk Enterprise to monitor this system, streamlining and improving its security and fraud detection capabilities. Previously, the fraud management team would have to manually create a complex multi-tier database and application stack in order to find anomalies or patterns in merchant transactions. Using the Splunk platform, PostFinance now automates a large part of this process, saving time and resources that can be deployed to other critical areas of IT operations. With the extra layer of operational insight provided by data generated through debit card transactions, the fraud management team can now proactively address potential issues by operationalizing a fraud workflow that reviews data. Detection mechanisms can then be added to the system within minutes including access to historical verification. This allows for the identification of new fraud patterns such as a suspiciously large number of new customers visiting a merchant, enabling PostFinance to escalate issues to law enforcement.

"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."

Patrick Hoffman, Head of IT Infrastructure
PostFinance

Better visibility across data results in better customer protection

As well as upgrading the fraud detection capabilities around debit card use, PostFinance has seen benefits from the Splunk platform across its online banking website and app, E-Finance. Before the deployment, attempts to track online security attacks had been hindered by a lack of holistic visibility into the data being produced at different stages of the attack. With Splunk Enterprise, all the data generated from, for example, potential phishing attacks can be tracked and mapped, so they can be identified and mitigated faster. Through this improved operational visibility, PostFinance is now able to offer a better online banking service to its customers, ensuring they are more secure against the growing volume of online threats.

Improved insight into merchant success and performance

With greater visibility into merchant data, the PostFinance product management team has been able to innovate its services and offer new tools and products to meet customer needs. One example is that the team can now view transactions and revenue of merchants using its payments services over a set period of time through a Splunk dashboard. This allows the team to make decisions based on previously inaccessible data, offering customers a value added service. This dynamic approach to customer service has contributed to the continued leadership of PostFinance in the payments field in Switzerland.

PSCU Safeguards Reliability, Security Through VictorOps and Splunk Enterprise

Executive summary

PSCU is the nation's premier payments credit union service organization, supporting more than 900 owner credit unions representing over two billion annual transactions. To better enable its credit unions to compete with banks, PSCU aimed to improve key IT performance metrics. Using Splunk Enterprise and VictorOps, PSCU has seen benefits including:

- Reductions in mean time to acknowledge (MTTA), from four hours to less than two minutes
- Stronger call-team accountability through "single pane of glass" monitoring visibility
- More efficient security monitoring for PCI compliance
- Cost-efficient use case expansion covering enterprise operations

The PSCU advantage

As member-owned, not-for-profit financial cooperatives, credit unions exist to serve their communities. They compete with banks by offering attractive services and rates.

Here's where PSCU comes in. Most credit unions do not have the resources to build and host their own products, so PSCU does it for them. PSCU delivers white-label applications for online bill pay, online lending, debit and credit card programs and other financial services.

"It is critical that our services and products are available for our credit union owners," says Earl Diem, PSCU IT operations manager.

Challenge: improve MTTA/MTTR

PSCU saw the value in reducing MTTA — an acknowledgment that in effect says "I'm on it" when an alert is received. MTTA is a key metric for reducing downtime because it triggers incident response — which lowers mean time to repair (MTTR).

Industry

- Financial services

Splunk Use Cases

- IT operations
- Infrastructure monitoring
- Security
- DevOps

Challenges

- Ensure product and service availability for credit unions
- Reduce MTTA and MTTR
- Aggregate disparate alerts under "single pane of glass"
- Drive greater accountability for meeting on-call responsibilities
- Protect data security, PCI compliance

Business Impact

- Accelerates MTTA from four hours to less than two minutes
- Enables collaboration, accountability across multiple departments
- Empowers staff with mobile monitoring access to deliver support from anywhere
- Ensures PCI security compliance for both activities and transactions
- Enables 900 credit unions to conduct two billion annual transactions
- Delivers an excellent customer experience

Data Sources

- Symantec security logs
- Application performance management logs
- SolarWinds
- New Relic
- Oracle Enterprise Manager
- Network devices

Splunk Products

- Splunk Enterprise
- VictorOps
- Splunk App for Infrastructure

"Our people were doing the 'rotating chair' methodology of support, using several point tools to monitor five or six disparate systems. We recognized the need for a better alternative to give us the MTTA we sought," Diem recalls. "We wanted to aggregate system-based alerts and gain additional traceability to more effectively manage staff accountability."

VictorOps slashes MTTA

PSCU solved its MTTA, MTTR and accountability challenges with VictorOps, which empowers on-call teams to find and fix problems faster with automated and insightful incident management routing, collaboration and reviews. PSCU employs VictorOps as a standard solution across 110 enterprise users. Diem keeps a graph on his wall of plummeting MTTA since PSCU started using VictorOps more than three years ago.

"In 12 months with VictorOps, our mean time to acknowledge came down from four hours to 20 minutes. Now we're three years in and we're under two minutes," Diem says. "Each PSCU IT department maintains an on-call schedule. VictorOps brought all the managers together with one tool. We understand what we're doing, and we all use the same escalation schedule. It drives accountability."

Staff members use VictorOps mobility features to perform their support jobs from anywhere. "You can interact with the system from your desktop, from a laptop, from an iPad, through your phone," Diem says. "The alerts in VictorOps give you the supporting data from the system (that) alerted. You know what went wrong even before you look at the system."

PSCU started using VictorOps for its production environment but has extended it also to Quality Assurance and DevOps. The organization employs offshore developers in the Asia-Pacific region and India. It cannot allow system issues to interfere with productivity. Now, PSCU detects performance degradations before they turn into failures.

Extending history of success with Splunk

Today PSCU has another reason to celebrate: the acquisition of VictorOps by Splunk. PSCU has long been a Splunk Enterprise customer, starting with security monitoring and Payment Card

"In 12 months with VictorOps, our mean time to acknowledge came down from four hours to 20 minutes. Now we're three years in and we're under two minutes."

Earl Diem, IT Operations Manager
PSCU

Industry (PCI) compliance — a must for financial services. PSCU's security team uses Splunk Enterprise to aggregate and index logs from tools monitoring network and security devices. Now, PSCU has decided to push its operational logs into Splunk Enterprise also.

Because PSCU already relied on Splunk Enterprise for PCI monitoring, "It didn't make financial sense to maintain a separate tool for operations when Splunk can serve the whole enterprise," Diem says.

Splunk's machine data analytics, combined with incident response from VictorOps, creates a "Platform of Engagement" that helps DevOps teams innovate faster for better customer experiences. Outstanding vendor support is another advantage, as PSCU's relationship with Splunk brings an active user community and educational resources.

"I'm pretty excited about VictorOps being a part of Splunk," Diem says.

PSCU is expanding its reliance on the Splunk platform with new use cases. One issue has been delays in detecting errors in new software releases — a problem solved by VictorOps and the Splunk App for Infrastructure.

"The errors we're not currently seeing will bubble up, alerting into VictorOps as warnings, and we'll have a team investigate," Diem says. "The next natural progression after that would be Splunk IT Service Intelligence for predictive insight."

The combination of Splunk and VictorOps software gives PSCU a powerful means to fulfill its mission of satisfying customers. "No matter what you do, you're going to have failures out there," Diem says. "The sooner you know, the sooner you can repair it, and the better you protect your user experience."

RAYMOND JAMES®

Raymond James Gains Fast Time to Value With Splunk Cloud

Executive summary

Raymond James is a full-service financial services company and trusted advisor to individuals and institutions throughout the U.S., and through its subsidiaries in Canada and Europe. The company adopted Splunk Cloud for security information and event management (SIEM) and has since expanded to additional use cases including application monitoring. Since deploying Splunk Cloud, Raymond James has seen benefits including:

- Fast time to value, with initial deployment completed in one weekend
- Decreased hardware requirements
- Reduced certain queries from 48 hours to 30 minutes

Why Splunk

At Raymond James, the security, engineering and operations department is responsible for network security, infrastructure security, and reporting and monitoring. According to Kevin Lane, a Raymond James security engineer, "With our previous platform, we wanted more consistent data, to correlate events across multiple systems and log types, and to decrease our time to resolve IT and security investigations."

A proof of concept (POC) enabled the team to determine that Splunk Cloud met its requirements, including increased query speed. "When you're doing investigative work for security reasons, you want to resolve incidents quickly," Lane says. "Certain queries over a month used to take about 48 hours to return, and then we ran the same query in Splunk Cloud, and it took approximately 30 minutes."

Industry

- Financial services

Splunk Use Cases

- Security
- IT operations

Challenges

- Correlate events across multiple systems and log types
- Needed a solution for fast IT and security investigations
- Wanted a cloud solution to reduce hardware maintenance time and spend

Business Impact

- Reduced certain queries from 48 hours to 30 minutes
- Improved user experience
- Saving costs by using far less hardware
- Rededicated people from maintaining its previous complex SIEM solution to higher-value tasks
- Enabled disaster recovery

Data Sources

- Firewall
- VPN
- Syslog
- Microsoft Windows
- Linux

Splunk Products

- Splunk Cloud
- Splunk Machine Learning Toolkit

"In the financial services industry, getting the right information, being able to correlate and search through data quickly is very beneficial to us," says Lauren Deren, security engineering and operations manager at Raymond James.

With Splunk Cloud, Raymond James would not have to purchase additional on-premises hardware and keep it up to date. It was also very important to the team that they would not have to set up an entirely new business continuity management and disaster recovery (BCP-DR) infrastructure. "With Splunk Cloud, our infrastructure is dynamic. We can lean on those resources and save manpower and a lot of time," shares Deren.

Ease of use

The initial Splunk Cloud deployment took place over a weekend. With fast time to value, Deren and team have opened Splunk Cloud up to more users, and many are taking advantage of the platform. "Running searches in Splunk is a lot easier for people outside of our specific area," Deren says. "With other SIEMs you have to learn about five different programming languages to manage it. Splunk uses one, so that helps from a user perspective."

"The cloud platform reduces administrative workload so that users can focus on company-specific information, such as alerting, monitoring and increasing visibility," says Deren. "Our team is maximizing efficiency, using their time for high-value projects."

Improved self-service

Another big benefit of Splunk Cloud is that the team has been able to offer self-service to its internal customers, such as other IT and HR teams. For example, the IT help desk can avoid escalating issues to multiple teams by using self-service Splunk Cloud dashboards to increase their call resolution.

Splunk Cloud dashboards help the HR teams perform basic self-service investigations without having to involve the security team. Even system administrators and other internal back office teams have begun using Splunk Cloud dashboards because of the overall positive user experience.

"With other SIEMs you have to learn about five different programming languages to manage it. Splunk uses one, so that helps from a user perspective."

Kevin Lane, Security Engineer, Security, Engineering and Operations
Raymond James

Expanded use cases

While security monitoring was the main reason why Raymond James selected Splunk Cloud, the team has discovered other use cases for it as well. "As we moved to Splunk, we identified several of the operational use cases that were well-suited for the platform and have taken a prominent role with our user base," Lane says.

"Since we've done the Splunk Cloud implementation, we've expanded our IT monitoring significantly," says Deren. "We're able to monitor many applications and look at application health. We're able to see if there's any performance degradation before a user calls in."

The team at Raymond James is looking at other premium Splunk solutions to complement the platform, such as Splunk User Behavior Analytics (UBA) and Splunk IT Service Intelligence (ITSI). "Our DevOps team is already using the Splunk Machine Learning Toolkit for monitoring standard deviations and website traffic," explains Lane.

"Certain queries over a month used to take about 48 hours to return, and then we ran the same query in Splunk Cloud, and it took approximately 30 minutes."

Kevin Lane, Security Engineer Security, Engineering and Operations
Raymond James

Seven Bank Fights Financial Crimes With Real-Time Log Correlation and Analytics

Executive summary

Seven Bank, Ltd., a Japanese bank offering a variety of cutting-edge financial services to a broad base of customers, opens approximately 17,000 new user accounts monthly and operates more than 24,000 automatic teller machines in Japan. With a growing focus on online transactions, the company has stringent security and risk management requirements. Since deploying Splunk Cloud, Seven Bank has seen benefits including:

- Integrated real-time visibility into anomalies and threats
- Streamlined operations and fraud analysis
- Improved risk assessment and management

Why Splunk

Seven Bank had been striving to mitigate financial fraud and unauthorized use of bank accounts by using siloed, manual solutions to monitor cash transactions and internet access. Although this process was able to safeguard individual points of operation, the lack of log correlation across organizational barriers restricted the bank's capability in capturing cross section data, responding to anomalies quickly, protecting its overall business and making effective business decisions. The bank also spent a considerable amount of time manually operating the applications.

Facing the challenge of fast business growth and an increasing number of user accounts, Seven Bank needed an effective approach to unauthorized access control and a flexible platform for operational analysis. After evaluating a few solutions, its financial crime countermeasures department decided to adopt Splunk Cloud. Splunk's market reputation and comprehensive

Industry

- Financial services

Splunk Use Cases

- Security
- Fraud

Challenges

- Needed advanced analytics and log correlation to identify anomalies
- Manual online fraud tracking was time-consuming
- Inefficiency in managing siloed applications and inflexibility in capturing cross-section data

Business Impact

- Enhanced crime prevention, thanks to the integrated real-time visibility into anomalies and threats
- Improved efficiency and staff morale due to streamlined operations and fraud analysis
- Business automation with improved risk assessment and management

Data Sources

- Internet banking access logs
- Bank account and cash transaction data
- Unauthorized access detection data
- Call detail records

Splunk Products

- Splunk Cloud

product training meet the bank's needs. The bank is also impressed by the rich array of Splunk apps available that enable the company to bring in new functions whenever needed.

Detecting anomalies and preventing crimes in real time

Splunk Cloud enables Seven Bank to integrate a broad range of data from multiple sources including internet banking access logs, cash transaction information, account information, phone call records and services data onto a central platform, and automatically collect, search, monitor, report and analyze all real-time and historical data using a cloud service. It then generates useful insights for spotting customer churn and patterns that indicate severe business impacts, as well as signs of unauthorized access through behavioral analysis, and notifies administrators of potential risks through a score-based alert system. This predictive analysis helps prevent unauthorized use of bank accounts, illegal money transfers and other financial crimes.

Seven Bank can also detect system outages before they occur and proactively keep its services up and running to meet business needs. Gigabytes of data in various formats are processed and correlated every day to produce operational insights for the bank to maintain a safe and healthy operation.

Boosting efficiency by eliminating human intervention

Splunk Cloud offers a single point of access and a holistic view across the organization that can support a wide range of analytics. More importantly, it standardizes and automates analysis tasks previously handled manually. The streamlined operation allows Seven Bank to keep pace with its business growth and retain talent while facilitating workflows and cutting human resources training time by one-half.

Moreover, the intuitive Splunk dashboard offers a painless operating experience by visualizing all information related to the detected account on a single monitor. Administrators can also predefine rules to track incidents and potential issues, perform analytics on

"The Splunk analytics solution not only helps us master financial crime challenges and facilitate our operations, but also acts as a major catalyst for our business growth and success, keeping us in pace with the ever-changing business world."

Takanori Yasuda
Seven Bank, Ltd.

historical and new real-time data, and derive meaningful, actionable insights to speed up decision-making processes.

Gone are the days when the system operators continually kept an eye on the monitor to trace anomalous behaviors and predict failures. Now, whenever unusual activities and events are detected, the operator will immediately receive an email alert. The improved consistency removes stresses from and boosts the staff morale. There is also no need for the bank to increase staff despite the increasing workload.

Improved risk management opens up new opportunities for business automation

With Splunk Cloud in place, Seven Bank can eliminate time-consuming manual procedures and stay focused on the core business. It can also analyze a larger variety of external data in a broader context and greater depth, generating unprecedented real-time insights and perspectives for better business planning and crime prevention.

In the future, Seven Bank plans to use the new risk scoring-based alert system to automate other business processes, such as freezing illegal accounts and blocking abnormal money transfers. It is also considering using the Splunk solution to detect hardware failure and track inventory while supporting other possible areas of business operations.

TransUnion Invests in Splunk Solutions for Enterprise Monitoring, Machine Learning

Executive summary

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. Behind the scenes, the company promotes reliable consumer transactions by consistently ensuring the stability of TransUnion's information technology systems. Since adopting Splunk Enterprise, Splunk IT Service Intelligence (ITSI) and the Splunk Machine Learning Toolkit for enterprise IT monitoring and machine learning-powered analytics, TransUnion has seen the following benefits:

- Help meeting customer SLAs
- Quick discovery of incident root causes
- Reduction in number of false alerts
- Increased customer satisfaction

Why Splunk

TransUnion provides consumer reports, risk scores, analytical services and more for over one billion consumers and business customers, including Tier-One financial institutions. Edward Bailey, senior monitoring and operations architect at TransUnion, works with a team of Splunk and other TransUnion engineers, who comprise the enterprise monitoring department. He says, "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."

Industry

- Financial services

Splunk Use Cases

- IT operations management

Challenges

- Needed to establish the baseline for external customer traffic and customer volume transactions

Business Impact

- Provide reliable transactions and meet customer SLAs
- Monitor, forecast and maintain transactions in real time, based on machine data
- Discover incident root causes in minutes instead of hours
- Reduce the number of false alerts
- Increase revenue by improving transaction processing

Data Sources

- Application servers
- Access logs
- Server logs
- InfoSec logs

Splunk Products

- Splunk Enterprise
- Splunk IT Service Intelligence
- Splunk Machine Learning Toolkit

Bailey's team looked for ways to improve performance monitoring for external customer traffic and customer volume transactions. Upon discovering Splunk, "We were excited to utilize machine learning to establish our customer activity baseline and help with performance monitoring of our applications," says Bailey. He brought in Steve Koelpin, lead Splunk developer at TransUnion, and took advantage of the Splunk Machine Learning Advisory Program, which helps customers solve business challenges using Splunk's Machine Learning Toolkit.

Faster issue resolution

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.

TransUnion is using Splunk ITSI to visualize and combine machine data from multiple applications to create an end-to-end transaction flow not available in commercial APM solutions. "With Splunk ITSI we have a new way to visualize the health of each app," Bailey says. "It helps us speed up root cause determination to achieve faster resolution."

"Understanding customer volume patterns is important for the business. If traffic falls outside of a certain range, an alert is created. Splunk machine learning allows us to investigate early to ensure a seamless customer experience."

Steve Koelpin, Lead Splunk Developer
TransUnion

"With Splunk ITSI, we have a way to visualize application flow and health from service to service. ITSI helps us speed root cause determination and resolve issues as fast as possible."

Edward Bailey, Senior Monitoring and Operations Architect
TransUnion

Machine learning for better customer service

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.

"Understanding customer volume patterns is important for the business. If traffic falls outside of a certain range, an alert is created," Koelpin says, adding, "Splunk machine learning allows us to investigate early to ensure a seamless customer experience."

Looking ahead

TransUnion's enterprise monitoring department will soon use accelerated data models to populate summary indexes to increase speed further. Plans are underway to make machine learning faster and more accurate. "Our ultimate goal is to reduce search times to seconds with the accelerated data model," Bailey concludes. "We also want to expand the training dataset to enable more accurate machine learning."

UniCredit Delivers Omni-Channel Excellence With Real-Time Operational Insights

Executive summary

UniCredit Business Integrated Solutions (UBIS) is the UniCredit Group's global services company. UBIS is dedicated to providing services in Information and Communication Technology (ICT), back office and middle office, real estate, security and procurement. UniCredit needed a way to collect, store and analyze machine data from multiple sites, systems and applications in order to provide optimal service for its banking customers. Since deploying Splunk Enterprise, UBIS has seen benefits including:

- Real-time operational insights
- Simplified adherence to compliance requirements
- Proactive incident management

Why Splunk

One of the most significant challenges faced by UBIS is keeping pace with and harnessing the massive amount of machine data generated across its multi-national infrastructure. Based in Milan, Italy, UBIS oversees activities in 10 other countries as well, including Austria, Germany, Poland, Great Britain, Czech Republic, Romania, Slovakia, Hungary, the United States and Singapore. UBIS runs approximately 1,000 applications on a variety of different platforms. The collection, storage and analysis of this data is critical in order to troubleshoot issues, identify security concerns, detect fraud and maintain a positive customer experience. With no single point of access, a significant amount of time was required to analyze machine data from disparate sources.

Industry

- Financial services
- Online services

Splunk Use Cases

- Security
- Compliance
- Application delivery
- IT operations
- Business analytics

Challenges

- Find a way to harness the growing flood of machine data generated by online banking and other services
- Establish a single point of access to enable new insight into business and operational data, including better reporting and analyses
- Improve service quality

Business Impact

- Enhanced customer experience thanks to reduced services downtime
- Improved service quality thanks to integrated view of IT operations across entire infrastructure
- Avoided costly penalties by better understanding and mitigating operational and security risks
- 40 percent of incidents proactively mitigated before customer is impacted
- MTTR reduction of 70 percent
- Simplified adherence to compliance requirements

Data Sources

- WebSphere and JBoss application data
- JVM (Java Virtual Machine) metrics
- Application mainframe (CICS/IMS/DB2)
- Network switch/router/firewall logs
- Systems and application events from TIBCO, Tuxedo, IMEX, Eurosig and Apache

Splunk Products

- Splunk Enterprise
- Splunk DB Connect
- Splunk for Windows
- Google Maps Add-on for Splunk

Splunk offered a more innovative approach to managing the big data challenge compared to competitive products. The UBIS team believed Splunk could help the firm reduce both the mean time to investigate (MTTI) and the mean time to resolve (MTTR) operational issues by means of real-time monitoring and proactive incident resolution. UBIS achieved fast implementation of Splunk Enterprise—in just one month—by working with Splunk partner Moviri. The company recently scaled up data collection from 250GB to 2.8TB per day.

Proactive incident management reduces costs, speeds resolution

Real-time and historical monitoring of data within Splunk has allowed UBIS to quickly identify issues and proactively prevent incidents. Specifically, UBIS is using Splunk Enterprise to monitor transactions at regular intervals and send alerts based on thresholds and conditions. With proactive monitoring in place, the customer service team has seen a significant improvement in service quality and gained new efficiencies. About 40 percent of incidents can now be managed before becoming evident to end-users.

Thanks to Splunk Enterprise, problems can be quickly localized and eliminated. Time spent on problem solving and troubleshooting has been reduced by as much as 70 percent—it now takes less than 15 minutes to resolve most issues, down from about an hour previously. As a result, the UBIS IT staff is able to focus on higher value, revenue-enhancing projects.

Deeper insight enhances compliance and savings

By providing a single view into all machine-generated data, Splunk software has also simplified adherence to compliance requirements. The UBIS compliance and control team uses impact analyses to calculate the actual effects of operational and security incidents. In this way, the Splunk solution helps the organization meet service level agreements (SLAs) with its customers, thus avoiding potential compensation payments. The resulting time savings, improved adherence to guidelines and reduction in downtimes have enabled UBIS to achieve important cost savings.

"Our aim was to reach beyond the silos and individual applications to achieve real-time visibility and Operational Intelligence. It is absolutely important to our business to have full and constant control across the entire IT infrastructure."

ICT Engineer
UniCredit Business Integrated Solutions

Splunk Competence Center enables superior customer experience

While Splunk software was initially used primarily for troubleshooting and application monitoring, UBIS has gradually introduced additional use cases, including security analysis and business analytics. About 700 UBIS employees in 180 departments are currently using the Splunk solution. The option of sharing information across all departments and business divisions has led to the creation of a Splunk Competence Center. Splunk enables centralized data access and correlation, allowing security and network specialists to collect and prioritize all queries, and create dashboards and reports.

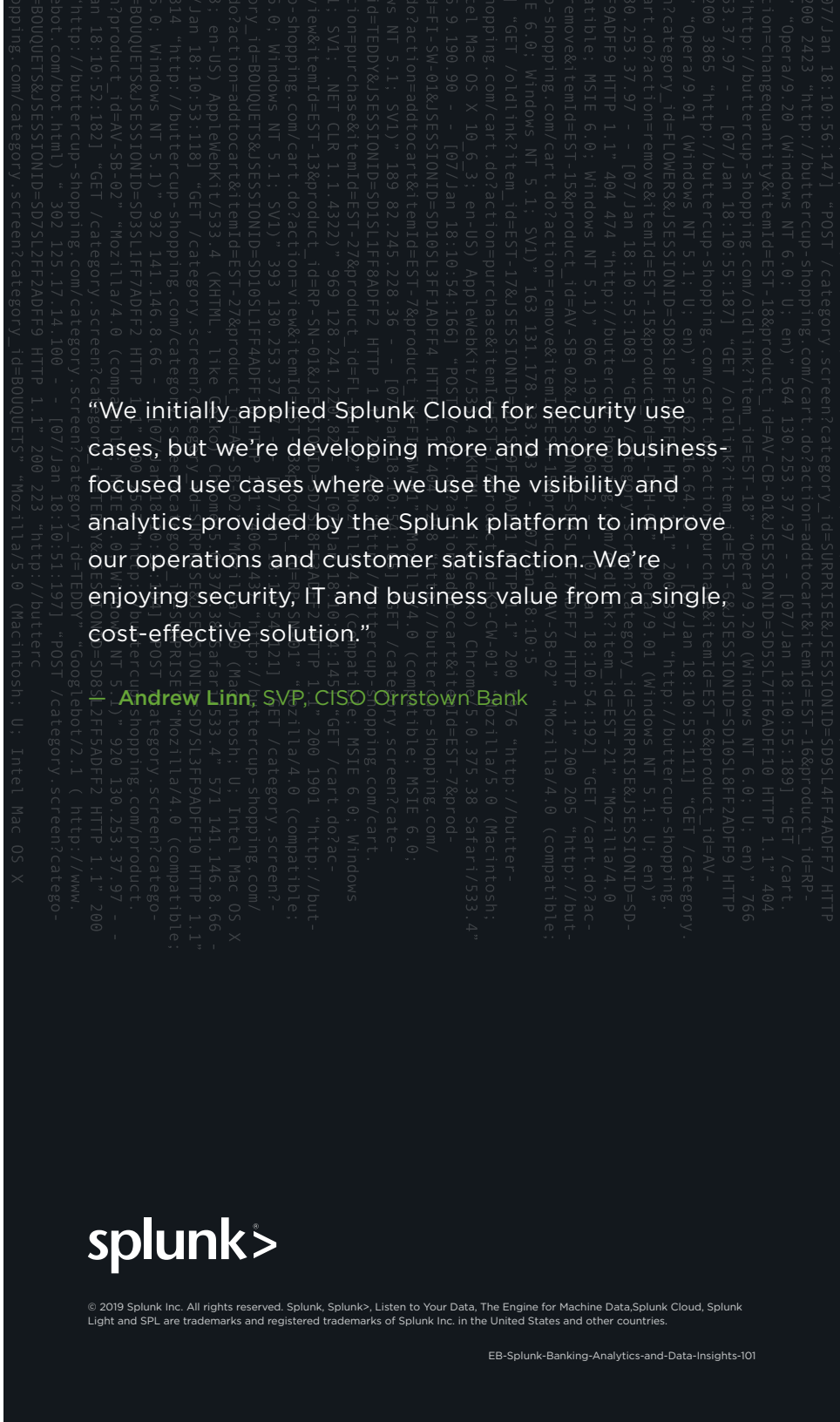
The troubleshooting and application monitoring teams can now create 24/7 alerts, monitor events in real time, and save and share effective searches. This allows the entire infrastructure to be searched for frequent or recurring problems and drilldowns can be engineered much faster.

UBIS business analysts are using Splunk software to create weekly reports for top management that provide real-time insights into key business metrics such as the number of clients served by brick and mortar branches, Internet and mobile banking channels, number of newly opened bank accounts, number of loans and revolving credit cards managed, as well as number of payments and bank transactions executed.

Splunk Enterprise is supporting the crucial goal of providing the best possible financial service experience for UBIS customers. By providing a single source for organization-wide data access, Splunk is enabling all UBIS divisions to share and correlate information.

Machine data has the power to drive new, powerful and unique business insights. Accessing and analyzing massive amounts of data in real time can propel your career and your organization forward.

If you'd like to learn more about Splunk customer success, please visit **splunk.com/fsi**. You can also try Splunk today — download our free trial versions: **splunk.com/download**.



"We initially applied Splunk Cloud for security use cases, but we're developing more and more business-focused use cases where we use the visibility and analytics provided by the Splunk platform to improve our operations and customer satisfaction. We're enjoying security, IT and business value from a single, cost-effective solution."

— **Andrew Linn**, SVP, CISO Orrstown Bank

About Splunk: Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Join millions of passionate users and try **Splunk for free today**.

splunk>

EB-Splunk-Banking-Analytics-and-Data-Insights-101