Splunk Enables Security and Improves Business Performance for the *Interac*® Organization: An EMA ROI Study

Introduction

In this study, Enterprise Management Associates (EMA) examines the Return on Investment (ROI) in Splunk realized by the *Interac* organization – Interac Association and Acxsys Corporation. Interac Association is responsible for the development and operations of the *Interac* network – Canada's national debit network – and Acxsys Corporation, whose shareholders are the architects of the *Interac* network, specializes in the development and operation of new payment service opportunities, as well as consulting and management services in the field of electronic payments, a leading provider of technologies that integrate secure access to Cloud Computing and complex application environments, and a fast-growing provider of its own Cloud services to meet these needs.

Splunk is distinctive in that multiple Splunk customers have provided impressive ROI stories across multiple areas of management – from IT operations to security, compliance, customer support and the integration of application development and operations. EMA explores the capabilities of Splunk that enable the organization to reduce the cost and complexity of IT and security management.

The organization is characterized by a highly diverse and complex operational environment composed of multiple business applications. This heightens the need for a solution that delivers operational visibility working within a wide diversity of technologies and business processes. As with many other cases, Splunk has enabled the organization to do far more in less time than it had been able to achieve before, with benefits ranging from better internal collaboration and simplifying the administration of complicated data sources, to improving the efficiency of IT infrastructure management within the organization's internal corporate environment.

Product Description

With over 3,300 customers since its founding in 2004, Splunk has won a considerable following among IT organizations that are often highly vocal about the distinctive flexibility Splunk provides for operational intelligence.

Splunk provides a combination of capabilities for data collection, indexing, search and analysis that give organizations substantial freedom for better understanding their operational data. The Splunk product is purely software, simply installed, and readily extended. Splunk can collect machine-generated data from a wide variety of sources. Its indexing and search capabilities free organizations from much of the overhead of competing monitoring approaches that require costly and time consuming normalization and rationalization of data before it can be made useful.

The Splunk platform is essentially very simple, centered on a Splunk server, with user access enabled via a Web console. This architecture can be easily extended across multiple data centers and Splunk servers, with role-based access controls that facilitate tailoring of reports and analysis to individual users and restricting access to sensitive information when required. Splunk forwarders, essentially lightweight software agents which broaden the range of data the Splunk platform can collect and transmit to Splunk servers, further support extensibility.

Splunk's flexibility and ease of deployment has resulted in an annual growth rate in the high double-digits according to the company. Splunk is currently in use by over half of the Fortune 100. In the second quarter of 2011, Splunk was granted U.S. Patent No. 7,937,344 for organizing and understanding machine data through the use of a "machine data web." The company has recently augmented its offerings with a hosted version of the technology, Splunk Storm. Scheduled to be made publicly available in April 2012, Splunk Storm offers Splunk as an elastic, multi-tenant service, able to monitor both Cloud-based and on-premises environments as well as leveraging the power and extensibility of Cloud computing for data analysis.

Subject Organization

Together, Interac Association and Acxsys Corporation operate an economical, world-class debit system. Interac Association was founded in 1984 and is comprised of a diverse membership that includes banks, trust companies, credit unions, caisses populaires, merchants, and technology and payment related companies. The Association is responsible for the development and operations of the *Interac* network, a national payment network that allows Canadians to access their money through 59,000 Automated Banking Machines and 727,000 point-of-sale terminals across Canada. Other related services offered by Acxsys Corporation, whose shareholders are the architects of the *Interac* network, include: *Interac* Online, for secure online payments made directly from a bank account; *Interac* e-Transfer™, for the transfer of money from one person's bank account to another person's bank account; and international services, which provide Canadian cardholders with point-of-sale access at nearly 2 million U.S. retailers, and PULSE, Discover, Diners Club International and UnionPay cardholders access to ABMs in Canada.

Interviewee

Senior Systems Administrator in a group supporting organizational security, infrastructure, storage and application development and operations.

Problem Scenario

Prior to its deployment of Splunk, the *Interac* organization had no way to centralize and correlate monitoring data across its diverse IT landscape. This posed a particularly burdensome problem when security issues within the organization's environment warranted investigation, requiring the organization to manually collect and correlate security-relevant data across multiple applications and infrastructure points. This severely hampered the organization's ability to respond in a timely manner, let alone maintain situational awareness on an ongoing basis.

While security may have been the primary motivation for the organization to investigate solutions, the lack of centralized and responsive operational data analysis affected other aspects of the organization as well. The breadth of this insight gap was substantial, making it difficult to understand and resolve issues from application availability and performance to business operations. The monitoring process was further complicated because it often required coordination with external parties.

The process of collecting and analyzing monitoring data from the organization's various systems was complex and time consuming, often involving multiple staff. To investigate a security event, organization staff estimate that obtaining necessary data from each individual infrastructure or application system would consume at least two to three hours, and may have involved ten or more different aspects of operations. Turnaround on analysis would routinely consume two to three days ("easily," according to organization personnel) for just a single incident.

This lengthy process had an impact on more than operational costs alone. It also limited investigation of problems and concerns to an on-request basis. Organization staff had no way of simply referring to available information on demand. This severely hampered the organization's ability to provide continuous monitoring and situational awareness and hindered its agility in response – significant concerns particularly in the face of threats that can have a measurable impact within minutes.

Acquisition Story

The *Interac* organization investigated a number of solutions for centralizing operational data collection, management and analysis, but found that many tools were either cost prohibitive or too siloed to embrace its diverse IT environment.

With security as the initial driver, the organization explored solutions such as Security Information and Event Management (SIEM), which would be well tuned to collect data from security point products, but less able to accommodate more diverse data. A similar limitation existed when exploring solutions that focused on other specific aspects of operations, such as systems monitoring and infrastructure management solutions.

The organization found that Splunk was able to deliver the needed adaptability, enabling it not only to incorporate data from a wide variety of inputs, but to facilitate data discovery, correlation and analysis across its varied operational landscape – and to do so for significantly less than the total cost of deployment for other solutions with less breadth or flexibility.

One alternative would have cost approximately four times more than Splunk when product licensing, deployment services and training of personnel were factored into the total cost of deployment. Even at this higher cost, this alternative would have focused only on one aspect of infrastructure, and would have been less capable than Splunk for handling the wider scope of data necessary to delivering more complete insight into security and/or operational issues. Initial savings delivered by Splunk over this product on licensing alone were more than $75,000 (CAD).

> The organization found that Splunk was able to deliver the needed adaptability, enabling it not only to incorporate data from a wide variety of inputs, but to facilitate data discovery, correlation and analysis across its varied operational landscape – and to do so for significantly less than the total cost of deployment for other solutions with less breadth or flexibility.

Outcomes

Splunk has given the organization much more than affordable flexibility and operational intelligence. The Splunk platform has helped the organization simplify the management of complicated data sources, allowing for better internal collaboration and improved organizational effectiveness and agility.

More Responsive Security Analysis

The deployment of Splunk provided immediate benefits to the organization's security initiatives. In place of the complexity of the information gathering exercise of the past, the organization's security teams today turn to Splunk on a daily basis to discover and correlate security-relevant operational data. The intensive manual effort required to gather this data has virtually been eliminated.

The organization estimates that fully-loaded personnel costs may range from approximately $75 to $125 per hour per person to address such issues, depending on the seniority and responsibility of personnel involved (and perhaps higher still if external consultants are engaged). Given that organization staff estimate that a representative example of such efforts in the past required a minimum of 20 to 30 hours of total staff time, and a minimum estimate of fully-loaded personnel costs of $75 per hour per person, Splunk's ability to deliver this insight daily on demand equates to a productivity gain of approximately $9,375 per week ($75 per hour for 25 person-hours per incident, vs. Splunk delivery of an equivalent level of intelligence on demand every day, five days per week) or approximately $500,000 per year.

The speed and completeness of response has also been accelerated with Splunk. When a recent incident suggested that the organization might be exposed to a security risk, Splunk enabled organization staff to quickly capture relevant monitoring data and perform a comprehensive analysis of any attempted exploits. Within two days, Splunk enabled the organization to collect and analyze enough monitoring data to confirm that they were not targeted. Real-time alerts set up in Splunk following this incident have since enabled the organization to proactively monitor for this and similar threat activity on an ongoing basis.

Greater Flexibility for Better Intelligence

The organization particularly values Splunk's ease of adaptation for in-house staff. In contrast to more elaborate products that require significant expertise in systems integration to deploy and maintain, a single administrator can quickly develop new applications for Splunk. In one recent case, the development of an application to explore proxy server logs through Splunk required only two days' effort by a single in-house administrator.

This same administrator was able to develop a transaction profiling "engine" based on Splunk that enabled security and operations teams to track a user's "footprint" beginning with the point of entry into the organization's internal environment. This not only helps troubleshoot business processes, but also gives the organization more granular insight into suspicious activity when warranted.

The flexibility of Splunk also enables the organization to better leverage existing security investments. For example, network activity can be monitored through Splunk to detect the unauthorized transmission of sensitive information, or the use of unauthorized data transfer mechanisms such as Cloud-based consumer storage services. This expands the security use cases for Splunk while easing or eliminating the need for additional security technologies in some instances.

Extending the Return on the Splunk Investment

This adaptability has led the organization to recognize how readily Splunk can be extended to other operational areas:

Intelligence for Storage Operations

The organization's business applications have a critical dependency on the performance of underlying storage systems. Highly granular visibility into monitoring data is essential to solving problems quickly and accurately to maintain this performance. Prior to Splunk, the team reported that it had essentially no real-time monitoring capability for this environment. When issues arose, the existing management system did not deliver the needed depth of monitoring information required to troubleshoot specific problems in detail.

As with the security use case, an investment in a monitoring solution specifically for this environment would have cost over $75,000 more than the total cost of Splunk deployment. Instead, the organization was able to extend its existing Splunk investment into highly granular monitoring of its storage systems. With Splunk, the organization's team developed an application that enables visibility into detailed metrics such as IOPS (input/output operations per second), transfer speed and utilization of its storage infrastructure, as well as correlation with factors such as identification of specific devices that saturate storage network bandwidth.

This has resulted in a similar reduction of time and effort as that experienced in security. Staff estimate that data collection and analysis to troubleshoot serious performance or availability issues in their storage environment prior to Splunk required approximately two days' effort on the part of two IT staff members. With Splunk, a single technician can diagnose and resolve similar issues within a few hours. At a fully loaded minimum personnel cost estimate of $75 per hour, and with an assumption of analysis time reduced to approximately four hours at most with Splunk, this equates to a cost savings of $2,100 per incident.

The organization saw tangible return on this extension of the Splunk investment within its first month. Estimating this cost savings for at least one such incident per month yields savings of $25,200 per year.

Optimizing Applications: Enabling Dev/Ops Collaboration

Business applications are another area where Splunk has helped optimize the organization's ability to optimize performance. In recent years, the organization has increased application development in-house. This, in turn, has increased the need to provide monitoring of production applications to developers in real time.

In the past, developers requiring raw logging data to troubleshoot business applications had to obtain this data through a cumbersome process of downloading and transferring raw logs from the operational environment. In some cases, this also introduced the possibility that sensitive information would be included with this data.

To address these challenges, the organization's IT team built a Splunk App that enabled their developers to monitor the data they needed most, while masking sensitive information. This enabled developers to see the performance data required, enabling them to walk through specific transactions to troubleshoot problems in application processes without risking the exposure of sensitive information.

Improving Business Performance

As the value of Splunk becomes increasingly recognized, additional use case possibilities have emerged. For example, the organization's business operations depend on the transfer of data files to and from various external organizations. These transfers must be completed according to minimum performance standards defined in Service Level Agreements (SLAs).

When problems in the business processes surrounding these transfers occurred prior to Splunk, resolution could often be tedious. Affected file transfer servers had to be determined, missing or erroneous files identified, and information relayed back to business operations. Affected external organizations would have to be notified, which could result in a delay of up to a week if the organization had to independently untangle problems at their end. Once the nature of a problem was determined, resolution would have to proceed through the organization's internal systems before normal operations could be restored.

With Splunk, even non-technical business operations personnel are able to quickly identify when external organizations fail to relay files as expected, correlate failures with successful activity to identify specific problems, and notify the affected organization swiftly – often before the entity is aware that a problem exists. In one such case, the external organization had seen an issue, but was unable to identify the cause on their side. At the organization, non-technical personnel were able to diagnose the problem when Splunk revealed that one file was interfering with the delivery of another.

Staff estimate that troubleshooting more involved problems of this nature in the past would require as much as two to three days full-time for approximately two staff members. Less serious issues might still require up to a day of personnel time to resolve. With Splunk, this time has been cut down to roughly one hour. A process of some ten steps has been reduced to three: identify the problem through Splunk, coordinate details with the affected entity, and confirm resolution internally. Assuming that such incidents on average represent a day's time for at least two staff members to resolve, the reduction in personnel costs alone equates to a savings of $1,125 per incident (16 hours staff time @ $75 per hour minimum fully-loaded personnel costs as estimated previously vs. one hour with Splunk). Staff report that such incidents occur approximately once every week, leading to an annualized savings estimate of $58,500.

This, however, estimates only the cost of personnel time to resolve the immediate problem at hand. Today, with problem details identifiable within an hour with Splunk, business operations within an affected organization can be restored within two to three hours in many cases, significantly reducing business disruptions and both the hard and soft costs that result from them.

Hard and Soft ROI Summary

Hard ROI	**Example Case**	**Before Splunk**	**After Splunk**	**Benefits**
Solution acquisition and deployment	Purchase and deployment of a centralized operational intelligence solution.	No centralized capability. Monitoring of individual applications and infrastructure largely siloed, and often inadequate for detailed problem analysis.	Unified platform with high flexibility, able to integrate monitoring data across silos for centralized analysis.	Four-fold savings over competing solutions. Initial savings over one alternative of **$75,000** on licensing alone.
Internal security intelligence	Integration and correlation of security-relevant monitoring data from multiple application and infrastructure sources.	Highly time-intensive manual collection and analysis of data from siloed sources, and only when required for a specific incident.	Centralized analysis of aggregated security data available on demand, for daily review by security teams as required.	Increase in annualized productivity of **approximately $500,000 per year** over previous labor-intensive processes requiring significant staff time.
Operational intelligence in IT	Detailed monitoring of storage infrastructure operations. Root cause analysis data available on demand.	$2,400 estimated per incident.	$300 estimated per incident.	Annualized savings: **$25,200 per year**. Highly labor-intensive manual data collection and correlation processes virtually eliminated.
Business process optimization	Troubleshooting of transaction data relaying problems.	$1,200 estimated per incident.	$75 estimated per incident.	Estimated annualized savings of approximately **$58,500 per year**. Additional hard and soft cost savings from reduced downstream impact on member organizations and affected groups within Acxsys Corporation.
Total Annual ROI				**$583,700**
Soft ROI	**Example Case**	**Before Splunk**	**After Splunk**	**Benefits**
Solution flexibility and extensibility	Analysis of non-technical business operations.	Limited insight into relevant operational data.	Ability to collect data from operational systems such as business applications, yielding direct insight into business performance.	Improved performance of business initiatives such as marketing campaigns, based on data such as user behavior collected from Web applications.

Quotes and Observations

An organization staff member describes it as "the agile BI tool for machine-generated data." He summarizes Splunk as "a tool that provides a looking glass into our environment for things we previously couldn't see or would otherwise have taken days to see." The variety of analytics available help with insight from trending to determining how and where to best spend limited resources.

Security in particular has benefited from Splunk deployment at the organization. "Once our security teams really grasped the value of Splunk, the analysis of operational data went from being a turtle in the security race to being a rabbit. Our capability just leaped ahead."

"Today, our security organization has an 'aha' on a monthly basis. They didn't expect the level of granularity Splunk delivers for analyzing activity on a per-host or per-device basis."

"Our security specialists told us that at professional conferences, attendees were often urged to adopt Splunk. When one member of our security team returned from one such conference, one of the first things he said to us was 'Thank You!' for our Splunk deployment, which helps to put us ahead of the game."

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook. 2435.032612