splunk>

PRODUCT DATA SHEET

Splunk® Enterprise

The Platform for Operational Intelligence

HIGHLIGHTS

- Deliver real-time Operational Intelligence to IT, security and business users
- Identify and resolve issues and reduce costly escalations by up to 90%
- Monitor systems, infrastructure and key performance indicators (KPIs) in real time to identify issues before they impact your business
- Proactively detect and investigate security incidents
- Understand trends, patterns of activity and behavior for customers, transactions and systems

Product Overview

Splunk Enterprise is the industry-leading platform for machine data. Machine data is one of the fastest growing, most complex areas of big data. It's also one of the most valuable, containing a categorical record of user transactions, customer activity, sensor readings, machine behavior, security threats, fraudulent activity and more.

Splunk Enterprise collects all your machine data from wherever it's generated, including physical, virtual and cloud environments (see Figure 1). It enables you to search, monitor and analyze your data from one place in real time. Troubleshoot problems and investigate security incidents in minutes. Monitor your end-to-end infrastructure to avoid service degradation or outages. Gain Operational Intelligence with real-time visibility and critical insights into customer experience, transactions and other key business metrics. Splunk Enterprise is available as a software download or cloud-based service that makes your machine data accessible, usable and valuable across the organization.

Delivering End-to-End Operational Intelligence

Collect and Index Any Machine Data. Using no predefined schema, Splunk Enterprise can collect and index any machine data from virtually any source, format or location in real time. Data streaming from packaged and custom applications, app servers, web servers, databases, wire data from networks, virtual machines, mobile devices, telecoms equipment, operating systems, sensors, mainframes and much more. Simply point Splunk Enterprise at your data and intuitive interfaces guide you through previewing, onboarding and preparing your data, making it more useful for further search and analysis. And for real-time DevOps and IoT data collection, it offers a high-capacity developer-standard HTTP/JSON API and SDKs. Finally, Splunk Enterprise can combine your machine data with data in your relational databases, data warehouses, and Hadoop and NoSQL data stores.

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 Search Processing Language (SPL™) simple enough for beginners and powerful enough for expert data analysts. Search using specific terms or expressions and powerful statistical and reporting commands. Correlate events across multiple data sources to reveal new insights. Automatically detect patterns across massive sets of data. Zoom in and out using a visual timeline to spot trends and spikes. Drill down into results and eliminate noise to find the needle in the haystack. Respond to important events, as they occur, in real time.

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. Use the pivot interface to enable any user to automatically discover relationships in the data and build powerful reports, without mastering the search language. Easily define data models that describe relationships in machine data. Enrich search results with information from external asset management databases, configuration management systems and user directories.

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 IT and business user to analyze machine data. Rapidly build powerful reports and dashboards and view them from your desktop or mobile device. Create PDFs and share them with key stakeholders on a scheduled or ad hoc basis. Embed charts into third-party business applications for broader accessibility. Drill down from anywhere in a chart to the underlying raw events or to another dashboard, form, view or external website. Make it easier for everyone in your organization to turn machine data into powerful insights.

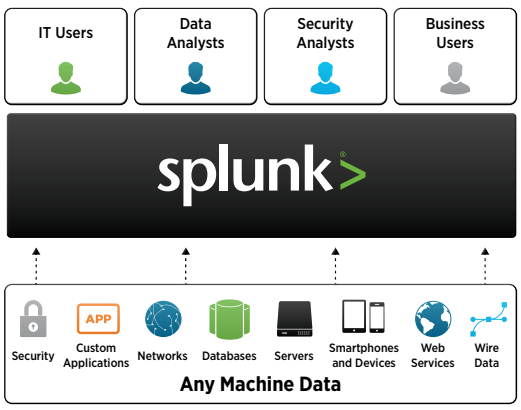

Figure 1: Splunk Enterprise collects machine data from wherever it's generated.

Custom Dashboards and Views. Build custom dashboards that meet the needs of the different users and groups in your organization. Quickly create custom dashboards using shareable panels that integrate multiple charts and views of your real-time data and access them from your desktop or mobile device. Personalize dashboards for different users in your organization—managers, business and security analysts, auditors, developers and operations teams. Users can re-use existing panels and edit dashboards using a simple drag-and-drop interface and can use integrated charting controls to change chart types or views dynamically.

Apps and Add-Ons. Do more by taking advantage of hundreds of apps that extend the power of Splunk Enterprise. Apps deliver a targeted user experience for different roles, use cases and data sources. The Splunkbase library has hundreds of apps and add-ons from Splunk, our partners and our community. With apps and add-ons, you can get powerful results, right out of the box, for most common data sources and user needs.

Splunk Premium Solutions. Splunk Premium Solutions go beyond apps to apply real-time data intelligence to manage your security posture, IT operations and more. These purpose-built solutions extend Splunk Enterprise to monitor your specific environment, offer multilevel views, and provide investigative capabilities and workflows that turn analysis into actions to maintain operational excellence.

Enterprise Ready. Splunk Enterprise scales to collect and index hundreds of terabytes of data per day across multigeography, multidatacenter, physical, virtual or cloud infrastructures. Out-of-the-box integration with traditional relational databases and open source data stores drive more value from your data. You can scale out your computing environment vertically with high capacity systems or horizontally with multiple systems. Use multisite clustering to deliver continuous availability in the event of an outage or disaster. The Distributed Management Console enables you to centrally monitor your enterprise deployment.

Role-Based Security. Much of an organization's critical business insights is found in 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 and SAML 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, HTML5 and Python.

Get up and running in minutes

Splunk Enterprise is available as a free download. Try it on your laptop and then deploy it to your datacenter or cloud environment. Splunk Cloud delivers a software as a service alternative, offering the industry's only 100 percent uptime SLA. Either way, you'll be up and running with an easy-to-use web interface and powerful enterprise platform for analyzing your machine data.

Features	Splunk Free	Splunk Enterprise	Splunk Cloud
Indexing Volume	500MB/day	Unlimited According to license	5GB/day to TB/day According to license
Data Onboarding	•	•	•
HTTP Event Collector	•	•	•
Universal Indexing	•	•	•
Search	•	•	•
Distributed Search		•	
Monitoring and Alerting		•	•
Reporting	•	•	•
Knowledge Mapping	•	•	•
Dashboards	•	•	•
Data Model	•	•	•
Pivot	•	•	•
Event Pattern Detection	•	•	•
High Performance Analytics Store	•	•	•
Report Acceleration	•	•	•
Embedded Reports	•	•	•
PDF Delivery		•	•
Data Integrity Control	•	•	
Mobile Access	•	•	•
Access Control & Single Sign-On		•	•
Single-Site Clustering		•	
Multisite Clustering		•	
Distributed Management Console		•	
Universal Forwarder	•	•	•
Forwarder Management	•	•	•
Rich Developer Environment	•	•	•
Apps	•	•	•
Premium Solutions		•	•
Standard Support	•		
Enterprise Support		•	•

Get Started Today–for Free

Splunk Enterprise. Download Splunk Enterprise for free. You'll get a Splunk Enterprise 6.3 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.

Splunk Cloud. Register for a free trial of Splunk Cloud and get started immediately with Splunk Enterprise delivered as a service.

** As of November 1, 2019, all Splunk products and services will feature term licenses. We will no longer sell any products with perpetual licenses.*

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 splunkbase.splunk.com

Item # DS-splunk-133

Splunk Product Features & Descriptions

Features	Definitions
Indexing Volume	Scales to hundreds of terabytes per day
Data Onboarding	Wizard-based workflow to simplify onboarding of any data source
HTTP Event Collector	Onboards data directly from any application or device using a standard HTTP/JSON API
Universal Indexing	Universal real-time indexing of machine data
Search	Ad hoc search across real-time and historical data
Hybrid Search	Search across multiple Splunk deployments and locations including Splunk Enteprise, Splunk Cloud and Hunk
Monitoring and Alerting	Monitor and alert for individual and correlated real-time events
Reporting	Ad hoc and pre-defined reports across real-time and historical data
Knowledge Mapping	Knowledge mapped to machine data artifacts
Dashboards	Highly customizable and interactive dashboards integrating real-time machine data and charts, reports and tables
Data Model	Used to define consistent relationships in machine data
Pivot	Drag-and-drop UI to explore, manipulate and visualize machine data
Anomaly and Pattern Detection	Automatically discovers patterns, commonalities and anomalies in your data with a single click
High Performance Analytics Store	High performance analytics technology
Report Acceleration	Transparent data summarization technology
Embedded Reports	Embed charts and reports in other third-party business applications external to Splunk Enterprise
PDF Delivery	Scheduled and automated PDF generation and delivery of reports and dashboards
Access Control & Single Sign-On	Integrated role-based access control and user authentication with LDAP directory and single sign-on via SAML
Data Integrity Control	Ensures security and compliance by detecting if indexed data has been compromised
Mobile Access	Delivers Splunk dashboards, reports and more to mobile devices
Single-Site Clustering	High availability architecture for machine data availability in a single site deployment
Multisite Clustering	High availability architecture for disaster recovery in a multisite deployment
Distributed Management Console	Centrally manage the health and performance of distributed Splunk deployments
Universal Forwarder	Forwarding of data securely and reliably from remote systems in real time
Forwarder Management	UI for monitoring and deploying forwarder configurations
Rich Developer Environment	Developer platform for building enterprise apps that leverage Splunk software with modern web languages
Apps and Add-Ons	Access to hundreds of partner, community and Splunk Apps from splunkbase.splunk.com
Premium Solutions	Packaged applications to manage your security posture, IT operations and more
Standard Support	Access full product documentation, Splunk Apps, Splunk Answers and IRC channel
Enterprise Support	Direct access to Splunk customer support, ability to manage cases online, tailored support levels

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 splunkbase.splunk.com

Item # DS-splunk-133