

Splunking Big Data

Making machine-generated data accessible, usable and valuable to everyone.

Most Challenging, Fastest Growing Segment of Big Data

While most companies don't realize it, machine data is the fastest growing, most complex and yet most valuable segment of big data. All websites, communications, networking and complex IT infrastructures generate massive streams of data every second of every day, in an array of unpredictable formats that are difficult to process and analyze by traditional methods or in a timely manner.

Making use of machine data can provide significant benefits to nearly every enterprise. Here are a few examples:

- Transaction monitoring for online businesses providing 24x7 operations
- Web activity and web asset usage data to gain customer intelligence, understand capacity use and track digital assets
- Service-level monitoring to fulfill internal SLAs and to monitor service provider agreements
- Call and event detail records to uncover keys to more profitable services for communications service providers
- Mobile data to better understand customer location and behavior
- Monitor social media networks to identify spot trends and sentiment analysis
- Map and visualize threat scenario behavior patterns to improve security posture

Machine data holds critical operational insights into user behavior, security risks, capacity consumption, service levels, fraudulent activity, customer experience and much more.

Making use of this data however, presents real challenges:

- 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 typically require extensive and time-consuming integration with other open source projects.

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.

Splunking Machine Data

Splunk is the leading enterprise solution for managing and analyzing machine data. It provides a unified way to organize and to extract actionable insights from the massive amounts of machine data generated across diverse sources.

Splunk turns your machine data into a NoSQL data fabric that can be searched, browsed, navigated, analyzed and visualized. This enables IT and business professionals to solve a wide range of mission-critical problems, all without the inherent limitations of traditional approaches based on relational databases.

An integrated, end-to-end solution. Splunk collects machine data from wherever it's generated 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.

Proven with over 3,000 enterprise customers. Organizations use Splunk in large-scale production deployments to manage huge amounts of new data a day, performing historical searches of upwards of 1PB of data to support a myriad of use cases. These can range from real-time error detection to business analytics.

Rapid time-to-value. Splunk can be downloaded and implemented in a matter of days, rather than having a team of people take months or even years to deploy a solution. Powerful search, drilldown and reporting capabilities meet the needs of novice users and expert analysts alike. Easy-to-create dashboards put critical insights from your machine data into the hands of the people who need it so you can scale your most useful resource—your people.

Scales efficiently to any data volume using commodity

hardware. Splunk can be downloaded and run on a single server in under 5 minutes. The same software can be scaled out across the largest global infrastructures, indexing tens of terabytes of data per day.

What Makes Splunk Unique

Splunk delivers key capabilities out-of-the-box to make large volumes of machine data accessible, useful and valuable for IT and the business:

- Universal indexing of any machine data, from any source in real time
- Enables free form search and analysis of real-time and historical data
- Automatically discovers knowledge from the data
- Monitors your data and provides real-time alerts
- Provides powerful ad hoc reporting and analysis
- Provides the ability to rapidly build custom dashboards and views
- Scales efficiently to any data volume using commodity hardware
- Provides granular role-based security and access controls
- Supports multi-tenancy and flexible deployment
- Integrates and is extensible via documented REST APIs, SDKs

Customer Success with Splunk

With over 3,000 licensed customers, many Splunking terabytes of data per day, our users are the best example of massive machine data in action.

Expedia

Expedia, the world's largest online travel company, initially used Splunk to avoid website outages, saving them 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 Expedia 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.

“Splunk provides 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. It's where we go first to perform rapid real-time analysis on tens of terabytes of unstructured, time-sensitive machine data.”

Eddie Satterly, Sr. Director Infrastructure Architecture & Engineering, Global Infrastructure Systems

Salesforce.com

Salesforce.com, the industry-leading enterprise cloud computing company, uses Splunk to mine the large quantities of data generated from across its 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 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

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.