Solving the Compliance Challenge

How Splunk Software Is Used To Meet Audit Requirements And Prevent Insider Fraud At An International Bank

CUSTOMER PROFILE

Splunk customer profiles are a collection of innovative, in-depth use cases that highlight the value that Splunk customers gain from collecting, analyzing and visualizing the massive streams of machine data generated by their IT systems and technology infrastructures.

Each “real world” customer profile introduces a unique business challenge and shows how leveraging machine data and Splunk software in new and interesting ways has helped drive powerful business and operational outcomes.

Executive Summary

You might expect that someone embezzling money, engaging in illegal stock trades or misdirecting funds would want to take time off to enjoy the bounty. Over the past decade, however, regulators discovered that several high profile, multimillion-dollar financial crimes had a common element: perpetrators of these crimes never took time off. They appeared to be model employees. They came in early and left late. They rarely took the vacation time that they had accrued. It turns out that in cases of financial fraud, perpetrators usually have to stay at work in order to deflect inquiries, hide the evidence and prevent others from noticing questionable transactions.

Because of this recent discovery, new compliance mandates have been enacted in most major economic markets around the globe, requiring that certain employees and contractors take at least two contiguous weeks off each year. The two weeks can begin and start at any time during the year, according to employee preference. During this leave, employees are not permitted to use a mobile device, laptop or tablet to log in to their work accounts in any way. While these employees are on vacation, auditors and management examine their electronic books and other work products in an attempt to discover any unusual activity.

In the U.S., vacation monitoring is a highly recommended internal control by the FDIC, the SEC and the FINRA. In Europe, vacation monitoring is mandatory; the European Banking Authority (EBA) maintains these guidelines. Because it's an unbroken block of time, this compliance regulation is known in various jurisdictions as "Mandatory Block Leave" or "Block Leave Monitoring." This regulation is so effective for averting fraud that national regulatory agencies have fined financial institutions millions of dollars in penalties for lax implementation of these internal controls. For example, in Hong Kong, one bank was fined $6 million by the Securities & Futures Commission for failing to properly implement Block Leave Monitoring that could have averted significant fraud.

When a European Banking Authority auditor contacted one Splunk customer to ensure that it was compliant to this new mandated control, the customer was deeply concerned. Although the customer is an international bank with billions in assets, a significant portion of its workforce did not use a consistent system to record time off. Vacation time was tracked by administrative staff, sometimes with pen and paper. With a global footprint, there was no standard method used between divisions or locations. Without enough time to change how vacations were tracked, how could the compliance team know which two-week period to analyze for "no activity"? And, how—and where—do you look for "nothing"? Employees might log on to a dozen systems a day, each system capturing the login credentials in a different way. It would be tedious and time consuming to look in the logs for every possible system for every relevant user and for every potential two-week timespan. Like proving a negative, this seemed like an impossible task.

The Information Technology team at the bank had recently replaced an existing SIEM with Splunk Enterprise. They had invested in training for key staff, and set up a Splunk Center of Excellence to share Splunk expertise and best practices. They continually discovered additional, valuable use cases for Splunk Enterprise that went far beyond the capabilities of their previous SIEM solution. Because of this expertise, the IT team quickly realized that Splunk software could be used to resolve this

Business Benefits at a Glance

Splunk Value	How Value Is Measured	Business Impact
State-of-the-art user interface and toolset	Speed to create meaningful reports for auditors; easy transfer of existing solutions to new use case	• $300K/year saved by avoiding the need to hire new personnel to meet compliance needs • The bank avoided millions of dollars in regulatory penalties
Holistic view of security; ability to ingest multiple types of data	Ability to see across multiple systems to detect and alert on unusual activity, revealing activity that had been masked by too much data "noise"	$1.5M/year staff costs redirected positively toward solutions rather than sleuthing
Ability to create alerts on high-risk behaviors	• Comprehensive visibility into fraudulent activity from its source to its intended target • Discovering and mitigating fraud before it is detected and reported to the public by regulatory agencies	• Ongoing loan fraud was detected before fraudulent loans were funded, preventing millions of dollars in lost funds • The bank avoided significant and costly damage to its reputation, which would have resulted in lost customers and decreased market share

compliance crisis. The team used the capabilities of Splunk software, adding key data to data that had already been ingested, as well as correlating relevant fields, in order to see activity across different systems by user. Block Leave Monitoring dashboards were created to reveal which employees had taken their two weeks off and when. The customer was able to quickly develop detailed, understandable, up-to-date reports for the auditor that demonstrated this compliance and prevented penalties. But Splunk software also exposed user activity beyond the compliance requirements.

Typical for the industry, the block leave search revealed that there were several rogue traders and rogue loan officers who were skipping their vacation in order to cover questionable trades or loan activity. But applying Splunk software also revealed this: some employees never seemed to log off, even those who could prove that they had been on vacation. Further investigation, made possible because of Splunk capabilities, revealed that employees had been using their vacationing colleagues' privileged IDs to misdirect funds, sometimes for years. Thanks to using Splunk software to look at both real-time and historical data, the customer was able to stop the fraud quickly, find out who was committing this fraud and learn the loopholes that they were exploiting to do so. Meeting the compliance needs and finding fraud prevented future legal issues, substantial penalties, large future losses and potential damage to the customer's reputation. And it didn't take a team of programmers to do it.

With Splunk software, the customer was able to:

- **Consolidate information from dozens of disparate systems to prove compliance.** Splunk software successfully found relationships across data from multiple systems, producing reports that either validated compliance or alerted staff that further investigation was warranted. Easy-to-build, easy-to-use dashboards presented a picture that would have been impossible to see any other way.
- **Detect and stop fraudulent activity.** By using Splunk software to compare machine locations of the valid employee with other login activity, compliance staff was able to hone in on the exact physical location of the fraud perpetrators.
- **Measure and mitigate fraudulent activity.** Once staff knew which internal devices and desktops to monitor, they used Splunk software to track exactly what the perpetrator was doing with the stolen credentials. They could use this knowledge to discover patterns, they could immediately shut down access and they would now have an understanding of what needed to be done to both stop ongoing damage and prevent future fraud.

Validating Vacations: Looking for Nothing

A government auditor demanded reports proving that one Splunk customer, an international financial institution, was compliant with Block Leave Monitoring. The Director of Compliance for the bank knew that he had no way to produce the reports because:

- For a significant portion of employees, administrative staff tracked vacation time manually, sometimes with pen and paper. Even for those using HRIS software to track time off, there was no standard method used between divisions or locations.
- Multiple systems had multiple logins; it was difficult to match employee name to the appropriate login.
- Several roles and employee levels were included in the compliance regulations, which meant that in the normal course of their work, employees used multiple systems for various functions, making anomalous behavior difficult to spot.

There are hundreds of sources of machine data at this global financial institution, with a handful available to each employee. Without the ability to change how leave was tracked historically, and no time to implement a new system, the compliance team was challenged to prove that they could analyze and report on "no activity" across multiple financial systems. Proving a negative is a difficult task. The Director of Compliance of the bank was desperate. Meeting the auditors' requests seemed impossible. He calculated that to validate Mandatory Block Leave for thousands of employees with the tools he had on hand, it would take new head count—half a dozen new employees—and thousands of tedious hours to organize and implement.

Enter Splunk

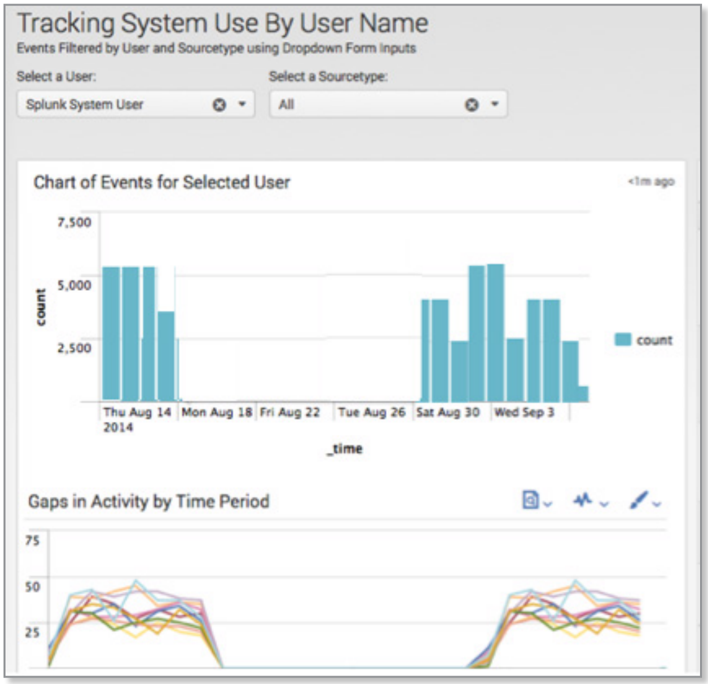
The bank's Director of Information Systems had recently used Splunk Enterprise to replace a Security Information & Event Management (SIEM) solution. The SIEM had not been able to handle the increasing volumes of data produced by the bank, but Splunk software had more than met this challenge, and the Information Technology group realized it could do far more. Specifically, it could be the solution to the Director of Compliance's crisis. Because the financial institution already had expertise with Splunk software, and had already ingested most of the machine data it needed into Splunk, the team was able to quickly determine how to create a Block Monitoring dashboard from a set of custom searches.

The first challenge was to correlate every possible way that a user might log in so that they could validate periods of "no activity" in all of these disparate systems for the specified employee. Since the field for capturing user identity was different in each system (for example, "username" in one, "userid" in another) the ability of Splunk software to correlate field names allowed the team to aggregate multiple login IDs into a single entity, revealing how any single entity was logging into and accessing any bank system. IT staff correlated user names from dozens of machine data sources, adding lookups to relevant content data sources for context:

- Email addresses from all mail and mobile systems
- Active Directory (to find those employees with the roles subject to the Block Leave requirement)
- Login names from all relevant financial systems
- Logins to all mobile and desktop systems
- ID badge swipe records

To test the validity of the new dashboards, IT staff entered in vacation time for an employee that they knew was legitimately out during a specific date range. The results can be seen in the dashboard shown in Figure 1.

Next, they decided to find employees that did not have a break in activity. The customer used a search such as the one shown



Tracking System Use By User Name

Events Filtered by User and Sourcetype using Dropdown Form Inputs

Select a User: Splunk System User

Select a Sourcetype: All

Chart of Events for Selected User

Gaps in Activity by Time Period

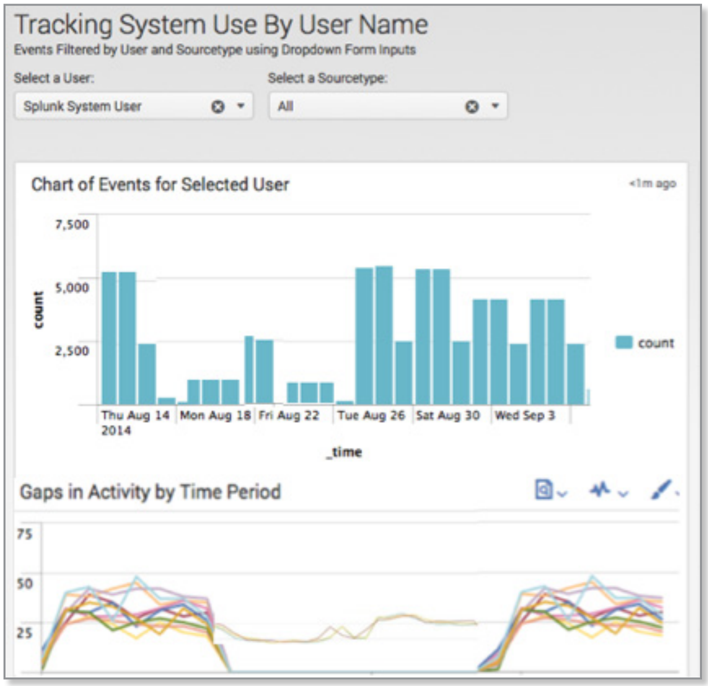
Figure 1. Validating an employee's Block Leave—"No Activity" (Each line represents a different system).

below to obtain a list of users who never had more than a 14-day break between logins. In the example below, "userid" had previously been defined to the login field for each system. The result of this search would be a listing of users whose "userid" had not been idle for more than two contiguous weeks.

```
Sourcetype=logins_to_systems

| streamstats global=f window=2 current=t

    earliest(_time) as previous_login_time

    latest(_time) as current_login_time

  by userid

| eval time_between_logins=current_login_
time - previous_login_time

| stats max(time_between_logins) as longest_
break by userid

| where longest_break < (14*24*60*60)
```

The result for an example specific user is displayed in the Tracking System dashboard shown in Figure 2. Further examination of this 'never vacationing' employee dashboard reveals some interesting anomalies.

As you can see in Figure 3, activity sharply dropped off for this employee during a two-week period, but it didn't stop entirely. There is a noticeable drop off over several weeks, except for access at a "normal rate" on some systems. While the original goal had been to find the few employees who had simply not taken the required leave, it was expected that this would mean that they were working continuously. However, this result indicates that employees were taking time off but continuing to access specific systems.



Tracking System Use By User Name

Events Filtered by User and Sourcetype using Dropdown Form Inputs

Select a User: Splunk System User

Select a Sourcetype: All

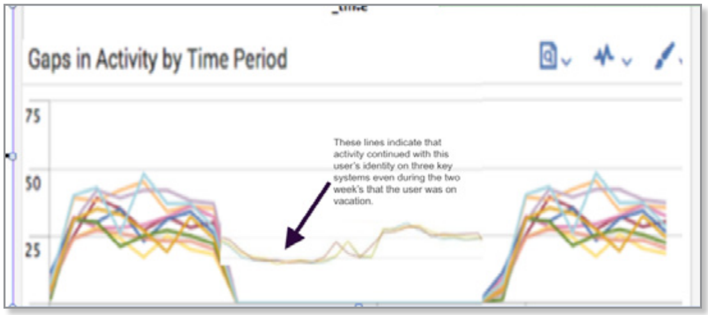
Chart of Events for Selected User

Gaps in Activity by Time Period

Figure 2. The Tracking dashboard for an employee who seemed to never fully disengage from the bank's systems.

Armed with these results, Internal Auditing contacted the employees who had apparently never fully logged off, which did uncover a few cases of people who simply couldn't disengage even on vacation, whether for innocent or suspicious reasons. But seeing the results on the Splunk dashboard made it clear: there were imposters fraudulently using the IDs of traders and loan officers—year round! Because of Splunk software, the bank was able to:

- Meet compliance requirements by clearly validating and reporting which employees had not logged in during the required leave.
- Detect internal fraud and violators of the Mandatory Block Leave mandate by identifying those employees who were in fact logging in during their required leave and uncovering activity that these employees were trying to hide.
- Detect an unexpected type of ongoing fraud by discovering that imposters were fraudulently using the IDs of the vacationing employees—continuously, not only when the employees were on vacation.
- Clearly see which systems the imposters were targeting, providing clues to the motive behind the spoofing.



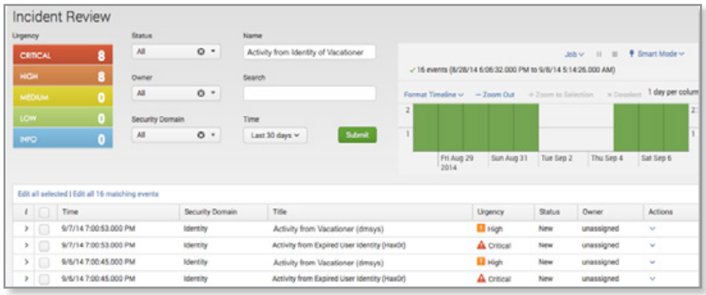
Gaps in Activity by Time Period

These lines indicate that activity continued with this user's identity on three key systems even during the two week's that the user was on vacation.

Figure 3. Magnified section from Figure 2. The arrow points to continuing activity despite the legitimate ID owner's reported vacation.

ID'ing the ID ring: When Crime Doesn't Play

The unusual intermittent access revealed that imposters were using the credentials of vacationing employees. The fraudulent activity was as clear as a Splunk dashboard and no longer buried in a fog of endless unstructured data. Until Splunk software revealed the fraud, it was masked by the legitimate activities of the rightful owners of the ID credentials.



Incident Review

Urgency: CRITICAL 8, HIGH 8, MEDIUM 0, LOW 0, INFO 0

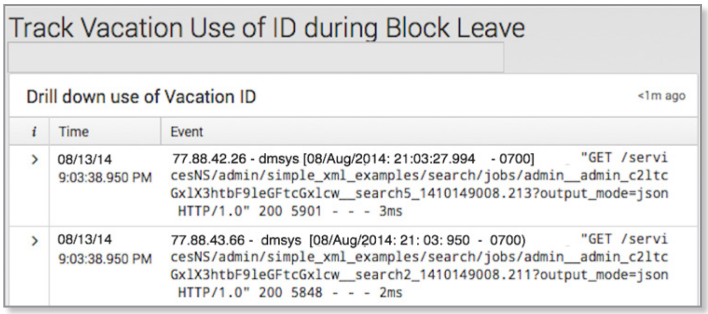
Status: All
Owner: All
Security Domain: All
Name: Activity from Identity of Vacationer
Search:
Time: Last 30 days

✓ 16 events (8/28/14 6:06:32.000 PM to 9/8/14 5:14:26.000 AM)

i	□	Time	Security Domain	Title	Urgency	Status	Owner	Actions
›	□	9/7/14 7:00:53.000 PM	Identity	Activity from Vacationer (dmsys)	High	New	unassigned	⌄
›	□	9/7/14 7:00:53.000 PM	Identity	Activity from Expired User Identity (Hax0r)	Critical	New	unassigned	⌄
›	□	9/6/14 7:00:45.000 PM	Identity	Activity from Vacationer (dmsys)	High	New	unassigned	⌄
›	□	9/6/14 7:00:45.000 PM	Identity	Activity from Expired User Identity (Hax0r)	Critical	New	unassigned	⌄

Figure 4. Incident Review from the Splunk App for Enterprise Security, modified to include Vacationing ID with other Identity Tracking.

Figure 4 displays an incident review dashboard that the bank configured to include suspicious use of vacationing employees' IDs with other suspicious identity events. Clicking on an event displayed the dashboard shown in Figure 5. When the IT team found a desktop or mobile device that had fraudulently used the ID of a vacationer (seen in the list in Figure 4), they used Splunk's drilldown capabilities to investigate further, by clicking on the line with the suspicious activity. This reveals event details, also shown in Figure 5.



Track Vacation Use of ID during Block Leave

Drill down use of Vacation ID

i	Time	Event
›	08/13/14 9:03:38.950 PM	77.88.42.26 - dmsys [08/Aug/2014: 21:03:27.994 - 0700] "GET /servicesNS/admin/simple_xml_examples/search/jobs/admin__admin_c2ltcGxlX3htbF9leGFtcGxlcw__search5_1410149008.213?output_mode=json HTTP/1.0" 200 5901 - - - 3ms
›	08/13/14 9:03:38.950 PM	77.88.43.66 - dmsys [08/Aug/2014: 21: 03: 950 - 0700] "GET /servicesNS/admin/simple_xml_examples/search/jobs/admin__admin_c2ltcGxlX3htbF9leGFtcGxlcw__search2_1410149008.211?output_mode=json HTTP/1.0" 200 5848 - - - 2ms

Figure 5. Drill down to discover the origin of the fraudulent access.

For an earlier security use case at the bank, Splunk software had been configured to ingest machine data related to the bank's physical assets, such as mobile devices, laptops, desktop PCs, etc. Correlations were created that tied each device's unique "MAC Address" and static IP address to valid users. The IT team leveraged this earlier work to pinpoint the identity of those fraudulently logging with vacationers' IDs. This took the investigators right to the desktop of the ID spoofer. Now the team could investigate further, discover which systems were being accessed with the ill-gotten IDs and determine the ultimate motive.

With the help of Splunk software, the team discovered:

- Which systems were fraudulently accessed
- How long this fraud had been going on
- Who was the likely perpetrator
- What systems they were trying to access

Instead of slogging through log files to validate compliance to Mandatory Block Leave, which would have taken many months and taxed its resources, the bank's IT staff was able to creatively use Splunk software to find the answers they needed, in weeks. And because of Splunk software, they had visibility into additional suspicious activity that had previously been masked by a deluge of data.

Discovering the Motive: Unmasking the Loan Arrangers

To prevent an employee who was reviewing a credit application from being more generous than rational, the bank had a complex multi-step approval process requiring multiple electronic sign-offs for mortgages or credit cards, unusual requests and other consumer loans or investments. In a simplified example, employees at Level One would do an initial screening, then electronically pass the file up to Level Two (a supervisor) for a second approval. The Level Two approval process was more robust and designed to filter out risky loans. But Level Two also had more authority and could be used to grant exceptions to loan applications for legitimate reason or with irregularities.

In the course of complying with Mandatory Block Leave, the customer discovered that some users never logged off, even during vacation leave. They soon discovered that the vacationing user's ID was being fraudulently used. Further sleuthing with Splunk software revealed why: several Level One approvers had somehow learned their Level Two approvers' login credentials. The Level One approvers were using the stolen Level Two login to sign off on financial transactions that their supervisor never saw.

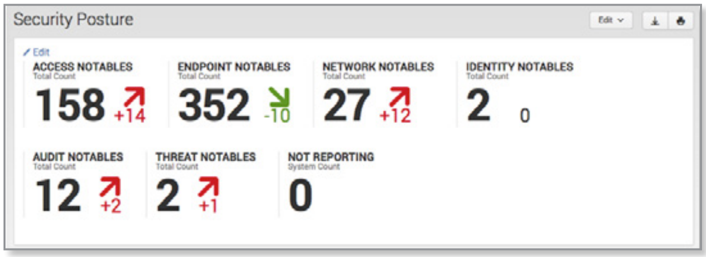
This type of fraud had the following impact:

- Granting loans without the proper procedures caused instability and exposed the bank to severe penalties from governments in every jurisdiction.
- Risk-mitigating steps that were normally taken to ensure that certain loans were a good bet for the bank were being totally ignored.
- Loans were granted to non-existent/fraudulent accounts, making them impossible to collect.
- Credit limits were increased on existing accounts that were not qualified to get the increased credit.

The fraudsters had been using the stolen IDs to sign off on transactions for years. The fraud ranged from serious multi-person rings processing hundreds of thousands of dollars worth of loans, to occasional perpetrators, such as the employee who ensured she would be popular at the next family reunion by upping the credit limit for relatives who did not have the required income. Or the employee who reveled in the recognition he received because he successfully processed more loans than his coworkers who followed the appropriate procedures. All of the fraud, of any size, put the bank's reputation and assets at risk. Finding it quickly, before external auditors or the media discovered it, was paramount. Based on compliance alone, bank management stated that Splunk software paid for itself almost as soon as it was launched. But because Splunk software also revealed significant fraud, Splunk software positively impacted the bottom line.

Using the Splunk App for Enterprise Security

To meet the goals of the audit, the Information Technology team was able to accomplish everything it needed by using the dashboards and searches they created with Splunk Enterprise. However, when the bank subsequently added the Splunk App for Enterprise Security (Splunk App for ES), the team realized that this app could be used to place identity and asset management—including Block Leave Monitoring and other compliance requirements—into a larger security context. (The screenshots shown in this story show modifications to the Splunk App for ES.) For example, as shown in Figure 6, the Identity Notables dashboard from Splunk App for ES was designed to alert whenever an ID of a terminated employee logs in or when a non-authorized user attempts to access privileged systems.



ACCESS NOTABLES
Total Count
158 +14

ENDPOINT NOTABLES
Total Count
352 -10

NETWORK NOTABLES
Total Count
27 +12

IDENTITY NOTABLES
Total Count
2 0

AUDIT NOTABLES
Total Count
12 +2

THREAT NOTABLES
Total Count
2 +1

NOT REPORTING
System Count
0

Figure 6. Vacation Identity Tracking was added to Identity Notables, and now it could be seen as part of the entire security picture.

To build on these capabilities, and to take full advantage of the Asset and Identity Center features provided by the app, the bank tailored identity dashboards and searches to include "Vacationing Employee Identity" activity tracking for relevant employees. At first, the bank's IT team added a control to make it easy to manually enter vacation time as reported by staff; later, the team devised a way to collect and feed the vacation dates in via a spreadsheet lookup table they had built. Finally, the bank required vacations to be entered into the Payroll/HRIS systems so that vacation dates of relevant employees could be automatically monitored for ID activity when the employee was on mandatory leave.

With Splunk, the Bank's Investment Paid Dividends

In this use case, we explored how Splunk software provided audit-quality visibility into bank operations, enabled easier reporting and provided unprecedented insight into day-to-day operations of key employees, causing the bank to discover fraud that had been concealed by a mask of disconnected data.

This use case demonstrated:

- **Making sense of disparate data.** Because Splunk software indexed data from multiple login IDs across multiple systems, the bank saved months of time that would have been required to manually comb through data, and was able provide real-time information to regulators, providing effective compliance verification to meet internal and external governance demands.
- **Solving big problems with easy-to-build, easy-to-use dashboards.** Vacation monitoring, which first seemed nearly impossible, became easy with targeted dashboards that the team created in Splunk Enterprise. When the customer later implemented the Splunk App for Enterprise Security, the IT team incorporated vacation monitoring into the app's identity monitoring dashboards, creating a holistic view of identity management tailored for the bank's compliance needs.
- **Knowledge and control.** This use case illustrates how Splunk software can use drilldowns to get to the source of a problem, then use these insights to create relevant alerts and stop issues before they happen.
- **Value generation across multiple use cases.** In addition to creating quick compliance reports, the customer discovered serious ongoing fraud. Prior to this, the company had more than recouped its investment in Splunk by gradually phasing out SIEMs and replacing them with Splunk software.

By building on its IT team's Splunk platform expertise and maximizing data that had already been ingested, this customer realizes escalating value from its Splunk implementation. It's like buying solar for your house and then realizing you have enough capacity to plug in a car. Once you've paid for the investment, the rest is profit. The more use cases you give Splunk software, the more it gives you back.

One Splunk. Many Uses.

While the business problems discussed in this case were specific to this customer and its industry, and the solution made creative use of Splunk software's features to solve these particular problems, the underlying theories apply to many business use cases.

With the right data, Splunk software can quickly find why website visitors are encountering difficulties, historically or as they happen. Once staff is alerted to these difficulties, Splunk dashboards lead to their source, exposing issues and leading to solutions. Finding and resolving these issues leads to increased customer retention and increased profits. While the possibilities are endless, the process is simple.

Next Steps

To learn more about Splunk customer success, customer snapshots, ROI stories, customer profiles and more, please visit: http://www.splunk.com/view/customer-case-studies/SP-CAAABB2

Splunk software is also available as a free download. Download Splunk Enterprise and get started today: http://www.splunk.com/download

If you would like to speak to a salesperson, please use our online form: http://www.splunk.com/index.php/ask_expert/2468/3117