splunk>

PRODUCT DATA SHEET

Splunk® Enterprise™ Product Data Sheet

The Engine for Machine Data™

HIGHLIGHTS

- Identify and resolve issues up to 70% faster and reduce costly escalations by up to 90%
- Monitor systems and infrastructure in real time to identify issues before they impact your business
- See the whole picture across IT to track key performance indicators and make better decisions
- Understand trends and patterns of activity and behavior; gain real-time Operational Intelligence for IT and the business

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 one of the fastest growing, most complex segments of data in your organization. It's also one of the most valuable, containing a definitive record of user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more.

Splunk collects machine data securely and reliably from wherever it's generated. It stores and indexes the data in real time in a centralized location and protects it with role-based access controls. Splunk lets you search, monitor, report and analyze your real-time and historical data. Now you have the ability to quickly visualize and share your data, no matter how unstructured, large or diverse it may be.

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. With Splunk you can gain rapid visibility, insights and intelligence for IT and business.

Splunk Capabilities

Collect and Index Any Machine Data. Splunk collects and indexes machine data in real time from virtually any source, format or location. This includes live data from your packaged and custom applications, app servers, web servers, databases, networks, virtual machines, telecoms equipment, OS's and more. No matter the source or format, Splunk indexes it the same way—without custom parsers or connectors to purchase, write or maintain. Once in Splunk, all your machine data is available for troubleshooting, security incident investigations, network monitoring, compliance reporting, business analytics and other valuable uses. And as your data needs grow, Splunk scales efficiently using commodity hardware.

Search and Investigate. Search and analyze real-time and historical machine data from one place with Splunk. 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.

Interact with your 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 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.

Splunk from your desktop, tablet or mobile device.

Monitor and Alert. Turn searches into real-time alerts that automatically trigger actions such as sending automated emails, running remediation scripts or posting to RSS feeds. Alerts can also send an SNMP trap to your system management console or generate a service desk ticket. Alerts can be set to any level of granularity and can be based 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. 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 view them all from your desktop or mobile device. 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, such as management, business or security analysts, auditors, developers and sysadmins. Users can edit dashboards using a simple drag and drop interface and change chart types on-the-fly with integrated charting controls.

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. The Splunk architecture is based on MapReduce and scales linearly across commodity hardware as data volumes grow. Start small on a single commodity Windows, Linux or Unix server and then deploy Splunk across multi-geography, multi-datacenter infrastructures generating tens of terabytes of data per day.

Security is important and role-based access controls govern how far a 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 it and Install it in Minutes. Splunk is enterprise software made easy. Try Splunk on your laptop and then deploy it to one or more datacenters. You're up and running with a web interface for users and a powerful engine for indexing your machine data.

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		•

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. You can convert to a perpetual Free license or purchase an Enterprise license by contacting 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