

Splunk Adds Real-time Search, Analysis and Monitoring

Unique Combination of Real-time and Unlimited Historical Search Drives IT-Business Alignment

MELBOURNE -- MAY 5, 2010 -- Splunk, the IT Search company, today announced the availability of Splunk 4.1, providing the unique ability for users to search, monitor and analyse live streaming IT data as well as terabytes of historical data, all from the same interface, delivering the best of both worlds for IT data management.

The ability to search, analyse and create live dashboards with streaming data from the IT infrastructure delivers immediate visibility to operational, application, security and compliance issues. Now users can see incidents and attacks as they occur, monitor application SLAs in real time, correlate and analyse events on streaming data and track live transactions and online activity.

"Traditional technologies direct users down two separate paths: either data warehouses for big data historical analysis or tools specifically for real-time monitoring, resulting in serious tradeoffs due to separate systems with fundamentally different technology architectures," said Erik Swan, co-founder and chief technology officer, Splunk. "Splunk 4.1 is unique in that it combines in one solution with one user interface the ability to search, monitor and analyse all streaming data sources with Splunk's proven strengths searching unlimited amounts of historical IT data."

Last year Splunk introduced Splunk 4.0, re-architected to deliver an order-of-magnitude improvement in speed and scale, as well as enable the creation of custom views and dashboards extending the benefits of Splunk to business users and IT professionals alike. The Splunk 4.0 release accelerated adoption across enterprises -- with 650 new customers being added in 2009 alone. Splunk 4.1 is based on a unique and patent-pending implementation of real-time search using MapReduce techniques, which delivers extreme scalability and enables the new real-time capabilities to scale linearly across commodity hardware.

"Splunk is delivering a powerful way for organisations to manage dynamic IT environments and identify data patterns, thwart security breaches, and correlate information across massive data sets, using live streaming data. Real-time IT Search allows organisations to gain immediate visibility into all of their IT infrastructure data and deliver visibility and meaning to all layers of the organisation," stated Rachel Chalmers, Research Director, The 451 Group.

In addition to new real-time capabilities, Splunk 4.1 includes new features designed to support enterprise deployments and individual user productivity, such as:

- o Single sign-on (SSO) -- Integrates with enterprise single sign-on solutions for transparent authentication of third-party credentials and simplifies credential management.
- o Event-level workflows -- Create workflows directly from data in search results and automate required next steps, such as opening a trouble ticket, blocking an IP address, or looking up a product ID in an external database.
- o Automatic and configurable data drilldown -- Drill down from charts to original events and determine root causes faster. Click on sections of charts to automatically refine searches without having to do so manually.
- o Scheduled PDF report delivery -- Create, schedule and deliver PDFs of any Splunk dashboard, view, search or report and share meaningful information across the organisation, even non-Splunk users.
- o Event type finder and builder -- Automatically identify new event types based on recurring patterns in the data.

For more on the Splunk 4.1 release, including the new real-time search architecture:

- o View the product demo video: <http://www.splunk.com/view/new-in-splunk-4-1/SP-CAAAFD5>
- o View the technical overview video: <http://www.splunk.com/view/real-time-in-splunk/SP-CAAAFD7>

About Splunk

=====

Splunk is software that provides unique visibility across your entire IT infrastructure from one place in real time. Only Splunk enables you to search, report, monitor and analyse all your real-time streaming and historical IT data. Now you can troubleshoot application problems and investigate security incidents in minutes instead of hours or days, monitor to avoid service degradation or outages, deliver compliance at lower cost and gain new business insights from your IT data. Over 1,750 enterprises, service providers and government organisations in 68 countries use Splunk to realise new levels of service quality, reduce IT operations costs and mitigate security risks in record time. The world's leading technology providers and over 50 system integrator, value-added reseller and managed service provider partners are driving new business and fueling their offerings with Splunk. Download your own free copy of Splunk today at www.splunk.com/download

Contacts

David Sanday

02 9387 2333

mailto: david.sanday@bowespr.com