splunk>

PRODUCT DATA SHEET

Splunk® Enterprise™

The Platform for Operational Intelligence

HIGHLIGHTS

- Deliver real-time operational intelligence to 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, patterns of activity and behavior for customers, transactions and systems

Product Overview

Splunk Enterprise is the industry-leading platform for operational intelligence. It's the easy, fast and secure way to analyze the massive streams of machine data generated by your IT systems and technology infrastructure—physical, virtual and 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 activity, sensor readings, machine behavior, security threats, fraudulent activity and more.

Splunk Enterprise takes all your machine data, so you can 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 other key business metrics. Splunk Enterprise makes your machine data accessible, usable and valuable across the organization (see *Figure 1*).

Delivering End-to-end Operational Intelligence

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 Enterprise at your data and it immediately starts collecting and indexing so you can start searching and analyzing.

Search and Investigate. Whether you're responsible for running, securing and auditing IT, developing applications or providing analytics to the business, search is the starting point for discovering a new world of possibilities from your data. Splunk Enterprise includes a powerful Search Processing Language (SPL™) simple enough for the beginner and powerful enough for the expert data analyst. 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. Use specific terms or expressions, Boolean operators and powerful statistical and reporting commands.

Add Knowledge. Splunk Enterprise 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 content, add-ons and apps from the Splunk apps website to leverage prepackaged inputs, views and searches for specific use cases, data sources and technologies. Enrich data with information from external asset management databases, configuration management systems and user directories. Define Data Models that describe relationships in the machine data to make it more meaningful and usable.

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 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. Empower every user, from IT to the business, to analyze machine data. Rapidly build advanced charts and dashboards that show important statistical trends. You can start with a Data Model and then use the Pivot interface to create

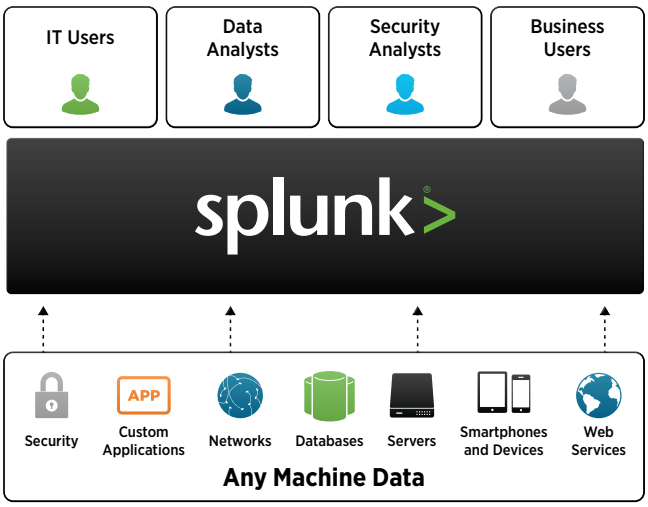

Figure 1: Splunk Enterprise collects machine data from wherever it's generated.

reports and analyze complex machine data with drag-and-drop ease, all without having to learn the search language.

Drill down from anywhere in a chart to the underlying 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 key stakeholders on a schedule or on an ad hoc basis. Splunk Enterprise makes it easier for everyone in your organization to turn machine data into powerful insights.

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 with 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 Splunk apps and other content that extend the power of Splunk Enterprise. Splunk apps deliver a targeted user experience for different roles, use cases and enterprise technologies. There are a growing number of apps built by our community, partners and Splunk. These apps can help you visualize data in new ways or provide pre-defined views of leading technologies such as VMware, Microsoft, Cisco and F5. Visit the Splunk apps website to browse content and apps or to create and post your own.

Enterprise Ready. Splunk Enterprise scales to collect and index tens of terabytes of data per day across multi-geography, multi-datacenter, physical or virtual infrastructures. Out-of-the-box integration with traditional relational databases and new open source data stores drive more value from your data. Because insights from your data are mission critical, clustering provides the high availability you need, even as you scale out your low-cost, distributed computing environment.

Role-based Security. Much of an organization's critical business insights is found in its machine data, which is why Splunk Enterprise provides robust security features, including secure data handling, role-based access controls, auditability and assurance of data integrity. Splunk Enterprise integrates with LDAP-compliant directory services like Microsoft® Active Directory to adhere to enterprise-wide security policies and support single sign-on.

Rich Developer Environment. Enable developers to integrate data and functionality from Splunk Enterprise into applications across the enterprise using software development kits (SDKs) for Java, JavaScript, C#, Python, PHP and Ruby. Developers can also build Splunk apps with custom dashboards, flexible UI components and custom data visualizations using common development languages such as JavaScript, Django and Python.

It's Software. Get Up and Running in Minutes. Download and install Splunk Enterprise on your laptop or server in under five minutes. You'll be up and running with an intuitive web user interface and a powerful enterprise platform for indexing, exploring and analyzing your machine data.

Features	Splunk Free	Splunk Enterprise
Indexing Volume	500MB/day	Unlimited (According to license)
Universal Indexing	•	•
Search	•	•
Distributed Search		•
Monitoring and Alerting		•
Reporting	•	•
Knowledge Mapping	•	•
Dashboards	•	•
Data Model	•	•
Pivot	•	•
High Performance Analytics Store	•	•
Report Acceleration	•	•
PDF Delivery		•
Access Control and Single Sign-On		•
Clustering		•
Cluster Management		•
Universal Forwarder	•	•
Forwarder Management	•	•
Rich Developer Environment	•	•
Splunk Apps	•	•
Premium Apps		•
Standard Support	•	•
Enterprise Support		•

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 6 license 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 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

Item # DS-splunk-121