Splunk's Big Data Analytics Free ThreatMetrix Security Experts from the Need to be Data Scientists: An EMA ROI Story

Introduction

In its analysis of enterprise IT management technologies and practices, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts conduct Return On Investment (ROI) studies on enterprise management products which demonstrate above-average customer value. Splunk is distinctive in that a number of 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.

This EMA case study profiles the benefits realized from Splunk by ThreatMetrix™, a company that offers a fast-growing integrated cybercrime prevention solution through an advanced threat defense platform delivered from the cloud. By providing high flexibility in analyzing large volumes of data from a wide diversity of sources, Splunk enables ThreatMetrix to focus on its primary business: data-driven insight into today's advanced and complex threats through a platform of integrated technologies and intelligence gathered and shared across the ThreatMetrix network. This enables ThreatMetrix to focus on maintaining its edge and expanding its growing business in a fast-moving – and highly competitive – market.

HIGHLIGHTS

splunk>

Vendor name: Splunk Inc.

Product area: IT Operational and Security Intelligence

Product name: Splunk® Enterprise™

Product version: 4.3

ThreatMetrix™

Customer name: ThreatMetrix™

Customer domain: Provider of Integrated Cybercrime Prevention Solutions

Product Description

With over 5,200 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 big data ready. Splunk can collect machine-generated data from a wide variety of sources and at massive scale. Its indexing and search capabilities free organizations from much of the overhead of competing approaches that require costly and time-consuming normalization and rationalization of data, or complex development resources, 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 extended across multiple data centers and Splunk servers, with role-based access controls that facilitate tailoring of reports and analysis to individual users and restrict access to sensitive information when required. Extensibility is further supported by Splunk forwarders, essentially lightweight software agents that broaden the range of data the Splunk platform can collect and securely transmit to Splunk servers.

Splunk's flexibility and ease of deployment has resulted in an annual growth rate that is in the high double-digits, according to the company. Splunk is currently in use by more than 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."

Splunk's most recent release, Splunk 5, adds enterprise class high availability and strengthens support for Hadoop (Splunk Hadoop Connect and Splunk App for HadoopOps). Splunk recently added the DB Connect App, allowing its customers to enrich machine data with business context from data located in relational databases.

Subject Organization

ThreatMetrix offers an innovative, cloud-based service that protects businesses from today's more sophisticated security and fraud threats. Its technology combines advanced device identification and malware detection in a single platform backed by a global network of shared intelligence. The ThreatMetrix Cybercrime Defender Platform helps businesses protect the integrity of online transactions, accounts and identities with layered and integrated defenses. Advanced device identification technology (TrustDefender™ ID) helps clients determine whether online visitors are legitimate customers or potential cybercriminals. Malware detection spots man-in-the-browser threats before they can corrupt transactions (TrustDefender™ Cloud), while malware defenses on the client secure the vulnerable endpoint (TrustDefender™ Client). Embeddable mobile threat intelligence (TrustDefender™ Mobile) defends mobile applications from fraud and criminal misuse.

As part of the ThreatMetrix Cybercrime Defender Platform, these technologies share information among each other and with the broader network of ThreatMetrix customers. ThreatMetrix serves a rapidly growing global customer base across a variety of industries, including financial services and online banking, e-commerce, payments, social networks, government and healthcare. These companies use ThreatMetrix to protect themselves from data breaches and online fraud, and to protect their customers from identity theft and fraud.

Integration of ThreatMetrix technologies with customer resources is typically straightforward. Web applications may require only a few lines of HTML code, or an API call when transactions flow through customer systems. A rules-based engine is tunable to an organization's specific business requirements. Clients can determine in real time whether Web visitors are using compromised devices, subject to malware attacks, hiding behind proxies, or disguising their true identity. This information can be used to protect online transactions and logins from theft, fraud, malware and data breaches.

Interviewees

VP of Marketing, and the Director of Field Services.

Problem Scenario

Analysis of activity from collected log, security and IT operational data is central to ThreatMetrix operations – but where the company sees its most significant differentiation is twofold. First, the centralized nature of a cloud-based approach to threat, fraud and cybercrime detection requires superior credibility in building a high-performance, high-availability environment capable of serving thousands of customers and hundreds of thousands of customer applications and endpoints. Second, the expertise required to recognize anomalies from large volumes of monitoring data is essential to differentiation in a highly competitive market. This expertise is highly valuable and often difficult to source. Making this expertise available to large numbers of businesses is a key value of a cloud-based offering for security and fraud prevention.

Analysis of activity from collected log, security and IT operational data is central to ThreatMetrix operations. When technologies are available that relieve ThreatMetrix from having to build its own solutions to tactical problems, they free the company to focus on its strategic priorities.

These fundamentals of ThreatMetrix's business demand that the company focus primarily on these capabilities. When technologies are available that relieve ThreatMetrix from having to build its own solutions to tactical problems, they free the company to focus on its strategic priorities. Eliminating the time required to develop such tools in-house also enables ThreatMetrix to be proactive in addressing new or emerging concerns and accelerate the introduction of new offerings – a critical priority in a fast-moving business where emerging competitors constantly seek to outpace each other in bringing new and superior capabilities to market.

Acquisition Story

Prior to the acquisition of the Splunk platform, ThreatMetrix would combine analysis of data in a SQL database environment with desktop analytics and reporting to discern activity and identify patterns in customer data. This information would then be translated into rules and procedures in the ThreatMetrix offering to detect fraud and abuse. As ThreatMetrix's business grew, this approach quickly became untenable. Traditional data management approaches were seen as too limited to handle the flexibility needed by an organization such as ThreatMetrix to recognize emerging threats in new and creative ways. Among the market of solutions to these problems, ThreatMetrix personnel – some of whom had prior familiarity with Splunk – report that Splunk stood out.

Today, Splunk has helped ThreatMetrix to expand its customer reach and provide coverage to more than 8,500 websites. ThreatMetrix uses Splunk software to ingest a wide variety of log data from unique customer environments and Web applications that are typically customized for a particular business or purpose. The flexibility of Splunk software allows ThreatMetrix to understand monitoring data specific to each application in order to define norms and identify anomalies that stand out. This enables ThreatMetrix to sharpen the effectiveness of its offerings while simultaneously enabling the company to grow its business with high agility.

Outcomes

From freeing ThreatMetrix to focus on its primary business, to equipping the company with a flexible data platform for capturing new business opportunities and responding proactively to existing customer needs, Splunk helps ThreatMetrix compete in a new and dynamic market of advanced, cloud-based defense.

Savings on Development

Among the most significant returns ThreatMetrix has realized from its investment in Splunk is the relief from having to build its own data collection systems where Splunk fulfills its needs. While Splunk software provides more than data collection with indexing, storage, visualization and data analysis, a significant saving in the data collection component readily lends itself to calculation in the ThreatMetrix case. Had ThreatMetrix sought to build its own data collection platform rather than turn to Splunk for this purpose, company personnel estimate the effort would have required at least six months of development time in construction.

Based on prior ROI research of similar cases in other organizations, EMA conservatively estimates personnel costs for such a project at approximately $70 to $90 per hour per fully loaded headcount. Assuming that this effort would require a minimum of two to three such developers, EMA estimates an initial savings of approximately $200,000 in personnel costs alone ($80 per hour per headcount X 2.5 headcount X 1,000 hours per full-time headcount in a six-month period).

This estimate, however, does not include the cost of ongoing tuning and maintenance of any such internally developed effort. A key advantage of working with a proven platform such as Splunk is that it has been deployed in a wide variety of production environments, and has matured and improved over time. Any internally developed big data effort would have to undergo similar rigor in order to meet production requirements, which represents ongoing costs for internal maintenance and support. With Splunk, these burdens can be shifted to commercial support of the Splunk product.

Freeing ThreatMetrix to Grow

Primary business demands require ThreatMetrix to maintain strong growth in a highly competitive, fast-moving, innovative market. ThreatMetrix personnel indicate that it would have been difficult, if not impossible, to spare highly valuable development expertise for building an extremely scalable data intake and analysis platform for the needs that Splunk fulfills. With Splunk, personnel are able to focus on solving customer problems rather than developing internal tools, building profits rather than operational costs.

The benefits of this choice are reflected in the company's growth. Prior to its deployment of Splunk, ThreatMetrix counted the number of customer resources protected in the hundreds. Today, that number is well into the thousands. This growth has also enabled ThreatMetrix to expand its personnel dedicated to data intake and analysis. But while this team, and the personnel costs it represents, has grown by a factor of four, the business (and the profitability it represents) has grown by a factor of approximately 10 (from hundreds of protected resources into the thousands).

Significant Cost Reductions in Data Analysis

With Splunk deployed, ThreatMetrix can focus on its core business priorities and discern evidence of fraud, attack or other malicious behavior gleaned from monitoring data collected from protected customer resources worldwide. Splunk enables ThreatMetrix to automate a substantial portion of this activity.

There are, however, two key areas where the analysis of ThreatMetrix experts is required. One is when new customers or new resources are added to the protection afforded by ThreatMetrix. Because of the many unique ways that customers and their applications differ from one another, a certain amount of fine-tuning may be required to optimize coverage. The second area has to do with the nature of fraud and threat defense. This is a game in a state of constant change as attackers continually seek to circumvent defenses, requiring defenders to adapt tactics accordingly.

Splunk's ability to handle large data volumes and variety and automate key analytics has contributed significantly to improving ThreatMetrix costs in these areas. ThreatMetrix personnel indicate that a typical data analysis case prior to Splunk would require four hours or longer for each team member involved. With Splunk in place, that time has been reduced to approximately 15 to 30 minutes. Using the previously cited EMA estimate of $80 per hour for each fully loaded headcount based on similar cases in other organizations, and approximately two such analyses per day, EMA estimates a savings of approximately $140,000 per headcount per year (3.5 hours reduction in analysis @ $80 per hour per fully loaded headcount X 2 such analyses per day X 250 days per year for each full-time employee). ThreatMetrix personnel estimate that eight analysts on average are currently engaged in such tasks today, representing an EMA-estimated savings of approximately $1,120,000 per year.

Enabling Success

What are the key values Splunk brings to ThreatMetrix that yield these advantages?

The ability to take in large amounts of customer data is a key factor. Each ThreatMetrix customer may have multiple Web applications; some have thousands. These applications handle hundreds of thousands of transactions each day, producing tens of millions of individual events and other data that must be processed and analyzed to identify norms, recognize anomalies and discern incidents that represent threats. Splunk's scalability not only exceeds the capability of ThreatMetrix's prior tools, but also allows ThreatMetrix to grow with increased business demand.

Splunk provides more than capacity and performance in data management, however. Splunk's ability to ingest data in its existing format and adapt analysis to the data rather than forcing data to fit the platform enables ThreatMetrix to find anomalies in details that other techniques might omit. Since Splunk ingests data in its native format and doesn't filter it, new findings can be realized when improvements are made to the ThreatMetrix platform that yield new data from protected customer resources, without the need to make changes to Splunk.

When adaptation to changing threat tactics is needed to identify a new or previously unseen threat, Splunk's flexibility in adapting analysis to the actual data makes discovery of new findings more straightforward. ThreatMetrix personnel indicate that Splunk software requires little training and analysts are able to come up to speed on its use quickly. They describe the Splunk platform as being intuitive to grasp and highly flexible in the way its capabilities can be applied. Regardless of the nature or format of customer data, Splunk's analytic capabilities enable it to see changes in data structure,

volume or frequency that indicate a threat. These findings can then be turned into new rules or other capabilities in the ThreatMetrix platform, as well as new ways to produce meaningful analytics for ThreatMetrix customers.

Examples of the intelligence gleaned from these capabilities include detections of account takeovers, the presence of botnets or automated attacks, and more advanced threats discovered through correlation of data from a variety of sources. These sources may include retail and e-commerce transactions that show evidence of illicit activity, customer records that indicate attempts to create fictitious accounts, evidence of malicious attempts to tarnish a customer's brand in social media, or geolocation data that pinpoints fraud sources. When customers report issues not previously encountered, Splunk provides ThreatMetrix with superior ad hoc analysis, often resulting in new capabilities that can be extended to all ThreatMetrix customers. ThreatMetrix personnel identify this strength in ad hoc analysis as one of the most important differentiators Splunk brings to their business.

This strength also plays a role in helping ThreatMetrix win new business. In competitive situations, Splunk's flexibility enables ThreatMetrix to prepare initial analysis of data from potential customers, develop visualizations, reports and presentations, and help turn prospects into new business. For existing customers, Splunk allows ThreatMetrix to be proactive in identifying new issues or concerns – which turn into additional opportunities for ThreatMetrix to prove its value and expand its role among current clients.

Hard and Soft ROI Summary

Hard ROI	Example Case	Before Splunk	After Splunk	Benefits
Solution acquisition and deployment	Savings on development of a highly scalable data collection and storage solution in-house.	Limited ability to scale; growth effectively hamstrung by existing techniques. Cost of internal development prohibitive when the priority is building an expanding business.	Proven data intake and analysis platform with high flexibility, able to integrate monitoring data across multiple customers and thousands of customer resources.	EMA estimates elimination of approximately **$200,000** in development costs that would have been required to build an internally developed solution, plus ongoing benefits from elimination of continuing maintenance and support of internal development.
Freeing ThreatMetrix to focus on business growth	Internal resources that would otherwise have focused on building internal tools can focus instead on meeting customer requirements.	Limited staff supporting hundreds of customer resources.	4x increase in analyst staff to date, supporting customer resources in the thousands (and growing).	EMA estimates approximately 10x increase in business volume, with only a 4x increase in analyst staff.
Significant cost reductions in data analysis	Analysis required to protect unique customer resources and detect ongoing change in the threat landscape.	Approximately 4 hours twice a day for each member of an expert analyst team.	Reduction of time each expert spends on analysis to approximately 15 to 30 minutes, coupled with 4x growth in the analyst team.	EMA estimates annual savings of approximately **$1,120,000** due to Splunk automation and performance in data management and analysis.
Total estimated annual ROI to date				**At least $1,120,000, but expected to expand with continued ThreatMetrix growth and new applications of Splunk analytics.**
Soft ROI	**Example Case**	**Before Splunk**	**After Splunk**	**Benefits**
Solution flexibility	Ad hoc analysis on demand.	Limited capability bound by performance or capacity limitations, inadequate flexibility in analysis.	Ability to adapt analysis as needed in response to specific customer scenarios.	Competitive advantage in new business. Enhanced customer loyalty and retention through proactive capability in identifying new customer issues or previously unseen threats.
Ease of use	Analyst orientation and training on Splunk platform use.	Limited capability, often requiring detailed knowledge of techniques such as SQL analysis.	Intuitive techniques that can be learned quickly and used with high flexibility by analysts.	Analysts become productive much more quickly, and can be more proactive in responding to customer needs.

Quotes and Observations

"We know how to build a solution delivered from the cloud – but saving us six months of development time in a fast-growth market is a make-or-break value for us."

"Splunk gives us the ability to perform ad hoc queries in a way that's more amenable to unstructured or semi-structured data. This also means that our people who don't have SQL backgrounds can use it. Our security and fraud subject matter experts don't have to be data scientists."

"When a customer reports a potential fraud or security issue with their application, Splunk's ad hoc flexibility allows us to break apart monitoring data for a specific incident and deconstruct exactly what happened. This also enables us to evolve the rules in the ThreatMetrix portfolio for all our customers."

"Splunk gives us the ability to perform ad hoc queries in a way that's more amenable to unstructured or semi-structured data. This also means that our people who don't have SQL backgrounds can use it. Our security and fraud subject matter experts don't have to be data scientists."

"Splunk also helps us detect possible issues with integrating customer applications and narrow down what they are. This helps us be even more proactive with customers and inform them of potential problems before they notice themselves."

About ThreatMetrix

ThreatMetrix is a fast-growing provider of integrated cybercrime prevention solutions. The ThreatMetrix™ Cybercrime Defender Platform helps companies protect customer data and secure transactions against payment fraud, malware, account takeover, fraudulent new registrations, data breaches, as well as man-in-the browser (MitB) and Trojan attacks. The platform consists of advanced cybersecurity technologies, including TrustDefender™ ID, which is cloud-based, real-time device identification, malware protection with TrustDefender™ Cloud and TrustDefender™ Client, as well as TrustDefender™ Mobile for smartphone applications. ThreatMetrix cybersecurity solutions protect more than 1,500 customers and 8,500 websites across a variety of industries, including financial services, enterprise, e-commerce, payments, social networks, government, and insurance. For more information, visit www.threatmetrix.com or call 1-408-200-5755.

To join in the cybersecurity conversation, follow us on Twitter @ThreatMetrix.