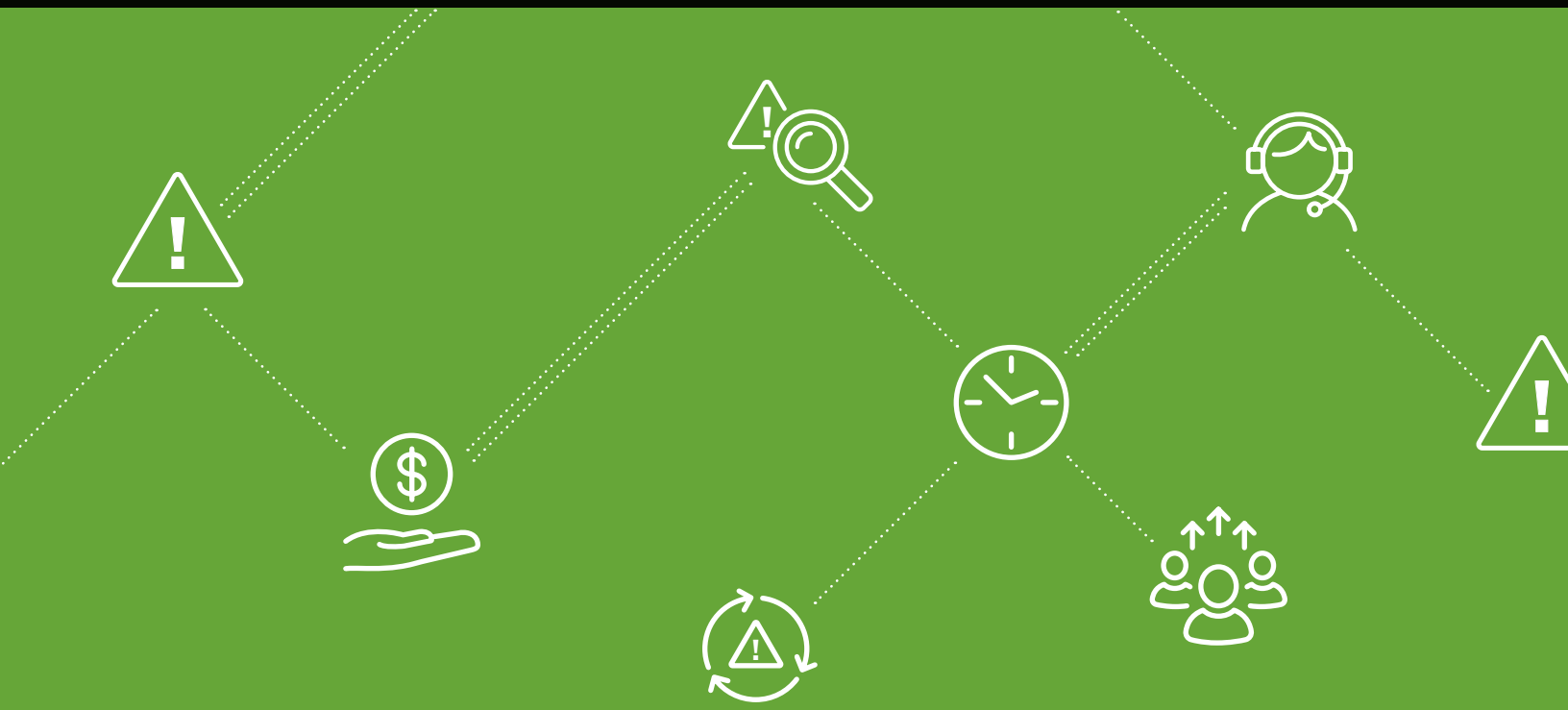
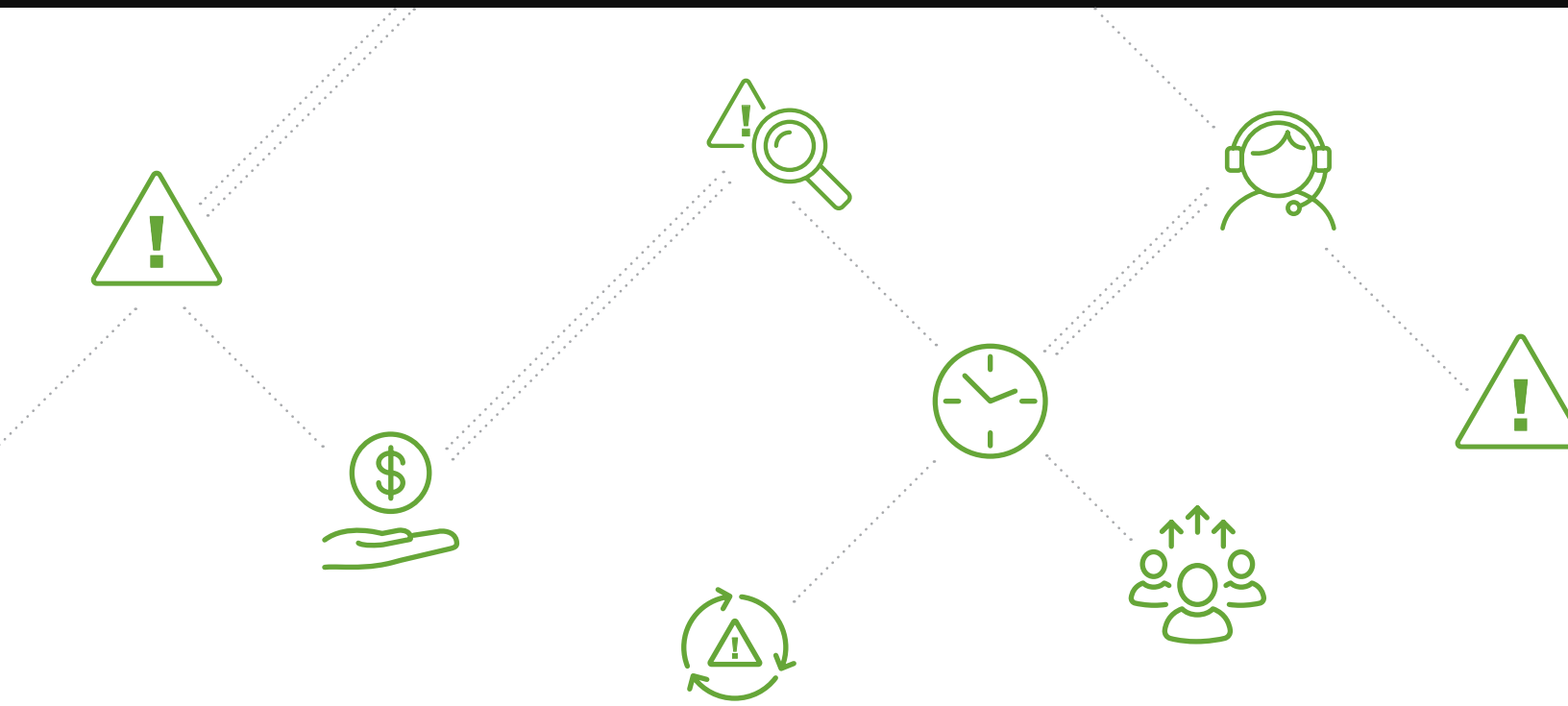


A GUIDE TO FRAUD IN THE REAL WORLD

How Machine Data Can Help Find Anomalies & Fight Fraud



Fraud is a growing problem because so many parts of everyday life are being digitized. Think of all the accounts in our lives, which are all susceptible to fraud. This can include credit card numbers, bank account numbers, an email address, a phone number, a home address, a user ID, prescriptions, loyalty rewards or a gamertag. And this is just to a name a few types of accounts.

Fraud is defined as a wrongful or criminal deception intended to result in financial or personal gain. Its forms can vary from stolen identity to the stealing of account credentials and personal information.

Protecting against fraud is a growing problem from online services, user accounts, healthcare providers, retailers, education and financial institutions, and more. The real questions then are:

- How does **Telefonica**, a large European telcom, prevent six thousand orders of premium smartphones from falling into the wrong hands?
- How does **PostFinance** ensure its users aren't tricked into a mirrored online banking site?
- How does **a large coffee shop** ensure its customer loyalty points aren't stolen?
- How does **Duke university** prevent fraudsters from siphoning faculty salary?
- How does **Surescripts** stop opioid or prescription fraud?

These are just some examples of fraud challenges being faced by real-world organizations. And these organizations have all taken steps to answer these questions by adopting a fraud detection plan.

Fraud detection is implementing a process and actions that protect customers and enterprise information, assets, accounts and transactions through the real-time, near-real-time or batch analysis of activities by users and other defined entities. It uses background server-based processes that examine users' and other defined entities' access and behavior patterns, and typically compares this information to a profile of what's expected. Fraud detection is not intrusive to a user unless the user's activity is suspected of fraudulent activities.

Although, there is new and ever changing digitalization, fraudsters generally use the same steps to commit fraud: They identify accounts and the information they need, find a vulnerability and expose it.

Whether it's account takeover (ATO), application fraud or card-not-present (CNP), there's no question that fraud is on the rise. The U.S. Department of Justice estimates that healthcare fraud alone costs the country **tens of billions of dollars a year**. It says some estimates "put the figure **closer to $100 billion**."

Fraud is not only costing organizations money, but it also accounted for 85 percent of all discoveries of breaches last year, **according to a study**. The stakes get even higher when you consider that with each breach organizational losses stretch beyond monetary losses, to damaged reputation, organizational efficiencies and the ability to meet compliance mandates.

If the steps to commit fraud are the same and it's possible to implement a fraud detection process, what makes it challenging for fraud teams to stay ahead of threats? Assuming that organizations don't want to lose money, right?

Typically, organizations are developing and adding new services at the speed of business, which is not the same rate that they are thinking about fraud or investing and implementing fraud detection actions and processes to find anomalies.

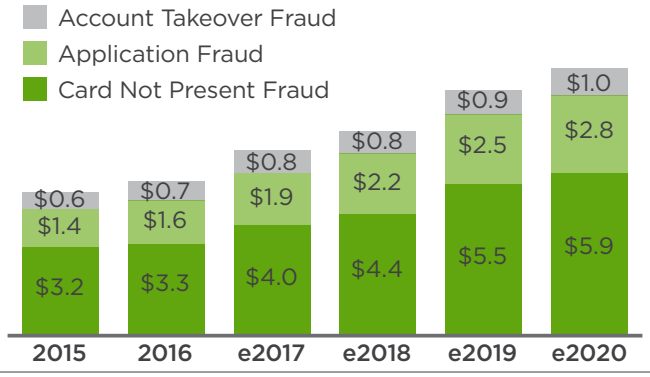
Organizations need the ability to centrally search, detect, monitor and investigate fraud attempts to keep the services offered, customers safe and to establish digital trust.

In any kind of digital services, **the fingerprints of fraudulent activities are written in machine data**. Organizations can leverage machine data to stay ahead of fraud. In the following, we will present six real-world scenarios where machine data can be used to stamp out fraud:

- Account Takeover: Credential Stuffing
- Account Takeover: Phishing
- Service Abuse
- Payment card information
- Financial account information
- U.S. Healthcare Fraud in the Real World

The Rise of Fraud by the Numbers

Fraud is a growing problem in the U.S. and is only expected to grow (Fraud Growth, 2015-e2020, in US$B)



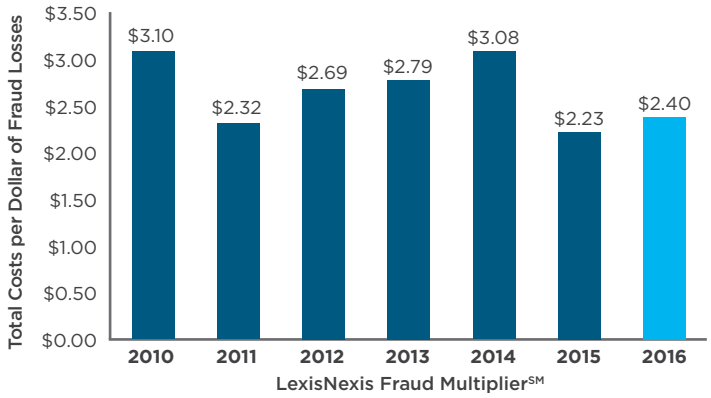
The LexisNexis Fraud Multiplier℠ is On the Rise

Weighted merchant data

Q: In thinking about the total fraud losses sufered by your company, please indicate the distribution of various fraud cost over the past 12 months.

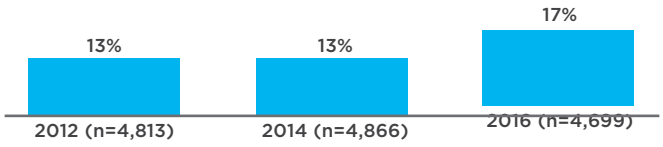
July 2010 – February 2016, n varies from 145 to 712

Base = Merchants experiencing fraud in the past 12 months



Source: Lexis Nexis True Cost of Fraud Study

Q: Have you experienced more than 1 incident of debit or credit card fraud in the past 5 Years?



Source: Aite Group, ACI Worldwide study of consumers in 20 countries, Q2 2016.

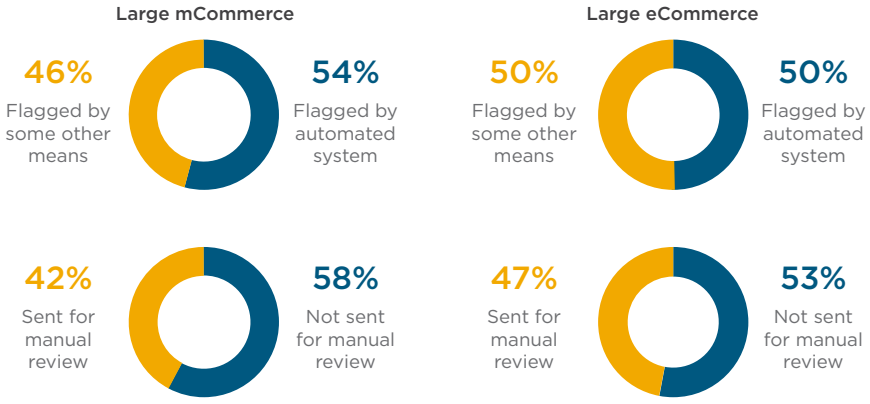
The Rise of Fraud by the Numbers (continued)

Flagged Transactions from Remote Channel Merchants

Weighted merchant data

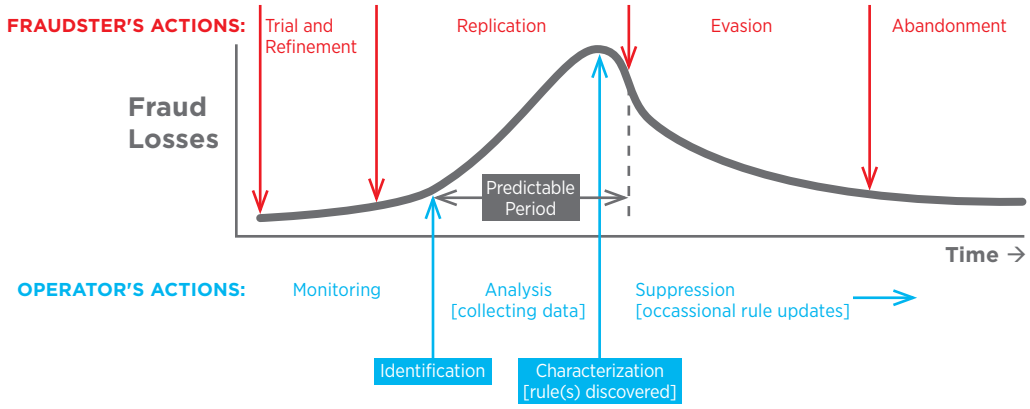
Q: Of all the transactions your company flagged as potentially fraudulent in the past 12 months, what percentage was flagged by your automated system?

Of this (...), what proportion are sent for manual review?



Source: Lexis Nexis **True Cost of Fraud Study**

Legacy Approaches Don't Work in the Face of Rapidly Evolving Fraud and Cybercrime



You want to identify new fraud before the inflection point where the fraud is replicated.

FRAUD IN THE REAL WORLD

Scenario 1: Account Takeover - Credential Stuffing

You have an online platform where your customers can sign up to make hotel reservations. During the registration process, customers choose a password, confirm their email address, add their payment details, their loyalty numbers of their favorite hotel chains and set up security questions in case they want to make a reservation or reset the password through the phone.

An email hosting company experiences a breach, which exposes email addresses and corresponding password hashes that be easily decoded. Attackers are now creating scripts and running through thousands of different systems attacks against online shops and booking websites to find accounts where the users used the same passwords.

What's the Impact and Why Should I Care?

You didn't have a breach but your service and your customers might be at risk. Attackers could take over an account without you recognizing it by posing as a legitimate user and get access to more sensitive data, book hotels on the payment options of the hapless user, redeem free hotel nights from a loyalty program. All of this can create significant costs and high risk of loss.

The Machine Data Solution

By using machine learning you can identify scripted, non-human logon attempts or deviation of the norm within machine data and identify the involved indicators. You can then block the fraud attempts within your business application or firewalls (like IPs or specific user agent strings etc.). Examples of indicators of fraud can be a country the user has never logged on from before, unusual time for the logon, new systems or browsers the fraudulent actor logged on from.

Scenario 2: Account Takeover - Phishing

You are a bank and you provide online banking to your customers. Bad actors can rebuild your online portal under a domain hosted outside your country. Then they attempt via spam emails to phish individuals who are a customer of yours to get them to click the link and logon on the phishing website that looks like your online portal. With those credentials the attackers then logon on your real portal and gain access to the user's account.

What's the Impact and Why Should I Care?

Attackers might use the credentials to execute fraudulent activities. For certain activities you might have additional security controls deployed such as TAN/One Time Password technology. Attackers can still use the knowledge of payment transactions, finance situation and finance balance to gain more intelligence about an individual and putting him at risk for further attacks.

The Machine Data Solution

While you're limited in your response, as much is outside your perimeter and happening without your influence — machine data is still there to help you! Most likely after a short period of time your fraud team will be informed (via phish tank, a national CERT, phished customers). Your fraud team can go to the phishing website, enter some demo credentials that look like a legitimate user, and then wait and monitor until the attackers are trying to get legitimate access to your portal.

Then you can let them into a demo account and observe what they are trying to achieve. By doing this — you can extract from the machine data indicators of compromise — like what IP addresses they used, from which countries they come, which systems and browsers they are using. You can use that information to block further activities including the IOC's. You can also start an investigation to determine which users have been impacted by the hacking group.

Scenario 3: Service Abuse

You're offering a free email service to your customers. Users can sign up and use your service. This service also offers free mobile texting. Attackers are signing up to your service and sending spam emails to thousands of people. They are also using your short message service to spam cell phones, inviting individuals to vist a malicious URL or call a pay-per-call number.

What's the Impact and Why Should I Care?

As the email service is utilized to send thousands of emails out, your email domain is quickly added to nearly every security vendor's spam list, affecting your users and your service. Additionally, the load of sent emails can put a heavy load on servers, which can lead to a larger than expected bill from the cloud provider who hosts the email servers. Also the SMS messages that are used for spam can end up being costly as well and they also carry the possibility of those on the receiving end asking for compensation.

The Machine Data Solution

Machine data allows your fraud team to gain insights into how the services are used, who the top users are and to detect any anomalies.

Scenario 4: Payment Card Information

There are two types of payment card fraud: card-present and card not-present fraud. You either have a customer with a card and that card can be stolen or the kiosk or card reader has been compromised. Otherwise, a card transaction can be made where the cardholder does not or cannot physically present the card for a merchant's visual examination at the time an order is given. The fraudsters could have stolen the card credentials or information of the card holder by using online phishing or through theft of a customers' credit cards. Those businesses now have a transaction that is fraudulent that will need to be reimbursed.

What's the Impact and Why Should I Care?

Card holders are generally not liable so this places the cost on the merchant, credit card company or insurance. These losses added up can be massive, especially when you take into account that you can also lose your customers' goodwill when they don't feel their information is being protected. When consumers begin to feel insecure they are less likely to use the credit card or go to certain locations. Simply replacing cards cannot always rebuild customer loyalty and financial institutions are impacted by the results. Having analysts assess every transaction is incredibly costly and time-consuming leaving much to be missed or possibly resulting in errors.

The Machine Data Solution

You can use machine data to define fraud rules on wire transfers and card transactions and to identify suspect activity. It is possible to implement multiple velocity-based rules such as geographic and merchant changes, which may indicate a cloned card. It's also possible to gain better visibility by filtering suspect card transactions a number of different ways, such as by time and merchant. You can also use machine data to better identify anomalous cards by identifying payment cards with highly anomalous transactions. It's also possible to identify merchants and card terminals that have interactions with an exceptionally high volume of risky cards.

Scenario 5: Financial Account Information

You're a university that has many professors and staff members on payroll. Faculty have reported email phishing attempts to gain access to bank account information. Some of the phishing attempts succeed, resulting in changes that route faculty payroll to fraudulent accounts.

What's the Impact and Why Should I Care?

The wages you believed were payed to your faculty and staff are now lost to fraudulent activities and the people still need to be paid, so you are double paying. Your team then also needs to conduct lengthy investigations to find out what happened to prevent fraud from recurring.

The Machine Data Solution

Using machine data, teams can detect and prevent phishing attempts and account takeovers before payroll runs and get all necessary information needed for investigations. It can also offer insights to identify unusual trends, data anomalies and control breakdowns, by developing repeatable tests and in some cases even serve as early warning systems before fraud becomes material.

Scenario 6: US Healthcare Provider

You're a healthcare provider in the US that encounters bad behavior among your many providers including prescription and distribution of opioids. Although you've been making sure to implement proper regulations and requirements you're still encountering providers writing illegal prescriptions.

What's the Impact and Why Should I Care?

More than 400 people across the country have been charged with participating in healthcare pharmaceutical fraud scams. This can impact regulations and requirements making it more difficult for providers to conduct daily business and harder on customers to get the prescriptions that are needed. You can also incur financial penalties and criminal charges.

The Machine Data Solution

You can use machine data to help identify anomalous providers with highly abnormal prescription drug distributions and volumes compared to peers, as well as, get better visibility into each provider and their specialty. You can begin to filter the data based on geography, specialty, drug type, total claims billed and anomalous drug percentages.

Enter Splunk

Fraud detection and prevention has become a global problem, impacting organizations of all sizes, across all industries.

Fraud detection and prevention is a big data challenge with machine data at the heart of the solution. As business moves online, the evidence or patterns of internal or external fraud often lie in the massive amounts of unstructured machine data, often logs, generated within your business applications, IT infrastructure and security systems.

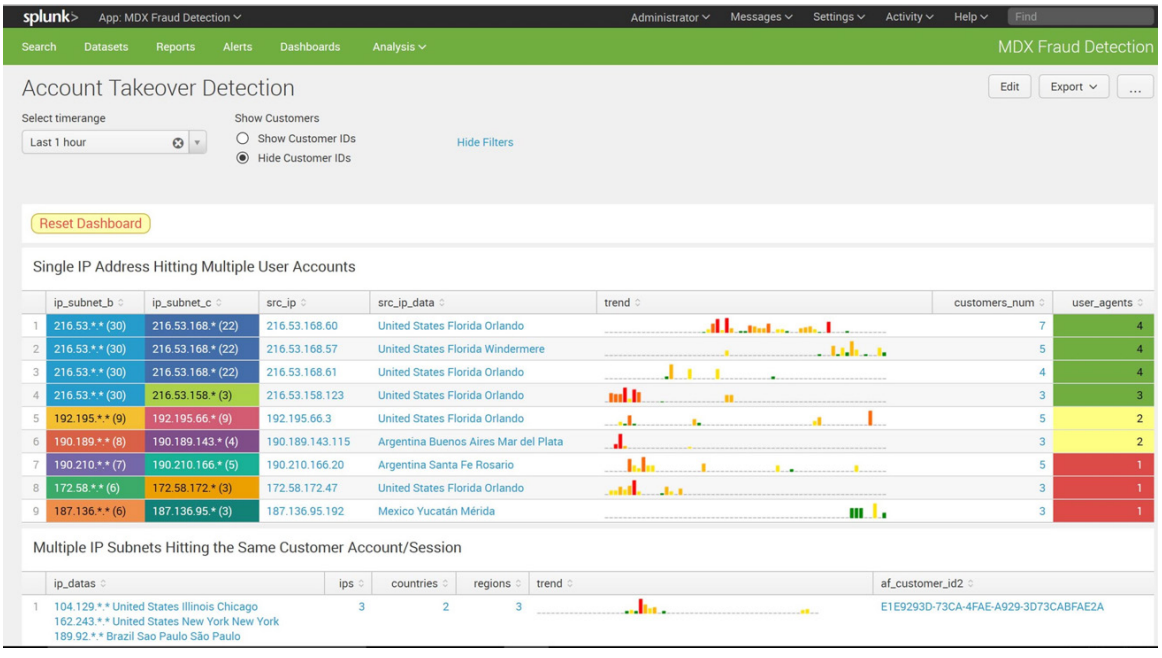
This fraud-relevant machine data comes from multiple sources such as web proxies, firewalls, authentication systems, transaction processing systems, payment and billing systems, databases, point of sale systems and operating systems. By indexing relevant machine data and searching and correlating on it to identify the patterns of fraud, an organization can detect and alert on fraud in real time and act to prevent it before it adversely impacts the bottom line.

Splunk is the analytics-driven platform that can onboard new data at the speed of the business to ensure fraud teams can search, detect and investigate data to quickly find anomalies to reduce the loss of money, reputation and organizational efficiencies. Splunk solutions enable customers to get better visibility across multiple data sources, even from other vendors' tools and fraud point solutions.

Other solutions don't have the ability to bring in all different types of data from various locations and correlate to provide information to detect all patterns forming anomalies. The Splunk platform enables organizations to harness this machine data to meet a wide range of anti-fraud, theft and abuse challenges including:

- Fraud detection: Correlation searches and anomaly detection can identify and alert on fraud as it happens so organizations can act to prevent the fraud before it adversely impacts the bottom line
- Fraud investigations: Quickly search and pivot through massive amounts of current or historical machine data to research possible fraud and to understand the "who, what, where, when and how" around a possibly fraudulent action

Account Takeover Detection:
Identify fraudulent attempts across different users' accounts in Splunk



- Fraud analytics and reporting: Make it easy to analyze, measure and manage fraud risk for a wide range of internal users
- Enhance existing anti-fraud tools. Index event data from siloed tools to create an aggregate fraud score for a single transaction
- Create consolidated reports and dashboards to view enterprise-wide fraud risk on a single pane of glass
- Leverage Splunk's Machine Learning Toolkit to more quickly identify different payment methods with highly anomalous transactions
- Use Splunk User Behavior Analytics (UBA) to detect account takeover by uncovering malicious or anomalous behavior associated with users (including root, service and other shared privileged accounts), devices, and applications

Splunk is used by hundreds of organizations from banks to healthcare organizations and government agencies to combat fraud. Here are some examples.

ATO Investigation: Monitor failed logins in Splunk for brute force attack detection (Below is a detailed view)

CASE STUDIES

mail.de Increases Performance and Availability Through Operational Intelligence

Executive Summary

mail.de, an email provider located in Gütersloh, Germany, prides itself on its innovative and secure email services. Since 2012, mail.de has offered users FreeMail, a product that combines the highest quality and security requirements with a free email address. The emerging company's IT infrastructure consists of an extremely varied server landscape, including different log-file formats and a rapidly growing volume of machine-generated data. mail.de needed a centralized system to turn this raw data into operational and business insight. Since deploying Splunk Enterprise, mail.de has seen benefits including:

- Enhanced customer service
- Real-time business insights
- Considerable time savings

Splunk Products

- Splunk Enterprise
- Google Maps Add-on for Splunk

Splunk Solution Areas

- IT Operations
- Application Delivery
- Business Analytics

Challenges

- Needed to consolidate and correlate logs from heterogeneous systems to enable easier monitoring and real-time alerting
- Wanted to provide a centralized view of IT landscape in order to identify and rectify system errors faster
- Mission to deliver more responsive customer support

Business Impact

- Real-time alerting resulting in faster troubleshooting, improved service availability and time savings for the IT team
- Enhanced customer support with the ability to investigate and resolve queries in real time
- Business intelligence can now be visualized more consistently and provided to management and marketing teams in a time-saving self-service manner

Data Sources

- Mail server logs
- Web server logs
- Database logs
- Application logs

Why Splunk

Because mail.de offers its customers secure, high-performance email communication, ensuring that the service is highly available is business critical. The company's IT infrastructure consists of a number of heterogeneous systems with different log-file formats and a continually increasing volume of machine-generated data. This made it difficult for mail.de to gain a holistic view of the state of its IT landscape in order to identify errors in the system and avoid or minimize system downtime. When disruptions occurred, the IT team had to search for the root cause on all the different systems—a protracted, time-consuming process—which negatively impacted the availability of services. mail.de wanted a new solution that would make it possible to centrally monitor all log files and introduce a real-time alerting system.

mail.de discovered Splunk Enterprise and a small team implemented it in just a few hours, without the need for external consultants. Whenever the mail.de IT team had questions, they were able rely on the support community at Splunk Answers (answers.splunk.com). mail.de quickly realized the potential of the Splunk platform and complemented the deployment with apps, including the Google Maps Add-on for Splunk.

"Before introducing Splunk software we had limited visibility into our own systems to a certain extent, which was impacting the service we could provide our customers. With Splunk Enterprise, we can localize errors in our system and proactively solve customer issues, all in real time. We have been able to greatly increase the availability of our services as a result, while also expanding our use of Splunk software to deliver real-time insights to our customers and executives. We see enormous potential for further Splunk use cases at mail.de."

– Fabian Bock, founder and CEO, mail.de GmbH

Optimized service through operational insight

Proactive real-time monitoring has proven to be an especially important feature for mail.de's IT division. When an error occurs in the system, the root cause must be found as quickly as possible. In order to constantly optimize its entire service offering, mail.de has set up various alerts that immediately transmit an email notification in case of system failure or other anomalies.

The mail.de support team also uses Splunk Enterprise to quickly diagnose any issues raised by customers. The team can quickly locate and fix problems when they occur. If a customer's email does not reach the intended recipient, it takes just seconds for the support team to determine whether an internal error exists or the problem is on the receiver's side.

Correlation results in time and money savings

Central indexing of all log files as well as the ability to correlate current and historical data in real time has resulted in considerable time savings for the entire company. With Splunk Enterprise, many different systems can be analyzed with just a few clicks. In addition, all divisions receive the information that is most important for them in a simple and easy-to-use format.

Teams also receive specific additional information ad hoc when necessary. For example, if a customer asks the support team about the whereabouts of a particular email, in just a few minutes the team can clarify whether the mail was delivered.

Business insights across divisions deliver clear value

The benefits of Splunk Enterprise have been realized by every division and group within mail.de, including management. mail.de's management looks at the performance of key business metrics via Splunk reports and dashboards. In this way, management is provided with a graphical display of the most important business figures, such as the number of new registrations for the FreeMail service. The marketing team uses insights from Splunk Enterprise to evaluate the effectiveness of certain campaigns and drill down into the behavior of customers. Performance and support issues can now be identified and resolved in the shortest possible time. Proactive alerting helps the firm head off issues before a customer is ever aware of them. Splunk Enterprise is helping mail.de fulfill its promise to provide the most reliable, secure and feature-rich email communications service available.

CASE STUDIES

PostFinance

PostFinance Delivers Improved Fraud Detection and Enhances Customer Experience

Executive Summary

PostFinance is the third largest retail bank in Switzerland with just under three million customers. It provides a full range of financial products to both consumers and merchants with an established position as the number one payments provider in Switzerland. The bank needed to improve visibility into its payments processing and online banking services to be more proactive in addressing threats and protecting customers from potentially fraudulent activity. Since deploying Splunk Enterprise, PostFinance has seen benefits including:

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

Splunk Products

- Splunk Enterprise
- Splunk Use Cases
- Security and Fraud
- Application Delivery

Challenges

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

Business Impact

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

Data Sources

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

Why Splunk

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

Splunk Enterprise is used by the fraud management team at PostFinance to provide insight into the online shopping solution used by 11,000 merchants in Switzerland. It monitors the technology at each stage of the buying process, providing useful data for the team to analyze. Around 50 automated fraud searches feed data into a dashboard that enables the fraud management team to track activity, as well as allowing for ad hoc searches and reporting according to the team's needs.

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

Insights shine a light on debit card fraud

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

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

– Patrick Hoffman, head of IT infrastructure, PostFinance

Better visibility across data results in better customer protection

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

"Protecting our customers' debit cards and personal information is critical to the business," said Patrick Hofmann, head of IT operations and IT infrastructure, PostFinance. "Splunk Enterprise supports the payments experience by providing useful data for the fraud management team to analyze."

Improved insight into merchant success and performance

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

CASE STUDIES

DUKE UNIVERSITY

Duke University Gains Powerful Security Insights and Fraud Protection

Executive Summary

Founded in 1838, Duke University (Duke) is a private research institution situated on an 8,500-acre campus in Durham, N.C. Duke is divided into 10 schools and colleges, serving nearly 15,000 undergraduate and graduate students. With faculty and staff added to the mix, Duke supports more than 68,000 active network users. The Duke IT Security Office was faced with data and usage challenges, including not having a SIEM solution. Since deploying Splunk Enterprise, Duke has seen benefits including:

- Incident investigation and remediation reduced from hours to minutes
- Improved security posture
- Prevented phishing attacks and payroll fraud

Splunk Products

- Splunk Enterprise
- Google Maps Add-on for Splunk Enterprise

Solution Areas

- Security

Challenges

- Lacked centralized log management system
- Difficulty detecting and investigating risks within IT environment
- Manual, laborious processes for incident investigation
- Wanted to improve reliability and security of email servers

Business Impact

- Reduces time to investigate and remediate security incidents from hours to minutes
- Provides quantifiable risk management information for use by academic business leadership
- Improves collaboration among formerly siloed departmental IT operations
- Extends security responsibility to entire organization through greater access and collaboration
- Meets need for customizable SIEM solution to accommodate the unique needs of a distributed IT environment
- Accelerates detection and correction of compromised user accounts, and helps detect and prevent phishing attacks and payroll fraud

Data Sources

- Web logs
- Sophos PureMessage anti-spam logs
- Postfix mail server logs
- Login event types: VPN, single sign on, SMTP
- Shibboleth single sign-on logs
- Operating systems, including Windows and *nix
- Network, IPS/IDS/Firewall logs
- LDAP

Why Splunk

Duke's Information Security Office (ISO) became aware of Splunk software and its potential in 2013 during its search for a SIEM solution. The Duke Office of Information Technology (OIT) is a lean operation and typically creates its own tools or demands purchased solutions meet multiple needs—any SIEM solution had to be usable by those outside of security operations. "The SIEM products we reviewed seemed very powerful in demonstrations," explains Richard Biever, Duke's chief information security officer (CISO). "But when we tried to use them ourselves or when we tried to get other teams to use the tools, there was a frustrating learning curve. Splunk Enterprise was easy to deploy and use, and also flexible enough that we could adapt it to meet a wide range of needs across the university."

Today, Duke has a 1.25TB Splunk license shared among the ITO/ ISO offices, the medical center and nine university departments. Nearly 3,000 devices run lightweight Splunk forwarders and capture data from more than 200 different source types, including syslogs, network/IPS/IDS/firewall devices, VPN, LDAP and operating systems.

"We wanted a solution that was not simply a security product," Richard Biever, chief information security officer, Duke University said. "We wanted something that could meet the unique needs of our systems team, our network team, application owners and identity management group. And that's what we got with Splunk Enterprise. There's no limit to what you can do with Splunk software. We have folks all over campus using it."

Strengthening security posture with real-time alerting and reporting

Splunk Enterprise has enabled Duke to move from a reactive to a proactive approach to security, helped automate threat identification and remediation, centralized log management and analysis, streamlined performance monitoring, and made reporting more accessible and quantitative. The Splunk platform also plays a key role in real-time threat analysis and alerting. When indexed logs meet the parameters of an SSH brute force attack, for instance, the relevant IP addresses are flagged and sent to the school's intrusion prevention system (IPS) for automated blocking.

Monitoring email traffic to increase security and identify DDoS attacks

In order to increase the security and reliability of the university's email servers, Duke wanted to pinpoint the source of incoming junk email. While it seemed that most of this type of email was coming from outside the U.S., there was no hard evidence to support the theory. Jeremy Hopkins, a senior analyst for Duke's enterprise internet services group, turned to Splunk Enterprise to make a case for geoIP-based filtering of email,

Hopkins and his team used advanced XML and the Google Maps Add-on for Splunk Enterprise to build a Splunk dashboard that could display recent junk email as geoIP hot spots on a global map view. This Splunk dashboard convinced management and Duke's technology architecture group that email traffic needed to be filtered.

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

Waging war on fraud

In December 2013, a phishing email attack resulted in the theft of payroll deposits for several Duke employees. Immediately after receiving word of the phishing attacks, the Duke security team used Splunk Enterprise to set up a tracking dashboard to record suspected phishing messages in a Splunk lookup table. Another Splunk dashboard was created to aggregate phishing messages and recipient information, and provide information on recent changes to direct deposit accounts. These dashboards allow investigators to correlate information and contact employees to determine whether changes to direct deposit accounts are legitimate or are the result of phishing fraud.

"This type of visibility into logs and other sources did not exist for us before Splunk Enterprise," said Jeremy Hopkins, a senior analyst for Duke's enterprise internet services group. "In the past, the security office had to request access to logs. This is really a game changer for the security group. We have saved thousands of hours of work with Splunk software."

CASE STUDIES

surescripts

Surescripts Protects Doctors and Patients With Improved Fraud Detection and Security

Executive Summary

Founded in 2001, Surescripts operates the largest health information network in the United States, designed to connect a diverse and expansive community of care partners including pharmacies, providers, benefit managers and health information exchanges. With vast amounts of data flowing across its technology-neutral platform, Surescripts needed to maintain a close watch over fraudulent activity and wanted real-time visibility into its entire security posture for faster reporting and incident response. Since deploying Splunk Enterprise, Surescripts has seen benefits including:

- Improved fraud detection accuracy
- Immediate insights into security events

Splunk Products

- Splunk Enterprise
- Splunk DB Connect
- Splunk for Palo Alto Networks
- Splunk on Splunk (S.o.S)
- Splunk Enterprise Security (planned)

Solution Areas

- Security
- Business Analytics

Challenges

- Safeguarding huge volume of sensitive information
- Time-consuming manual process for identifying and analyzing fraudulent transactions
- 24-hour latencies on existing SIEM solution
- Lack of real-time visibility into processes

Business Impact

- Increased automation of daily fraud checks on billions of transactions
- Faster and improved fraud detection accuracy
- More in-depth real-time and historical data fraud analysis
- Immediate insights into security events
- Significantly reduced incident response times
- Ability to create customized, in-depth, intricate reports

Data Sources

- 3,000 data sources
- VPN, firewall and server logs
- Malware IDs
- Failed password attempts

Why Splunk

Surescripts processes more than six billion transactions each year, including more than 700 million medication histories, one billion e-prescriptions and nearly ten million clinical messages. Prior to Splunk, identifying and analyzing fraudulent transactions was a tedious, time-consuming process for Surescripts' Information Security and Risk Management team. The team would receive unique alerts from each disparate platform, decipher each alert individually and then export the associated raw log data into Excel for analysis. Additionally, Surescripts was experiencing 24-hour latencies on investigations with its existing SIEM, which was too long of a delay.

Surescripts deployed Splunk Enterprise across its complicated infrastructure—consisting of multiple datacenters and extensive virtual and in-house hardware—for enterprise security and fraud management. "We realized our investment the minute we deployed the Splunk solution. Splunk software has empowered Surescripts to determine what is important—to take full control of all our data," says Paul Calatayud, Surescripts' chief information security officer (CISO).

"Healthcare fraud costs medical providers, pharmaceutical companies, pharmacies and patients billions of dollars per year. Surescripts uses Splunk software to pinpoint and help put a stop to those trying to take advantage of our customers," said Paul Calatayud, chief information security officer, Surescripts.

Automating and improving real-time fraud detection

Since deploying Splunk Enterprise, Surescripts has streamlined processes and automated the analysis of fraudulent activity. All raw log event data now comes through the Splunk interface, significantly reducing the time needed to detect, analyze and mitigate fraud.

With Splunk software, Surescripts now sees patterns within the data that identify physicians who may be self-prescribing medications. Similarly, Surescripts can recognize legitimate doctors on the network writing valid prescriptions—and protect them from identity theft. More complex fraud queries in Splunk Enterprise have enabled Surescripts to introduce and monitor multiple "risk" variables, such as data about doctors prescribing restricted and commonly abused medications over a set time period in a particular location. Splunk provides historical trending for these variables so that Surescripts can identify pattern anomalies and determine whether a doctor's credentials have been compromised.

Replacing a legacy SIEM solution to gain instant answers

After replacing its legacy SIEM solution with Splunk software, Surescripts gained immediate insights from its unstructured data. Calatayud explains, "Splunk allows you to look beyond your data into security areas, so you're getting an all-encompassing view. Our team's expertise becomes a key variable in the analysis of what is meaningful. That just can't be done with your typical SIEM."

"Not only are we achieving better response times, we're able to pivot and dig deeper whenever we find something of interest," says Steve Olson, manager of security services for Surescripts. "We're able to build velocities around patterns using Splunk's reporting engine to create intricately customized and in-depth reports. It is much easier to do that with Splunk software than the old SIEM. Moreover, reports that previously took 15 minutes to generate for each state are now generated automatically and instantaneously."

In addition, Splunk DB Connect gives Surescripts access to data stored in relational databases. Previously, the team logged remotely into the production environment and the needed data wasn't always available due to dependency on upstream processes. "With DB Connect, as the data shows up, it's immediately imported. It makes our lives much easier," Olson explains.

Increased interoperability across entire infrastructure

The Surescripts network integrates with a variety of clinical, electronic prescribing and pharmacy management software systems. Interoperability is critical to these systems, especially in view of increasingly stringent federal regulations for the healthcare industry. Thanks to Splunk software, Surescripts now exchanges and interprets shared data across these internal platforms. This ensures that the electronic exchange of prescription information is carried out smoothly across Surescripts' entire infrastructure—while safeguarding patient privacy.

Currently, more than 200 individuals across Surescripts use the Splunk reporting interface, including IT, server, network, database and development staff. There are plans for the quality, products and formal business intelligence teams to use the Splunk solution as well. Calatayud concludes, "We're going to start to see Splunk software move from internal utilization to supporting all our products indirectly."

What We Hope You Think Now

- An IT or security team needs to know what transactions and behavior can be exposed to fraud and who monitors/remediates
- Machine data is the most detailed source of information that can be used for fraud detection
- Unlocking machine data will strengthen business operations
- There is a solution that gives visibility into all fraudulent transactions and behaviors, and teams can quickly adopt techniques and solutions to detect, investigate and respond to that fraud
- Implementing a fraudulent behavior mitigation model doesn't need to take one or two weeks
- Business value for IT rather than cost center
- Point solutions don't fix everything or show what else might be happening in the environment

What You Should, and Shouldn't, Be Doing Now

- Create demand and flag the need for a flexible fraud detection and investigation platform that can consume all kinds of machine data quickly to identify anomalies and create baselines
- Demand log data from business applications to answer the who, what, where, when, why and how to make the data accessible to the fraud team
- Understand fraud analysts should be trained on Splunk platform, software or solutions to protect their businesses and customers

Ready to get started fighting fraud with the Splunk platform? Try the **Splunk Security Essentials for Fraud** app.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com