

Splunk Helps Ping Identity Contain Costs, Improve Cloud Security and Deliver Business Insights: An EMA ROI Study

Introduction

Enabled by virtualization and the flexibility of the Web, Cloud computing technologies have revolutionized today's approaches to IT. From Software-as-a-Service (SaaS) to providers that enable businesses to outsource an entire IT infrastructure, Cloud services have brought enterprise-class computing within the reach of organizations of all sizes.

But with the scale of Cloud, complexity soon follows. Without tools that enable providers to tame highly dynamic growth and change, Cloud computing services will fall short of delivering the reliability and efficiency that customers demand. The pressures on Cloud providers go beyond those of the enterprise seeking to get ahead of IT "firefighting." Cloud providers must deliver an attractive alternative to on-premises IT or a similar level of service – *or better* – where on-premises approaches are impractical. If they fail, their business fails as well.

In this study, Enterprise Management Associates (EMA) examines the Return On Investment (ROI) in Splunk realized by Ping Identity, 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 Ping Identity to reduce the cost and complexity of Cloud scale and deliver a superior service that helps Ping maintain its competitive edge in the highly dynamic market of Cloud security and access management services.

The pressures on Cloud providers go beyond those of the enterprise seeking to get ahead of IT "firefighting." Cloud providers must deliver an attractive alternative to on-premises IT or a similar level of service – *or better* – where on-premises approaches are impractical. If they fail, their business fails as well.

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 Company

Based in Denver, Colorado, Ping Identity is a technology company that provides Cloud identity security solutions to more than 800 of the world's largest organizations in both the private and public sectors. These organizations depend on integrated applications for serving large-scale demands, and are among the most vocal advocates of the advantages of Cloud computing.

Ping Identity has long emphasized ease of adoption and deployment for technologies that protect access to sensitive information resources using secure, open standards such as SAML (the Security Assertions Markup Language), OpenID and OAuth. Because these technologies play a central role in extending enterprise identity and access management to Cloud applications, the company has expanded its offerings and has placed high emphasis on solutions delivered "as a Service" via a Cloud-based model.

Ping Identity serves 42 of the Fortune 100 to secure hundreds of millions of employees, customers, consumers and partners, and claims a 99% customer satisfaction rating. Businesses that depend on the Cloud rely on Ping Identity to deliver simple, proven and secure Cloud identity management through single sign-on, federated identity management, mobile identity security, API security, social media integration and centralized access control.

Ping Identity serves 42 of the Fortune 100 to secure hundreds of millions of employees, customers, consumers and partners, and claims a 99% customer satisfaction rating. Businesses that depend on the Cloud rely on Ping Identity to deliver simple, proven and secure Cloud identity management.

Interviewee

Lead Site Reliability Engineer

Problem Scenario

Few technology trends have captured the interest of both business and IT professionals as Cloud computing. Regardless whether offered as Software-as-a-Service (SaaS) or as hosted infrastructure or application platforms, organizations see substantial promise in IT as a service, while the potential for offloading many of the demands of technology management has significant appeal for IT – if Cloud technologies can be adopted securely, with minimal risk to the business.

Ping Identity has targeted the growth potential of the Cloud as an ideal "sweet spot" that aligns with the company's strategic objectives. Organizations often make a substantial investment in identity and access management. Technologies such as single-sign-on simplify the user experience of access to a wide range of information assets, regardless whether facilitating a single login for accessing multiple resources, or assuring seamless integration of the many moving parts of complex applications. In order to capture the benefits of Cloud computing, businesses must extend these security technologies to third-party service providers without exposing the business to additional risk – and Ping Identity is in a strong position to capitalize on this need.

Ping Identity is a well-established veteran of the realm of federated identity management, and with the acceleration of SaaS and Cloud computing, the company has seen substantial growth. With the release of the company's PingOne offering for on-demand Cloud single-sign-on and "just in time" user provisioning for SaaS applications, Ping Identity has increased its employee headcount by 300% and continues to expand. Today, the company delivers its solutions from three data centers supporting over 400 virtualized servers...and counting.

The management of this growth has raised the bar significantly for Ping Identity's internal IT operations. Cumbersome processes that limit visibility throughout the environment are not an option for Cloud providers who must meet high standards for IT service delivery. Threats to the IT team's ability to anticipate service issues pose significant risks to Service Level Agreements (SLAs) and customer satisfaction. These SLAs often require resolution of service availability or performance problems within specific time windows – sometimes as narrow as 30 minutes. Such obligations are no small matter for a service offering that depends on performance and availability in order to attract and retain customers and maintain the solid growth that Ping Identity has experienced.

Acquisition Story

Before its deployment of Splunk, Ping Identity was largely dependent on system-level monitoring of individual virtual machines, facilitated by nightly log harvesting and cumbersome manual processes. Ping needed a solution that would automate and eliminate the excess costs and give it the flexibility to keep pace with the demands of a growing Cloud services business.

With the release of Splunk 4.0, Ping realized the power that the Splunk platform offers for a service provider. The ability to correlate monitoring data from each component of Ping's Cloud platform with specific customers and services – something the company's existing solutions could not provide to the same level of granularity or depth throughout the IT environment – was "just huge for us," according to the company's lead site reliability engineer. Responsive and easy-to-use search capability that scales across three data centers and more than 400 virtual instances of Ping services has become fundamental to enabling Ping to expand its services and meet its obligations to its Cloud customers. The flexibility provided for constructing applications, dashboards and reports tailored to the Ping environment helps the company's Cloud IT operations to avoid reactive "firefighting" – an extreme risk for a service provider obligated to stay ahead of problems in order to remain competitive – enabling Ping to anticipate service problems before they appear.

Outcomes

For the Ping Identity team, hard cost savings were realized early on following the deployment of Splunk. Of equal or greater importance to the company, however, is the deep and highly adaptable visibility Splunk provides into the complex, large-scale IT environment on which Ping is building its long-term business strategy.

Reducing Costs of IT Support

Among the most immediate benefits Splunk delivered for Ping was a reduction in the time and effort – and associated costs – required to resolve availability and performance problems. Prior to the deployment of Splunk, Ping's IT team had to export log files from individual hosts and determine complex root cause issues based on visibility limited to system-level insight into Virtual Machines (VMs). Ping's IT staff estimate that troubleshooting service issues before Splunk required approximately four hours on average for a typical case.

With Splunk in place, Ping's IT organization estimates that this troubleshooting time has been reduced by approximately 70%.

With Splunk in place, Ping's IT organization estimates that this troubleshooting time has been reduced by approximately 70%. Estimating an average of three such issues per week and fully-loaded personnel costs of approximately \$70 per hour (averaged between front-line support staff and Site Reliability Engineers), this represents a cost reduction of approximately \$30,576 per year.

Optimizing the Investment in Cloud Scale

Reduction in the cost of troubleshooting was only the beginning for Ping. The scale of a Cloud operation inevitably leads to complexity. Cloud providers must do more than simply stay ahead of that complexity. They must deliver a quality of service that exceeds that which customers can provide for themselves – and must compete against others seeking to deliver the same or better service. Reliance on flexible, adaptable automation is only part of the solution. Costs on keeping Cloud-scale complexity in line must be kept at a minimum, in order to pass along to customers the efficiencies they expect from the Cloud alternative.

Without Splunk, Ping personnel estimate that they would currently need three to four additional Site Reliability Engineers familiar with its environment in order to manage the company's Cloud servers, harvest and export log data, and coordinate troubleshooting with front-line customer support. Ping personnel estimate the fully-loaded cost of site reliability engineers at the level of expertise required is between \$80 and \$100 per hour. Using an average of \$90 per hour and 2,000 full-time hours per year equates to a personnel savings of \$630,000 annually for the additional three to four engineers the company would require to keep up with the rapidly growing scale of its Cloud operations without Splunk. This enables Ping to allow its personnel to focus on expanding the company's already strong growth, rather than "throwing bodies" at reactive coping with problems that could be better solved with a flexible management tool such as Splunk.

A personnel savings of \$630,000 annually for the additional three to four engineers the company would require to keep up with the rapidly growing scale of its Cloud operations without Splunk.

Consolidating and Eliminating Management Tools

Splunk has also enabled Ping to consolidate monitoring tasks and eliminate some tools that were either inadequate to support Ping's strategic goals – or which, in some cases, actually caused problems of their own. One such tool would write incoming log data to a traditional relational database not designed to handle Cloud scale. This tool was easily overwhelmed by as little as a single network device generating large amounts of log data in the case of a specific failure.

Ping has been able to repurpose or retire such systems in favor of the scalability, flexibility and responsiveness of Splunk and its ability to centralize monitoring for a large, distributed Cloud service environment. In particular, the ability to transfer licenses of existing tools to the company's corporate IT department resulted in a cost savings for the On Demand group maintaining the company's Software-as-a-Service offering of approximately \$10,000.

Security Advantages

Identity management technologies such as those of Ping Identity serve primarily to secure information assets against unauthorized access. One of the primary values of Ping's technology is that it does not store user passwords, relying instead on standards-based techniques for authentication in distributed environments such as SAML (the Security Assertions Markup Language), which enables the secure integration of single-sign-on across applications and environments without exposing sensitive password data.

Splunk supports Ping's security values by enabling log data to be collected and transmitted securely, encrypting monitoring data in transmission from the point of collection to centralized management. Splunk Indexing is used to assure access to the data to authorized groups, without exposing additional information unnecessarily. Splunk indexes are encrypted to further protect monitoring data against unauthorized access. Together, these capabilities help to assure the security objectives Ping Identity seeks to implement throughout its architecture, and enhance the fundamental value of Ping Identity services for its customers.

More Proactive Response to Customer Needs

Identity and access management and single sign-on integrated between customers and Cloud service providers requires coordination of services between the customer, the customer's Cloud services and the Ping environment. Splunk's responsive centralized visibility and correlation of detailed monitoring data to individual customers enables Ping to deliver a high quality of service across this interwoven landscape.

Splunk enables Ping to keep a close eye on issues such as events resulting from changes in a customer's Active Directory environment that can affect the customer's access to SaaS applications enabled by Ping's Cloud services. This helps customers maintain uninterrupted access to services beyond those Ping supports directly, enhancing the value customers realize from Ping Identity.

Ping Identity IT operations personnel rate Splunk as "one of the best products we've ever invested in."

With Splunk, Ping has the ability to coordinate customer account information with service delivery, preserve uninterrupted operations and assure more seamless customer retention.

Enabling Ping's Future with Business Insight

In addition to the highly granular visibility Splunk provides to technical and support personnel, Splunk enables Ping Identity's executive team to keep a closer eye on the business, monitor trends and maintain more detailed awareness of activity over any time period.

The ability to monitor and trend system usage and the uptake of specific services helps Ping executives to determine where their product investments are yielding the best results, where further investment should be made and where less productive efforts may be contained. Reports are generated daily, weekly and monthly, while ad hoc queries for specific data can be conducted simply and easily with Splunk. Usage patterns and geographic data help Ping to better drive sales, tailor offerings to customer needs, balance service loads and respond to the demands a Cloud provider must meet in serving organizations both large and small.

Ping Identity's plans to expand the value of Splunk include the ability to develop custom reports for end-user customers to provide more direct visibility into their services. Ping also foresees the expansion of Splunk into the monitoring of more detailed system data, such as CPU, memory and disk utilization, system uptime, and other parameters. Already, Ping is using Splunk to monitor "Big Data" platforms such as Cassandra that other tools may not yet be able to manage as well. This adaptability will help Ping continue to optimize its IT environment, contain costs, further reduce dependence on an assortment of IT management tools and enable the company to deliver more value for its customers.

Hard and Soft ROI Summary

Hard ROI	Example Case	Before Splunk	After Splunk	Benefits
Support cost reduction.	SLAs must be met, not only to assure customer satisfaction but to maintain competitive advantage. Example: 30-minute problem resolution deadlines.	Approximately 4 hours required on average to collect log data, transfer to analysts, manually correlate and implement solution.	Estimated reduction of mean time to resolve (MTTR) of 70%.	Based on estimates of 3 such incidents per week and average fully loaded personnel costs of \$70 per hour, Splunk yields approximate annual savings of \$30,576 .
Optimizing the investment in Cloud scale.	Without tools flexible enough to manage the elasticity and dynamic growth of Cloud environments, personnel and other IT operations costs can skyrocket.	Limited capabilities of existing tools curtailed company's ability to manage highly dynamic growth, shifting the burden to human effort.	Without Splunk, company estimates it would require at least 3-4 additional highly skilled engineers to manage existing growth.	Estimated cost savings of \$630,000 per year (based on 3.5 full-time engineers at a fully loaded personnel cost estimate of \$90 per hour). Personnel can focus instead on more strategic priorities to further Ping's already rapid growth.
Consolidation and elimination of management tools.	Organizations typically collect a number of disparate tools to monitor different aspects of the environment.	Existing tools lacked flexibility to provide monitoring beyond system-level VM logs. Tools based on legacy approaches to data management easily overwhelmed with data.	Enables Ping to eliminate unnecessary or redundant tools and repurpose others.	\$10,000 in licensing costs recovered by the company's On Demand group through transfer of monitoring software licenses to internal IT operations, resulting in better utilization of monitoring tools for the company as a whole.
Total Annual ROI:				\$660,576
Soft ROI	Example Case	Before Splunk	After Splunk	Benefits
Security advantages.	Ping Identity regards <i>any</i> evidence of customer activity as potentially sensitive information.	Limited ability to protect monitoring data from unauthorized access.	Log data encrypted in transit to Splunk indexers. Encryption of Splunk indexes and splitting of indexes to enable more finely grained access to specific monitoring data.	Enhances the security of the Ping Identity Cloud environment values in support of company's primary mission of securing access to Cloud resources and supporting customers' regulatory compliance requirements. Adds to Ping's competitive advantage in the marketplace.
Optimizing response to customer needs.	Identity and access management integrated between Cloud services and customer sites requires coordination of multiple moving parts.	Limit ability to anticipate service issues inhibited Ping's ability to proactively resolve customer issues.	With more flexible and responsive monitoring, Ping is often able to inform customers of potential issues before the customer is aware of a problem.	Supports customer loyalty and retention. Integration with customer account data helps prevent service outages due to service renewal gaps, which further supports customer retention.
Strategic insight for Ping Identity business executives.	Guidance for strategic direction of Ping Identity's Cloud services based usage, performance and customer preference information gathered from IT operations data.	Limited monitoring unable to deliver the needed depth and dimensions of information.	Readily adapted reporting capability that informs executives of actual customer usage patterns that help tune management efforts.	Improving product and services capability mix to drive higher revenues and better customer engagement.

Quotes and Observations

Ping Identity IT operations personnel rate Splunk as "one of the best products we've ever invested in."

"Managing the scale we're at right now would be next to impossible," says the company's lead site reliability engineer, noting that he is able to "sleep better at night knowing Splunk can handle the amount of data it does."

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](#). 2417.032712