IT Silos Are Hurting Your Company: Make Machine Data a Strategic Asset

WHITE PAPER

splunk>

Abstract:

At a time when it's tougher than ever to compete, the ability to use IT to achieve results is more business critical than ever. The pressures are relentless: new technology layers, strict governance practices, regulatory mandates, and evolving security threats have all combined to increase the cost and complexity of running IT. In 2010 alone, organizations spent well over $1 trillion globally managing all of this.[1]

The key to effectively managing, securing and gaining better intelligence from IT is locked in the data IT systems generate. This **machine data** holds the answers to what customers, users, applications, networks and devices have been doing. Until now, companies have had to manually traverse silos of data to get all this information—a cumbersome and expensive activity, far removed from the business decision-making process. To ensure the right information is available to the right people at the right time a dramatic shift is needed. A data-agnostic approach is required to integrate all this machine data and provide visibility regardless of format or location.

Splunk Enterprise is changing how organizations manage, secure and gain operational intelligence from IT. By enabling organizations to search and analyze their machine data from a single location in real time, they can now troubleshoot application outages, investigate security incidents, and gain new levels of insight in seconds or minutes, not hours or days. This paper outlines the struggles organizations face managing silos of machine data and how by using Splunk they are seeing dramatic improvements in user productivity and are elevating the role of IT.

Introduction: The Rise of Machine Data

IT is Under a Lot of Pressure

In 2010 IT spend reached more than $1.5 Trillion globally. Unfortunately, 75% of this budget was spent on legacy systems, including support, maintenance, application troubleshooting, security and compliance.[2] Enterprises invest far too much managing their IT infrastructures and too little on innovation. This drains precious resources and prevents IT from being a strategic business enabler.

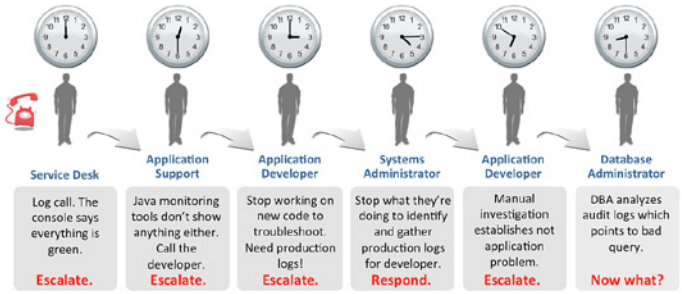
Existing Approaches Are Cumbersome, Costly and Don't Scale

Traditional approaches to managing IT are limited and locked into technology or functional silos. A separate tool is required for each kind of data and every type of task. As IT complexity increases, organizations now find themselves with many point solutions that don't work together, are expensive to maintain, and don't deliver the answers they need. Or they have deployed layer upon layer of high-level management systems, which filter out much of the essential data, requiring people to still pick through systems by hand.

The tools we have to manage IT have not kept pace with the rapid change in technology. Innovations designed to help us maximize resources, like service-oriented architecture (SOA), virtualization and cloud computing, can't be realized due to ineffective IT management.

IT Silos Drive Enormous Inefficiencies

Take a look at the time consuming, manual labor-based, application troubleshooting scenario below.



Time spent (8.5 hours) in human latency to troubleshoot a failure.

Is this picture familiar? Hundreds of times a day, in every IT organization, trouble tickets, security incidents and requests for compliance audits arrive at the service desk. Lacking information, service desk staff create tickets and escalate the issue to other teams. Silos of data, tools and processes hinder any effective collaboration, and the escalations bounce around IT departments like pin balls. Industry analyst firm, Forrester Research, estimates that over 70% of service desk issues are escalated beyond Tier 1 staff. [3]

Manually traversing these silos of data takes hours or days, when in fact the business needs answers immediately. It's no wonder 75% of IT budgets are spent managing and maintaining existing applications and infrastructure.

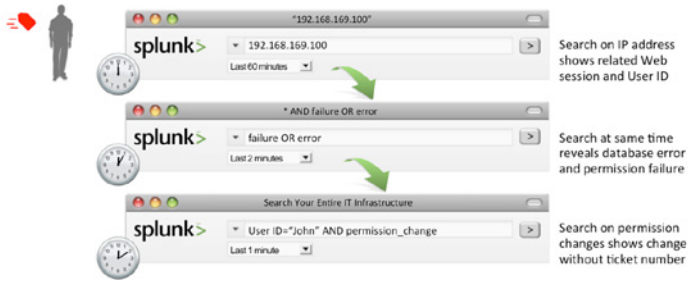
In today's scale out, virtualized and dynamic IT environments, achieving better results requires thinking differently. Managing and monitoring individual IT technologies or functions as silos is no longer the answer. Organizations must achieve visibility and gain insight across the IT silos to eliminate massive inefficiencies and ensure that the right information is available to the right people at the right time.

> "The product innovation needed to meet some of today's IT infrastructure challenges remains in the hands of the smaller, more-agile vendors."
> "Has Market Consolidation Killed IT Operations Management Tool Innovation? Gartner, March 2009

In the Trenches with Splunk

In the previous example, troubleshooting an application failure resulted in an escalation to network operations, application development, database administration, security and then systems administration. Using Splunk Enterprise, the service

desk can search and analyze all the organization's machine data from one place in real time. They can search on a combination of IP address, database errors and permission changes to correlate diagnostic information across different silos of data, identifying the root cause in minutes, instead of the 24 hours seen in the earlier example.



In the trenches and troubleshooting with Splunk takes just minutes.

The Answer is in the Machine Data

Splunk has recognized that the key to managing, securing and auditing IT more effectively is locked inside the data that IT systems generate. Every second of every day, hundreds to thousands of IT components record the activities of the enterprise, from the details on application transactions, to the access and use of sensitive data, to potential security attacks.

This machine data is the critical source of the truth regarding what's happening within and at the perimeter of an IT infrastructure. It's vital for identifying application failures, understanding attacks, investigating who accessed sensitive data, or summarizing authorized and unauthorized configurations. It's also needed for maintaining and improving service levels, providing proof of compliance with regulatory and corporate governance mandates and ensuring security. The problem has been getting to and making sense of all this data.

A New Approach: Real-time Visibility of All Your Machine Data

Introducing Splunk

Splunk is the engine for machine data. It was developed to solve the machine data challenge and collects, indexes and harnesses all of an organization's unstructured, time-series machine data. Splunk can read data from virtually any source, such as network traffic, web servers, custom applications, application servers, hypervisors, GPS systems, stock market feeds, social media, and preexisting structured databases. Splunk delivers a real-time understanding of what's happening and deep analysis of what's happened across your IT systems and infrastructure. It turns your machine data into the insights you need to make informed decisions.

Splunk introduces powerful capabilities to address multiple functions of IT.

Splunk makes an organization's machine data available for a variety of functions from application management, security and compliance, to operations management and web analytics. For the first time, organizations can analyze their machine data from one place in real time regardless of source, format, location or volume. Both technical and business users can search, alert, report and analyze IT activities and do in minutes what used to take hours or days.

With Splunk, users, departments, and functions can become dramatically more productive and move from reactive to proactive over time. The key capabilities of Splunk are as follows:

- Universally index machine data, from virtually any source
- Enable freeform search and incident investigations from one place
- Automatically discover knowledge from the data and let users add their own
- Monitor data and provide real-time alerts when specific conditions arise
- Provide powerful reporting and analysis
- Provide the ability to create custom dashboards and views for different roles
- Scale efficiently using commodity hardware
- Provide granular role-based security and access controls
- Support multi-tenancy and be flexibly deployed

With an organization's machine data indexed together, departments and functions no longer need to operate as individual silos with limited views. Splunk provides the means to manage IT more efficiently and leverage the full value of machine data.

Dramatic Payback: See Immediate Value

Focus on the Users

Technology and functional silos hinder productivity and the ability of IT to meet the needs of the business. At a time when organizations must drive more value from IT, they are demanding even greater performance from their IT spending. Enter Splunk.

Splunk is a new approach to managing, securing and auditing your entire IT infrastructure. Provided as a free download or low-cost enterprise license, Splunk is simple to deploy, scales from a single server deployment to global large-scale operations, and delivers immediate payback.

The power of Splunk is the exponential value it delivers to users and to the business. Machine data is vast in volume, unstructured, dynamic and captive in silos of traditional point

solutions. Splunk invented a new approach to managing machine data and unlocking its enormous value. Using Splunk as the engine to search and analyze machine data is changing the way users do their jobs and elevating the role of IT in their organizations.

Better Productivity

Users experience significantly higher productivity using Splunk in the following ways

- Rapid troubleshooting and incident investigations

  "We used to spend hours, now Splunk does the troubleshooting in seconds."
  Voxeo

  "Before Splunk we couldn't prove compliance, we couldn't consolidate all the data, and queries took 4-5 days to run. Splunk indexes everything and returns results and reports in seconds. Now we're passing every audit."
  CVS Caremark

- Avoid escalations—Tier 1 service desk resolves issues on their own

  "Splunk help cut our MTTR in half, without escalating beyond first tier agents."
  Dow Jones

  "Splunk reduced escalations by 90% and problem resolution time by 67%."
  Vodafone

- Improve automation and performance by monitoring for early warning signs on all IT components

  "We use Splunk for our change monitoring requirements. Splunk's change management application does this more efficiently and with better functionality."
  Monash University

Improved Uptime, Revenue and Customer Satisfaction

Businesses experience more uptime, less revenue disruption and happier customers

- Reduce mean time to resolving issues and incidents causing downtime

  "When we peak at 130 orders per minute, downtime is not an option. With Splunk we can zero in on a problem in seconds. Our speed of problem resolution has increased 5x. For the first time in six years, we had zero downtime on Macys.com during the peak season."
  Macy's

- Find and resolve problems before they affect your customers

  "Splunk gives our customer service, NOC staff and network engineers comprehensive real-time event data for incident response, chronic problem identification and optimization."
  BT

  "Splunk' s transaction search enables my team to quickly determine if a trade was executed. It's so fast they can do it while the broker is still on the phone."
  Nexa

- Resolve customer issues faster

  "It used to take hours, even days to track transactions. Now our Tier 1 support can respond to inquiries in seconds – while the customer is still on the phone."
  Pegasus Solutions

Higher Service Levels for the Business

Businesses drive service-level excellence and implement more complete compliance and security at lower cost

- Automatic monitoring for early warnings and faster MTTR ensures less downtime

  "Splunk allows us to quickly consolidate and correlate disparate log sources, which in turn allows sophisticated monitoring and response previously thought impossible."
  Cisco

- Demonstrate compliance faster and with less effort by monitoring all your IT data and rapidly responding to ad-hoc auditor requests

  "Failure to comply with PCI equates to failure for our business. Splunk enables us to demonstrate compliance across all PCI DSS requirements."
  Gala Coral

  "The QSA auditors love Splunk. We generate ad-hoc reports to track any transaction or user activity and easily show we are PCI compliant in minutes."
  Carlson Marketing

- Improve protection by detecting attacks, fraud and insider threats that previously went undetected

  "Splunk is faster, provides a more complete view and is more efficient than SIEMs or log mgmt. We now monitor for security risks that traditional tools may not find."
  Booz Allen Hamilton

New Levels of Visibility and Insight

The business experiences new levels of visibility and insight using Splunk in the following ways:

- Real-time business dashboards deliver new insights

  "With Splunk we build management dashboards in minutes. We now correlate business and machine data for true operational visibility."
  nTelos

  "Splunk dashboards trend visualizations and indicate when something will stop working—that's priceless."
  Comcast

  "With Splunk we optimized our partner tariffs and delivered unprecedented ARPU visibility—and they delivered this all in two weeks."
  Leading US-based Fixed-price Wireless Provider

Value across the Enterprise

Splunk is free to download and has a rich set of capabilities out-of-the-box. A simple Splunk deployment can start small, pulling logs, metrics or configurations from a single source. As users exploit the value of their machine data, they find other more strategic uses for Splunk, normally in one of the following areas – security & compliance, application management, IT operations and web analytics. Over time, organizations find the value of Splunk and their machine data belongs enterprise wide, expanding first to more sites, geographies and data sources. And finally Splunk becomes the enterprise standard for multiple uses and multiple diverse roles in the organization. Consequently Splunk deployments have become distributed and mission critical for thousands of organizations worldwide.

Recognized by the Industry

In addition to a growing community of users and partners the leading analysts have taken notice of Splunk:

"Splunk is predictive and forward thinking. Splunk helps you understand what's happened, what's happening, and what's likely to occur."
David Williams, Research Vice President"
IT Operations and Enterprise Management, Gartner

"The sky is the limit on what you can do with Splunk."
Glenn O'Donnell, Senior Analyst,
IT Infrastructure & Operations, Forrester

"Far ahead of the curve in addressing diagnosis, RCA, and Continual Service Improvement."
Liam McGlynn, Senior Analyst,
IT Management, EMA

"Splunk is awesome: it's multi-platform, easy to install and use. And with an abstraction layer of logs, configuration files and system messages, traps and alerts, it's seriously useful."
Nick Selby, Research Director,
Enterprise Security Practice, 451 Group

A Different Type of Software Company

Splunk was conceived to fill a technology void. The company's founders, all with IT management and datacenter backgrounds, created software they wanted to use and a business model that was transparent and innovative. Splunk is available as a free download, runs on the leading operating systems and installs in a few minutes.

At a time when businesses need every competitive advantage and IT is challenged to do more with less, Splunk offers a radically different approach. Splunk empowers organizations to massively improve the efficiency of IT, delivering relevant information, to the people who need it, in less time and with fewer resources.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

1 Forrester, Global IT Survey, 2011
2 Forrester, Global IT Survey, 2011
3 Forrester, Enteprise Software Trends, 2009

250 Brannan St, San Francisco, CA, 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.splunkbase.com

Copyright © 2012 Splunk Inc. All rights reserved. Splunk Enterprise is protected by U.S. and international copyright and intellectual property laws. Splunk is a registered trademark or trademark of Splunk Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item # WP-Splunk-ITSILOS HURT-101