splunk> CONSIST Group

SOLUTIONS GUIDE

Splunk and Big Data

Turn machine-generated data into real-time insights for IT and the business.

Big Data Comes from Machines

All your IT applications, systems and technology infrastructure generate data every millisecond of every day. This machine data is one of the fastest growing, most complex areas of big data. It's also one of the most valuable, containing a definitive record of user transactions, customer behavior, sensor activity, machine behavior, security threats, fraudulent activity and more.

Machine data holds critical insights useful across the enterprise. Here are a few examples:

- Monitor end-to-end transactions for online businesses providing 24x7 operations
- Understand customer experience, behavior and usage of services in real-time
- Fulfill internal SLAs and to monitor service provider agreements
- Identify spot trends and sentiment analysis on social platforms
- Map and visualize threat scenario behavior patterns to improve security posture

Making use of machine is challenging. It's difficult to process and analyze by traditional methods or in a timely manner.

- Machine data is generated by a multitude of disparate sources; correlating meaningful events across these is complex
- The data is unstructured and difficult to fit into a pre-defined schema
- Machine data is high-volume and time-series based, requiring new approaches for management and analysis
- The most valuable insights from this data are often needed in real time

Existing business intelligence and data warehouse solutions are simply not engineered for this type of high-volume, dynamic and unstructured data. Emerging open source technologies can provide part of the answer, but require extensive and time-consuming integration with other open source projects and highly specialized skill sets.

Today's agile enterprises can't wait. Key stakeholders across the organization need to keep pace and adapt to rapidly changing business environments. They need a technology that supports real-time data discovery, ad hoc reports and rapid analysis. A solution that can give them answers as fast as they think of questions.

Making Machine-generated Data Accessible, Usable and Valuable to Everyone

Splunk is the first enterprise-class platform that collects and indexes any machine data. Splunk can read data from just about any source imaginable, such as network traffic, Web servers, custom applications, application servers, hypervisors, GPS systems, stock market feeds, social media, sensors and preexisting structured databases. It gives you a real-time understanding of what's happening and deep analysis of what's happened across your IT systems and technology infrastructure, so you can make informed decisions. This is operational intelligence.

Integrated, end-to-end and real-time. Splunk collects and indexes any machine data from virtually any source, format or location in real time. It stores and indexes all of the data in a centralized location and keeps it secure with role-based access controls. Once in Splunk, you can search, monitor, report and analyze your data, no matter how unstructured, large or diverse it may be.

Enterprise-scale big data. Splunk scales to collect and index tens of terabytes of data per day, across multi-geography, multi-datacenter infrastructures. And because the insights from your data are mission-critical, Splunk provides the resilience you need, even as you scale out your low-cost, distributed computing environment.

Robust platform for developing big data apps. Developer teams will find a whole host of ways to leverage Splunk and maximize enterprise technology investments. Built-in SDKs for JavaScript and JSON with additional downloadable SDKs for Java, Python and PHP makes it easy to customize and extend the power of Splunk.

Powerful integrations. Splunk Hadoop Connect provides bi-directional integration to easily and reliably move data between Splunk and Hadoop. The Splunk App for HadoopOps provides real-time monitoring and analysis of the health and performance of the end-to-end Hadoop environment.

Proven ROI. The Splunk Enterprise platform is proven with over 4,400 enterprise customers using Splunk to improve service levels, reduce operations costs, mitigate security risks, enable compliance, enhance DevOps collaboration and create new product and service offerings. Splunk customers typically achieve an ROI measured in weeks or months, sometimes even before being deployed into production.

What Makes Splunk Unique

Splunk Enterprise is an integrated, end-to-end, real-time solution for machine data delivering the following core capabilities:

- Universal collection and indexing of machine data, from virtually any source
- Powerful search processing language to search and analyze real-time and historical data
- Real-time monitoring for patterns and thresholds, provide real-time alerts when specific conditions arise
- Powerful reporting and analysis
- Custom dashboards and views for different roles
- Resilience and scale on commodity hardware
- Granular role-based security and access controls
- Support for multi-tenancy and flexible, distributed deployments
- Splunk Hadoop integration for reliable, bi-directional interoperability
- Robust, flexible platform for big data apps

Customer Success with Splunk

With over 4,400 licensed customers, our customers are the best examples of machine big data in action.

Salesforce.com®

Salesforce.com, the industry-leading enterprise cloud computing company, uses Splunk software to mine large quantities of data generated from across their entire technology stack.

Salesforce.com has over 500 users of Splunk dashboards from IT users monitoring customer experience to product managers performing analytics on new services like 'Chatter.'

"The fact that we had a data treasure chest was not obvious until Splunk came in to the picture. With Splunk, we have taken application troubleshooting for 97,000 customers to the next level. Splunk has augmented our ability to make data-driven decisions."
Narayan Bharadwaj, Director Product Management, Salesforce.com

NPR®

NPR, the award winning, multimedia news organization reaching 26.8 million listeners per week, uses Splunk software to gain better visibility and insight of their digital asset infrastructure.

NPR initially used Splunk to monitor and troubleshoot their end-to-end asset delivery infrastructure. Before Splunk, there were critical business metrics they couldn't get from their traditional web analytics solutions. They expanded their deployment of Splunk and now measure program popularity, views by device, reconcile royalty payments for digital rights, measure abandonment rates and more.

"Only Splunk easily gives us the business reports about our web-based digital assets that we need."
Sondra Russel, Online Metrics Analyst

Pegasus Solutions

Pegasus Solutions, a major power behind the travel and hospitality industry, caters to hundreds of thousands of hotels, websites and travel agencies and processes 4-5 billion transactions per month. Pegasus uses Splunk to gather real-time insights from their operational data. Results from using Splunk include reduced escalations and troubleshooting, accelerated response to customer inquiries and unparalleled insights on the health of their system and business.

"Splunk scales to give us real-time monitoring as well as deep historical trend analysis across 50+ systems and 2 billion transactions a month. It is amazingly flexible—we get deep, detailed information and high-level health metrics—all from the same set of data."
Peter Elhke, Principal Systems Engineer, Pegasus Solutions

Online Travel Company

One of the world's leading online travel companies initially used Splunk software to avoid website outages, saving millions of dollars in lost revenue. They quickly expanded their use of Splunk and within 10 months were monitoring 98% of their infrastructure. Today, over 2,700 users at this organization use Splunk to gain real-time insights of not only their IT infrastructure, but also online bookings, performance of air-travel coupons and optimizing SEM.

"We achieved real-time visibility and insights across a wide range of critical areas from server and application health and performance monitoring to bookings trends, coupon use and deal analysis with Splunk. We gained the ability to perform rapid, real-time analysis on tens of terabytes of unstructured, time-sensitive machine data."
Sr. Director Infrastructure Architecture

Free Download

Download Splunk for free. You'll automatically get all of the Enterprise features of Splunk for 60 days and you can index up to 500 megabytes of data per day. Or if you want to get started right away with an Enterprise license contact sales@splunk.com.

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

splunk> listen to your data™