

# Splunk Product Data Sheet

Search and analyze all the data generated in your IT universe from one place in real time.

## Real-time Business Needs Real-time IT

At a time when the speed of IT impacts the pace of business, a fast acting and responsive IT organization is vital. Yet the data you need to manage, secure, audit and gain intelligence for the business is locked in siloed technologies located across your IT infrastructure. Manually sifting through this IT data with existing tools and terminals is time-consuming, costly and doesn't scale.

Splunk took a different approach. We asked the question "how can we make IT data more accessible, usable and valuable for everyone?" We responded by pioneering the use of search for IT data. Search is agile, versatile and scales to enormous data volumes.

Search is just the beginning. Splunk enables rapid troubleshooting and incident investigations. It delivers powerful statistical analysis and correlation and it provides an interactive user interface for alerting, monitoring, reporting and analytics.

Splunk is flexible enough to handle all IT data, versatile enough to work with all your streaming and historical data, scalable enough to run across all of your datacenters and powerful enough to deliver information in a meaningful context to anyone in your organization.

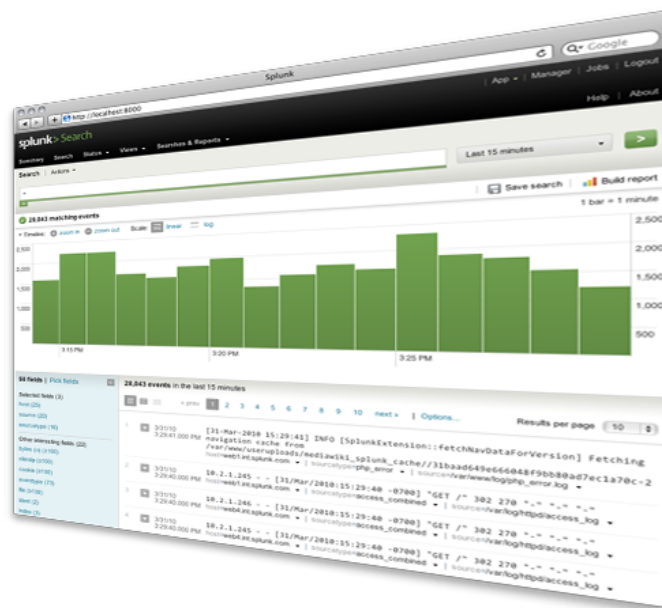
## Product Overview

Splunk software lets you search, report, monitor and analyze live streaming and historical data across your entire IT infrastructure from one place in real time. Splunk offers unique visibility into IT data that represents user transactions, customer behavior, machine behavior, security threats and fraudulent activity. Use Splunk to 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

### Index Any IT Data, From Any Source

Splunk indexes machine-generated IT data from any source in real time including your live custom and packaged application logs, stack traces, message queues, database audit trails and even logs, status, configurations and metrics from your hypervisor, OS and network layers. No matter the source or format, Splunk indexes it the same way - without specific parsers or adapters to purchase, write or maintain. The Splunk MapReduce-based architecture means that it performs quickly and scales to 100% of your IT data. No product for managing or searching IT data delivers this kind of speed and flexibility. Period.



### Search and Investigate Anything

With Splunk you can search live streaming data and indexed historical data using the same interface. Familiar Boolean reporting commands let you update transaction counts, calculate metrics and even look for specific conditions within a rolling time window. Search Assistant offers type-ahead and contextual help so that you can leverage 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 a ticket 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 means you see incidents and attacks as they occur, monitor application SLAs in real time, correlate and analyze events on streaming data and track live transactions and online activity.

### Add Knowledge

Splunk extracts knowledge from your IT data automatically at search time so you can start using new data sources immediately. You can also add context and meaning to your IT data by identifying, naming and tagging fields and data points. Splunk even lets you 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 alerts that automatically trigger actions such as email or RSS notifications or remediation scripts. 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

Use the report builder to 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. 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

Create live dashboards in a few clicks with 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.

## Build and Deploy IT Apps

Enrich your Splunk installation with Apps built by Splunk, our partners or our customers. Apps are available for different platforms, such as Windows, Linux and Unix, for different technologies such as virtualization and networking and for use cases such as security and compliance. Share your App with the community or browse other Apps by visiting [www.splunkbase.com](http://www.splunkbase.com).

## Scale from Single Server to Datacenter

The Splunk distributed architecture lets your search span multiple deployments within a datacenter or globally across all of your datacenters. With role-based access you control 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 that 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

Underlying everything Splunk does 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 indexing engine for all of your IT data.

## Free Download

The free Splunk download automatically includes all Enterprise features for 60 days and lets you index 500 megabytes of data per day. After 60 days, or anytime before, you can convert to a perpetual Free license or purchase an Enterprise license to continue using the expanded functionality designed for multi-user Enterprises.

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Varies by 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 2.6+)/ x86\_64 or x86; Solaris (8,9,10)/ SPARC; Solaris (9, 10) / x86; Solaris 10 / x86\_64; FreeBSD (5.4, 6.2) / x86
- **Windows:** XP (32-bit), Vista (32-bit and 64-bit), Windows Server 2003 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit)
- **Mac:** Mac OS (10.4+) / PPC or x86

### Server Hardware

- 2x3.4 GHz CPU, 4 GB RAM (min.)

### 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](http://www.splunk.com)

Address: 250 Brannan St, San Francisco, CA, USA, 94107

Email: [info@splunk.com](mailto:info@splunk.com) | [sales@splunk.com](mailto:sales@splunk.com)

Phone: +1 866-438-7758 | +1 415-848-8400

Free Download: [www.splunk.com/download](http://www.splunk.com/download)