



Splunk Product Data Sheet

The Engine for Machine Data.

Product Overview

Splunk is the engine for machine data. It collects, indexes and harnesses the machine data generated by all your IT systems and infrastructure—physical, virtual and in the cloud.

Machine data is a valuable resource. It contains a definitive record of all user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. It's also dynamic, unstructured, non-standard and makes up the majority of the data in your organization.

Organizations rarely get the value they need from their machine data. Existing data analysis, management and monitoring solutions are simply not engineered for this type of high-volume, variable and dynamic data.

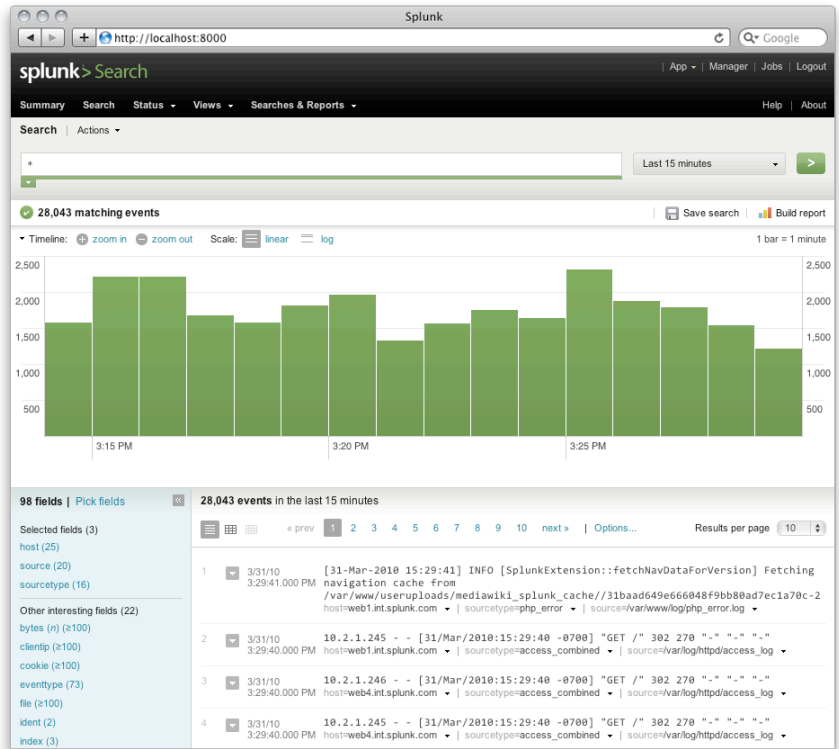
Splunk is the engine for machine data. It was developed to solve the whole machine data challenge and collects, indexes and harnesses all your unstructured, time-series machine data. Search, report, monitor and analyze live streaming and historical data from one place in real time. Gain a real-time understanding of what is happening and what has happened across your IT systems and infrastructure.

Use Splunk to gain rapid visibility, insights and intelligence across IT and the business. Troubleshoot application problems and investigate security incidents in minutes instead of hours or days, avoid service degradation or outages, deliver compliance at lower cost and gain new business insights.

Splunk Capabilities

Universally Index Any Machine Data, From Any Source Splunk indexes machine data in real time from any source, format or location. This includes live data from your packaged and custom applications, app servers, web servers, databases, networks, virtual machines, OSs and more. No matter the source or format, Splunk indexes it the same way - without custom parsers or connectors to purchase, write or maintain. Splunk indexes your data quickly and it's distributed architecture scales to 100% of your machine data. No product for indexing or searching machine data delivers this kind of speed and flexibility. Period.

Search and Investigate Anything Splunk lets you search real-time and historical machine data from one place. Search for specific terms or expressions. Use Boolean operators to refine your search. Trace transactions across multiple systems. Powerful statistical and reporting commands let you update transaction counts, calculate metrics and look for specific conditions within a rolling time window. Search Assistant offers type-ahead and contextual help so that you can access the full power of the Splunk search language.



You can interact with search results in real time. Zoom in and out on a timeline to quickly reveal trends, spikes and anomalies. Click to drill down into results and eliminate noise to find the needle in the haystack. Whether you're troubleshooting or investigating an alert, you'll find the answer in seconds or minutes rather than hours and without escalating to other groups. Real-time search and alerting means you can correlate, analyze and respond to real-time events, Track live transactions and online activity, see and respond to incidents and attacks as they occur, monitor application SLAs in real-time,

Add Knowledge Splunk automatically discovers knowledge from your machine data at search time so you can start using new data sources immediately. You can also add context and meaning to your machine data by identifying, naming and tagging fields and data points. Add information from external source asset management databases, configuration management systems and user directories, making the system smarter for all users.

Monitor and Alert You can turn searches into real-time alerts that automatically trigger actions such sending automated emails, running scripts, or posting to an RSS feed. Alerts can also send an SNMP trap to your system management console or generate a service desk ticket. You can base alerts on a variety of thresholds, trend-based conditions and complex patterns, such as abandoned shopping carts, brute force attacks and fraud scenarios.

Report and Analyze Report builder lets you quickly build advanced charts, graphs and dashboards that show important trends, highs and lows, summaries of top values and frequency of occurrences.

Create robust, information-rich reports from scratch without any advanced knowledge of search commands. Drill down from anywhere in the chart to the raw events. Save reports, integrate them into dashboards and create PDFs on a scheduled basis to share with management, business users or other IT stakeholders.

Create Custom Dashboards and Views Create live dashboards in a few clicks using the dashboard editor. Dashboards integrate multiple charts and views of your real-time data to satisfy the needs of different users. You can personalize dashboards for management, business or security analysts, auditors, developers and sysadmins. And schedule delivery via PDF.

Splunk Apps Create apps on Splunk that deliver a targeted user experience for different roles and use cases. You can share and reuse apps within your organization and the rest of the Splunk community. There are a growing number of apps available on our community site (www.splunkbase.com), built by our community, partners and Splunk. Apps that help visualize data geographically, or that provide pre-canned compliance views; Apps for different technologies such as Windows, Linux, Unix, Virtualization, Networking and more.

Scale to the Largest IT Infrastructures Scale your Splunk installation from a single commodity Windows, Linux or Unix server, to index the largest most complex multi-geography, multi-datacenter infrastructures generating tens of terabytes of data per day. The Splunk architecture is based on MapReduce and scales linearly across commodity servers to unlimited data volumes.

Security is important and role-based access controls govern how far a given user's search can extend. Regional users can see data from the systems within their region and enterprise wide users can reach all datacenters. The Splunk vision is for every authorized employee to have the data view they need—whether for investigations, reports and dashboards, or analysis to improve IT operations and gain valuable business insights.

Secure Data Access and Single Sign-on At the core of Splunk is a robust security model. Every Splunk transaction is authenticated, including system activities and user activities through web and command line interfaces. Splunk also integrates with LDAP-compliant directory servers and Active Directory to enforce enterprise-wide security policies.

Single sign-on integration enables pass-through authentication of user credentials. Since all of the data you need to troubleshoot, investigate security incidents and demonstrate compliance persists in Splunk, you can safeguard access to your sensitive production servers.

It's Software. Download and Install It in Minutes. Splunk is enterprise software made easy. Try Splunk on your laptop and then scale it to your datacenter. Just pick your platform, download and install. You're up and running with a web interface and an engine for your machine data.

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. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license to continue using the expanded functionality designed for multi-user Enterprise deployments.

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Unlimited (based on license)
Universal, real-time indexing	✓	✓
Real-time and historical search	✓	✓
Reporting	✓	✓
Knowledge mapping	✓	✓
Dashboards	✓	✓
Monitoring and alerting		✓
Distributed search		✓
Data forwarding and receiving	✓	✓
Role-based access controls		✓
Single sign-on		✓
Developer APIs	✓	✓
Community Apps	✓	✓
Enterprise Apps		✓
Standard support	✓	✓
Enterprise support		✓

System Requirements

Server Operating System

- **Unix:** Linux (kernel version 2.6x and above (x86, 32- and 64-bit); AIX 5.2 and 5.3; HO-UX 11iv2 (11.22) and 11iv3 (11.31) (PA-RISC or Itanium); Solaris 9,10 (x86 SPARC); FreeBSD 6.1 and 6.2 (x86; 32- and 64-bit)
- **Windows:** XP (32-bit); Vista (32-bit and 64-bit); Windows 7 (32-bit and 64-bit); Windows Server 2003 (64-bit); Windows Server 2008 (64-bit)
- **Mac:** MacOSX 10.5 (32-bit and 64-bit); MacOSX 10.6 (32-bit mode)

Server Hardware

- 2x quad-core Xeon, 3GHz, 8GB RAM (recommended)

Storage

- 12-48% of raw data size depending on indexing density/data source

Supported Browsers

- Firefox 2.0+ / Windows, Linux and Mac OSX; IE 6+ / Windows; Safari 4

Get Started Today !

Website: www.splunk.com
Address: 250 Brannan St, San Francisco, CA, USA, 94107
Email: info@splunk.com | sales@splunk.com
Phone: +1 866-438-7758 | +1 415-848-8400
Free Download: www.splunk.com/download
Community: Splunk Answers | community@splunk.com