Ceryx Turns to Splunk to Improve Business IT Service Integrity

Introduction

Despite the return towards normal rates of investment in Information Technology (IT), IT pros must continue to justify expenditures by understanding how each new product or solution will improve operational cost or otherwise contribute to business success. ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts use a case-based approach for understanding Return on Investment (ROI), studying the actual experiences that practitioners have had for any particular technology deployment. Splunk offers an innovative management product that has found a wide (and growing) range of uses when applied as part of monitoring and management architectures, delivering operational intelligence for system, network, and security professionals.

In this EMA ROI case study, managed cloud services provider Ceryx is profiled to illustrate an example of how Splunk's solutions delivered measurable operational efficiencies that far exceeded the cost of deployment.

HIGHLIGHTS

splunk>

Vendor name: Splunk Inc.

Product area: Operational Intelligence

Product name: Splunk® Enterprise™

Product version: 4.3

CERYX

The benefits of the cloud, without the compromise.™

Customer name:CERYX

Customer domain: Cloud-based Unified Communications and Collaboration solutions

Product: Splunk

Per Splunk's website: "Splunk … provide(s) Google-like search capabilities for … IT infrastructure (log) data. Users … (utilize) Splunk to index, search and report across all of their IT data to troubleshoot issues, find root causes, investigate security incidents and report on findings. ... Splunk lets (companies) harness their IT data to gain the insights needed to innovate and make informed decisions. (They) compare real-time data against historical trend/baseline/KPI data, enabling them to respond quickly and effectively to emerging conditions. … We call this delivering Operational Intelligence."

Interviewee

Title: Director of Software Development, Ceryx

Role: Manages the team responsible for developing software used for cloud service management, billing, ticketing, and monitoring. Past responsibilities (at the time the Splunk solution was procured) included system architecture and design, as manager of the Systems Development group.

Company

Ceryx Inc. is a leading outsourcer of reliable, secure Unified Communications and Collaboration (UC) solutions for large enterprise using cloud-based delivery models. Ceryx has managed advanced, customized solutions for mid-market and enterprise clients for more than ten years. As a Microsoft Gold Certified Partner of Excellence and repeat winner of the Impact Award for Hosting Solutions, Ceryx has extensive knowledge with Microsoft Exchange, Lync, and SharePoint. The company also offers managed archiving, advanced security and a range of complementary products and services. When clients entrust their unified messaging and collaboration requirements to Ceryx, they gain the efficiencies associated with cloud computing without sacrificing the control that accompanies an on-premise solution.

Problem Scenario

One of the services that Ceryx provides is email hygiene, where mail flow is monitored to identify and proactively protect Ceryx customers from spam and illicit email activity. A significant customer service challenge occurs when a message gets blocked and the customer subsequently wants to know why. When faced with such a question, Ceryx undertakes a message-tracking process to trace individual mail messages through the system and determine what actions occurred in their handling. Prior to deploying Splunk, this was a resource-intensive process. Existing processes also had to be expanded due to a new set of requirements raised by one of its customers – long-term data retention and compliance reporting – and Ceryx realized an automated management tool or solution would be needed.

Splunk Procurement

Ceryx made an initial investment of about $100k in the Splunk solution in May 2010. The original cost justification was built around two elements – better service to their customers, and improved efficiency in monitoring and troubleshooting its cloud-delivered services.

Outcomes

After the initial deployment of Splunk in 2010, the Ceryx team saw dramatic improvements in staff efficiency. "Message tracking was a difficult and complex process – message blocking might be caused by the Exchange servers or other mail servers, but could also be caused by unexpected end-user behavior. All of these systems need to be checked to see where a message was blocked, and in the past only the senior staff understood the complexities sufficiently to get this analysis done."

"With the Splunk software in place, we now send log files from all of the systems to Splunk and use it for rapidly focusing in and finding specific mail messages and tracking how they work through the various steps along the way. We saw two immediate benefits from an operational efficiency perspective. First, particularly complex message-tracking workflows that used to take over eight hours now could be completed in under one hour. In fact, our average workflows are eight times quicker with Splunk. Second, these tasks used to take up the time and effort of our senior operators, and could now be fully accomplished by junior staff members."

The Ceryx senior staff found other workflow improvements as well. "One of their responsibilities is to respond to accounts that have been compromised and then conduct analyses to decide if action is truly required. Through the use of Splunk, these workflows can now be handled in minutes, enhancing efficiency while improving security."

"And there were other benefits as well. Splunk was much easier to use, so training time for new hires dropped by a factor of eight. We were also able to cut the time our staff spent on producing weekly and monthly reports by a factor of four."

The Splunk solution also met new requirements for compliance monitoring and reporting. "It provides all of the historical records retention that we need to meet customer expectations and can scale to accommodate our anticipated growth. We've also been able to maintain compliance certifications – SSAE-16 Type II, as well as ISO/IEC 27001 – that are critical for our line of business and that are more challenging without the automated features we get from Splunk." As a result, Ceryx was able to avoid procuring, deploying, administering, and maintaining a separate, dedicated SIEM system for this purpose.

"We see many more opportunities to leverage the power that the Splunk software offers. In the last six months, we started moving towards using it to broadly monitor mail service activity, allowing us to easily recognize unusual activity like phishing and sudden volume spikes. We also see opportunities to start using the data we are getting through the Splunk software for capacity planning and application performance, down the road."

As of the end of 2011, the organization is realizing an estimated $329,500 of annual cost savings versus roughly $100,000 invested in Splunk solution costs made in 2010. Savings include a number of striking workflow efficiency improvements as well as reduced need to grow staff in response to continued business growth. Without even taking into account operational cost savings in the initial year the Splunk solution was deployed, the software development team calculates that with Splunk in place, they have more than doubled returns on their investment and expect significant compounded returns looking forward.

Based on their reported ROI, Ceryx has exceeded a 3x return on their Splunk investment ($147,000 in annual staff efficiency improvements and 1.5 FTE hires avoided at EMA estimate of $55-75,000/year, plus $85,000 SIEM system purchase avoided versus roughly $100,000 invested in the Splunk solution).

Hard and Soft ROI Summary

Hard ROI	After Splunk	Annual Savings
Analysis Efficiency – Message-tracking	8:1 time reduced for message-tracking workflows and allowing junior techs to do the work rather than senior techs	$90,000
Analysis Efficiency – Identifying Compromised Accounts	50:1 time reduced for senior techs to analyze and identify customer accounts requiring remediation	$45,000
Reporting Efficiency	4:1 hours reduced preparing weekly and monthly reports	$9,500
Reduced Training Time	8:1 reduction in training time required for newly hired operators	$2,500
Estimated FTE Staff Savings	$55,000-$75,000 annually (EMA estimated standard loaded rate for junior administrator) due to expanded capacity for existing staff	$65,000 (average of EMA industry estimates)
SIEM procurement and deployment avoidance	First year - $50,000 license fees plus $25000 deployment services in the first year; Annually – $10,000 maintenance / support services plus $27,500-$37,500 (EMA estimated) for ½ time junior administrator for system admin	$117,500 (first year, based on EMA average estimate personnel costs)
Total Hard ROI		**$329,500**
Soft ROI	**After Splunk**	**Benefits**
Compliance Auditing Automation	Splunk has allowed full automation of SSAE-16 Type II, and ISO/IEC 27001 audit reporting	The new level of compliance is an important edge for attracting and retaining customers.
Improved Operational Visibility	Significant changes in mail flow volumes now visible to staff within minutes, or even seconds	Puts operations team in position to proactively analyze anomalies and take preventative actions, improving control and protecting service quality
Customer Retention	Customers frustrated with active mail blocking (due to excessive volumes) mitigated through presentation of clear evidence of customer-based root causes	Customer relations improved and dialogue quickly shifted from service quality accusations to collaborative problem solving

Quotes and Observations

"We had one upset customer that thought we were blocking their e-mail. The Splunk solution helped us identify the root cause – the client was having problems on their end with runaway mail servers, tripping our firewall. With this in hand, we were able to work with them collaboratively to address the issue, and the customer was fully satisfied in the end."

"The Splunk system has been instrumental in helping us control operating costs while still keeping up with growth."

"With the Splunk system, compliance reporting not only became a practical opportunity, it has become almost trivial through automation."

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. 2557.100212