splunk>

PRODUCT DATA SHEET

Splunk® Enterprise™ Product Data Sheet

The Platform for Machine Data

HIGHLIGHTS

- Gain real-time Operational Intelligence for IT and business users
- 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 for customers, transactions and systems

Product Overview

Splunk is the platform for machine data. It's the easy, fast and resilient way to collect, analyze and secure the massive streams of machine data generated by your IT systems and technology infrastructure—whether it's physical, virtual or in the cloud.

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.

Splunk software 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 problems and investigate security incidents in minutes (not hours or days). Monitor your end-to-end infrastructure to avoid service degradation or outages. Gain real-time visibility and critical insights into customer experience, transactions and behavior. Use Splunk software and make your data accessible, usable and valuable across the enterprise.

Splunk Capabilities

Collect and Index Any Machine Data. Collect and index any machine data from virtually any source, format or location in real time. This includes data streaming from packaged and custom applications, app servers, web servers, databases, networks, virtual machines, telecoms equipment, operating systems, sensors and much more. There's no requirement to "understand" the data upfront. Just point Splunk software at your data and it immediately starts collecting and indexing, so you can start searching and analyzing. Troubleshoot applications issues, investigate security incidents, monitor networks and performance, monitor compliance, analyze new products and service. These are just a few of the valuable uses you will find from your data. And as your data needs grow, Splunk Enterprise scales easily and reliably on commodity servers and storage.

Search and Investigate. Splunk software offers a powerful search processing language simple enough for the beginner and powerful enough for the expert data analyst. Whether you're in the business of running, securing and auditing IT, developing applications, or providing analytics for the business. Search is the starting point for opening up a whole new world of possibilities from your data.

Search, analyze and correlate real-time and historical machine data. Use specific terms or expressions, Boolean operators and powerful statistical and reporting commands. The search assistant offers type-ahead and contextual help so that you can access the full power of the Splunk search language.

Interact with your data to reveal powerful new insights. Zoom in and out on a timeline to spot trends, spikes and anomalies. Drill down into results and eliminate noise to find the needle in the haystack; correlate, analyze and respond to real-time events. Whether you're troubleshooting or investigating an alert, you'll find the answer in minutes instead of hours and without escalating to other teams.

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. Install non-standard data sources from Splunkbase so they appear automatically. Add information from external asset management databases, configuration management systems and user directories, making the system smarter for all users.

Monitor and Alert. Turn searches into real-time alerts to monitor threshold conditions around the clock. Automatically trigger actions such as sending automated emails, executing remediation

Use Splunk Enterprise on your desktop, tablet or mobile device.

scripts or posting to RSS feeds. 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. Rapidly 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. Or to another dashboard, form, view, or external website. Save reports, integrate them into dashboards and view them all from your desktop or mobile device. Create PDFs and share reports and dashboards with management, business users or other IT stakeholders.

Custom Dashboards and Views. Combine multiple views into interactive dashboards with ease 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. Do more by taking advantage of hundreds of Apps and other content that run on top of the Splunk platform. Apps deliver a targeted user experience for different roles and use cases. There are a growing number of apps, built by our community, partners and Splunk. These apps help you visualize data geographically, or provide pre-defined compliance views for your mission critical technologies such as VMware, Exchange, Cisco and Citrix. There are apps for different technologies such as Windows, Linux, Unix, virtualization, networking technologies and more. Browse apps, or event create and post your own, all through the Splunk community website http://splunk-base.splunk.com/.

Enterprise-class Scale and Resilience. 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. Automatic load balancing optimizes workloads and response times and provides built-in failover support. Out-of-the-box reporting and analytics capabilities deliver rapid insights from your data.

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-directories and Microsoft® 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 control access to your sensitive production servers and data.

A Platform for Enterprise Apps. Developer teams will find a whole host of ways to leverage Splunk Enterprise. Debug and troubleshoot applications during development and test cycles or integrate data from Splunk Enterprise into custom applications. Output data from any API endpoint in JSON and ensure custom Splunk development over time, with API versioning. Splunk Enterprise ships with the JavaScript SDK with additional downloadable SDKs for Java, Python and PHP making it easy to customize and extend the power of Splunk Enterprise.

It's Software. Get up and Running in Minutes. Splunk is enterprise software made easy. Try Splunk Enterprise on your laptop and then deploy it to your datacenter or cloud environment. You'll be up and running with an intuitive web user interface and a powerful enterprise platform for indexing your machine data.

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	**500MB**	**Unlimited** (According to license)
Universal, real-time indexing	•	•
Index replication		•
Real-time and historical search	•	•
Distributed search		•
Monitoring and alerting		•
Reporting and sharing	•	•
Accelerated reporting	•	•
Knowledge mapping	•	•
Dashboards	•	•
Role-based access controls		•
Single sign-on		•
Data forwarding and receiving	•	•
Developer platform (API, SDKs)	•	•
Splunk 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

splunk> listen to your data™

www.splunk.com