splunk>

40 WAYS TO USE SPLUNK
IN FINANCIAL SERVICES

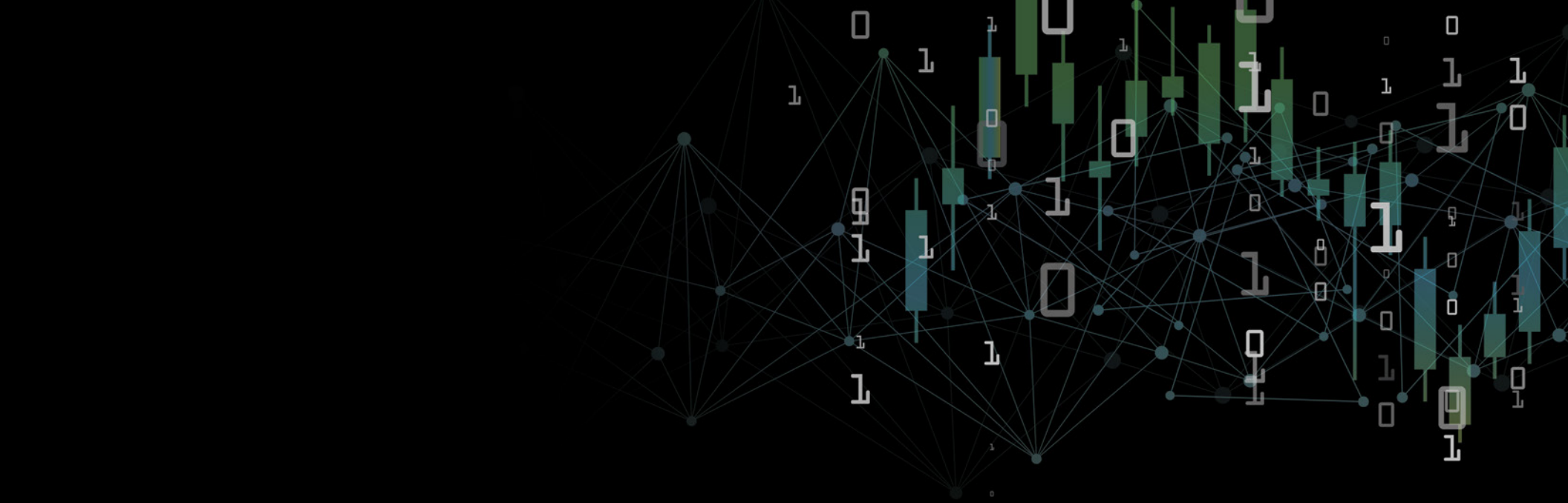


TABLE OF CONTENTS

THE ONLY CONSTANT FOR FINANCIAL SERVICES INSTITUTIONS IS CHANGE.

Regulations are constantly shifting, as are customer expectations, competition, security threats, geopolitical trends or just, technology– financial services organizations are constantly being disrupted.

Open banking demands open APIs and “opens” up a whole new suite of operational and security challenges, but also uncovers new opportunities to deliver a better customer journey. As the array of offerings and associated platforms and touchpoints grows, firms must be mindful of the exposure to security or performance breaches that could result in regulatory, reputational or financial impact.

Financial services organizations need to reimagine existing data analytics strategies to capitalize on the product innovation, risk optimization, improved customer experience and enhanced security posture that only a real-time data analytics platform can provide.

ENTER SPLUNK:

Splunk is well known throughout the financial services community. For many years, firms have been deploying Splunk solutions within IT departments and data-centers, for IT operations, infrastructure monitoring, DevOps, and event management.

The Splunk platform is used extensively for security, with deployments in the security operations center (SOC) at some of the world's largest banks and insurance companies. Splunk software covers a broad spectrum of security use cases, from advanced threat detection to orchestration, automation and response.

Splunk software is also used for fraud detection and prevention, anti-money laundering, sanctions compliance, and insider threat detection.

Splunk's real-time analytics capabilities lend themselves well to analyzing transactions, and as a result some of the world's largest payments networks and gateways are using Splunk for a wide variety of use cases, which range from payment aggregation, merchant analysis, card-fraud prevention, and Payment Card Industry Data Security Standard (PCI DSS).

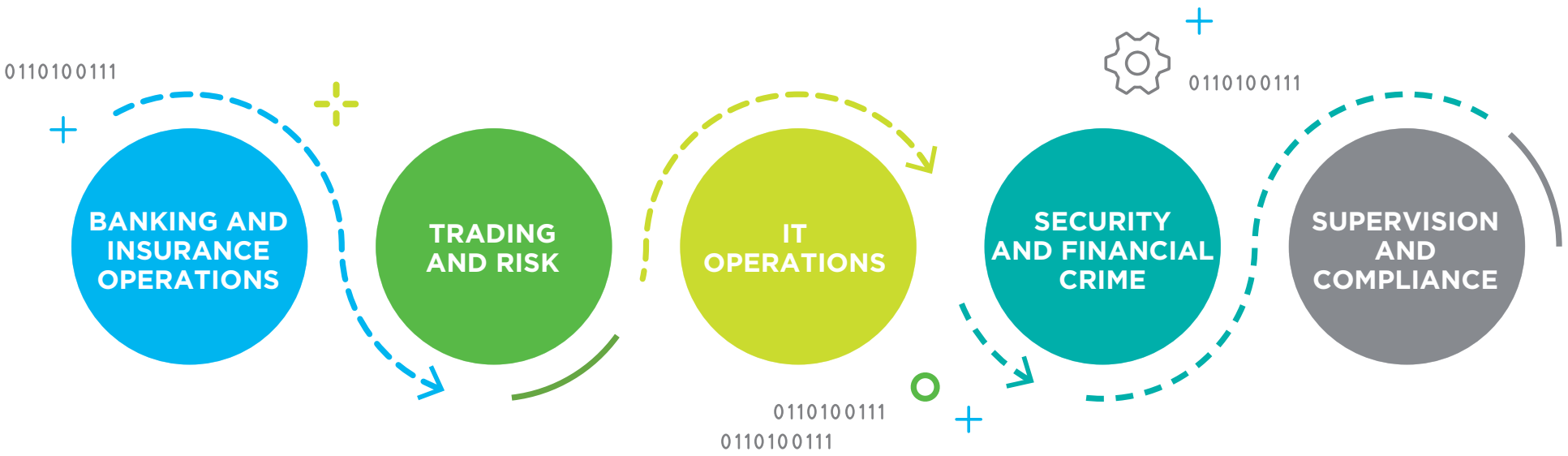
Several trading firms and their risk management teams use Splunk for use cases from design and development of low-latency trading strategies to the building of trading and risk operations centers for chief risk officers and their staff.

Why is Splunk used for such a broad range of use cases?

In the financial world, users normally don't know the next question until it is time to ask it. Splunk is always ready for almost anything you throw at it. Users can design new questions, and watch the answers update in real time as new data streams in.

Splunk is a real-time analytics platform. The software has a robust and scalable architecture that handles the massive volume and low-latency requirements that financial firms demand. It doesn't force users to design data models before they load the data, and it is flexible enough to allow users or developers to ask any question of the data and get an immediate response. Splunk software doesn't care where the data comes from, or what format it is in. You just load the data.

This book illustrates some of the amazing things that our customers are doing with Splunk. The uses are broad and vary considerably and this is just the tip of the iceberg. Splunk is constantly being pushed to new limits by the creativity of the people using it.


0110100111
BANKING AND INSURANCE OPERATIONS
TRADING AND RISK
IT OPERATIONS
0110100111
0110100111
SECURITY AND FINANCIAL CRIME
0110100111
SUPERVISION AND COMPLIANCE

BANKING AND INSURANCE OPERATIONS

INTERNET BANKING OPERATIONS AND SECURITY

The business challenge:

Banks are looking to differentiate their services and win market share by offering customers a superior online and app-based banking experience. As more internet banking services become available, the emphasis on visiting the branch decreases due to the convenience of carrying out routine tasks online. Internet banking is mainstream, and app-based banking is growing four times faster; it is expected to overtake internet banking at many banks this year.

Internet banking traditionally referred to the ability to bank online and perform daily activities, such as checking balances and viewing transactions and statements. More recently, these platforms have become far more complex, integrating numerous digital services such as payments, product promotions, chatbots and mobile apps, as banks look to facilitate multi-channel convergence on their internet banking platforms.

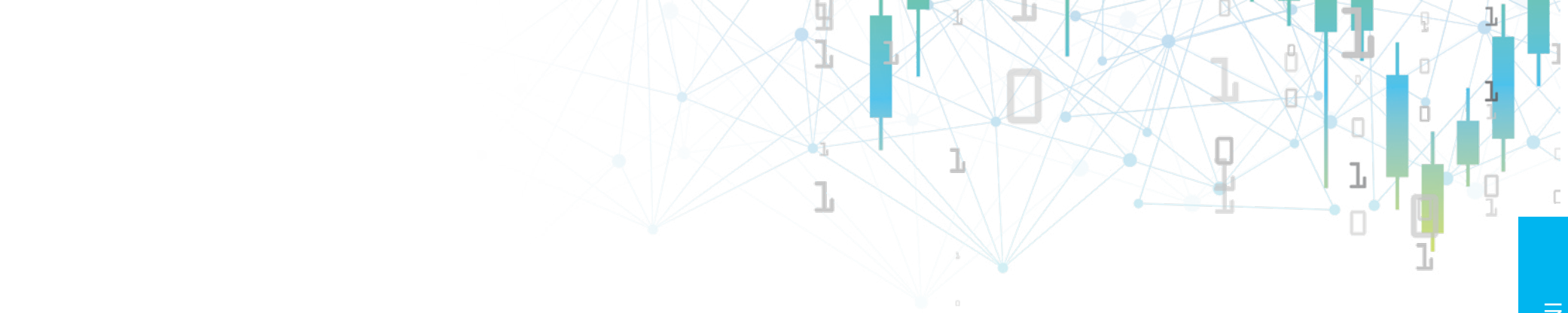
Securing complex online applications that depend on numerous technologies presents many security challenges. Unsurprisingly, cyber criminals target internet banking websites with the hope of collecting enough information to gain access to personal accounts, severely damaging customer confidence, impacting customer loyalty and inflicting brand damage.

Splunk's approach:

Cyber criminals are using increasingly advanced attack vectors to find and exploit potential vulnerabilities in internet banking applications, which are harder to detect and go beyond the realms of any single security product.

Splunk provides a technology-agnostic portfolio of security products that analyze, track, monitor and alert on key aspects of internet banking applications in real time, extending the bank's security ecosystem regardless of the incumbent technologies. Splunk can be used to highlight abnormal behavior, even if the behavior in isolation is legitimate. For example, during a credential stuffing attack, many accounts are accessed simultaneously, causing a spike, which may go unnoticed by traditional security rules.

By leveraging all the data associated with an internet banking application, generated from the development process and into production, Splunk provides complete coverage of the hardware, network, storage, virtualization, cloud and application estate to help detect anomalous internal or external behavior and indicators of compromise through dashboards, statistical analysis and machine learning capabilities.



Internet banking platforms are susceptible to many forms of attack, both internal and external, as shown below:

External Threats

- Cross site scripting
- SQL injection
- DOS, DDoS
- Phishing
- Stolen credentials/identity
- Brute force logons
- Failed 2FA attempts
- Failed reset passwords
- Spoofing

Internal Threats

- BotNets
- Malware
- Viruses
- Worms
- Trojan horses
- Spyware
- Adware

Splunk can help to detect all forms of threats using its advanced correlation rules and workflows.

As a prime target for hackers, security teams must ensure that comprehensive real-time log monitoring of the entire platform is in place. Splunk Enterprise Security (ES) goes beyond traditional security incident event management (SIEM) solutions by providing a data-driven analytics approach to security. By capturing the raw data from the internet banking platform and its supporting architecture, Splunk correlation searches can look for abnormal behavior through mathematical approaches, using statistics and machine learning to trigger events for review by security operations center (SOC) analysts.

Analysts can triage security events and perform forensic investigations within Splunk ES by leveraging the raw data. Investigation steps are journaled, so incomplete investigations can be handed to other analysts for completion.

Value:

Internet and app-based banking has become mainstream with platforms servicing tens of thousands of concurrent users at larger banks, while ensuring security, resilience and performance at all times.

Using Splunk, financial services firms can be confident of maintaining their security posture by detecting malicious attacks in real time and taking blocking measures through Phantom, Splunk's security orchestration automation response platform, which can automate necessary actions to stop and remediate an ongoing attack.

SALES PERFORMANCE AND CLIENT PROFITABILITY ANALYTICS

The business challenge:

Financial firms strive for simplicity in their products and services. They go to great lengths to design, measure and refine their customer experience so customers can consume their products with the minimum of effort, and hopefully with that comes loyalty and a high net-promoter score (NPS).

This is great in theory, but financial firms design such complexity into their own operations that it can often become difficult to deliver on what seems like a simple set of requirements.

Complexity starts with organizational design. Many firms have operations in multiple countries. They operate in multiple time zones with numerous currencies, their staff and customers speak many languages and they have to answer to multiple regulators who examine every word in every communication.

It gets worse. Firms have hundreds or sometimes thousands of products, some of which are current, and some of which are legacy, but all still have to be supported for years. The regulatory rules about how to sell each product differ in each market, and a product that is profitable in one place can take a loss in another.

In addition to this built-in complexity, firms are still holding financial provisions to compensate for the mistakes of the past, and in some markets, the banks are under a full governmental review for not treating customers fairly.

Consequently, the concept of a simple product or service appears harder to reach.

Splunk's approach:

Hope is not lost. Splunk is widely used to help break down the complexity of these operations and provide leaders with simpler, actionable information. That information is delivered in real time, which is what really sets Splunk apart.

Real-time views of customer journeys can dramatically improve the ability of a firm to respond to a breakdown in process and prevent a small issue from becoming a breakdown in a customer relationship.

Firms with sales teams use Splunk to deliver operational dashboards that show how those sales teams are performing and enable managers to study the variance across a team, allowing them to see who is performing well and who needs to be developed in a specific area. Not everyone will perform well across all KPIs.

Profitability can be measured at a client level, or by product, team or country — by just about any measure you choose. One of the standout capabilities of Splunk is the ability to craft just about any question you like and watch the answers flow through in real time. No more waiting for overnight batches. Splunk users get their answers when they need them and can act upon them immediately.

This information can be priceless for people who work in a head office, but it doesn't stop there. Splunk can be used by teams wherever they are. Dashboards can be designed to show the appropriate set of information

required for a person in any role, in any location. This includes mobile relationship managers and branch teams.

Many banks have tried to build analytical systems to provide branch employees with the correct information, but they have struggled with the complexity of data models, volume of data or age of the data. Splunk breaks that cycle by providing the data in real time, across any data source, variety or velocity to provide answers in real time.

Value:

Providing actionable operational information to people in the field or in customer support is incredibly valuable. Being able to spot a problem before it becomes an issue is the key to customer success. Customer loyalty improves, churn goes down, profitability goes up and employee retention improves because support staff are dealing with happier customers.

The ability to see which products or services are the most profitable, where and why is the tool leaders can use to define strategies and also to react to changes in demand in real time. It leads to profitable outcomes.

Regulators demand that customers are treated fairly. Splunk enables firms to measure how they are doing and to record their actions accurately, and it gives them enough information to make changes when mistakes are made.

ING Bank uses Splunk Enterprise for business analytics and customer insight. By indexing web and mobile applications, the bank can now see—in real time—which pages within the ING BankOnLine service customers are visiting. The business unit uses this insight to make business decisions, such as tailored product offerings and other marketing activities.

ING BANK

Read more about Splunk at ING Bank.

CREDIT PIPELINE FORECASTING

The business challenge:

Sales leaders spend far too much time forecasting — often for another sales leader who is under pressure to hit a specific quota. And there is a lot that can go wrong during this process.

However, because many of these challenges are well-documented, there are also many sales forecasting methodologies that organizations can use to great effect.

Firms that sell credit products have an additional dimension to consider — the credit quality of the individual or company seeking the line of credit. In order to balance their overall credit portfolio, credit firms typically have a strategy for achieving credit quality in new deals. Some are more conservative than others. Larger firms also have to contend with credit applications coming into the pipeline from multiple agents or brokers. Thus, questions about customers often don't emerge until late in the process.

Firms that do a good job of forecasting are able to appropriately balance the probability of the sale with the credit quality and price. Accurate pricing leads to winning desired business and achieving the credit risk portfolio that fits the company's strategy. Get the price wrong and you either attract the wrong kind of business or lose the deal.

It might sound easy, but it's not. And credit sales leaders who are able to forecast well are highly desirable because there's more at stake than just revenue.

Splunk's approach:

The solution to this problem is quite technical. From a data perspective, firms need to understand historical sales behavior in order to predict future sales volumes. It is also necessary for firms to understand the desired balance of different credit qualities, and how these trends impact the overall business.

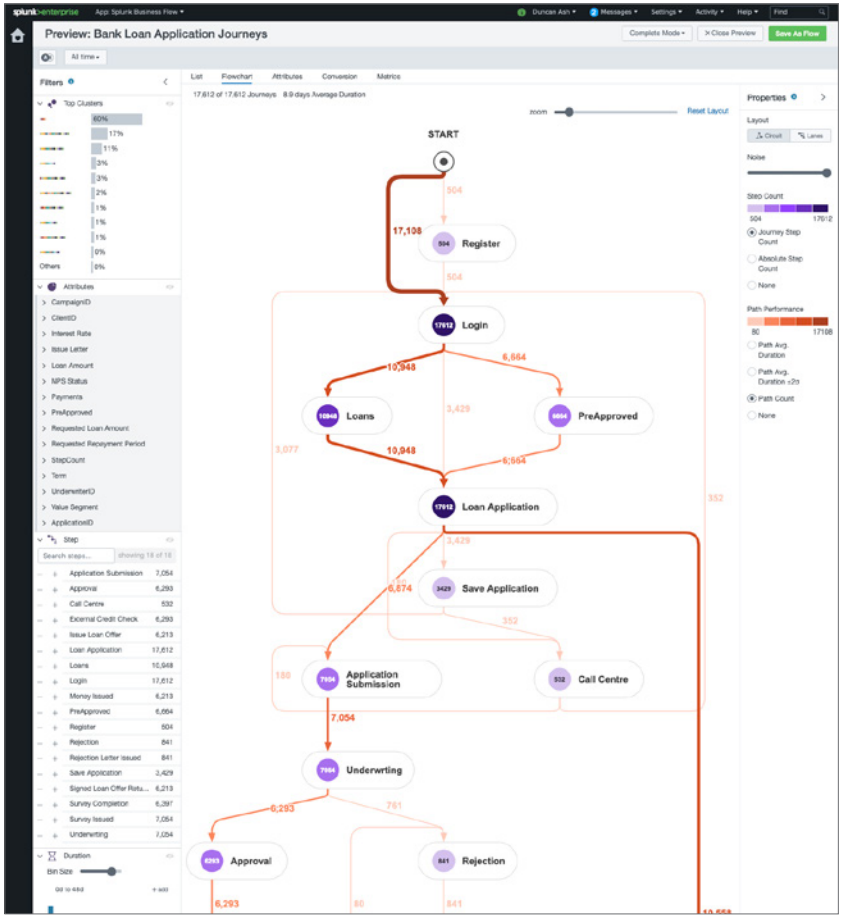
Because applications enter and exit the pipeline on a regular basis, the average credit quality of the pipeline constantly shifts. This can be plotted over time and is reasonably predictable. The credit quality trend is a strong indicator of changes in external factors, and can highlight mis-pricing or bad deals from individual agencies or brokers.

Splunk can forecast the trends that guide the sales part of the process while also considering the credit quality of the application. Splunk simplifies the process by using machine learning models to forecast both sales volume and credit quality mix. Analysts then have access to the information to feed their pricing models, and can continually refine pricing to achieve desired credit quality.

Value:

Implementing Splunk will improve forecast accuracy for individual sales leaders and for the overall business. The credit portfolio mix can be optimized and more accurately forecasted. Subsequently, pricing can be improved, and the overall credit risk position can be moved closer to the efficient frontier. Using machine learning models to manage the forecast can be automated, saving time and effort.

This in turn will lead to higher profitability and a better credit position.



A complete picture of the credit application process allows lenders to accurately view credit requirements and forecast demand.

BRANCH BANKING

The business challenge:

In recent years, retail banks have overhauled the way they serve customers in branches. One of the reasons is that branches are expensive operations, accounting for half of a bank's operating costs in many cases. Thus, they've placed a strong emphasis on reducing both staff and the number of branches, while driving up efficiency through clever use of technology and automation.

Advances in technology have allowed banks to digitize many of their service offerings, allowing customers to more frequently self-serve.

Banks are continuously assessing and balancing the costs of desired, but expensive, customer service with the opportunity to digitize and automate as many processes as possible.

And many banks are still in the dark when it comes to extracting value from branch data to optimize customer service levels. For the new style of branches to operate seamlessly, real-time, end-to-end monitoring becomes imperative. Failures of in-branch ATMs, immediate deposit machines (IDM's), self-service machines, meet and greet terminals, Wi-Fi networks and tablets will disrupt and harm the customer experience in the branch and must be minimized to maintain customer satisfaction.

By leveraging tablets, now widely deployed to employees to conduct business, banks can provide a sense of familiarity and ease of use to increase customer satisfaction. At the same time, tablets introduce a host of new management, tracking and operating challenges.

Even basic visibility into tablet inventory can be a blind spot for support teams, resulting in a degraded customer experience. In light of staff turnover, thefts and devices going offline, , there is no easy way to keep track of them. And it's likely that the resulting device loss could lead to an inconsistent user experience between branches.

And finally, security also needs to be considered. Because Wi-Fi networks are integral to many user interactions, security becomes critical to the services offered by the branch.

Splunk's approach:

While branch activity can be derived by monitoring backend systems, such as the application of a personal loan, using Splunk to collect information directly from devices in the branch can provide more detailed insights into customer journey and employee behaviors. Ultimately, this results in greater visibility, better decision making and improved branch operations, yielding a competitive advantage.

Tablets running banking applications are designed to quickly process in-branch customer requests. Gathering the usage patterns from mobile apps running on the tablets provides critical insights into both the customer journey and user experience.

The Splunk Mobile Intelligence framework ensures that mobile app developers can log directly from their apps to Splunk to ensure that usage patterns and trends can be analyzed to support branch-based decisions.

By correlating data collected from mobile apps with infrastructure data from the network, you can derive a more accurate device count from the Wi-Fi logs, ensuring correct inventory levels per branch.

In the event of an outage, banks can benefit from developing a disruption impact model using Splunk's powerful analytical, machine learning and data visualization capabilities. This allows them to quantify the number of customers and/or transaction numbers affected to help the bank measure the impact and cost of the failure.

Value:

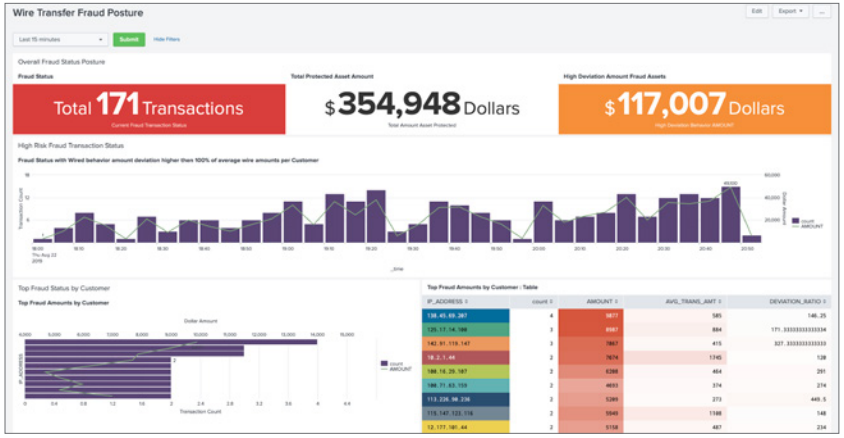
The evolution of running leaner branches that are heavily dependent on technology requires every component to work optimally while necessitating a real-time view of operational efficiency and reliability.

Splunk can gather the data from the branch's infrastructure and provide analytics allowing the bank to increase security, track inventory and optimize processes, ensuring that it can service more customers in the same space, or less.

And as new technologies, such as video-enabled ATMs, are introduced into branches, monitoring strategy needs to be flexible enough to cope with new data sources that can be correlated across infrastructure and applications.

Splunk's data platform ensures that branch monitoring can keep pace with the influx of new technologies adopted to better serve customers.

Correlating customer activity and analyzing how customers interact with the bank is imperative when making decisions on whether to expand or close branches. While some customers prefer to bank online, others may prefer to visit a branch. Banks also need to serve their high-net-worth customers in branches. Going forward, banks will need to leverage analytics to ensure they have this information on hand before making critical business decisions.



A pattern of wire transfer activity from a bank branch.

MOBILE BANKING OPERATIONS AND SECURITY

The business challenge:

Mobile banking applications on the Apple or Google platforms enable numerous banking services to be offered to consumers by their respective banks. Apps allow users to have a native, engaging and responsive experience with features like push notifications, making it easier to alert customers about important updates.

Due to the portable nature of mobile devices, handsets and tablets running mobile banking apps can easily fall into the wrong hands when lost or stolen; therefore, robust security controls are needed to ensure user confidence and adoption.

Splunk's approach:

Splunk Mobile Intelligence (MINT) is an app that extends Splunk's operational intelligence to mobile applications, allowing firms to deliver better-performing, more reliable and secure apps. Splunk's MINT provides mobile intelligence across mobile app releases in production, across different types of devices and on multiple operating systems.

The Splunk MINT Software Development Kits (SDKs) programmatically collect data from mobile apps and then send that data to Splunk Enterprise.

MINT integration to Splunk provides deep insights into applications, user behavior and experience data useful for identifying unusual activity or anomalous activity, as follows:

Find the root causes of crashes and poor app performance.

- Find out which errors are occurring the most by OS, device and app version.
- Determine what users were doing when a crash occurred.
- View the stack trace and instance occurrences for specific errors.
- Capture LogCat and NSLog output from devices.

View network information to analyze system capacity.

- Measure latency, volume and status codes for all HTTP calls.
- Monitor specific events and transactions.
- Filter information by connection type and carrier.

Follow end-to-end processes in mobile apps to understand user experience.

- Report custom-defined events in apps.
- Use transactions to follow specific tasks from start to finish.
- Add breadcrumbs to crash reports to indicate when specific actions occur.

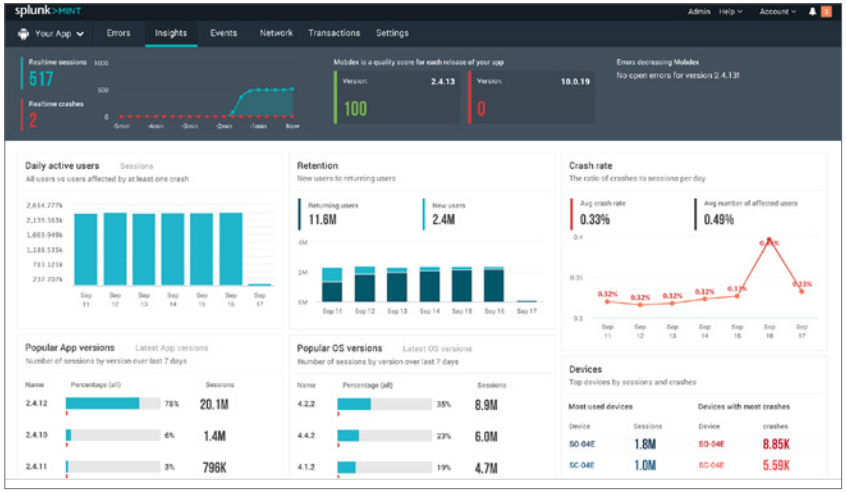
Get insights about the usage of mobile apps.

- Learn which platforms and devices are being used most.
- Find out how apps are performing on each OS and device.
- See how many users are affected by errors.
- Gain insight on usage and performance by users' locations.
- Correlate the performance and usage of apps across mobile devices, web and other channels.

Value:

Mobile apps play a huge part in how banking users interact with their banks, and a great mobile experience can improve brand reputation and customer loyalty and increase net-promoter scores (NPS).

Splunk MINT allows financial services firms to collect data directly from mobile devices and correlate that data with internal data to identify security issues and perform root cause analysis, facilitating faster mean time to resolution (MTTR).



Deliver the omni-channel and mobile experience your customers expect with mobile app visibility correlated with your broader data platform with Splunk.

ATM OPERATIONS AND SECURITY

The business challenge:

Most retail banks have extensive ATM networks, many of which operate in multiple countries, and are usually members of interbank networks like NYCE or LINK.

The traffic flows of ATM usage vary significantly and are subject to seasonality and one-off events. It is therefore necessary to have systems in place to monitor and forecast usage so that machines can be replenished on time.

ATMs are at the mercy of the external environment; they often have to rely on external sources of power and network connectivity. They are susceptible to paper jams caused by damaged bank notes, network outages and power failures, and they are also seen as easy targets for criminal activity.

All of these factors combined mean that banks have to monitor their networks carefully and pay close attention to where they locate their ATMs.

Splunk's approach:

Many banks rely on Splunk to give them a holistic view of their ATM network. ATMs generate detailed telemetry, so it is easy to find out the status of a specific ATM.

What Splunk can deliver is a set of real-time dashboards showing the status of the entire network. These dashboards include:

- Network status
- Overview of incidents
- Predicted incidents
- Suspicious activity
- Network performance
- Financial performance
- Security status

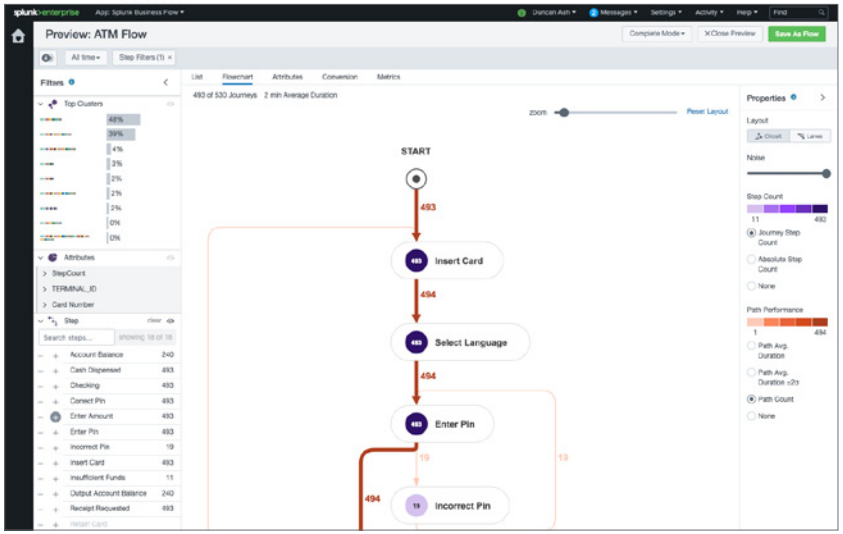
Splunk dashboards look at the history of incidents over time and use machine learning algorithms to forecast future incidents. These algorithms can predict when incidents are most likely to occur, by location and also by type. This ability to forecast incidents allows the bank to become proactive and schedule maintenance routines based on the predictions, saving time and money and improving the uptime of the network.

Security is a key consideration for ATM networks, and Splunk is able to identify threats in real time and automate the response when a threat is detected.

ATM Networks need to be compliant with PCI DSS 3.2. Splunk has a full solution to this regulation, which is described in more detail in another section of this paper.

Security is a key consideration for ATM networks, and Splunk is able to identify threats in real-time, and can automate the response when a threat is detected. Predictive maintenance results in both higher uptime, and lower costs, by building replenishment into maintenance schedules and paying special attention to highly utilized ATMs.

Banks rely on Splunk to give them a holistic view of their ATM network. ATMs generate detailed telemetry, so it is easy to find out the status of a specific ATM.



Understanding the processes involved in ATM transactions enables a bank to troubleshoot those that take too long, or that could be indicators of fraudulent activity.

Value:

ATM outages reflect badly on a bank's brand, so maintaining uptime is vital. Ensuring security is maintained reduces fraud losses and downtime. Predictive maintenance results in both higher uptime and lower costs, by building replenishment into maintenance schedules and paying special attention to highly utilized ATMs.

OPEN BANKING AND PSD II
OPERATIONS AND SECURITY

The business challenge:

The revised payment services directive 2 (PSD2), often referred to as "Open Banking," became applicable in January 2018 and is intended to modernize the EU retail payment market by enforcing new legislation that fosters increased innovation, competition and security in the form of new digital services for consumers.

Banks are obliged to make certain data they hold about their customers (e.g., account balances) available to third-party payment service providers (TPPs) over secure communication interfaces (APIs) once consent has been given by the customer, while ensuring the same levels of availability and performance as if the customer was accessing their services directly.

Open banking facilitates TPPs such as FinTechs or other banks to innovate and provide new product offerings, giving consumers greater choice. These services can be categorized into the following:

1. Aggregators and account information service providers (AISPs): these give an overview of available accounts and balances to their customers.

2. Payment initiation service providers (PISPs): these initiate payments on behalf of customers. They give assurance to retailers that the money is on its way.

Security is a cornerstone of PSD2 with the regulatory technical standards (RTS) specifying strong customer authentication (SCA) via two-factor authentication and one-time passwords for online transactions to reduce fraud. Banks have until September 2019 to upgrade their payment security systems so that they meet the RTS requirements.

Splunk's approach:

To meet PSD2 legislation, banks must establish a communication channel to TPPs by either adapting their customer online banking interface or creating a new dedicated interface, both of which will be inevitable targets for cyber criminals who will attempt to steal information, gain unauthorized access or perform denial of service (DoS) attacks to affect service availability.

Security and performance monitoring of APIs will be of crucial importance not only to the bank, to monitor uptime, speed, latency and endpoint usage frequency, but also to regulators, who will want to ensure that TPPs are not being disadvantaged, since APIs will expose additional load on legacy infrastructure.

With threats to the Open Banking API infrastructure coming directly, from direct attack vectors, or indirectly, as a culmination of an attacker exploiting a vulnerability elsewhere in the network and laterally moving across to inflict damage or exfiltrate data, API monitoring alone is insufficient, because it will provide a siloed view of the API activity. Effective security monitoring of the Open Banking API infrastructure requires a holistic approach.

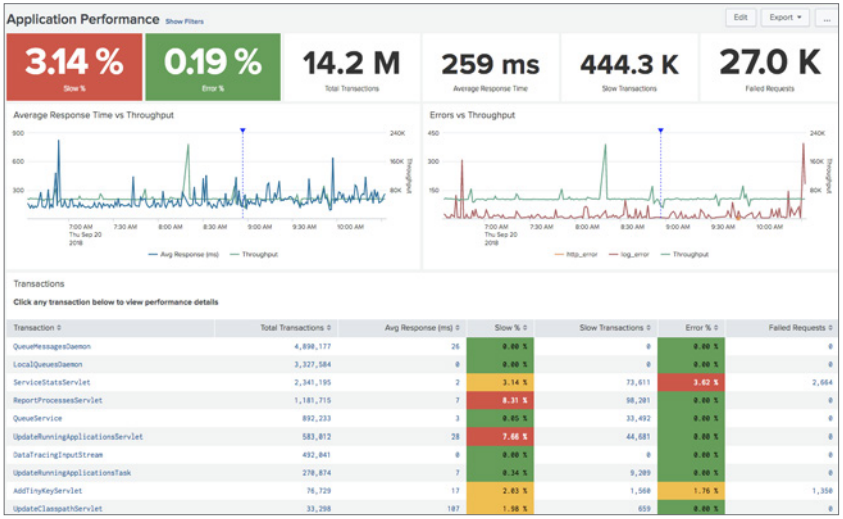
While indications of abnormal behavior with regard to latency, usage and uptime are useful for a service engineer, they could all be symptoms of a cyberattack and have relevance to the SOC analysts, who will look at the same data with a different perspective.

Correlation with other sources can quickly isolate the abnormalities to a platform stability issue or provide visibility of a wider IT operations or security exposure.

Value:

With Splunk, banks will easily be able to extend their security monitoring coverage to encompass the new Open Banking APIs without having to invest in new security tooling or point solutions.

Leading banks will see new opportunities to improve their own products and services by uncovering new insights using Splunk. They can data mine PSD2 APIs to understand how customers are interacting with their own native services compared to those offered by TPPs in order to develop a better customer experience and reduce customer churn.



Monitor uptime and security of APIs at the partner level to better manage your customer experience and security posture.

BLOCKCHAIN OPERATIONS AND SECURITY

The business challenge:

The rise in popularity of blockchain within financial services stems from the belief that it has many applicable use cases which have the potential to remove intermediaries and therefore reduce costs. Banks, brokerages, insurers, regulators, and others are actively experimenting with ways to harness the benefits of blockchain and offshoots of its technology like Smart Contracts.

Potential use cases can range from speeding up and simplifying cross-border payments, to improved identity management of customers and optimized share trading by improving the settlement process. In insurance, a shared ledger amongst insurers would provide immediate visibility on fraudsters who make multiple claims against different insurers.

So far, regulators haven't yet set standards around controls and protections for blockchain-based systems. As firms press ahead with blockchain projects, expect more focus on issues like security and monitoring.

Whilst in theory, blockchain will help organizations become more secure, with the inherent security built into protecting the integrity of the blockchain, and a de-cartelized distributed ledger ensures there is no single weak point for an attacker to exploit, traditional security monitoring of the infrastructure that runs the peer-to-peer network will still be required to ensure hackers cannot have a playground in which to wreak havoc.

As with any technology in its relative infancy, blockchain and the way organizations choose to implement it could expose vulnerabilities that are yet undiscovered. The dependence on new programming code and its associated complexity could also introduce flaws that could be exploited and puts extra emphasis on the DevOps process requiring it to have a high emphasis on security.

It is important that any financial services firm embarking on blockchain projects include colleagues from IT and security as early as possible to give them as much time as possible to adapt to the new technology and analyze where the potential threats could come from.

Splunk's approach:

Security

Splunk's schema-less data store ensures that firms can quickly onboard relevant feeds of log data from their blockchain projects and leverage analytics and artificial intelligence (AI) powered by machine learning to baseline behavior and look for anomalies. The SOC will be able to detect unusual signatures against the backdrop of normal behavior.

Security data ingested into the platform can be surfaced to Splunk Enterprise Security, so that security events can be raised, triaged, investigated and remediated.

IT

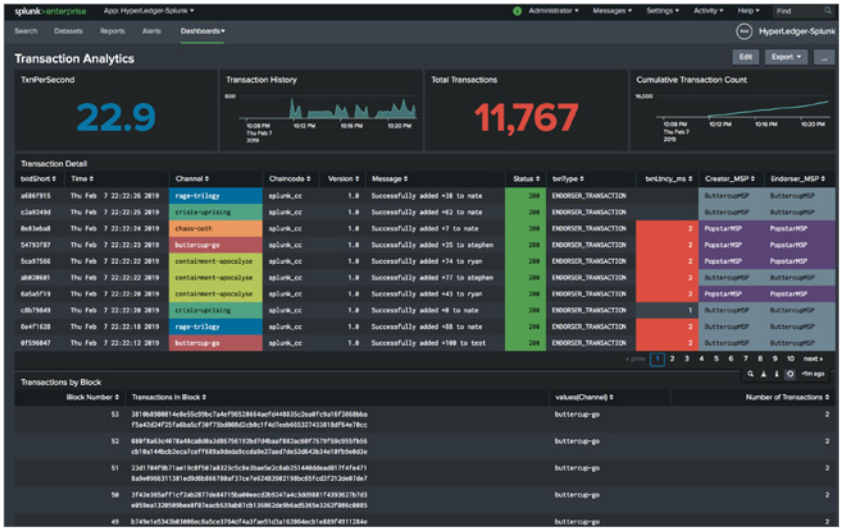
The same data leveraged by the security team would also be useful to IT support teams who are required to ensure the blockchain infrastructure remains operational and healthy. Splunk can provide end-to-end visibility through the combination of logs and metrics, providing visibility on system issues, utilization and capacity planning.

DevOps

With expertise around blockchain development still scarce, extra security emphasis should be placed on the software development life cycle (SDLC) with firms adopting a security by design mantra. End to end monitoring of the DevOps process and associated tooling could be the difference between spotting an internal hacker within the ranks of the development team, identifying malicious code or unauthorized third party extensions which could contain vulnerabilities.

Value:

There are still many unknowns about blockchain, its full potential and the security risks associated with implementing it. Splunk is well positioned to ensure that firms can respond to development, security and stability challenges that can be addressed through better visibility of data.



Monitor the security and operational health of your blockchain and distributed ledger infrastructure with Splunk.

REAL-TIME PAYMENT OPERATIONS AND SECURITY

The business challenge:

Payment gateways and networks need to deliver 100 percent uptime to their customers, while protecting all aspects of the network from security breaches and fraud.

Payment networks have to maintain a complex set of network communications with banks and deal with the multitude of international differences between systems and processes.

Merchants require seamless operational reliability while preventing fraudulent transactions and meeting PCI compliance.

Banks that receive and process payments also have to cope with a multitude of systems and varying levels of performance. Banks need to aggregate the payments received across all of the supported networks so that they can obtain a single view of customers, merchants and networks; it helps them make things secure and identify suspicious behavior faster.

Payments generate large and complex messages that include information on the payment, merchant and recipient and the routing data that allows the payment to reach its destination. All of these factors, combined with very high volumes and inconsistent traffic, require all of the participants to deliver high levels of technical performance.

Splunk's approach:

Many of the top payment networks and gateways have already chosen to use Splunk to manage multiple aspects of their operations. Splunk solutions impact the payments process on multiple levels, these include:

DevOps and DevSecOps

Firms building payment applications use Splunk DevOps capabilities to improve application delivery and allow continuous updates. Real-time updates provide developers with real-time insights across all stages of the development lifecycle. Developers are able to adopt a continuous release methodology.

IT and Network Operations

Providing 100 percent uptime requires a specialist approach to managing applications, infrastructure, security and monitoring. Splunk can monitor the entire process end to end, highlighting bottlenecks and forecasting demand. Splunk uses AI, based on machine learning, to predict where problems are going to occur, which allows engineers to proactively fix problems before they cause an outage. Splunk's VictorOps automates incident management and allows teams to collaborate on problems remotely.

Security Operations

Security has long been an issue in the payment industry. The breadth of products and services and the associated complexities make it harder to protect a payment system.

PSD II has raised the bar on security, forcing banks to improve authentication and process security around APIs.

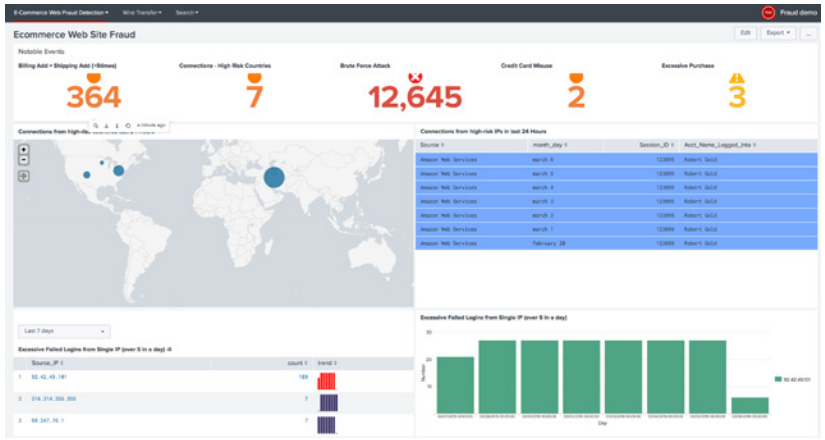
PCI Data Security Standard (DSS) requires that all merchants, service providers and financial institutions meet minimum levels of security and monitoring of the systems in their cardholder data environment (CDE).

Any business that stores, processes or transmits payment cardholder data is required to regularly monitor its CDE in accordance with the PCI DSS standard.

The DSS is made up of 12 requirements that businesses are expected to comply with, consisting of security policies, procedures and guidelines for storage, processing and transmission of cardholder data. These are detailed on page 60 of this book.

Value:

Gateways, networks and banks all report higher availability, lower payment latency, lower rates of fraud and lower cost of operations. All participants are able to meet PCI DSS compliance and achieve a data platform upon which other regulations and reports can be managed. Many firms have commented that Splunk makes it easier for them to develop new products and services. The time and cost of delivery is reduced.



Splunk dashboards make it easy to track common security issues, or KPIs important to your business, so you can make informed decisions and take action to protect and grow your business.

Worldpay are one of the leading global payments providers. They use Splunk to monitor, analyze and protect their payments infrastructure. The organization processes 40 billion transactions a year from ecommerce payments, equalling $1.5T from 146 different countries, in 126 different currencies. They ingest 6TB of data a day from over 25,000 different sources. Splunk is Worldpay's data platform across security and infrastructure, using machine data for cloud monitoring, real-time transaction insights, and monitoring application health.

Worldpay are one of the leading global payments providers. They use Splunk to monitor, analyze and protect their payments infrastructure. The organization processes 40 billion transactions a year from ecommerce payments, equalling $1.5T from 146 different countries, in 126 different currencies. They ingest 6TB of data a day from over 25,000 different sources. Splunk is Worldpay's data platform across security and infrastructure, using machine data for cloud monitoring, real-time transaction insights, and monitoring application health.

worldpay

Hear more about Splunk at Worldpay.

TRANSACTION TRACING

The business challenge:

It is vital for financial firms to be able to track transactions throughout their lifecycle. This capability enables them to offer a better service level to their customers, improve security and rapidly resolve technical issues.

Application Performance Management (APM) tools use Bytecode Instrumentation to change the code of compiled applications on the fly; allowing organizations to trace business transactions as they pass through multiple stages in a process. The output allows firms to gain deeper insights into the performance of their key applications by exposing new metrics related to the inner workings of the application code, so inefficiencies can be exposed and remedied.

One of the undesirable drawbacks of bytecode instrumentation is that it is considered an intrusive form of monitoring because it introduces additional resource consumption on the underlying host, which can sometimes be unacceptable depending on the nature of the application.

For example, additional resource consumption on high frequency trading systems may increase the latency to a point where it impacts the speed at which a firm can execute trades.

The additional latency means the firm won't have the most up to date view of the market conditions which can impact trading decisions and can result in losing opportunities to other firms who have a more recent view of the market, allowing them to react to market changes more quickly.

In another scenario, using Bytecode instrumentation on a global internet banking site that serves tens of thousands of concurrent users may have an unacceptable performance impact on the platform rendering a bad user experience for end users.

Banks look to achieve low level monitoring with alternatives to Bytecode instrumentation on systems that are sensitive to additional resource overheads.

Not all applications can be monitored using Bytecode instrumentation, particularly commercial software which does not provide the appropriate hooks to expose their internal components, resulting in customers leveraging the logs and metrics available.

Splunk's approach:

Applications that require detailed low-level performance monitoring but cannot afford the resource consumption overhead introduced by Bytecode instrumentation require a different approach.

With Splunk, customers can engineer synthetic transaction IDs into their logging semantics for critical applications, so that transactions can be stitched together and traced throughout the process flow using the application's log files without the use of Bytecode instrumentation. This approach is considered non-intrusive and significantly reduces the resource overhead on target hosts compared to Bytecode Instrumentation.

With Splunk, logged events can be stored, retrieved and displayed in real time to show transaction journeys whilst ensuring application performance isn't affected by the monitoring process.

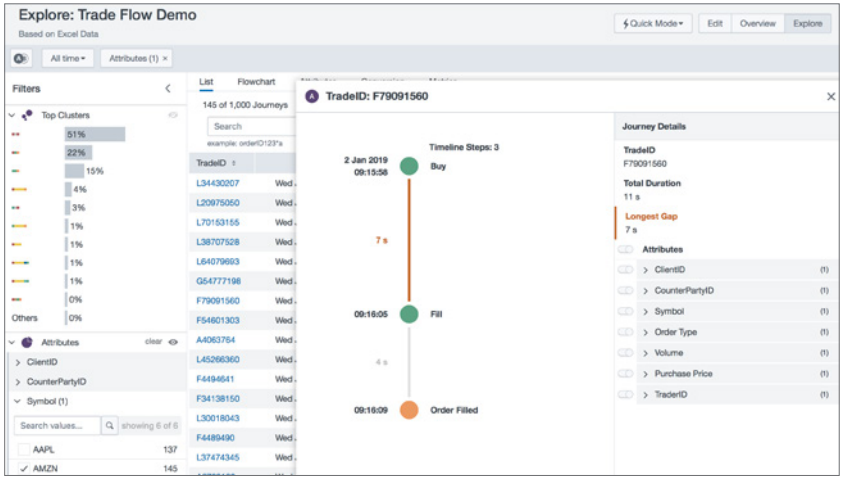
The Splunk forwarder is used to collect and forward data from the host to the Splunk Indexers. The forwarder is designed to introduce minimal resource overhead because it essentially just tails the log files and streams the data directly to the Splunk Indexers where the parsing takes place.

Within seconds of a customer logging into a platform and navigating through various services, Splunk users will be able to track the customer journey and identify troublespots.

Where a performance overhead is acceptable, APM tools can be used to instrument applications with Bytecode injection to gather server metrics, to detect poorly performing code and to calculate user response times; however, APM's have critical limitations and cannot offer full stack monitoring required to troubleshoot complex IT incidents. This is where Splunk excels as it can provide coverage across the entire software and hardware stack, whilst also consuming low-level metrics captured by APM solutions if required.

Value:

With Splunk, firms can achieve low-level application monitoring without putting undue load on system resources. By introducing a constant traceable ID into the logs for each transaction, support teams can monitor end-to-end flows and benefit from more detailed insights into the inner workings of the application code and identify potential bottlenecks without the need for APM tooling, aiding tool consolidation and cost savings.



Visualize a transaction from start to finish—across systems, users and geographies. Splunk provides a single source of truth for transaction tracing.

OPEN TRACING

The business challenge:

The complexity of modern architectures can create troubleshooting headaches for IT and DevOps teams. Numerous layers and dependencies exist across the entire technology stack and granular issues can reach the code level, making it difficult to identify root cause and remediate the issue.

Distributed tracing adds a persistent ID across a distributed technology environment yielding many benefits in modern software architectures, such as server-less and micro-services environments, where each microservice is decoupled and has its own log files. A traceable ID makes it possible to understand the flow of execution between microservices.

Tools such as Zipkin and Jaeger are monitoring tools that can link transactions together to create a trace representing the entire transaction. However, they lack the ability to provide full stack log and metric correlation to IT and developers looking to identify root cause and perform remediation – especially when issues are not code related.

Customers are now less willing to inject a Byte Code Injection agent into a micro-services or server-less environment in favor of distributed tracing, which is emerging as the norm.

Distributed tracing enables IT and developers to track a request through software components that are distributed across multiple applications, services and databases as well as intermediaries like proxies. Tags can be added to the data so users can filter by business context and the traces can be analyzed and presented to show the journey of each request and how much time was taken for every step.

Traditional monitoring is about machines, networks and apps — transaction tracing extends beyond traditional monitoring to provide the observability of interactions, helping with:

- Debugging
- Distributed tracing
- Performance analysis
- Behavioral analysis

OpenTracing is a standard for performing Distributed Tracing. It specifies key information such as where a call is coming from, where it is going, the transaction ID and type. This information can be logged without needing an obtrusive agent performing Byte Code Injection which consumes resources and adds latency. As we move toward micro-services, containerizations and serverless technologies, developers are willing to add OpenTracing code to their application code as it makes it easier to identify issues and improve service levels.

Each request receives a unique ID injected into the header to identify the transaction directly in the application code. The transaction is normally called a trace, which represents the entire end-to-end transaction journey. Each trace is made up of multiple spans, similar to a service call or a database request. Each span has a unique ID, and can create subsequent “child” spans that can have multiple parents.

Splunk's approach:

OpenTracing comprises an API specification, frameworks, libraries and documentation that provide specifications for the project. OpenTracing allows developers to add instrumentation to their application code using open APIs that are vendor agnostic to log to a tracer such as Splunk through the use of the HTTP Event Collector (HEC). This ensures that application performance data and transaction traces can be gathered and correlated across other sources, such as OS, application, network, storage, virtualization and others for troubleshooting and performance monitoring.

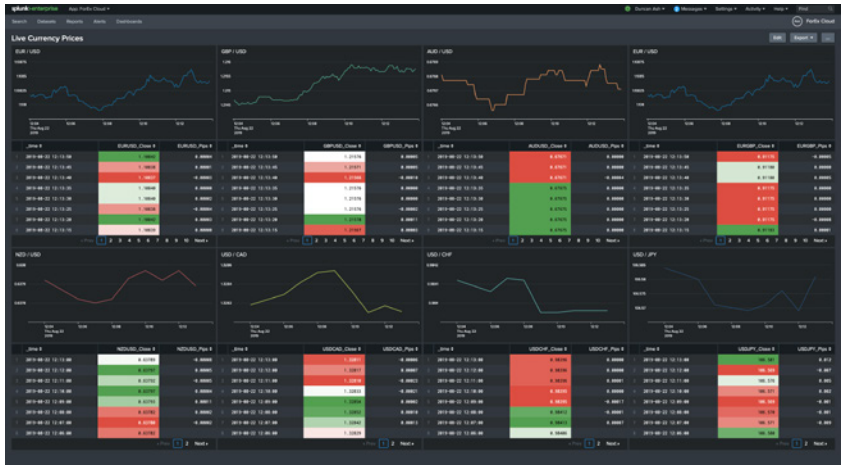
Developers can use distributed tracing to profile and monitor their applications to help with debugging and optimizing their code.

Once the application code is instrumented, IT and development teams will be able to detect and diagnose complex application performance problems and better maintain an expected level of service.

Users reviewing the data can then isolate where the system is experiencing latencies or blockages with the Splunk Machine Learning Toolkit, and can more readily detect anomalous application patterns that may arise between code releases.

Value:

With a few lines of code, Splunk can replace existing tracers, and transaction traces can be used to augment the infrastructure and log data already collected to provide greater visibility into modern distributed software architectures. This results in fewer incidents, greater visibility in application hotspots and bottlenecks and improved service levels that lead to increased user satisfaction and NPS.



There are numerous benefits to monitoring traces and transactions in real time. Here currency prices are being updated in a model.

TRADING AND RISK

THE RISK OPERATIONS CENTER

The business challenge:

Chief risk officers (CRO) and their teams are overwhelmed with information. They have to process everything from the macro view of a firm's capital and liquidity down to leaf-level information on individual transactions. Then they have to put it all together in context so that the business can understand it and make appropriate decisions.

The data that risk teams must process varies from the aggregated high-level weekly and monthly regulatory submissions to the daily limits and real-time exposures on traded instruments. This data environment is so complex that it is common for the CRO to have his or her own IT department (CRO/IT) that has specialist skills and systems to deal with the complexity, volume and latency requirements.

Added to the data challenge are the complexity and cost of low-latency circuits (networks between the banks and trading venues), the complexity and regulatory requirements of trading and the ever-increasing regulatory frameworks that must be followed in order to meet compliance and stay within the boundaries of the banks' desired risk appetite.

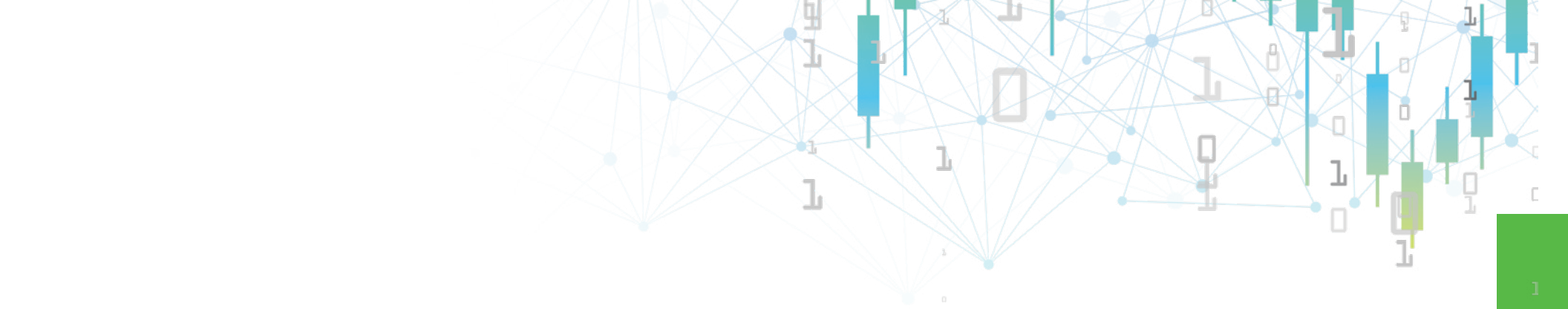
Splunk's approach:

Many chief risk officers have established a risk operations center, where the risk teams and senior bank staff can go to see all of the key risk information in context — and, importantly, in real time.

Some of the common risk areas and measures include the following:

- Economic capital
- Regulatory capital
- Liquidity risk metrics: net-stable funding ratios
- Market risk metrics: risk-weighted assets, sensitivities and Value at Risk (VaR), collateral
- Credit risk metrics: limits, exposures, expected potential exposures, credit charge-off
- Counter party credit risk and Credit Value Adjustment (CVA)
- FX trading
- Operational risk factors
- Cybersecurity threats
- Payment network status
- ATM network status

The technical challenges associated with providing such a diverse range of information are nontrivial and are perfectly suited to Splunk. Many tier one banks are using Splunk to monitor and capture thousands of data sources. Splunk is able to correlate across thousands of sources and highlight those correlations in real time; that same data can be stored for a defined period (the retention periods are automated) and made available for future investigations or for regulatory reporting (e.g., MiFID II).



Splunk is then used to create dashboard-style applications, but unlike regular dashboards, Splunk can update individual elements in real time, allowing a bank to mix slow and fast moving measures with ease. Aggregations can be defined on an ad hoc basis, so that business users can ask any question they need based on the market conditions that day. Regular drill down operations are easy, and if someone wants to ask a new, very complex question of the data, then Splunk's search capabilities allow for nearly any type of question to be answered and updated in real time. This could include, for example, an ad hoc exposure calculation or even something more complex like pricing a new instrument.

The ability to define an aggregation, design a search and stream real-time data through the search sets Splunk apart.

Many banks are using Splunk's AI to build insightful risk applications and highly graphical views of the business — looking for patterns and exceptions and finding emerging trends in the data that might otherwise go unnoticed. Splunk is able to feed the ML models with real-time data, which gives the business a more competitive operating model to work from.

Value:

Firms that build their risk operations center using Splunk obtain a firm-wide view of risk. They can see multiple asset classes in context and gain new levels of flexibility. Information can be aggregated at any level required.

Crucially, they get the flexibility of a platform that can drive the operations center and also be used by many different operational teams, from those involved in planning to the teams that prepare regulatory submissions.

Splunk allows firms to take a real-time, firm-wide view of risk, with the flexibility to adapt to the markets and the ever-changing demands of the regulator.

"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

Read more about Splunk at FINRA.

FINANCIAL STRESS TESTING FOR BANKS AND INSURERS

The business challenge:

Banks and insurers have had to produce stress tests for a long time now. This is becoming more and more difficult each year with the increase in frequency and complexity of the stress tests that are devised by the various regulators and the requirements to stress test portfolios internally for credit and market risk.

Splunk is typically used for two types of stress test: (a) individual traders stressing a portfolio, and (b) regulatory stress testing, typically for the whole firm (banking or insurance).

Whole firm stress tests are mandatory under Basel III, Solvency 2, CCARS and other equivalent regulations, and the reporting frequency varies between weekly, monthly and quarterly. Some firms run tests every day, depending on their business model.

Stress tests are simple in concept, the simplest being where a test is run to see how a single position is sensitive to a change in a single market risk factor — for example, a one basis point change in the price of crude oil.

Alternatively a test might be run to see how the same position responds to a number of market risk factors: the price of crude oil, the GBP:USD rate and the level of the S&P 500.

Adding complexity, we could test for a large number of combinations of the above, maybe 1,000 different combinations.

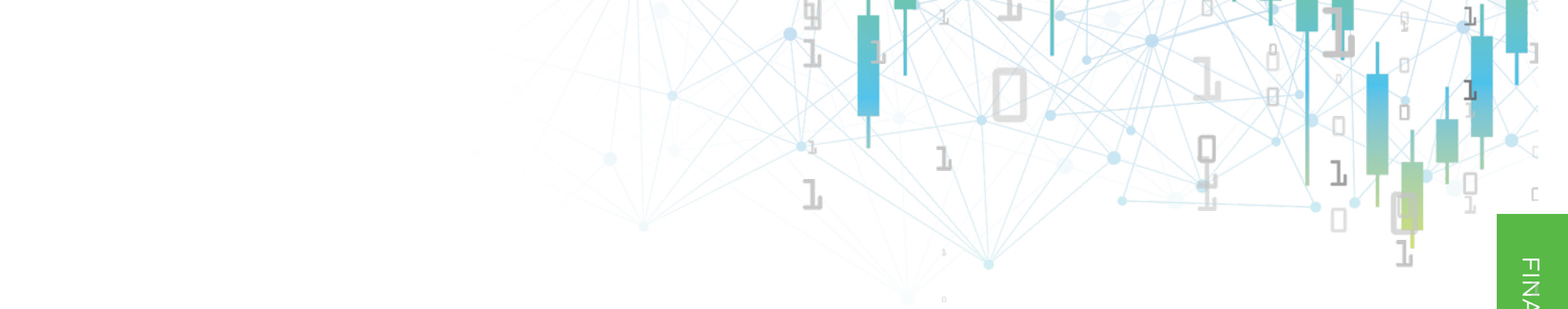
In a whole-firm stress test, every single position is tested against a wide range of stress scenarios, which are designed to test for a major market event or deterioration in economic conditions. These tests can leverage the firm's existing pricing engines but have to run additional jobs in order to run the stress test. Often these are highly compute-intensive and can take many hours or even days, even with substantial hardware. Some firms test for 50,000 different scenarios.

Firms specifically calculating conditional value at risk (CVaR) sometimes have even higher volumes — 500,000 simulations is not uncommon.

Stress tests produce massive data files that include the results of each test. Often, the risk engines produce data files in a complex format that is hard for conventional software to read. These must be aggregated and loaded into a suitable analytics engine to be viewed and interpreted.

The results of the tests need to be communicated in a specific reporting format to the regulator on a regular basis. Risk managers need to analyze the data carefully to help decide if and how to modify their portfolios to a position of more or less risk, based on what they discover.

Before starting this process, a firm needs to have aggregated all of their relevant risk data and made it available to the stress-testing process.



Splunk's approach:

Stress testing, and the subsequent analysis and distribution of results, is a perfect match for Splunk's capabilities.

Splunk can be used to aggregate risk data from multiple locations and is able to do so in near real time while also coping with the huge data volumes required.

Splunk can load the outputs of the pricing engines, the outputs of the stress-scenario, monte-carlo engines, the outputs for CVaR and any relevant external data, and it can make it all available in a single environment.

Risk managers who need to run complex searches can utilize the horizontal scalability of Splunk and deploy it on the appropriate hardware for their data.

Firms that only run the tests monthly may choose to run Splunk in the cloud (private or public) and take advantage of the elastic scalability on offer, only paying the cloud provider for the capacity when it is actually needed.

Risk managers can take advantage of the machine learning capabilities built into Splunk to run analytical models based on the data loaded into Splunk for stress testing. This means that the firm can derive additional value from the stress testing platform and use the risk data and stress-testing results for further decision making.

Value:

Firms taking advantage of Splunk for stress testing can save thousands of hours of effort when dealing with their risk data. The ability to load data first, without having to design a data model is a significant factor.

Splunk's ability to load events from multiple sources and then join/aggregate on demand means that the system is much more agile and that up-front development is reduced.

Being able to demonstrate to the regulator that a firm's risk data and stress-testing process is robust means that the regulator is less likely to impose any constraints on a firm's operations.

HIGH-FREQUENCY AND LOW-LATENCY TRADING

The business challenge:

Participants in low-latency trading are operating at the highest extremes of technical performance. Their requirements push hardware, software, networks and people to their limits. Anything below the fastest performance with the highest reliability will result in missed opportunities, lost trades and potential trading losses. A few nanoseconds can be the difference between a good day and a disaster.

Participants need to develop, monitor and optimize algorithms for low-latency strategies. Often, a firm will have hundreds of different models that can be deployed in an instant, depending on the type of instrument being traded, the venue where it is traded and the market conditions on the day. It is essential to have the best possible algorithm in production at any given point in time.

Participants also must understand and manage the different "circuits" — private networks between their data centers and the different trading venues. Many trading venues allow for a co-location strategy (placing a server at the venue), and those need to be managed and optimized to deliver the lowest possible latency (compared to other co-located servers) and 100 percent availability.

They also need to monitor the performance of each venue: how they perform technically but also how well they fill orders — for example, what proportion of attempted trades are executed. High "fill rates" are essential in order to maintain a client's business; it is common for a client to take its business elsewhere if performance is not up to the expected level.

Participants need to monitor and optimize information from algorithms, PC-based systems, networks, FPGA-based execution systems and APIs, all of which need to perform well together in order to deliver the desired performance.

Splunk's approach:

Many participants in low-latency trading use Splunk within their trading operations. Most use it to monitor their trading infrastructure; measure the performance of the various networks, venues and algorithms; and report anomalies.

Developers are using Splunk's DevOps capabilities extensively, inserting meta-tags into the trading algorithms so that they can measure the effectiveness of an algorithm and correlate the performance against the market conditions, venue and instrument.

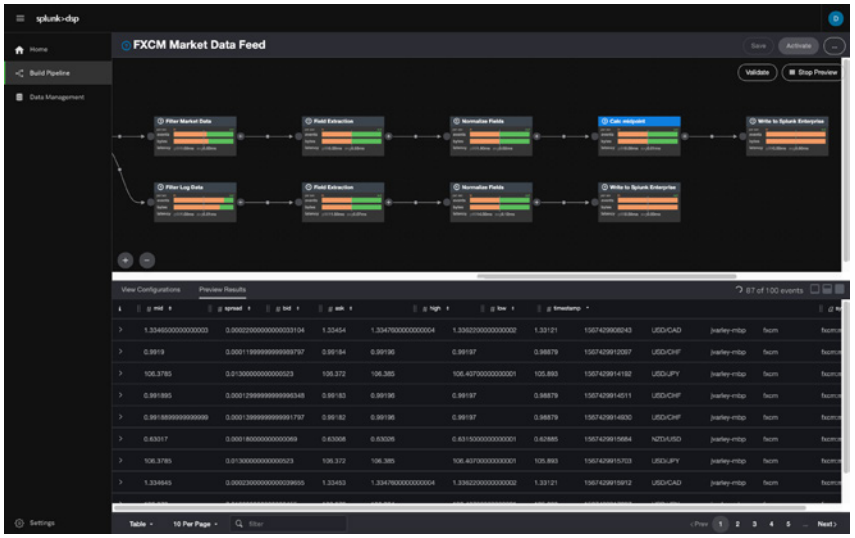
Splunk is able to take a time-series view of events and correlate across thousands of concurrent events, highlighting previously unseen insights to traders and algorithm developers. These insights are used to refine the algorithms and drive new strategies.

Algorithm developers frequently have to test new strategies against historical data, and due to the frequency of trades, the associated data can be large. It is common to analyze data sets of 50TB or more, which requires a scalable platform. Fortunately, the horizontal scalability of Splunk facilitates this kind of analysis. In fact, Splunk's largest customers index more than 5 petabytes of data per day.

Technical teams managing the infrastructure are able to see a whole-network view of operations and can see spikes in CPU or network latency, allowing them to troubleshoot performance problems and improve reliability.

Splunk isn't responding at the nanosecond level of the algorithms, but it is able to monitor and record data at a nanosecond level for analysis and deliver insights within seconds of events. This capability is vital for compliance with Markets in Financial Instruments Directive (MiFID II), which requires a bank to have accurate records of trades and prices for the proof of "best execution." MiFID II specifies having clock synchronization to an accuracy of 100 microseconds, which Splunk enables. The 100-microsecond limit may later need to be improved upon in order to keep up with the pace of the industry.

Splunk is also able to trigger the processes that automate the resolution of any variance in quality.



Being able to monitor the entire low-latency trading environment enables the highest performance to be delivered, as well as being able to identify charictaristics of trading venues that could lead to better performance.

Value:

Splunk enables firms to achieve a holistic view of their low-latency trading operations. It enables algorithm developers to refine their models and design better strategies. It identifies correlations between related events that enable teams to deliver a higher quality of service. Firms using Splunk in their low-latency trading operations will be more reliable and potentially more profitable.

REAL-TIME RISK DATA AGGREGATION

The business challenge:

Most banks and insurance firms have already built some kind of centralized risk data store in order to comply with the risk data aggregation requirements of either Basel Committee on Banking Supervision (BCBS 239), Comprehensive Capital Analysis and Review (CCARs) (banks) or Solvency II (insurers).

Many firms built solutions in a hurry using legacy relational databases or data-lakes. Others are still struggling to deliver on the daily requirements to aggregate risk data and make it available for stress-testing and regulatory reporting and submissions.

The sheer volume of data, variety of sources and systems, complexity of data and logistical aspects of running a global 24x7 operation mean that many firms are looking for a simpler, more cost-effective solution, and one that can cope with the constantly changing regulations as well as the changes in products and markets.

Many of the requirements from the business and the regulators are pushing firms toward a real-time environment for risk data management. It makes sense for them to manage risk data using a similar real-time operating model to their production trading environments.

Below are two extracts from the BCBS 239 regulation on risk data aggregation that demonstrate the requirement:

BCBS 239: Principle 5

Timeliness: A bank should be able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, based on the characteristics and overall risk profile of the bank.

BCBS 239: Principle 6

Adaptability: A bank should be able to generate aggregate risk data to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries.

Splunk's approach:

Splunk can be used as the aggregator and central repository for all risk data. Splunk is able to load data from a plethora of different trading systems, risk engines and market data feeds, both local and remote.

Splunk doesn't require data models to be built in advance, so you can just load any new data into Splunk. Schemas are only created on demand, based on the type of search that the user or process requires.

Data is loaded in real time, and dashboards show risk officers, traders and other interested parties the real-time risk position of the firm.

As well as the real-time dashboards, firms also need the historical data for stress-testing, modeling, simulations and regulatory submissions. Splunk is able to support all of these tasks as it can scale horizontally to large data volumes and time series analysis of risk data.

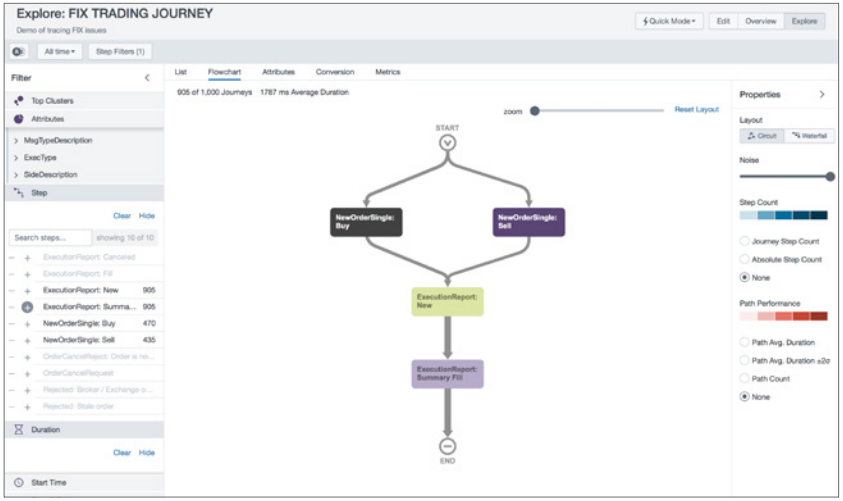
Splunk's integrated machine learning capabilities allow users to build and deploy a wide range of different modeling techniques and apply statistical analysis based on historical and very recent data.

Value:

Firms gain considerable value from using Splunk as their centralized source of risk data.

Not only can firms meet all of their regulatory risk obligations, but they can manage their risk data in a highly scalable, flexible, secure environment with the capability to serve up data for a wide range of use cases — from daily reporting to stress-testing.

Firms can use Splunk as the repository that feeds all of their regulatory submissions, as well as the engine that powers the dashboards in a chief risk officer dashboard or in a risk operations center.



Firms can meet the requirements of elements of BCBS 239, by providing a robust platform that enables the aggregation, storage, and analysis of risk data.

CANCELLED AND AMENDED TRADES

The business challenge:

Not every trade gets filled. Not every trade is entered correctly. Often, there are legitimate reasons for canceling a trade or making a subsequent amendment: simple things like filling in a missing piece of information that wasn't available at the time of the trade or perhaps adding a counter party code or a legal-entity identifier. Some products are simply difficult to trade, and the volume of amended trades can be high.

All of this is perfectly normal behavior — except when it's not.

Splunk's approach:

Everyone who works in a trading environment has seen a cancels and amends report. They are produced every day by every bank, generally at the end of the day, after the market has closed or sometimes the following morning.

These reports are crucial when it comes to determining whether a trade has been legitimately stopped or modified, and they are required to balance a daily profit and loss statement and correct errors. They often show patterns, such as where a specific product or instrument is difficult to trade or where a specific person is not performing well — the so-called fat finger error, where a trader is liberal with zeros or puts a decimal point in the wrong place. It happens. Red/green color blindness can also be an issue.

The other reason that the cancel and amends report is so useful is that it can highlight rogue-trading behavior.

Sequences of trades that are routinely canceled and rebooked can lead an investigator to a rogue trader and are one of the key signals that are used in operational risk controls. Banks are well aware of the types of sequences that are suspicious and know how to look for them. They also need to reconcile trades across multiple accounts that may have been used by a specific trader.

Unfortunately, the data isn't real time, so investigators are usually dealing with events that occurred in the past and trying to reconcile what actually happened.

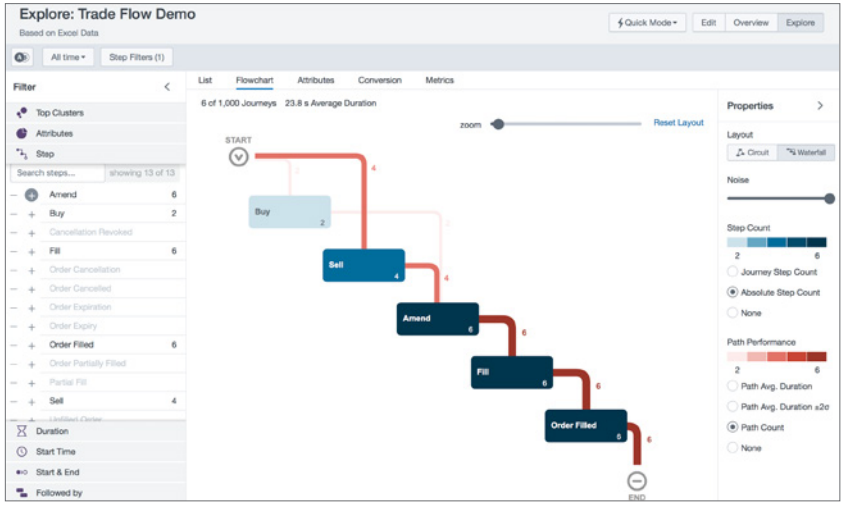
Not so with Splunk. Events can be monitored in real time, enabling reconciliation to happen quickly and also facilitating triggers, so that when a particular sequence of events occurs, a risk officer can be alerted.

Splunk uses machine learning algorithms to monitor behavior and look for suspicious patterns and sequences of events that fall outside of what is considered to be "normal behavior." Splunk's Phantom product can be used to automate the orchestration and response to an incident.

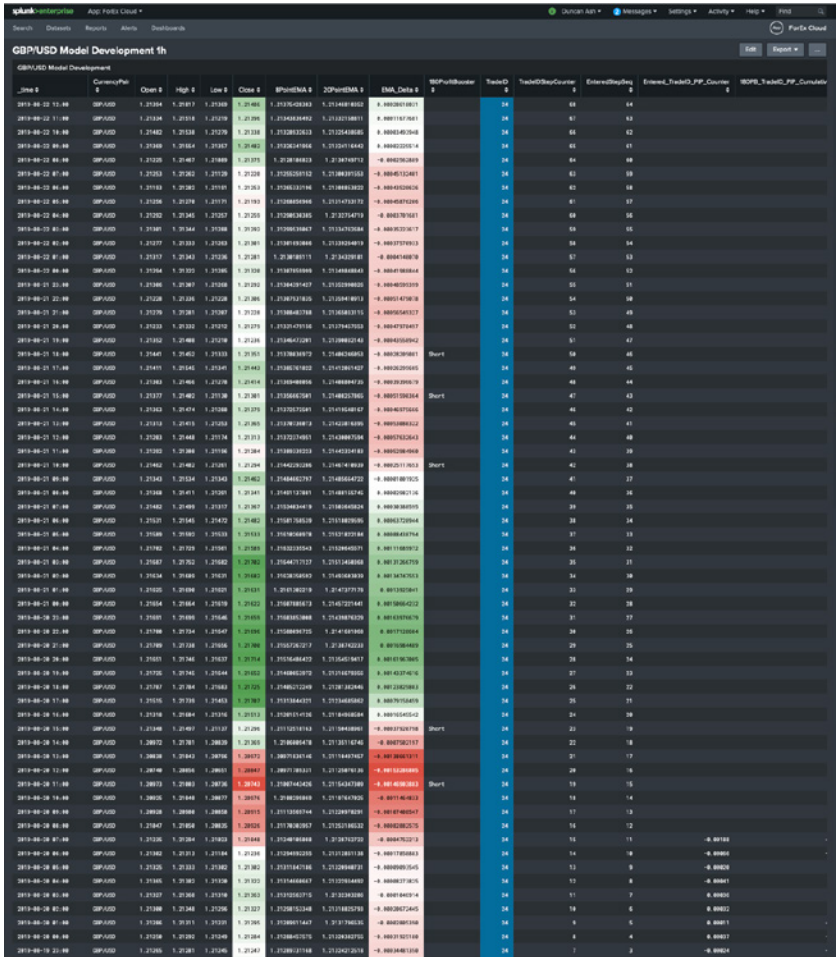
Value:

Reconciling the P&L quickly after a canceled or amended trade saves time and money and allows operational issues with specific products to be highlighted and resolved quickly.

Catching a trader who is acting outside of the allowed boundaries can save cost, reputation and sometimes large trading losses.



Firms that manage their trading and risk data in Splunk can build and manage their cancels and amends reports effectively, and refresh the data in near real-time. Thus you can easily spot anomalous activity and conduct further investigation.



By monitoring every trade in real-time, it is possible to understand the root cause of cancelled, ammended, or rejected trades, and identify the people and processes involved.

MiFID II – PREVENTING CLOCK-DRIFT AND FAILED TRADES

The business challenge:

Transparency, reporting and traceability underpin many of MiFID II's regulatory technical standards (RTS), including the requirement for an accurately recorded trail of events for audit and compliance.

Accurate time-stamping on financial transactions and messages involved in a trade life-cycle is a must, because it is essential for conducting cross-venue monitoring of orders and detecting instances of market abuse. It also allows for a clearer comparison between the transaction and market conditions prevailing at the time of execution. RTS 25 stipulates the following:

- Operators of trading venues, and their members or participants, shall establish a system of traceability of their business clocks to UTC.
- Operators of trading venues, and their members or participants, shall be able to provide evidence that their systems meet the requirements.

MiFID II requires that application servers be synced to UTC time with a maximum allowable divergence from UTC based on the type of trading platform. Problems in the network such as jitter, network load and instability can cause time offset inaccuracies, creating divergence from UTC and putting firms at the risk of breaching RTS standards. Firms must stay within the MiFID II boundaries specified below:

- High-frequency Trading Operations
- 100 microsecond maximum divergence from UTC
- 1 microsecond granularity
- General Automated Trading Operations
- 1 millisecond maximum divergence from UTC
- 1 millisecond granularity
- Manual Trading Operations
- 1 second maximum divergence from UTC

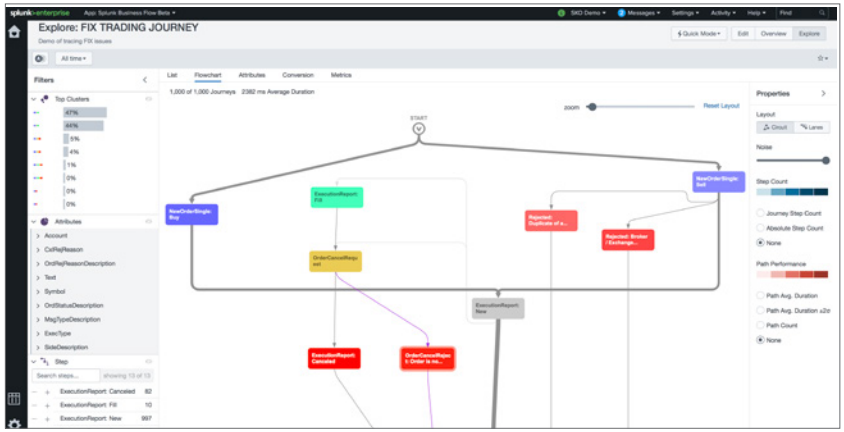
Reportable events, such as servers with clock drift beyond the tolerable thresholds and impacted trades, must be made available to regulators either continuously or on-demand with a five year history. Using established protocols, such as NTP and PTP, point monitoring solutions can be leveraged to report on clock drift across the infrastructure. However, identifying trades that have potentially been impacted with inaccurate timestamps is more difficult.

Splunk's approach:

Banks aware of the challenges associated with becoming MiFID II compliant are able to quickly build solutions to address the various reporting and monitoring requirements with Splunk in days instead of weeks.

Splunk is well positioned to report on clock drift across the trading infrastructure because it is a platform that can ingest and visualize all types of machine-generated data. Offering capabilities to correlate PTP and NTP time sources with trade messages (e.g., FIX), this gives trading venues and regulators a consolidated view of their compliance posture. Clock jitter can be visualized and alerts automatically raised in real time when drift exceeds allowable limits.

With Splunk, it is possible to quickly isolate trades that may have inaccurate timestamps due to excessive clock drift for further investigation and reporting to the regulators. Splunk could also highlight trades that have a different price from the Market National Best Bid and Offer (NBBO or EBBO for the European market) due to inaccurate clocks.



With Splunk, banks can monitor and report on business clock synchronization posture with Splunk, to help meet MiFID II RTS 25 compliance. Through clock data correlation with trade data, Splunk can enable you to identify individual trades that may have been impacted by clock drift.

Value:

Ingesting trade messages and clock drift data into Splunk can help banks become compliant with RTS 25 and save money at the same time by avoiding unnecessary purchases in expensive point solutions to help with RTS 25 compliance or high development costs associated with building a bespoke solution in-house.

Ingesting trade data into Splunk can open many other unintended areas of optimization. Banks often struggle to troubleshoot failed trades due to complex workflows and disparate systems. Troubleshooting the why and where a trade failed can take a significant amount of manual effort and time to rectify. Splunk can reduce the time to investigate failed trades down to minutes, ensuring fewer failed transactions.

IT OPERATIONS FOR FINANCIAL FIRMS

The business challenge:

Financial firms have some of the most demanding IT requirements of any industry. The global business operations that IT organizations must support create significant complexity. This includes:

- Global offices, employees and market operations
- A large customer base, distributed across multiple geographies, requiring 24x7 operations
- Diverse business partners, counter-parties, payment networks and trading venues
- Multiple public and private networks, including low-latency operations
- Thousands of applications, products and services
- Multiple regulators, currencies, languages and time zones
- Development teams with multiple environments.
- Technology being used as a competitive asset for the firm
- A challenging security environment with continuous cyber threats and data privacy concerns

The outcome of these complexities is typically a large IT organization, with very challenging service-level agreements, and the requirement for almost 100 percent uptime in a high-security environment.

Splunk's approach:

IT operations is where Splunk started, and it is the core that all of Splunk's products originated from. The first versions of Splunk were designed to address the challenges faced by an IT department when an application failed and the teams were faced with having to manually search through log files to diagnose a fault. Things have matured considerably since then as Splunk has evolved; it can now monitor thousands of systems in real time and correlate across thousands of data feeds, using the insights detected in real time to drive decision-making. IT professionals can make full use of machine learning algorithms that take signals from real-time data to predict when a system is likely to fail, and they can warn the staff before the event occurs, often preventing a system failure.

For teams managing IT in financial firms, this is close to utopia. Splunk enables teams in IT to proactively manage their entire environments; it enables the network operations center (NOC) to monitor the network in real time and allocate new resources as demand increases. It enables applications teams to forecast demand for their applications and make sure they have enough resources available.

Software developers use Splunk's DevOps capabilities to manage all aspects of the development lifecycle — this means that they have better controls around new code and better testing procedures and audit abilities, and they have the ability to change their operating model to one where new releases can be issued multiple times a day.

This improves customer satisfaction and results in higher quality code with fewer bugs.

IT operations teams must work closely with their security counterparts, and both teams can make full use of the same Splunk data platform to solve a multitude of use cases across IT and security, which are required in order to deliver high-quality services with the highest levels of security.

Value:

Value is realized by delivering exceptional levels of service with very high levels of availability and very fast resolution of problems. The operating model made possible through Splunk's machine learning and predictive maintenance means that many problems don't result in outages; in fact, they are never noticed by the users.

The trading teams that rely on low-latency operations are entirely dependent on IT to deliver 100 percent uptime and exceptional low levels of latency across their networks and trading systems. Failure in this area would lead to trading losses. Conversely, technology leadership that results in lower latency can lead to competitive advantage and higher profits.

Thousands of financial firms depend on Splunk to keep their operations running securely, delivering on the extreme technical demands of a financial organization.

"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

Read more about Splunk at TransUnion.

GLOBAL GRID COMPUTER PLATFORM OPERATIONS AND SECURITY

The business challenge:

Global banks and hedge funds are running highly complex distributed grid compute clusters, often comprised of thousands of hosts running hundreds of applications to power the risk and pricing systems that support trading, risk management and regulatory obligations.

FS firms have a heavy dependency on overnight batch cycles where workloads are predictable; however, the load on the grid platform can vary greatly and tends to service workloads run by quantitative analysts that are more ad hoc in nature.

Compute grids are used for the execution of large workloads that have to complete within a specific time. For example, an overnight risk batch may require hundreds of hours of CPU time, can only start at the end of the trading day and needs to complete before the start of trading the next day. The work is divided into tasks that run in parallel on the grid.

In recent years, these platforms have moved to leverage additional compute power from both the private and public cloud. Workloads still prioritize on-premise compute but leverage additional resources on demand in the following order on the grid — on-premise physical servers > private cloud > public cloud. A hybrid compute architecture complicates tracking and monitoring the health, performance and security of the grid platform as hosts dynamically join and leave the grid depending on the demand.

Quants effectively act as DevOps teams, continuously pushing new code releases to the grid platform. Grid platforms often run fully, or partly, on shared infrastructure, making it difficult to diagnose the root cause of system slowdowns, as problems cannot be diagnosed easily due to a lack of visibility into the shared environment. Grid teams are left to establish whether issues are related to code releases or contention/infrastructure issues for hardware, which can be a time-consuming and frustrating task.

The scaling-out of platforms and the distributed nature of the infrastructure demands tooling, which can build a comprehensive view of all components in near real time over a broad range of technology silos.

Splunk's approach:

Managing an efficient grid compute platform creates many challenges. Grid teams require complete visibility and end-to-end monitoring of system performance to ensure the proper running and health of the platform.

Multiple global banking customers use Splunk to monitor their distributed grid compute platforms, collecting log and metric data in the process from resource groups. Examples of such data include:

Logs from:

- Grid daemons
- Grid applications

OS Performance Counters:

- CPU, memory, network activity, etc.
- Virtualization tier metrics
- Storage tier metrics — IO, etc.

Scripted Inputs:

- Grid API calls — e.g., from the grid job scheduler
- DB queries

These data sources can be analyzed and correlated to help grid teams understand the behavior of their platforms and perform the following tasks more efficiently:

- Track and monitor system health in real time
- Decrease incident resolution and problem investigation times
- Improve efficiency and capacity management
- Driving system evolution and optimization
- Orchestrate more compute via Splunk when capacity on the platform cannot meet demand

Value:

Through the use of real-time proactive alerting, Splunk is able to notify grid teams when discrepancies arise on the platform, reducing screen time and freeing up engineers to work on implementing efficiencies.

Platform usage metrics can be monetized via unit cost lookups to help the business managers identify any inefficiencies in their use of the grid.

Real-time monitoring of the grid environment helps to keep the operations running at 100 percent, and predict future issues

MAINFRAME CONNECTIVITY AND ANALYTICS

The business challenge:

Mainframes exist in a heavily polarized environment. A 2018 Forrester investigation found that there is in fact an increase in the number of enterprises running critical applications on the mainframe, contrary to rumors of its demise, and with that comes a demand for increased capacity. The latest figures suggest that the value of credit card transactions processed on mainframes alone is $6 trillion annually. Skills shortages are becoming an ever-growing problem in the field, however, as is the reality that mainframes and their supporting staff often sit literally and figuratively separated from the rest of the IT in their environment.

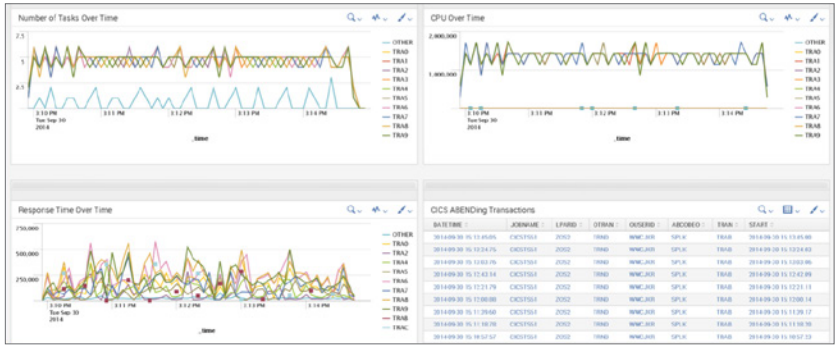
The growth is in no small part due to the fact that the mainframe's reliability, availability and system security is unmatched by any other platform, but this isn't without its challenges. Lack of visibility into million service units (MSUs) and rolling four-hour averages can have a serious knock on monthly license charges. This impact is particularly painful when the mainframe sits outside the visibility of an otherwise data-driven organization, siloed behind archaic and abstruse terminal tools that limit access to the transactional layer of an application's function. Managing the challenges of this silo is even more difficult when security and compliance become part of the picture, an issue recognized as the top one or two objectives by over 60 percent of mainframe customers.

Splunk's approach:

Point-based solutions are limiting when trying to monitor a mainframe as part of the wider landscape of IT and security platforms in an enterprise. With the support of Splunk and our vendor partners, it is possible to integrate even the expansive and complex logs found in system management facility (SMF) and mainframe SYSLOG into one platform that provides a real-time, 360-degree view of the whole IT infrastructure.

Integrating with Splunk's IT Service Intelligence (ITSI) helps organizations map KPIs to the mainframe components in their critical business applications, enabling complete awareness of the underlying services and visualization of the relationships within the application flow.

When the focus turns to security, Splunk can not only offer the ability to monitor and detect the course of data on and off the mainframe, but also provide cross-platform visibility to reduce the risk of insider threats while maintaining a reliable audit trail to satisfy security officers and auditors.



Track Customer Information Control System (CICS) transactions and gain visibility into overall performance, resource utilization and easily compare to historical data for trend analysis.

Value:

Manual processes for analyzing data are no longer sufficient. With the speed, volume and criticality of transactions, businesses can no longer afford to be purely reactive. Using Splunk to examine this vast data source in a broader context and to proactively identify problems can vastly reduce the MTTR. The ability to easily search and dashboard data in Splunk means that the mainframe data that was once virtually inaccessible to those who weren't mainframe experts is now accessible to more teams in business and IT, despite the diminishing pools of mainframe talent.

SERVER CONFIGURATION MONITORING AND MANAGEMENT

The business challenge:

Server configuration management and compliance go hand-in-hand when adhering to control frameworks from authorities such as the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), Payment Card Industry (PCI) or the British Standards Institution (BSI). These control frameworks outline recommended configurations and best practices designed to strengthen IT environments against attacks and to close obvious loopholes easily exploited by malicious actors.

In light of these frameworks, more and more organizations are required to scan their infrastructure to determine whether they comply with standardized security and hardening benchmarks. However, these requirements entail numerous challenges. For one, maintaining server configuration across multiple sites and data centers often creates significant administrative and maintenance overhead for IT teams.

Server misconfiguration can also create openings for hackers. Undocumented configurations that complicate the troubleshooting process can also be sourced to system outages resulting in extended downtime.

Additionally, loosely implemented change management policies and procedures can result in configuration drift, where servers become increasingly divergent over time due to manual ad hoc changes and updates.

Gaining a holistic view of server compliance, understanding which servers are repeatedly failing compliance checks, or identifying servers that have fallen out of compliance is challenging. More broadly, tracking whether the environment is trending toward becoming more or less compliant across multiple control frameworks requires a flexible approach to analytics and reporting — all of which is well suited to Splunk.

Splunk's approach:

There are multiple ways to leverage both Splunk technology and/or complementary technologies such as Puppet Software's 'Bolt' product to test for compliance. This can be done by scanning servers in an environment and checking for expected configurations, then creating a log event containing the relevant metadata to facilitate reporting in Splunk.

Puppet's 'Bolt' uses an agentless approach that connects to a server remotely via SSH or WinRM. Scripts can be developed in any framework such as Python, PowerShell or Bash and executed by any platform. Using this approach, it is possible to write scripts that check for configurations stipulated in frameworks such as the CIS controls and report on the results in real time.

Alternatively, scripted inputs can be developed as an app and deployed to the Splunk Universal Forwarders (UF) running on each host where they can execute the compliance checks and log directly to Splunk. Typically, the UF will already be widely deployed across a server estate at existing Splunk customers, which lowers the barrier to realizing the full benefits of the use case.

Going beyond configurations, Splunk allows you to retrieve other useful information from each host, such as a snapshot of installed programs. Scripted inputs can be configured to run at set intervals to constantly monitor installed applications. The data sent to Splunk can then be compared to a wish list of approved applications to spot mismatches and un-approved software.

Using both agent-based or agentless approaches, compliance checking can run multiple times a day, providing firms with an up-to-date view of posture against a controls framework with interactive Splunk dashboards.

PCI Compliance

The Splunk App for PCI Compliance is a Splunk-developed and supported app designed to help organizations meet PCI DSS 3.2 requirements. It reviews and measures the effectiveness and status of PCI compliance in real time. It can also identify and prioritize any control areas and let you quickly address any auditor report or data request.

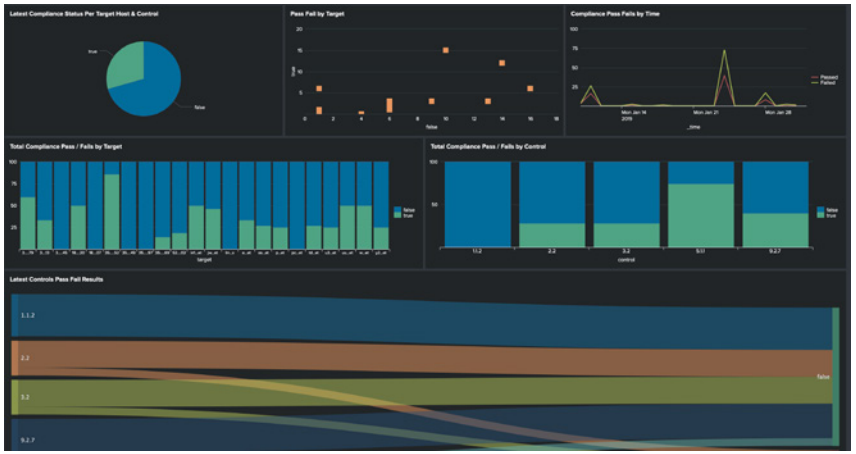
The app provides out-of-the-box searches, dashboards, reports, an incident response framework, and integration with employee and asset information to give you visibility into system, application and device activity relevant to PCI compliance.

Value:

With operational human errors and device mismanagement, two of the leading causes of IT outages, effective configuration monitoring becomes critical —not only to safeguard against attackers, but to help avoid downtime and to reduce lost revenue.

Splunk's ability to collect and visualize data from hosts and endpoints, as well as to execute custom scripts on the UF or other technologies, makes it an obvious choice for compliance monitoring across an IT estate.

With out-of-the-box solutions for many control frameworks, such as PCI compliance, along with community developed assets and scripts, Splunk is the ideal platform on which to execute a compliance monitoring strategy.



Real-time scanning of servers ensures that they are configured to the appropriate specification.

SYSTEM MISCONFIGURATION

The business challenge:

The foundation for securing any system is the operating system. Securing the operating system reduces the exposed attack surface when middleware or other applications fail to prevent direct access to the underlying system.

To this end, the Center for Internet Security (CIS) maintains that one of the most critical areas for securing an organization is "secure configuration for hardware and software on mobile devices, laptops, workstations and servers."

Among other things, this underscores the need for default secure operating system configurations that reduce the attack surface both on the network and locally on the system. Many operating systems ship with configurations that ease setup and use, but these systems often expand the attack surface by allowing easy execution of arbitrary code and escalation of privileges. Controlling and monitoring changes to system configurations enables users to maintain system security integrity while receiving alerts on unauthorized changes.

What is the impact?

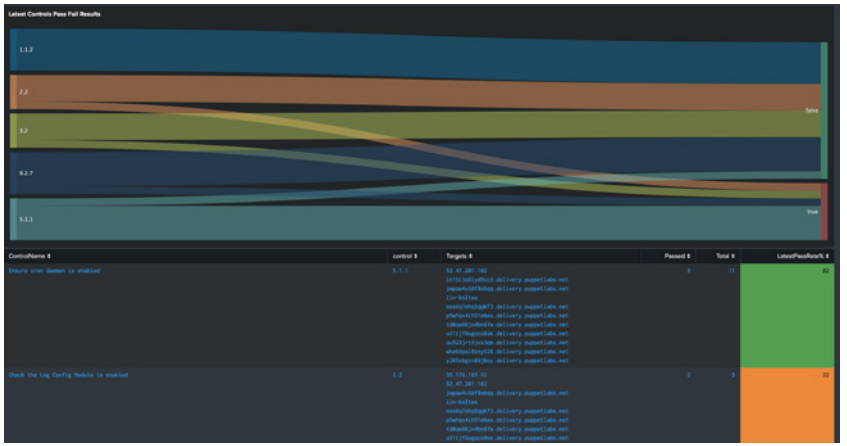
Systems that don't have secure configurations open the attack surface by providing a greater potential for miscreants to install malware or escalate privileges. Allowing malware to be installed provides the attacker with new vectors for control. In addition, allowing changes to the system without control or monitoring increases the ability for attackers to use the system as a base of operations for network scans, or give them the ability to spread malware and exfiltrate data.

Splunk's Approach:

Splunk can ingest data from system and network monitoring software, such as file integrity management (FIM) solutions, which can read content and permissions of files, as well as create checksums of static files. Splunk can also ingest data from port scanners, which check each port on an IP and reports on which ones answer.

In addition to ingesting reports and alerts generated by FIM and port scans, Splunk can compare the results against previously stored data and notify administrators about any changes.

Splunk can then act on the results in a number of ways. It can send alerts via email, or to external systems via API calls. It can open or otherwise interact with external ticketing systems, or initiate the orchestration or automation via a SOAR product, such as Splunk Phantom, which allows for immediate security response.



This screen shows how Splunk can be used to monitor configuration drift and notify an administrator about required changes.

Splunk Solutions:

Splunk Enterprise, Splunk Enterprise Security, Splunk Phantom.

MiFID II — TECHNICAL STRESS TESTING OF HIGH FREQUENCY TRADING SYSTEMS

The business challenge:

Transparency, reporting and traceability underpin many of MiFID II's RTS, including the requirement for an accurately recorded trail of events for audit and compliance.

MiFID II/Markets in Financial Instruments Regulation (MiFIR) sets out a number of reporting obligations in relation to the disclosure of trade data to the public and competent authorities.

The asset classes within the scope of MiFID II include:

- Equities
- Bonds
- Indices/baskets
- FX
- Interest rates
- Commodities

The legislation has several core objectives, including:

- Strengthening investor protection
- Reducing the risks of a disorderly market
- Reducing systemic risks
- Increasing the efficiency of financial markets and reducing unnecessary costs for participants

The regulations are designed to modernize and regulate new practices in trading, especially algorithmic trading and high-frequency trading, which have changed the face of trading in recent years, rendering the previous regulation set outdated.

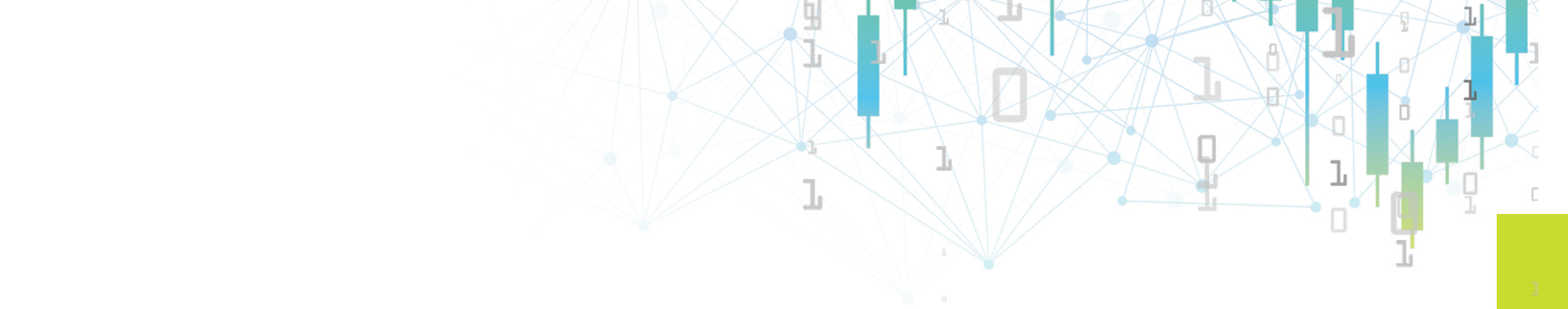
As more organizations have become dependent on algorithmic trading, there is a greater need to prove compliance — and the best way to do so is by providing real-time visibility into the underlying infrastructure.

Regulatory Technical Standards (RTS 6) — Stress Testing

As part of their annual self-assessment, investment firms shall test their algorithmic trading systems and related procedures and controls to ensure that they are capable of withstanding increased order flows or market stresses:

Such tests shall at least consist of the following:

- Running high messaging volume tests using at least twice the highest volume of messaging received and sent by the firm over the previous six-month period
- Running high trade volume tests using at least twice the highest volume of trading reached by the firm over the previous six-month period



Splunk's approach:

Below are extracts from MiFID II's regulatory technical standards pertinent to Splunk:

- Stress testing/capacity management (trading applications must handle >= 2* the throughput of peak volumes)
- Real-time monitoring and alerting of high-frequency trading and algorithmic trading systems
- Monitoring the performance and degree of usage of the elements of their trading systems in real time
- Retaining data for five years
- Identifying suspicious transactions or orders (machine learning)
- Avoiding unauthorized access to the whole or to any part of their trading system
- Monitoring access to investment firms' IT systems to ensure traceability at all times (privileged access review).

Splunk allows firms to leverage their existing Splunk platform to become MiFID II compliant more quickly, eliminating the need for point solutions or custom-built software to meet specific regulatory requirements.

Trading venues can meet obligations to report data to authorities, allowing the determination of the pre- and post-trade transparency.

Splunk's data retention capability allows firms to meet the data-retention requirements outlined by MiFID II while storing data. Data that reaches its retention age will automatically be deleted, ensuring data isn't kept longer than is necessary for compliance purposes.

Splunk's real-time engine allows customers to exceed the reporting and real-time alerting requirements stipulated by MiFID II and provides full visibility on authorized and unauthorized access through IT and application logs. The capacity of trading systems can be tracked during stress tests to ensure that there is enough capacity to meet the stipulated regulations.

Value:

Splunk can help customers become MiFID compliant without acquiring and deploying additional IT solutions.

The scalability of Splunk and its wide-ranging capability with real-time monitoring extends to data analytics, reporting, machine learning, alerting and monitoring of data that is pertinent to MiFID II.

CROSS BORDER INTERNATIONAL OPERATIONS

The business challenge:

Financial services firms that operate globally do so under a blanket of complex regulatory compliance requirements that subject them to different laws in each jurisdiction. Countries like Switzerland, Singapore and Brazil have strict data-protection laws pertinent to data leaving their borders. Banks often refer to these data safe havens as "restricted zones," meaning only employees located inside the respective restricted zone can access data stored in that zone.

Firms looking to standardize their data management across their global operations can struggle to design solutions that provide privacy in restricted zones and openness in unrestricted zones.

Splunk's approach:

Splunk's ability to support a highly scalable and distributed data architecture helps firms meet cross-border access requirements, ensuring that data generated in restricted zones can be stored at the point of origin to meet the regulatory obligations of each respective jurisdiction.

A user domiciled in a restricted zone will have access to data in that zone as well as access to data in unrestricted zones, job spec permitting. A user in a restricted zone will be unable to access data in another adjacent restricted zone.

For unrestricted zones, data can be consolidated in an enterprise Splunk cluster, ensuring that firms can search across their global dataset from a single location while excluding data located in restricted zones.

Splunk's enterprise-level feature set ensures that firms can design and deploy Splunk to meet their own data privacy requirements without custom development due to the almost unlimited number of deployment topologies available.

In addition to ensuring physical partitions in the Splunk architecture and segregating restricted and unrestricted zones, Splunk can also detect and report cross-border access attempts to management.

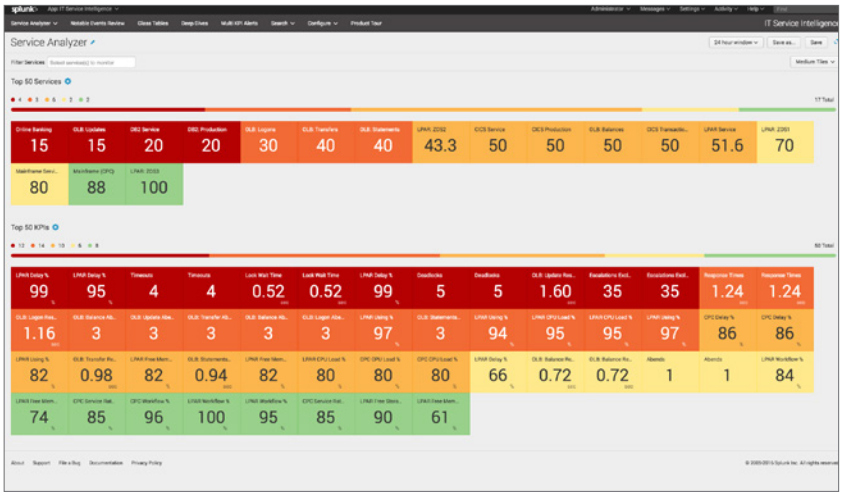
Splunk can ingest login data from Active Directory, network data and HR data to highlight users who are logging into systems outside of their domicile country. Splunk's mapping visualizations make it easy to identify cross-border access, where an employee is attempting to access systems and data in a restricted zone from outside, highlighting a possible compliance breach.

Login data can be visualized on a map and correlated with office locations to highlight logins from countries where there is no office presence, indicating potential rogue activity or hacking attempts.

Value:

Splunk ensures that companies can deploy the correct global enterprise architecture from the outset, ensuring that data segregation is built in by design and demonstrating to regulators that the architecture is compliant with their data-privacy and cross-border rules and regulations.

Splunk's ability to detect cross border access and hacks ensures that security teams have full visibility on cross border attempts, increasing the overall security and compliance posture of the firm.



Splunk ensures that companies can deploy the correct global enterprise architecture from the outset, ensuring data segregation is built in by design, and demonstrating to regulators that the architecture is compliant with their data privacy and cross border rules and regulations.

SECURITY AND FINANCIAL CRIME

FINANCIAL SERVICES SECURITY

The business challenge:

Security is a board-level issue in the financial services industry. Firms that experience a security breach quickly become headline news, and they have a lot at stake.

Securing a financial institution is one of the most complex tasks for security professionals; this is due to multiple contributing factors:

- Complex organizational structures and global operations
- A wide range of highly diverse products and the requirement to support legacy products for years
- High numbers of customers and employees
- A diverse range of access points for customers and employees
- Multiple networks including high-speed private networks
- Multiple counter-parties and third-party relationships with payment networks, exchanges and data providers
- Intense regulation and multiple regulators to comply with
- Being almost constantly under attack
- Social media

Most critically, banks have the most to lose. Physical bank robberies may be less common today, but cyberattacks are on the rise and continue to increase in their sophistication.

Splunk's approach:

Financial firms frequently rely on Splunk as the nerve center that supports their SOC. Splunk provides a platform of security products that allow a firm to conduct a wide range of security activities, from real-time data capture and advanced detection and threat intelligence to orchestration, automation and response. Splunk's products, including Enterprise Security and Phantom, come armed with hundreds of predefined scenarios that allow a firm to rapidly deploy its SOC and become effective very quickly.

Splunk's key strengths are its flexibility to correlate across thousands of data sources in real time while maintaining the flexibility to react to a new type of attack at short notice. Splunk's search processing language (SPL) allows users to build new searches at short notice so that they can maintain exceptional flexibility during an investigation and deliver results quickly, even in the most complex scenarios.

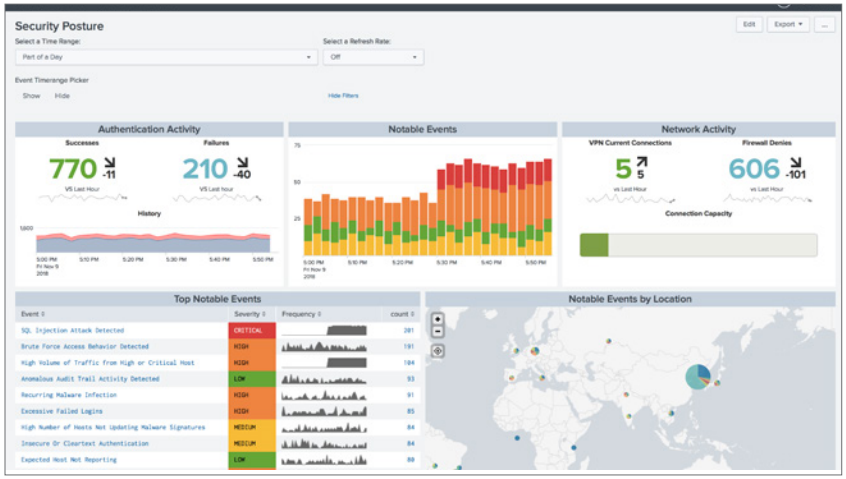
Splunk is used by the most diverse types of organization, from Aflac to the Bank of England and FINRA. Their business models are all different and their organizations vary considerably, but they are all able to deliver on their security obligations due to the flexibility of the Splunk platform.

Value:

The value of being able to stop an attack before it becomes an incident is hard to quantify in monetary terms, but it is of clear value to any organization.

In a security environment, it is necessary to have multiple tools and services — there is no single product that does everything. Splunk acts as the nerve center for security operations and is able to bring in data from any system and monitor all of your systems and operations in real time. Splunk Phantom handles the orchestration and automation of security events, making sure that critical issues are responded to promptly.

There are clear benefits associated with being efficient in security operations, being able to react quickly and being able to minimize time spent chasing false positives. Splunk allows firms to manage those operations while maintaining excellent service levels.



Security posture dashboards aggregate and prioritize notable events from across your ecosystem of security tools to help analysts respond with all of the context they need, or automate responses where appropriate.

"The success of a Security Operations Center starts and ends with knowing what is inside of your network. As hackers become increasingly sophisticated, that level of visibility is often challenging, especially when you are consuming more than 20 different security data sources like we are. Since implementing Splunk Enterprise Security as the brain in our security nerve center, we have found Splunk to be the right solution to quickly and effectively create and implement security analytics across a wide array of data sources and security use cases."

Tim Callahan, Senior Vice President,
Chief Global Security Officer at Aflac

Read more about Splunk at Aflac.

CREDIT AND DEBIT CARD FRAUD — DETECTION AND RESOLUTION

The business challenge:

Global card fraud has increased from an average of 4.78 cents per $100 in 2006 to 7.2 cents per $100 today, marking a significant increase in 12 years, fueled by growth in card payments and the increase in card-not-present (CNP) transactions. The U.S. accounts for 40 percent of the world's fraud in 2016, despite producing only 24 percent of the card transactions.

Credit and debit card fraudsters are utilizing a wide range of scams to obtain personal information, using tricks like malicious phone calls, phishing emails/websites and fake Wi-Fi hotspots on unsuspecting victims.

Skimming, a common method used, involves placing a discreet card reader on an ATM or point of sale unit (POS) to copy card details as unsuspecting customers withdraw cash. The details are later retrieved and used to make purchases or sold on the black market.

Contactless payment technology brings greater convenience to consumers but has resulted in an increase in card fraud as fraudsters look to exploit new card features.

Fraudsters can obtain radio frequency identification (RFID) scanners to steal payment card details by placing the reader in close proximity to the card. Similarly, near-field communication (NFC) can be used to share credit card information with point of sale units. Apple Pay, Google Wallet, Visa and similar apps use this technology for payments. A compromised NFC reader could be giving credit card information to a criminal.

Once card details and other personal details have been stolen, fraudsters can commit application fraud by taking out financial products using the details of others.

Splunk's approach:

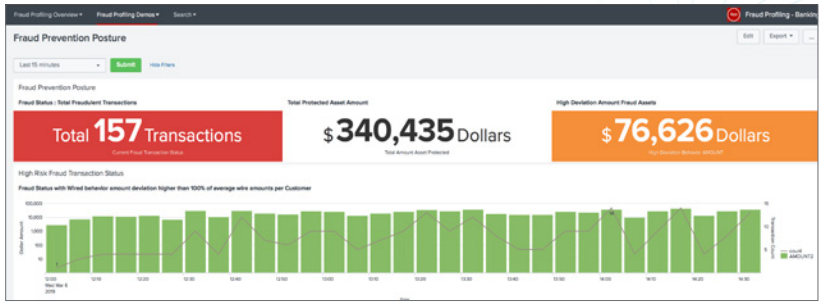
One of the most powerful tools in the fight against fraud is data and real-time analytics with machine learning. Using data, suspicious behaviors can be observed and acted upon. Below are examples of fraud use cases that are frequently delivered in Splunk.

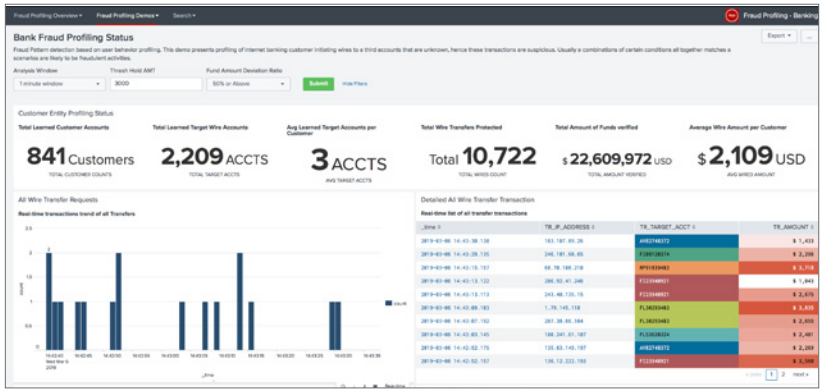
External fraud:

- Near-simultaneous ATM withdrawals from two or more geographically disparate ATMs involving a single account
- Single account having daily withdrawals in excess of normal limits
- Abnormally large wire transfers or a large number of transactions compared to the baseline
- Wire transfers going to high-risk countries/regions or financial institutions associated with fraud
- Multiple smaller payments from an account over a consecutive number of days

Internal fraud:

- Bank tellers conducting transactions out of normal hours or processing their own transactions
- IT staff or developers logging into an application to conduct trades
- Trader using credentials that don't match the owner of the physical workstation





Applying machine learning helps to pinpoint activity that is likely fraudulent, providing a near real-time view of fraud posture, to prioritize investigation or automate other mitigating actions.

Value:

Some fraud use cases require recent data to be detected. One such example helps providers detect cloned cards by identifying multiple withdrawals in quick succession from ATMs that are geographically distant. This attack is often referred to as a Superman attack, as it would typically be physically impossible for a human to travel from one ATM to another in the time frame to make multiple withdrawals.

Other use cases require vast amounts of historic data to create baselines of card holder behavior. For example, the average minimum and maximum amount transacted per account per day, so that deviations and anomalies can be identified.

Splunk can scale to analyze petabytes of data per day, allowing payment providers to formulate more advanced fraud detection and to alert in real time. **Splunk Phantom** can be used to automate playbooks that act, removing manual user intervention when fraud is detected; for example, canceling a credit card and ordering a new one.

Most banks provide fraud cover as part of their services to their customers. If a card holder is the victim of fraud and he or she hasn't acted negligently, the bank will reimburse losses; therefore, identifying fraud more quickly has a direct impact on profitability.

"PostFinance is using Splunk as a fraud platform, using the insights to protect their customers' bank accounts and digital payments. In their online banking portal alone they have over 1.6 million customers they have to protect. They are not just detecting and identifying new fraud patterns with Splunk, they are also operationalizing their fraud workflow which enables them to escalate issues to law enforcement and easily make all required details available."

PostFinance DIE POST

Read more about Splunk at PostFinance.

INSIDER THREAT DETECTION

The business challenge:

A rogue trader can act independently, often in a reckless fashion, pursuing high risk/reward strategies and bypassing internal controls in the process. Over the years, banks have developed sophisticated risk models to control the trading of instruments; however, internal controls are not infallible. A determined trader can find a way to circumvent the system in an attempt to reap increased gains.

Banks are looking to bolster their compliance and operational risk control functions by designing and developing complex employee intelligence capability systems to monitor employee behavior and proactively identify potential insider threat risks to the firm. Such systems provide a holistic oversight and monitoring of employees, helping to detect and prevent rogue activities, data leakage and fraud using advanced analytics and machine learning capabilities.

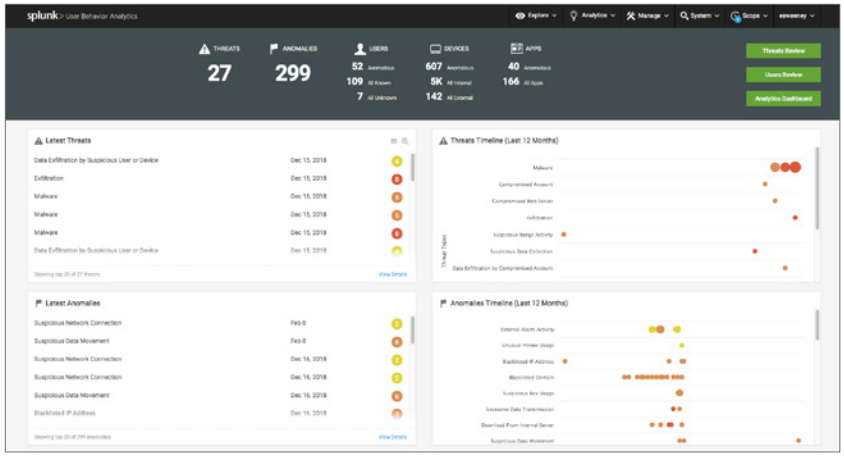
Identifying areas or employees of concern through analytics can allow banks to take preventative action in the form of training and awareness initiatives, modifying internal controls, introducing new rules and procedures or even applying disciplinary action in extreme cases to maintain integrity, promote accountability and prevent fraud — all of which will reduce risk.

Splunk's approach:

Each organization develops its own criteria to identify insider threats or rogue employees and to catch illegal conduct. This is initially accomplished with rudimentary rules and progresses to more complex use cases over time, incorporating techniques like peer group analytics. Customers who have implemented Splunk and on-boarded common IT ops and security–related data feeds will be able to leverage this data to build employee intelligence monitoring use cases immediately, leveraging their existing investment and reducing the time taken to source data, improving their compliance posture.

Splunk allows customers to build custom dashboards for employee monitoring. Splunk Enterprise Security contains prebuilt dashboards that provide visibility on common user activities that indicate risky behavior, and Splunk User Behavior Analytics (UBA), with its advanced threat detection capability, discovers abnormalities and unknown threats that traditional security tools miss by using deep investigative capabilities and powerful behavior baselines on any entity, anomaly or threat.

Banks are required to enforce a period of mandatory block leave for each employee every year, ensuring that any illegal scam or trading arrangement can be uncovered. By correlating login data to IT systems with building access data and HR data, banks can check to see whether employees have accessed systems or buildings during that time, violating their block leave.



Automate threat detection using machine learning so you can spend more time hunting with higher fidelity, behavior-based alerts for quick review and resolution.

Value:

Leveraging the Splunk analytics platform, banks can report across a wide variety of employee behavior use cases to spot anomalous behavior through various statistical and machine learning techniques. Below are a few examples that are commonly delivered using Splunk.

- Malware detection — Indicates employees accessing harmful sites
- Accounts that are frequently locked out
- Users with high web traffic, uploads/downloads
- Users with non corporate email activity
- Users logging in from distant locations compared to their previous logon in a short time window
- Learning from prior offenders to highlight likely future offenders before they offend
- Using company credit cards up to their limits
- Unusual phone bills compared to peers
- Access during block leave

"Splunk has positively impacted our business in a number of ways. We've gained an efficiency level of over 50% in our analysts' ability to speed investigations. Splunk UBA is giving us deep insight into our insider threat within NASDAQ and also what our trusted users are doing at any point in time."

AVP, NASDAQ

Nasdaq

Read more about Splunk at NASDAQ.

DATA EXFILTRATION

The business challenge:

Data exfiltration is the unauthorized transfer of data from an organization. It is often one of the last steps in a cyber-attack. One of the most challenging aspects of data exfiltration is that it can be carried out in many different ways including via automated scripting, data encryption, network protocols, truncation data and physical exfiltration.

This makes it very difficult to know how to mitigate the threat. For financial services firms, data exfiltration present a significant challenge attributed to increasingly open IT architectures, customer focused technology adoption trends and the complexity of legacy IT systems. While these challenges heighten the opportunity for hidden data tunnels, they also allow exfiltration to happen in plain sight.

Data exfiltration within financial firms can have a serious impact on financial posture and reputation. The September 2017 Equifax breach entailed the data exfiltration of personal identifiable information (PII) that affected more than 148 million people. During the 76-day cyberassault, attackers leveraged more than 9,000 undetected queries to access an unencrypted database holding PII data . Reports indicated that the total cost to Equifax was in excess of $275 million coupled with another $200 million spent on security infrastructure.

Splunk's approach:

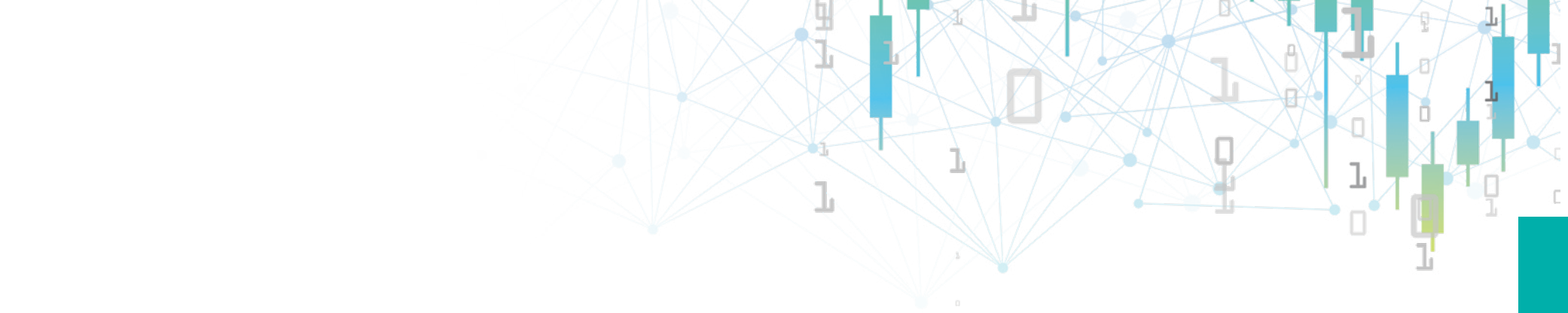
Our approach to detecting and responding to data exfiltration is founded on effective security analytics. Splunk enables organizations to deploy a range of data-driven approaches to detect and respond to data exfiltration attempts. A good first step is to understand the location and criticality of the data you hold and how this data could be accessed.

Once this is known, the Splunk Enterprise analytics platform, along with its security applications, can be put to work to detect and help respond to data exfiltration indicators. (These applications are listed at the end).

This can take the form of anomalous pattern detection within network traffic to leveraging advanced machine learning algorithms to identify unknown or suspicious behaviors. It could also include automating investigation or response workflows to decrease detection or response times as well as the overall dwell time of the attack.

With prescriptive analytics, Splunk also supports mapping to many industry standards such as the MITRE ATT&CK framework and the Cyber Kill Chain — both of which help financial firms take an industry framework approach to developing effective mitigation.

Financial firms need to develop these techniques in conjunction with good security hygiene practices such as operational maintenance and IT systems patch management, as well as the deployment of effective security measures such as data encryption and access controls.



Value:

Preventing data exfiltration has multiple benefits, including:

- Intellectual property and trade secrets protection
- Personal data protection, including information covered under GDPR and the California Consumer Protection Act
- Brand and reputation protection
- Avoiding fines and penalties
- Improved competitiveness

Relevant Splunk Solutions include: Splunk Security Operations Suite (SOS or Enterprise, ES, UBA and Phantom).

Extra information:

Customer reference: JPMorgan Chase – conf17 Talk: https://conf.splunk.com/files/2017/slides/advanced-security-monitoring-for-critical-groups-or-applications.pdf

Customer reference: Bank of England – conf18 Talk: https://static.rainfocus.com/splunk/splunkconf18/sess/1523600777506001XL1W/finalPDF/ SEC1930_Protecting1TrillionEveryday_Final_1538667181374001 2mEd.pdf

News Story:

[1] Hutchins et al.. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Retrieved August 18, 2016.Â

[2] https://attack.mitre.org/tactics/TA0010/Â

[3] https://www.teiss.co.uk/threats/is-data-exfiltration-an-insurmountable-challenge-for-the-financial-services-industry/Â

[4] https://threatpost.com/financial-services-sector-rife-with-hidden-tunnels/132987Â

Link to Threat:

[1] http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

[2] https://www.gao.gov/products/GAO-18-559

ADVANCED TARGETED ATTACKS

The business challenge:

Advanced Targeted Attacks and advanced threats, including Advanced Persistent Threats (APTs) pose some of the biggest risks to enterprise systems. These threats, which are typically executed by nation-state actors, have a long lifecycle, and their impact can be devastating.

Attackers can infiltrate the network and stay undetected for weeks, months or even years, silently collecting information about their target before finally exploiting detected vulnerabilities.

One of the most infamous of such attacks was the Bank of Bangladesh Heist, in which attackers reportedly transferred $81 million to remote accounts in the Philippines and Sri Lanka — an attack that became one of the biggest digital robberies of our time [1]. During this assault, attackers used the SWIFT network to execute the fund transfers after first taking over the account.

Once the attackers gained access to the network, they installed malware designed to hide any traces of the fraudulent payments from the bank's local databases [2].

What is the impact?

Financial Risk: There is clear and obvious obvious financial impact for the affected institution. In these attacks, cybercriminals will exploit vulnerabilities to transfer funds externally with the goal of significant financial gain. In the Bank of Bangladesh attack, attackers managed to steal only $81 million because of a typo in the forged fund transfer instruction that prevented the remaining $900 million from being pilfered. And once money is transferred via SWIFT, it is typically irreversible.

Reputational risk: It can be argued that reputational risk has a more significant impact on an organization than financial loss. If an organization earns a reputation for being lackadaisical about security controls following a breach, it will likely lose critical trust from shareholders and customers alike.

Splunk's approach:

Splunk's platform offers a full Security Operations Suite addressing the entire security lifecycle, from threat investigation to monitoring, analysis and orchestration functions. By ingesting both machine data and any type of structured data, anomalous behaviors can easily be detected by identifying correlations between associated data points.

For example, streamed network data can be correlated with real-time transactions and structured customer and account data to provide full visibility across the entity's entire profile. Endpoint data can also be monitored, for example, to check if an anomalous process is executed on the SWIFT system after a user accesses an account at an abnormal time.

These capabilities are coupled with 'Content Updates' within Splunk's Enterprise Security product — a set of correlation searches developed by researchers and released monthly to all ES users. As soon as a detection occurs, Splunk's Phantom product can take automated actions to orchestrate the environment and connect to more than 260 third-party technologies to act in real time.

Finally, Splunk's User Behaviour Analytics product uses machine learning (ML) models to detect insider threats, which are vital in an ATA scenario.

Splunk Solutions:

Splunk Security Operations Suite (Splunk ES, Splunk Phantom, Splunk UBA).

Extra information:

Customer Reference & Link: https://www.computerweekly.com/news/252449918/How-Bank-of-England-is-using-Splunk-for-proactive-security

Related news story to the threat:

https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

https://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv/bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DR

Link to specific threat:

[1] https://www.splunk.com/blog/2016/04/29/lessons-learned-from-the-swift-attack.html

[2] https://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

Monitoring for malicious URLs is one of many defenses and controls in a security environment.

PHISHING

The business challenge:

Phishing continues to be the top threat vector for cyberattacks, in part because exploiting human vulnerabilities is one of the most successful paths for threat actors targeting organizations and individuals. Thus, traditional phishing attacks have increased 12 percent, accounting for 47 percent of all fraud attacks types detected in 2018.

A phishing attack is one in which where the attacker exploits social engineering techniques to perform identity theft. Phishing traditionally functions by sending a forged message, often through email, DM or social media, mimicking an online bank or payment sites. The message directs users to a bogus web page that is carefully designed to look like a login to the actual site. From there, the attackers attempt to collect sensitive and personal information such as usernames, passwords, credit card numbers, and even money by impersonating a legitimate entity in cyberspace [2].

A phishing attack has three main characteristics: 1) a legitimate entity must be spoofed; 2) the spoofing process must involve a website, which distinguishes itself from some scams (e.g., muling); and 3) sensitive information about the entity must be solicited [3].

A variant of phishing attacks, spear-phishing, targets specific personas in an organization by sending them highly personalized messages. This type of attack is becoming more prevalent, and is now associated with many of the largest cyberattacks in recent history including those on JPMorgan Chase & Co., eBay, Target, Anthem, Sony and numerous U.S. government agencies [4].

What is the impact?

Phishing attacks can have serious consequences for victims.

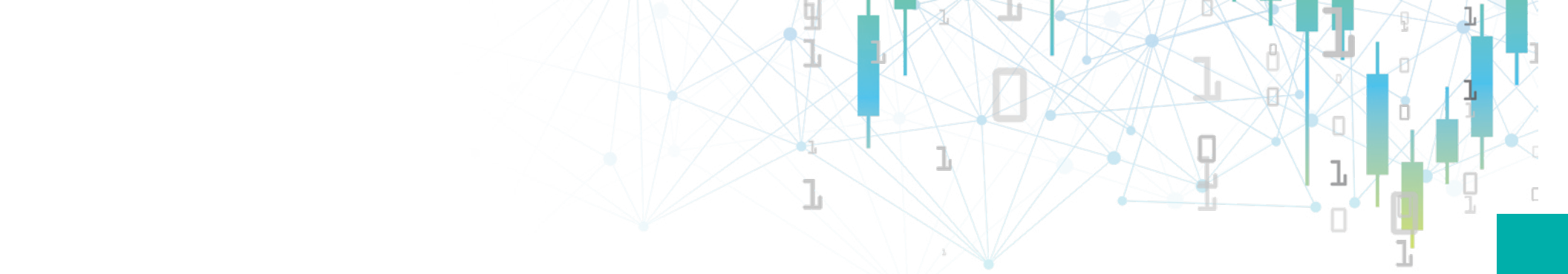
More than anything else, these attacks are incredibly costly for organizations. According to Accenture & Ponemon's "Cost of Cyber Crime report 2019," the average annual cost of cybercrime for banking accounted for $16.55m in losses, with the average annual cost for a phishing attack increasing from $1.3 million in 2017 to $1.4 million in 2018.

It's not surprising that more than 80 percent of companies that experienced a spear phishing attack reported copious damage and loss to their businesses. The most significant losses included employee productivity (41 percent), financial (32 percent), company reputation (29 percent), damage to brand reputation (27 percent), customers (25 percent) and intellectual property (25 percent). What's more, following these attacks, some organizations experienced drops in stock prices to the tune of 15 percent [5].

These attacks occur on a regular basis and are only increasing. According to recent studies, 84 percent of organizations said spear phishers successfully penetrated their organization. A recent Cloudmark spear phishing survey found that roughly 70 percent of respondents reported that their organizations implemented a specific solution to prevent spear phishing, investing an average of $319,327 over the past 12 months. However, 84 percent of respondents estimated that spearphishers had penetrated their organization's security solution, estimating that 28 percent of attacks had gotten through.

Looking ahead, phishing attacks are moving to mobile devices. Since 2015, mobile phishing attacks have increased by 680 percent, with one in five now attributed to mobile apps. Hardly surprising, as 82 rogue apps are being published every day on mobile app stores, according to RSA.

These mobile attacks include Smishing, or using SMS texts instead of email to deliver the payload; Mobile 2FA Phishing, a variant of Smishing, in which the attacker attempts to bypass two-factor authentication; and mobile malware which exploits mobile OS vulnerabilities to gain access and control over a user's mobile device. Whether via email, social media or mobile devices, phishing still works — and it's not likely to go away anytime soon [8].



Splunk's Approach:

Many firms have already implemented solutions to address phishing incidents. Standard detection and remediation solutions allow customers to check, sanitize, and/or remediate malware from a single email item, a process which takes from 30 minutes up to six hours. This is where automation comes in, which can reduce these times to less than a minute.

Phantom — the leading Security, Orchestration, Automation and Response (SOAR) platform — provides an orchestration and automation platform aimed at reducing a phishing investigation to mere seconds. Specifically, Phantom helps create automated workflows, which facilitate automated actions, decisions and analyst interactions with the flow involving various technologies. This in turn invokes API commands and orchestrates them so that the analyst won't have to operate these tools manually. Phantom offers by far the largest library (250+ integrations) of apps, with new ones being created almost every week.

Splunk and Phantom work seamlessly together: The Phantom app for Splunk allows for bidirectional integration of the two so that users can search, run queries or ingest events, among other actions. This enables workflow initiation for existing investigations to be enriched, or vice versa. To help the security teams visualize their work, Splunk taps into the Phantom database to create complex reports and dashboards based on your data.

By bringing the time these investigations to under a minute for a single email, we help organizations to minimize their effort as well as empower them to take action on every single malicious item. Thus, we help our customers save time, frustration and costs, while ensuring they run a successful and happy security team.

Splunk Solutions:

Splunk Phantom, Splunk Core or ES.

Extra information:

https://www.splunk.com/pdfs/customer-success-stories/blackstone-case-study.pdf

Blackstone [9]

Related news story to the threat:

Works Cited

[1] Phishlabs, "2018 PHISHING TRENDS & INTELLIGENCE REPORT," www.phishlabs.com, 2018.

[2] L. Z. AHMED ALEROUD, "Phishing Environments, Techniques, and Countermeasures: A Survey," 2017.

[3] Z. &. W. C. Ramzan, "Phishing Attacks: Analyzing Trends in 2006," in Fourth Conference on Email and Anti-Spam , California, USA, 2007.

[4] Cloudmark, " Spear Phishing: The Secret Weapon Behind the Worst Cyber Attacks," 2016. [Online]. Available: https://blog.cloudmark.com/2016/01/13/spear-phishing-secret-weapon-in-worst-cyber-attacks/.

[5] Fireeye, " SPEAR-PHISHING ATTACKS WHY THEY ARE SUCCESSFUL AND HOW TO STOP THEM," Fireeye, 2018. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf.

[6] Ponemon Institute, "THE COST OF CYBERCRIME," Accenture Security, 2019.

[7] CSO, "This is how much spear phishing costs companies," 13 January 2016. [Online]. Available: https://www.csoonline.com/article/3022164/this-is-how-much-spear-phishing-costs-companies.html.

[8] RSA, "2019 CURRENT STATE OF CYBERCRIME The Digital Transformation of Cybercrime," RSA, 2019.

[9] Splunk, "Automating Malware Investigation at One of the World's Leading Investment Firms," 2018. [Online]. Available: https://www.splunk.com/pdfs/customer-success-stories/blackstone-case-study.pdf.

ANTI-MONEY LAUNDERING

The business challenge:

Global money laundering is estimated at two percent to five percent of global GDP by the International Monetary Fund, equating to approximately $800 million and $2 trillion, yet only one percent is seized by authorities due to outdated anti-money laundering systems.

Many financial services firms operate in a decentralized fashion and have not conducted thorough anti-money laundering (AML) risk assessments across their global portfolio, leaving the possibility for shrewd money launderers to operate between the cracks.

There have been recent cases in which banks have been criminally charged and heavily fined to the magnitude of hundreds of millions of dollars for failing to investigate and report suspicious transactions and having inadequate controls and checks on customers.

Adding to challenges, old technology and outdated AML systems lack coverage across a global enterprise and generate a high degree of false positives, rendering them of limited use. The Financial Action Task Force (FATF), states that financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Financial data that spans five years can grow to huge volumes that make managing and accessing the data to produce reports challenging, typically requiring a high level of technical expertise to produce.

Splunk's approach:

Splunk can help financial services in the fight against money launderers through its data analytics platform, which is able to centralize deriving insights from data, providing FS firms with a holistic view across data sources that have relevance to money laundering. Where data cannot be moved out of country, Splunk's architecture allows for the data to be searched remotely, providing access and visibility to geographically disparate data sources, alerts and contextual reference data needed to effectively detect money laundering attempts.

Splunk's scalable enterprise architecture allows organizations to ingest and store vast amounts of raw data, both structured and unstructured, for the purposes of meeting compliance requirements and providing monitoring of existing blind spots.

Users have the ability to easily search, correlate and visualize the stored data without programming skills, democratizing AML and allowing compliance teams to monitor transactions, perform investigations and automate tasks. More advanced users can use the Machine Learning Toolkit to develop AML models able to identify outliers.

Splunk AML apps exist on Splunkbase to help customers get started and help analysts and bank officers in:

- Detecting suspicious patterns of transactions based on individual historical data
- Discovering attempts to split up large amounts of cash transactions over time

- Alerting to unexpected activity on dormant bank accounts
- Identifying transactions between parties with virtual offices
- Screening sanctions/blacklists

Splunk's analytical capabilities help customers identify fraud as an entity, rather than just an analysis of unusual transactions.

Dashboard and summary view of ATM transactions help to pinpoint anomalous activities worthy of investigation.

Value:

Money laundering is illegal because it allows criminals to profit from crime and it usually involves the accomplishing of more than one illegal step. AML efforts require FS firms to invest in new technologies that address the vulnerabilities in the current approaches, in order to have a chance of significantly reducing the large amount of money laundering that goes undetected today. This demonstrates to regulators that they are taking AML seriously and helps them to avoid heavy fines.

INSURANCE FRAUD
DETECTION AND PREVENTION

The business challenge:

Tackling insurance fraud remains a strategic industry priority. Currently, billions of dollars worth of false insurance claims are filed annually with the intent to defraud insurance providers. While insurers are implementing increasingly advanced detection strategies, due to the pervasive nature of the problem, it is estimated that billions more in fraudulent claims go undetected. Fraud negatively impacts insurers' claims loss ratios, used to calculate pricing, while honest policy holders are left to foot the bill through higher insurance premiums each year.

Insurance companies are investing heavily to combat fraud with innovative data-driven approaches to aid detection. Typical fraud methods, such as identifying policy holders who increase their level of cover shortly before damage or theft occurs, can be highlighted through simple queries on policy holder and claim data obtainable from the insurer's database.

Using telematics, some insurers are incentivizing their policyholders with lower premiums on the condition that they fit specific tracking devices to their vehicles that record millions of data points. These devices capture information such as GPS location, driving speed, distance, time, rapid or smooth acceleration style and braking and cornering habits, all of which can be used to create a crash reconstruction report, shortening the investigation time and equipping the insurer with valuable data that can help them dispute false claims, such as whiplash in minor bumps or crashes.

Splunk's approach:

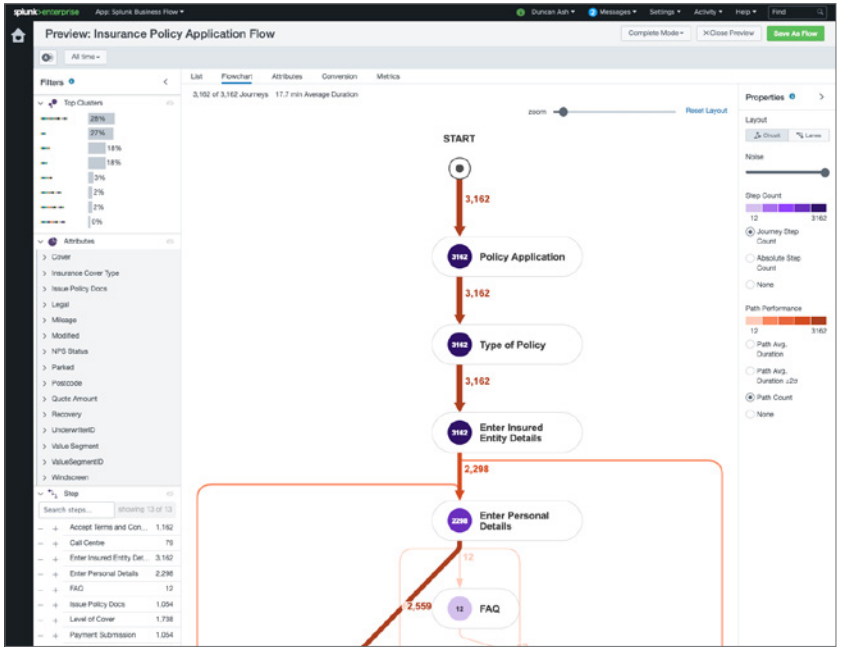
One of the most powerful tools in the fight against fraud is data. Insurers are realizing that the more data they have, the better able they are to apply analytics to detect fraud with a greater degree of accuracy and coverage. Identifying and predicting fraud no longer relies solely on data from the policy and claims database, but from a much broader range of external sources, such as social media, IoT devices, call center data, website data, credit scoring agencies and even weather data.

Splunk acts as an integrated data platform allowing insurers to fully harness disparate data sources to build a more accurate picture of fraud in real time. This enables them to deliver a broad range of searches, from simple query-based use cases to predicting fraud candidates with more complex techniques that leverage guided machine learning models built with Splunk's Machine Learning Toolkit.

Value:

An integrated data solution will enable insurers to automate decisions and mine valuable insights, a key to running a more profitable business and gaining a competitive advantage in the sector.

Splunk's real-time engine enables claims assessors to be alerted that they are working on potentially fraudulent claims even before they have completed assessing the claim, saving the organization time and money while ensuring that fraudulent pay-outs are reduced.



Being able to see the premium application process in full allows a carrier to understand where to process is not performig, or where customers are changing their details to get a beter quote.

Splunk 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. 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."

Blackstone

Read more about Splunk at Blackstone.

SUPERVISION AND COMPLIANCE

SANCTIONS COMPLIANCE

The business challenge:

Increased globalization and a changing adversarial landscape can complicate the ability of financial services firms to comply with sanctions administered in multiple jurisdictions and by multiple agencies, increasing the risk of sanctions violations occurring through operational oversight.

Financial firms are expected to highlight suspicious transactions and have adequate controls, checks and balances in place on customers to identify sanctions violations or money laundering attempts and are encouraged to voluntarily disclose violations for both past and present transactions. Self-disclosure is viewed favorably by regulators and is considered a mitigating factor.

Regulatory reviews typically inspect the violation reported and the quality of a company's sanction compliance program for signs of negligence. Having robust tools and processes to monitor for sanctions abuse is critical to increase a firm's confidence in meeting regulatory expectations, meaning regulators will look at cases more favorably and the banks will avoid hefty fines and brand damage.

Splunk's approach:

Financial firms must leverage threat intelligence sources that contain data about identified targets and correlate them with internal processes and systems to identify when sanctions abuse may occur. The nature of the data provided tends to be unstructured, making it difficult to store and analyze except by using a tool like Splunk that can correlate structured and unstructured data together and provides a mechanism to enter free-form text search to quickly pinpoint screen names for known or suspected targets.

Splunk's real-time engine can be used to alert compliance staff every time a known target is correlated between data from a threat feed and data from other operational sources with incident tickets being raised automatically to ensure incidents are handled with the correct level of severity and urgency.

Sanctioned parties constantly seek new methods to circumvent controls and evade sanctions, making the screening of names alone an insufficient control. It is crucial that financial firms have a security analytics platform that provides the ability to detect violations with more advanced approaches, such as performing geographical lookups on all incoming traffic to identify clients that may be connecting from prohibited locations.

Value:

The fines for sanctions violations can be substantial. In many cases, civil and criminal penalties can run to several million dollars. Large penalties directly impact profitability and the reputation of the firm. Demonstrating to regulators that due care and diligence have been applied to sanctions compliance through a demonstrable monitoring and reporting platform with effective controls to detect illegal activity will go a long way toward reducing the chance of fines.

With the Splunk analytics platform in place, The Japan Net Bank, Ltd. (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.

Japan Net Bank

Read more about Splunk at Japan Net Bank.

AUTOMATION MONITORING

The business challenge:

Traditional Banks are being threatened by smaller and more agile FinTechs that can innovate and quickly move from idea inception to product launch, giving them a time-to-market advantage.

Banks are looking for optimizations across technology, such as automating routine and repeatable tasks. Subsequently, they are investing in toolsets that allow them to reduce manual intervention for processes in an effort to become better, faster and more cost effective, allowing them to do more with less.

The challenge is that every new banking opportunity presents risks. Some of these risks include a repeated task behaving in an undesirable way, either accidentally or maliciously. They also include risks with automation that could return an undesirable result hundreds or even thousands of times before anyone notices — if they do at all — or the risk of automation exposing confidential or otherwise sensitive data.

The risks are clear, and banks should consider how they can ensure that there is an immutable trail and proactive monitoring of their automation tools and tasks. If a bank needs to explain to regulators why an automated task existed, what it interacted with, when it took place, what it queried and what was changed, they will have readily available proof at their fingertips.

Rules around monitoring people exist to protect their privacy; however, unlike humans, automations should be monitored unreservedly to ensure all actions are understood at all times. Controls like mandatory block leave exist to help companies identify rogue employee behavior. However, no such controls exist around automation, which means in theory a rogue employee could create an automation to carry out malicious tasks that could go undetected.

The degree of visibility for a process automation flow, as well as when it deviated from its normal flow and who was responsible, are all questions that organizations need to answer with 100 percent confidence.

Splunk's Approach:

Splunk has the ability to capture each step in an automated playbook and hold it in its immutable data store, from automation tool logs to the systems they interact with, such as programs, applications, databases and security-controlled services.

Because automation tends to generate dynamic events, data from these systems is naturally unstructured. This includes information like:

- Inputs (DB queries, OS commands, RPA clicks)
- Resultant outputs received (exceptions, textual results, return codes)

This data is difficult to process using traditional analytics and fixed rulesets. Splunk can work with this data to observe patterns that deviate from the normal path and behavior.

With Splunk, banks can report on automation statistics, like the number of automations successfully completed, time taken to execute, and other related performance KPIs. They can also proactively monitor playbooks for unusual activity in real time.

Is a playbook calling the password vault as expected, or has a username and password been hard-coded into the automation, allowing it to bypass this step? Is the automation leveraging the CMDB, or is it using a static list of assets uploaded as a csv file? Does an automation that has been migrated to production still call assets in the Dev and UAT environments?

By capturing logs from the automation tools as they occur, banks can prevent logs from being modified by a rogue automation engineer subsequently validating them across all automation tooling.

Using Splunk's analytical capabilities, playbooks can be baselined and reported on, while anomalous automations can be detected when deviations from typical behavior occur.

Splunk Business Flow can present the journey of each playbook in a flow diagram, making it easier to identify when playbooks are behaving unusually or have changed behavior altogether.

Business Flow plots each journey and the number of times it occurs, illuminating latency between each step to show typical behavior while also identifying edge cases.

Splunk can help to ensure due diligence, and that calls to other systems fall in line with expected behavior.

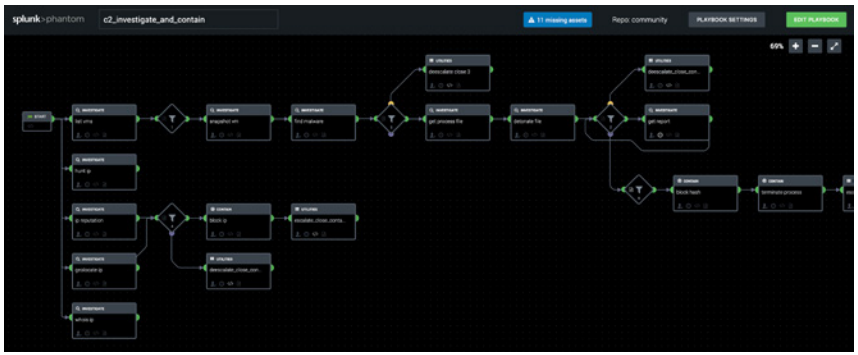
Value:

Automation has now become a board-level discussion item, due to the efficiencies, cost savings and return on investment (ROI) that it brings to an organization. And because the ROI can be quantified, banks are actively looking to automate as much as possible with roll-outs monitored at a management level.

Like any technology, automation tools can be subject to abuse. Used in the wrong way, they can potentially wreak havoc or cause long-term damage to a bank on a large scale.

Banks need to ensure that the automation technology is used in the correct and expected manner, while implementing certain precautions to protect against malicious use.

Implementing monitoring with Splunk to provide observability will mitigate the risk of abuse or unintentional mistakes, while also providing agility in response to regulator requests.



Automating processes allows firms to compete more effectively, but requires real-time monitoring to ensure that the automated systems are performing to required standards.

PAYMENT CARD INDUSTRY (PCI) COMPLIANCE

The business challenge:

Since early 2005, it is estimated that at least 1.1 billion records of sensitive information have been compromised in publicly announced data breaches.

Ensuring the security of electronic payments in the eCommerce and card space continues to create new challenges as criminals are using increasingly sophisticated techniques to carry out network intrusions, wiretapping attacks, and device tampering schemes.

PCI data can be breached in several ways:

- Hackers can exploit networks and internet connections without the latest security updates.
- Thieves, and sometimes even rogue insiders, can physically steal flash drives, CDs or DVDs.

PCI DSS, is an industry standard for all organizations that handle cardholder data. This data can include credit cards, debit cards and ATM cards, and PCI DSS protects cardholder data, minimizing the possibility of cardholder data theft and/or loss.

PCI DSS requires that all merchants, service providers and financial institutions meet minimum levels of security and monitoring of the systems in their cardholder data environment (CDE).

Any business that stores, processes, or transmits payment cardholder data is required to regularly monitor its CDE in accordance with the PCI DSS standard.

The data security standard is made up of 12 requirements that businesses are expected to comply with, consisting of security policies, procedures and guidelines for storage, processing and transmission of cardholder data:

Build and Maintain a Secure Network and Systems:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data:

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program:

5. Protect all systems against malware and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures:

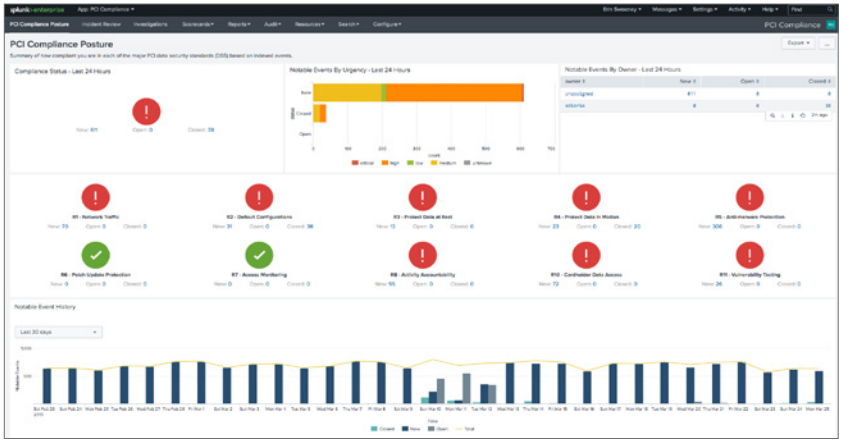
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks:

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy:

12. Maintain a policy that addresses information security for all personnel.



The Splunk App for PCI Compliance dashboards show status of your PCI compliance technical controls, to identify and investigate any control areas that may need to be addressed, and to quickly answer auditor data requests.

Splunk's approach:

Reports are the official mechanism by which merchants and other entities report their PCI DSS compliance status to their respective acquiring financial institutions or payment card brand. Depending on payment card brand requirements, merchants and service providers may need to submit a report on compliance for on-site assessments on a quarterly basis.

The Splunk App for PCI Compliance is a Splunk developed and supported app designed to help organizations meet PCI DSS 3.2 requirements. It reviews and measures the effectiveness and status of PCI compliance technical controls in real time, whilst retaining data to provide a historic view of PCI compliance posture to give a trending view over time. It can also identify and prioritize any control areas that may need to be addressed and lets users quickly address any auditor report or data request.

PAYMENT CARD INDUSTRY (PCI) COMPLIANCE (Continued)

Value:

The Splunk App for PCI Compliance captures information from applications, systems and devices in the PCI CDE, providing a singular view of PCI posture across the entire organization. The App delivers the following capabilities:

- Capture, monitor and report on data from enterprise devices, systems and applications in the cardholder data environment.
- Monitor access attempts to PCI assets.
- Monitor traffic between PCI domains.
- Identify vulnerabilities found on PCI assets.
- Notify administrators of malware found on PCI assets.
- Investigate and resolve compliance issues.
- Enable PCI compliance managers to monitor and report on PCI DSS compliance by producing views and reports of significant activity.
- Report-based views for each of the relevant compliance controls.
- Compliance scorecards provide an overview of compliance for each major PCI requirement.
- Alert, assign, evaluate risk and respond to potential security incidents.
- Asset and identity correlation facilitates compliance reporting against specific assets and users in the PCI CDE.

To ensure that security controls continue to be properly fulfilled, the Splunk App for PCI Compliance allows for easy integration of PCI monitoring into business-as-usual (BAU) activities as part of an organization's overall security strategy, ensuring effective monitoring of its security controls on an ongoing basis and maintaining its PCI DSS compliant environment between PCI DSS assessments.

PagSeguro is the leader in online payment solutions in the Brazilian market. PagSeguro lacked a flexible real-time monitoring solution and wanted full visibility into its production environment, especially in light of having to meet PCI compliance auditing requirements. Since deploying Splunk Enterprise, PagSeguro has seen benefits including:

- Better compliance to PCI security standards
- Increased customer satisfaction
- Full visibility into infrastructure

Read more about Splunk at PagSeguro.

CENTRAL BANK AND SUPERVISOR COMPLIANCE

The business challenge:

Central banks have a wide set of responsibilities that differ from country to country, but above all they must act as a "lender of last resort" — lending money to banks when they are in difficulty. Normal responsibilities include implementing monetary policy and supervising banking institutions with a macroprudential approach.

Supervision typically involves monitoring and oversight of firms to ensure they develop supervisory policy (including regulations, policy statements and guidance). Firms must also remain in compliance with law and regulation. Central banks check whether firms are engaging in unsafe practices and take remediation steps to make the firms correct any unsafe practices when necessary.

When corrective action is needed, central banks can issue time-bound instructions with varying levels of severity directly to a firm's board of directors, instructing the firm to address unsafe practices. These written instructions, often referred to as Matter Requiring Attention (MRA) and Matter Requiring Immediate Attention (MRIA) take priority over other in-flight projects and place a huge unplanned burden on internal departments. Key personnel are often pulled from potentially revenue-generating projects to work toward addressing the concerns, usually related to the institution's risk management controls and systems.

Failure to meet MRA/MRIA deadlines can result in heavy fines or even the revocation of trade licensing in extreme cases; therefore, banks shift their focus from innovation to becoming compliant.

Central banks regularly issue MRAs/MRIAs, and so being able to react quickly and efficiently to incoming instructions from the central authority can quickly become a competitive advantage, allowing firms to save millions by fast tracking responses, freeing personnel to focus on innovating the core business.

Splunk's approach:

One of the core tenets of safe banking, a key theme in new legislation passed since the 2008 banking crisis, is transparency and visibility.

As an example of this, MiFID II and MiFIR ensure fairer, safer and more efficient markets and facilitate greater transparency for all participants.

With much of a bank's services being digitized, more transparency translates to better access to data generated across the entire organization so that internal and external auditors have the opportunity to understand how the business is operating and can reconstruct events when incidents occur.

Splunk is able to quickly consolidate a global financial firm's structured and unstructured data into a single repository, ensuring that an exact copy of the raw data is available for auditors to analyze.

Built-in data integrity technology ensures that auditors and regulators can be certain that data stored in Splunk has not been modified from its original form. Splunk achieves this by computing hashes (using SHA 256) on every slice of data; it then stores those hashes so that verification checks can be run to ensure the integrity of the data.

Data onboarding can become an onerous task when there are potentially hundreds of data sources that could be required by regulators. Not so with Splunk. Other solutions require a detailed study to be conducted to fully understand each data source before a schema can be designed and built to answer known questions. On the other hand, onboarding data with Splunk only requires the timestamp and record boundaries to be defined upfront, saving time, money and effort in onboarding and ensuring firms can quickly react to requests for data. Splunk builds a dynamic schema on the fly as users ask questions of the data, meaning that schemas do not need to be re-engineered every time a new question is asked that cannot be catered for by the schema.

Central banks can also directly benefit from running Splunk. Report requests made from central banks to banking firms, particularly those reports that are financial in nature, must often be transmitted as eXtensible Business Reporting Language (XBRL). Central banks can use Splunk to parse and ingest XBRL reports natively, making them immediately searchable and analyzable. Central banks can join together multiple recurring reports to create a view over time, making it possible to spot trends and anomalies that would otherwise be missed when analyzing multiple reports manually.

Value:

MRAs/MRIAs can cause significant disruptions to a bank's operations. Pre-empting requests from the central authority by having data logged and available for analysis will help the bank become more agile at responding effectively, saving key personnel unplanned work.

With MRA/MRIA being time bound, Splunk can help large financial firms onboard the necessary data feeds faster than other solutions on the market, ensuring that regulator deadlines can be met and exceeded, keeping the bank complaint.

"When you get an alert, there will be questions you want to answer: have I seen anything like this before, or this exact thing? Using Splunk as a data platform means we can build out that threat and see what other incidents could be part of this puzzle, giving us an instant triage platform to bring that straight to the analyst."

Jonathan Pagett, head of the security operations center at the Bank of England

---

Hear more about Splunk at the Bank of England.

SWIFT COMPLIANCE AND ISO 20022

The business challenge:

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a vast messaging network used by approximately 10,000 banks and other financial institutions globally to securely send tens of millions of messages daily. There are multiple message types, including (but not limited to):

Message Type	Description
MT0xx	System Messages
MT1xx	Customer Payments and Cheques
MT2xx	Financial Institution Transfers
MT3xx	Treasury Markets
MT4xx	Collection and Cash Letters
MT5xx	Securities Markets
MT6xx	Treasury Markets - Metals and Syndications
MT7xx	Documentary Credits and Guarantees
MT8xx	Travellers Cheques
MT9xx	Cash Management and Customer Status

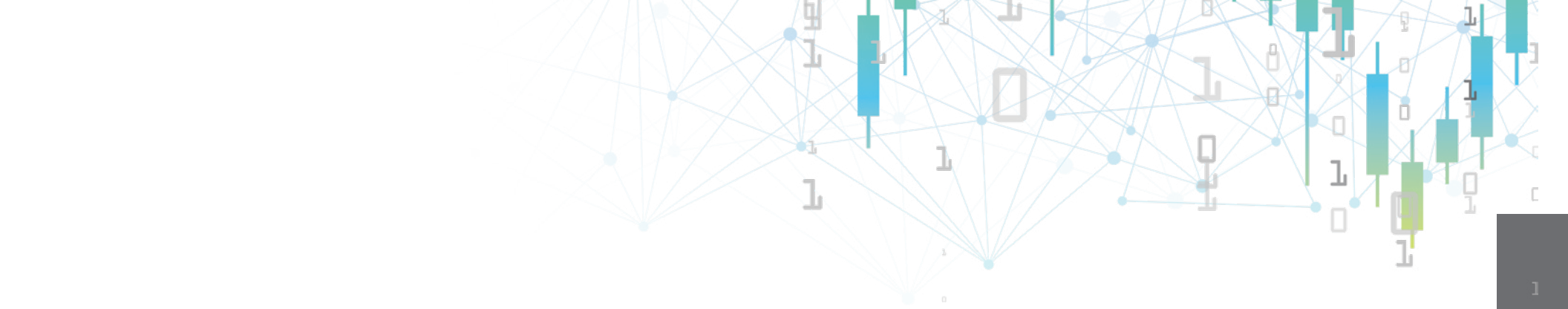
The SWIFT network doesn't process any transactions but rather relays formatted messages between its member banks with instructions regarding financial transactions or other business communications.

In February 2016, The Bank of Bangladesh famously fell victim to a cyberattack targeting its SWIFT infrastructure. Since then, the industry has placed increased focus on improving cybersecurity protections across the SWIFT network.

In another attack, the Bank of Chile was targeted by a virus in May 2018 affecting thousands of workstations. Later, it was believed that the malware was just a decoy to divert attention from the real attack, which defrauded the bank out of $10 million through its SWIFT payments system.

In addition to the brand damage and exfiltrated data resulting from breaches, SWIFT attacks can lead to fraud, money laundering, sanctions abuse, the funding of criminal activity and national security issues.

In addition, malicious actors are using increasingly complex attack strategies to avoid detection, as well as evasive techniques such as issuing fraudulent payments outside of business hours in an attempt to avoid scrutiny. More recently, they have started to issue payments in smaller amounts during business hours to blend in with normal business traffic while using new, previously unexplored payment corridors (combinations of target and beneficiary banks) in an attempt to circumvent detection.



Attackers are spending significant time in the reconnaissance phase, penetrating user workstations and observing patterns of behavior over a prolonged period before attempting to access the bank's payment systems. During this phase, banks need to be proactive and vigilant about tackling seemingly insignificant and common threats such as malware to ensure larger attacks are averted at the root.

According to recent SWIFT studies, the attackers' then generally use the 'Single Customer Credit Transfer' or MT103 message type to conduct cross-border fraud. In almost all cases, the fraudulent transactions issued during customer cyber incidents known to SWIFT involved MT103 messages.

While SWIFT messages contain a wealth of information related to transactions, they lack contextual reference data, such as the name of the client relationship manager. The current MT and MX message formats are less responsive to changes in the economy, emerging technologies and innovation and will eventually be superseded by a new standard, ISO20022, which yields many benefits.

Among other things, ISO20022 will be able to carry far more data in the message payload, providing banks with more detailed reference information that will ultimately prove invaluable to help detect fraud and target financial crime.

Splunk's approach:

SWIFT messages can be ingested into Splunk and field extractions applied to ensure analytics can be conducted on the data with ease.

Correlating cyberattacks and unusual payment transactions has traditionally been done independent of each other. Cybersecurity teams look for signs of infections in IT systems using legacy security incident event management (SIEM) tools while fraud teams create models that attempt to detect suspicious transactions. Historically, there has been a lack of tools allowing both IT data and business data correlation at the scale required by a global financial institution.

Splunk changes that, enabling firms to correlate the outbreak of malware with unusual transaction behavior to quickly assess whether a piece of malware is part of a more serious attack. Spot checks on message volumes and distributions can then be used as initial tracking indicators.

In the early phases of an attack, Splunk Enterprise Security can be used to detect the presence of malware, ensuring that the reconnaissance phase that attackers use to execute more sophisticated attacks is minimized.

SWIFT COMPLIANCE AND ISO 20022 (Continued)

Splunk's analytics capabilities can be used in many ways to detect signs of suspicious transactions. Analyzing unusual payment corridors used by money launderers or performing simple checks against missing data in SWIFT records could indicate that attackers are intentionally hiding data to avoid detection by sanctions and AML filters.

Addressing this, ISO20022 is designed to carry significantly more data in the message payload, which in turn will open up many new detection possibilities.

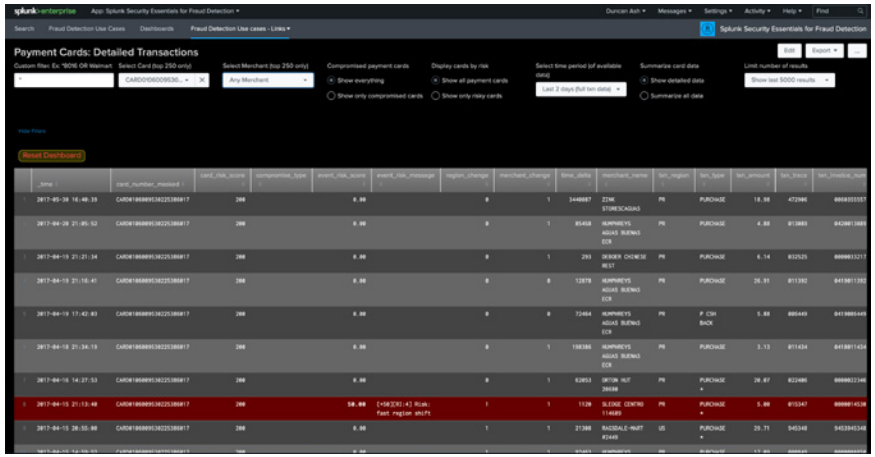
And as firms adopt SWIFT's new messaging standard , data analytics will play a greater part in the fight against financial crime. Large firms will often have their SWIFT messages stored in multiple locations to satisfy data privacy and cross border requirements. Splunk's architecture is perfectly suited to ensuring that data can be stored in appropriate regions and maintaining the required level of access controls. It also makes the data searchable and accessible in a timely manner to those who need it.

Also with Splunk, banks will have additional opportunities to enrich their SWIFT messages with additional data. Among other things, Splunk will enable users analyzing SWIFT to further enrich data with greater context on the fly.

Finally, while it should be approached with care, firms that use Splunk's Search Processing Language can link messages together to form an end-to-end view of a complete transaction. And Splunk Business Flow can provide a complete view of the message journey.

Value:

In recent years, many high profile attacks have successfully targeted the SWIFT infrastructure. Addressing this mounting challenge, Splunk provides a cohesive analytics platform that integrates security, fraud detection, AML and sanctions abuse detection, elevating the ability to detect malicious behavior targeting payments systems. And the elevated sophistication in banks' security defenses coupled with significantly reduced detection time are a welcome addition by regulating authorities.



In order to adhere to payments-related compliance mandates, you need to be able to view all of your transactions in real-time.

CALL RECORDING

The business challenge:

Trading floors face strict trading regulations that require the capture and archiving of all trade communications of regulated employees, with the ability to easily access the information and respond to compliance queries in a timely manner.

In the U.S., the Dodd-Frank Wall Street Reform Act is a law that regulates the financial markets and protects consumers to help prevent a repeat of the 2008 financial crisis.

A component of Dodd-Frank is the ability to record, play back and analyze any phone call, from any device, that discusses a transaction or gives verbal consent to a trade or deal.

Dodd-Frank stipulates the following:

- Call records must be maintained, tagged and made searchable by transaction for 12 months.
- Voice recording cannot be at the discretion of the caller or call recipient. It must always be on.

Other financial regulatory bodies around the world stipulate similar requirements to Dodd-Frank with regards to call recording, such as COBS 11.8 mandated by the Financial Conduct Authority in the UK.

Mobile and VoIP calls related to trades must be centrally recorded to ensure compliance. Firms are required to implement resilience and strong security controls to ensure that call recording systems are protected against downtime as a result of cyberattacks or IT related outages.

Conversely, to comply with privacy laws, firms must ensure that when an employee leaves a department where call recording is mandatory to join one where it isn't, they stop recording the individual's calls.

Splunk's approach:

To adhere to compliance requirements, firms must ensure the uptime and security of call recording systems. Splunk's machine data platform is able to ingest all data associated with running a call recording system, ensuring that cyberattacks can be detected, and the health and general welfare of the application can be monitored in real time to ensure the maximum uptime so calls do not get missed.

Customers normally analyze the following data from their call recording systems with Splunk:

- OS logs and metrics
- Infrastructure logs and metrics (storage, network, hypervisor)
- Call recording application logs and metrics (e.g., Nice NTR)
- Enrichment data sources (syslogs, metadata, CDR, VOX, etc.) to enrich information and provide enhanced visibility for health and assurance
- *.WAV header information to further enrich data and assist with assurance (voice quality, clipping, etc.)
- Instant message chat
- Speech-to-text call transcription

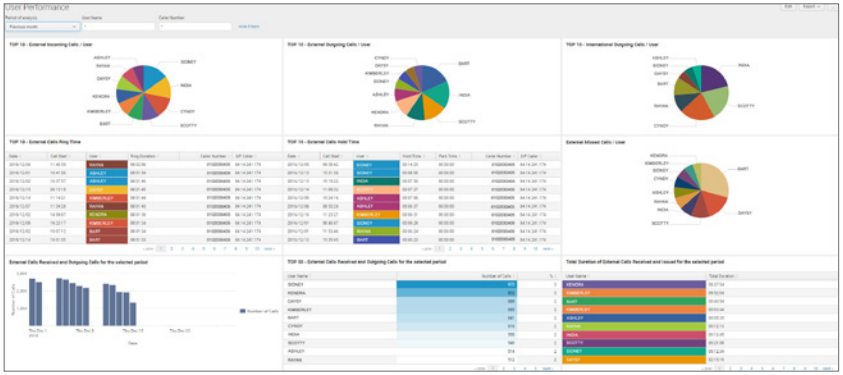
Firms can use Splunk to enrich call recording data with HR data, to ensure that recording only takes place for individuals in sensitive roles and departments that require mandatory recording. Using the same approach, exception reports generated by Splunk can highlight employees that are being recorded that shouldn't (for example, when an employee transfers from a role in a sensitive part of the business to a less sensitive part), improving compliance and avoiding privacy law breaches.

Value:

Monitoring with Splunk will yield a more reliable and secure call recording system that will help firms demonstrate to regulators that they are compliant, while reducing business risk and ensuring company and employee protection from disputes, complaints and legal matters.

Splunk ensures that application downtime can be reduced and offers string detection rules against cyberattacks, safeguarding the system and the call recordings themselves. A major bank reported a 97 percent reduction in hours required for health checks and investigations.

Firms will also have a chance to improve customer experience by monitoring and analyzing the data in Splunk, allowing them to visualize metrics such as call quality, waiting times and customer interactions.



Splunk helps ensure firms remain compliant by maximizing call recording system uptime, required legally to monitor all activity related to trades. Firms will also have a chance to improve customer experience by monitoring and analyzing the data in Splunk, allowing them to visualize metrics such as call quality, waiting times and customer interactions.

PRIVILEGED ACCESS REVIEW

The business challenge:

Privileged access review (PAR), sometimes referred to as privileged activity review, requires banks to track and monitor employees who are able to make changes to critical IT systems. While the regulators stipulate that a privileged access monitoring program is required, they do not define how banks should implement it, leaving it to the discretion of each firm to design and deploy as they see fit.

To protect against insider threats, banks must operate under the principle of least privilege, meaning they should limit access permissions for users to the bare minimum they need to do their jobs effectively.

Privileged access monitoring plays a key part in ensuring that users with elevated permissions and access to critical systems have authorized access requests prior to running privileged commands on any server/application.

Every intrusive command (e.g., insert, update, delete) across relevant and in-scope applications and technologies must first be identified. Then it must be correlated and reconciled to an approval process and granted access to the request record for the work that specifies details about the change, the time window of when the change can happen and who can implement the change.

Typical sources in scope are:

- Databases
- Business applications
- Unix
- Windows
- Networks and network devices

Each firm will have to go through an internal process to define what "privileged" means for each of the in-scope technologies and the pattern-matching rules needed to identify an intrusive command from the log data. This is usually done with the assistance of SMEs in each domain.

Splunk's approach:

Once the scope has been defined, the data must be collected in Splunk. In addition to the log data, the change request tickets, typically stored in an IT service management system, must also be ingested for correlation purposes.

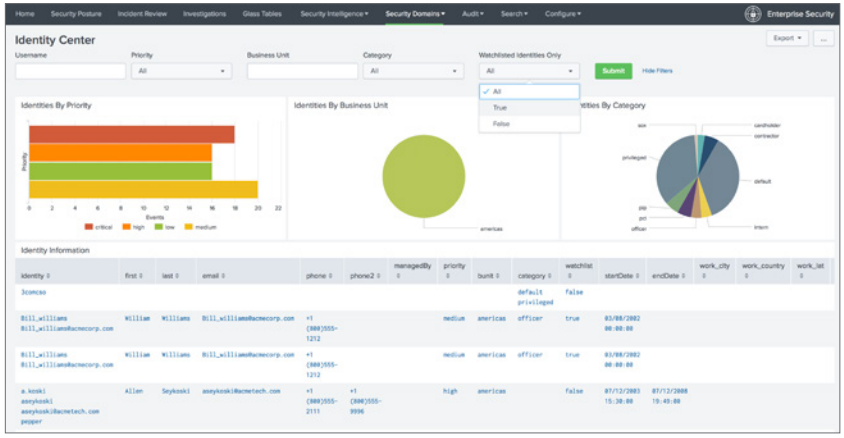
Millions or even billions of log records are produced and ingested, depending on the size of the organization. However, Splunk's horizontally scalable platform ensures that intrusive commands can be isolated through pattern matching, making the job of identifying privileged changes significantly easier.

Splunk can filter down events based on their level of importance, and privileged commands that are deemed intrusive or have been blacklisted can be retained. The remaining events are then correlated with change ticket data to ensure that intrusive commands occurred in the approved time window and by the approved resource.

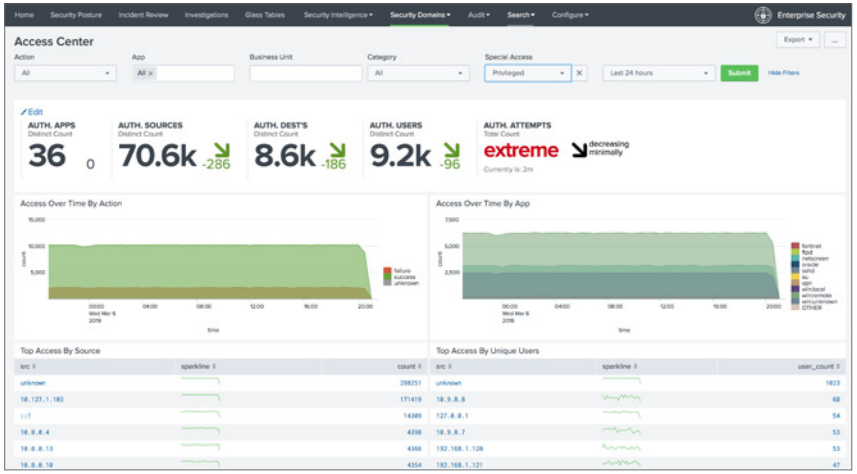
Millions of log entries can be triaged to thousands of privileged activities and into hundreds of potential violations that need to be reviewed. Any exceptions will need escalation to management for further investigation.

A PAR program is ongoing, as IT systems and applications are continuously upgraded to later versions, resulting in inevitable changes to the logging semantics.

False positives may surface, requiring changes to the pattern matching logic in Splunk to drive down occurrences and optimize reviews.



New or upgraded applications may log differently and break existing pattern matching rules resulting in privileged access getting missed. Splunk is agile enough to allow companies to keep pace and tweak their pattern matching to detect privileged access without restructuring or re-ingesting the data.



Millions or billions of log lines need to be analyzed and enriched with IT Service Management and Human Resources data to provide reviewers with the full context required to spot privileged access abuse—this requires a highly scalable data solution. Customers can multiply the value they receive from the data ingested for PAR by using it to help with incident remediation and to investigate security incidents.

Value:

Implementing PAR in Splunk demonstrates to auditors that firms know what is happening inside their IT organizations through detailed logging of key activities. PAR can also be used to help with incident remediation, because it captures so much important data about what took place on the box or application. Firms already ingesting large amounts of data into Splunk will have the materials to build PAR applications in Splunk without purchasing or custom-building new solutions.

GDPR COMPLIANCE

The business challenge:

The European Parliament recently adopted the new General Data Protection Regulation (GDPR), a single, harmonized law, binding across all member states of the EU. The GDPR provides greater predictability and efficiency for business and offers EU citizens increased data protection rights in the new digital age, which came into effect in May 2018.

Key requirements of the GDPR include:

- Increased rights for data subjects, including the right to "be forgotten" and data portability
- Software developed with security in mind (privacy by design and by default)
- Pseudonymization or encryption of personal data (privacy by design and by default)
- Secure processing of data
- 72-hour notification for breaches of personal data
- Fines of up to €20 million or four percent of annual revenue, whichever is greater
- Further, the GDPR applies to all companies worldwide that target their goods and services to European citizens

Splunk has identified three solutions that can help support a GDPR compliance program.

1. Security management and breach notification

Article 32: Security of Processing

The GDPR requires security of processing (Article 32), meaning that organizations processing personal information must implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." This includes state of the art technical measures to prevent unauthorized access to personal data.

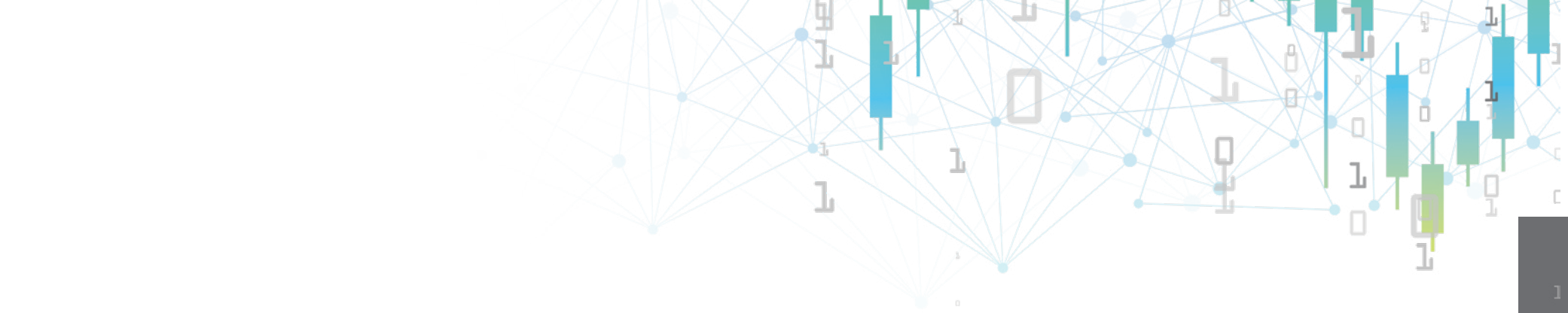
Articles 33 and 34: Notification

The GDPR requires breach notification and communication. This means that organizations must notify supervisory authorities within 72 hours of becoming aware of a personal data breach that could harm the rights and freedoms of EU citizens (Article 33) and must notify the affected individuals without undue delay (Article 34). The notification must contain, among other things, information about the nature of the breach, including the number of data subjects affected, and your steps for remediation.

2. Data Protection Audits

Article 58: Supervisory Investigative Powers

The GDPR grants each supervisory authority the power to carry out investigations in the form of data protection audits and issue warnings, reprimands or bans on data processing (Article 58). Article 82 gives any person who has suffered material or nonmaterial damages the right



to receive compensation. Fines can only be avoided if a party can show that it was not in any way responsible for the event giving rise to the damage. To do this, organizations will need to document their actions and demonstrate their compliance to the supervisory authority.

3. Search and Report on Personal Data Processing

Articles 15, 17, 18 and 28: Data Subject Rights

The GDPR grants EU citizens the right to know what personal data is being processed about them, with whom it is shared and where it is processed (Article 15). Data subjects can also ask that their personal data be corrected (Article 16) or deleted (Article 17). Processors are required to ensure that only authorized persons process the personal data, and when the processing is complete and the contract terminated, the controller can request that all personal data be deleted or returned, including in some cases any existing backup copies.

Splunk's approach:

Machine data provides the historical information that organizations need to demonstrate to supervisory authorities that they had appropriate security controls. By recording the activity of customers, users, processed transactions, applications, servers, networks and mobile devices, organizations can demonstrate to supervisory authorities that they had appropriate security controls in place and proactively worked to mitigate risk (Articles 32, 58).

Splunk provides visibility into processing activities, exposing anomalous behavior and unauthorized access — critical for GDPR compliance. Splunk alerts companies as to when personal data was accessed, by whom and how it was used (Article 15, 17, 18 and 28), all of which helps companies meet their notification requirements (Article 33 and 34). Splunk's industry leading SIEM solution, Splunk ES, is a demonstration of a control put in place to mitigate risk, providing out-of-the-box reporting that helps organizations demonstrate they are GDPR compliant.

Value:

Firms that harness Splunk for security analytics with Splunk ES clearly demonstrate to authorities that they are serious about GDPR requirements, by demonstrating they can adhere to the articles mentioned above, significantly reducing the chance of heavy fines.

ABOUT SPLUNK.

Machine data has the power to address complex problems unique to the financial services sector and—using that same data—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.

Learn more about how Splunk's real-time data analytics platform can benefit your financial services organization: www.splunk.com/FSI

splunk>

© 2019 Splunk Inc. All rights reserved. Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data,Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries.

EB-Splunk-Top-40-FSI-ebook-117