



Perspectives by:

Mark Smith

CEO & EVP of Research



Splunk: Big Data Machine for Operational Intelligence

By Mark Smith | 04/27/2012 | Article Type: VentanaResearch Blog | © 2012 Ventana Research

[Splunk](#) recently entered the financial markets as a publicly traded company (NASDAQ: SPLK) and also entered a new phase in its corporate growth. Splunk combines the power of search and discovery with analytics on data generated by IT systems, that they call machine data, and provide insight for a new generation of operational intelligence that helps everyone in IT including the CIO determine the efficiency of its systems that support business. The company has built a platform that can index data on a large scale ("big data") for rapid analysis and search. They also through its analytics provide the ability to perform visual and data discovery which is critical to reduce the time to determining unknown issues in existing IT systems. This helps IT staff ascertain not just the performance but the efficiency of systems that operate on a 24-by-7 basis. Splunk's software operates in real time, surpassing the traditional methods of applying business intelligence against a data warehouse – a practice that's ineffective for use in IT, where time is not the CIO's friend when it comes to understanding issues or opportunities for improvement. Splunk has grown rapidly, partly because it's simple to download and try, and then to license for use in production. It has more than 3,300 licensed customers in 75 countries. The management team is led by CEO Godfrey Sullivan, who has experience and a track record at companies such as Hyperion.

Where is Splunk finding its opportunity? IT organizations have been like the cobbler's children who have no shoes. While they deliver applications and technology to business, IT departments seldom have time to analyze and optimize their own processes, systems, applications and projects. While this might sound counterintuitive, it is true. Almost seven years ago, I started investigating whether performance management being applied elsewhere in a business was occurring in IT. I discovered that CIOs lack critical tools to define goals and track the performance of their people and machines. Our [IT Performance Management benchmark research](#) identified lack of resources, budget and awareness as major contributing factors to this situation. It also showed that organizations that deploying appropriate tools were increasing IT effectiveness and supporting the needs of business more efficiently. Machine data or files were the top data source within 43 percent of IT organizations, and balancing loads between networks and servers, doing root cause analysis and doing impact analysis were key tasks in at least 52 percent of them. Splunk, which addresses this niche, has had significant growth over the last three years even though economic conditions have been shaky.

[Our analysis of Splunk's latest release of software, version 4.3](#), found a series of advancements, including supporting access from tablets such as Apple's iPad, support for data in cloud-based applications and the ability to operate in VMware environments, making it easier to deploy Splunk in the cloud. This version expands the enterprise scale of the platform, supporting more concurrent users and faster search. Users can preview machine data then start indexing against it for further discovery and analytics. These are all critical tasks as Splunk becomes a platform for harvesting machine data for search and discovery across the IT organization. Splunk must continue to expand its footprint with more collaborative capabilities to help IT understand issues and opportunities where analytics on

the machine data are the starting point for dialogue and action. Introducing more collaborative capabilities and the ability to correlate data toward actions and notifications will help Splunk further differentiate its technology.

Since our analysis, Splunk has continued to support [new machine data environments, including Hadoop](#). It can run MapReduce queries against data in Hadoop and then bring the data into Splunk for analysis. Our benchmark research into [Hadoop and Information Management](#) found that users of Hadoop are most often focused on integrating machine data from application and Web logs with the events and network monitoring data that Splunk is designed to address. Hadoop users need to analyze data much faster than others, with 77 percent of organizations indicating they need analysis within a day and 25 percent within an hour. One challenge for organizations using Hadoop is staffing and training; Splunk addresses those obstacles with a tool that is easier to use than creating custom programs, and it provides real-time and integration features, each sought by two-thirds of organizations. The growth of Hadoop comes from the need to address big data needs but also the simple access to download the software and then use it which is also what Splunk does with its download to use its software.

Splunk has a promising opportunity in the market, considering the size of IT spending on technology every year and the legacy of applications and systems that must be optimized for business use. Also, as IT organizations continue to advance their IT security and compliance and increase their use of cloud computing, the need not just to monitor but to analyze and act on issues and opportunities grows larger. Our [last benchmark research on Operational Intelligence in IT](#) found that IT has prioritized to manage IT performance through metrics in 71 percent of organizations, and more than half (58%) plan to improve their IT organization's responsiveness. The research found more than half of organizations have at least 11 information sources to routinely interact with, which is part of why Splunk fits these needs on machine data. Splunk has little competition, with IT management software vendors like Computer Associates, Hewlett-Packard, IBM and Oracle providing little innovation or capabilities to address operational intelligence needs through discovery and analysis of machine data in IT. Eventually they or others will realize their shortcomings, but at that point I would expect to see Splunk be significantly larger with an expanded portfolio of capabilities for meeting a CIO's need to truly become an information officer of his own IT organization.

Regards,

Mark Smith – CEO & Chief Research Officer

About Ventana Research

Ventana Research is the most authoritative and respected benchmark business technology research and advisory services firm. We provide insight and expert guidance on mainstream and disruptive technologies through a unique set of research-based offerings including benchmark research and technology evaluation assessments, education workshops and our research and advisory services, Ventana OnDemand. Our unparalleled understanding of the role of technology in optimizing business processes and performance and our best practices guidance are rooted in our rigorous research-based benchmarking of people, processes, information and technology across business and IT functions in every industry. This benchmark research plus our market coverage and in-depth knowledge of hundreds of technology providers means we can deliver education and expertise to our clients to increase the value they derive from technology investments while reducing time, cost and risk.

Ventana Research provides the most comprehensive analyst and research coverage in the industry; business and IT professionals worldwide are members of our community and benefit from Ventana Research's insights, as do highly regarded media and association partners around the globe. Our views and analyses are distributed daily through blogs and social media channels including [Twitter](#), [Facebook](#), [LinkedIn](#) and [Google+](#).

To learn how Ventana Research advances the maturity of organizations' use of information and technology through benchmark research, education and advisory services, visit www.ventanaresearch.com.

Ventana Research Corporate Headquarters

6150 Stoneridge Mall Road, Suite 350
Pleasanton, CA 94588

info@ventanaresearch.com
(925) 474-0060