Splunk 4

The data needed to manage, secure and audit IT is locked in silos.
Existing tools and manual methods are slow, costly and don't scale.

The Next Generation of IT Search

When it comes to troubleshooting application issues, managing your IT infrastructure and meeting security and compliance mandates, the data you need is locked in silos of people and technology across your organization. Using existing tools and manually sifting through siloed data is time-consuming, costly and doesn't scale.

Back in 2006 Splunk introduced IT Search as a new and better way to open up these silos. Users were amazed with how Splunk let them search and analyze all their IT data from a single location in real time. They started to see dramatic results, solving problems in minutes that used to take them hours or days. For many, Splunk soon became indispensable. And they wanted more: more speed and scalability for massive datasets, manageability for global deployments, custom dashboards designed for users across the enterprise, more use capabilities, more Splunk.

Splunk 4 is the result of passionate user feedback. With over 1,800 enhancements, **Splunk 4** includes 50+ new features that are helping to transform the award-winning IT Search engine beyond a useful tool into the enterprise standard for IT visibility and insight. **Splunk 4** is next generation IT Search.

Product Overview

Splunk 4 takes all the strengths of the past release and supercharges them for wider enterprise adoption and scale. Significant advances include: **speed and scale** - 10x faster search and 2x faster indexing - index hundreds of gigabytes per day on a single commodity server; **usability** - create custom dashboards and provide views for any role in the business, well beyond the traditional technical Splunk user; **manageability** - centrally deploy, manage and monitor Splunk servers, or delegate management to departments and users; **apps** - build and deploy IT Apps powered by the Splunk Engine.

Splunk 4 Capabilities

Index Any IT Data

Splunk Universal Indexing lets users index any IT data, from any source, in real time. Point your servers or network devices' syslog at Splunk, set up WMI polling, monitor any live logfiles, enable change monitoring on your filesystem or the Windows registry, schedule a script to grab system metrics and more. No matter how you get the data, or the format, Splunk will index it the same way - without custom parsers or adapters to write or maintain. **Splunk 4** delivers an order of magnitude improvement in indexing speed. No product for searching IT data delivers this kind of speed and flexibility. Period.

Search and Investigate Anything

Once indexed, you can search for anything in your IT data. Don't know what you're looking for? Just start typing and the **Splunk 4** Search Assistant will offer typeahead suggestions based on what's in your data. You'll also see suggested searches based on your search history and contextual help so that you can leverage the full power of the Splunk search language. You can use familiar Boolean operators, wildcards and quoted strings, or search on a particular field like a user name, an IP address or a particular message ID. With **Splunk 4** search is ten times faster, providing the ability to search billions of events in seconds, getting you the results you need quickly.

Splunk also lets you interact with your search results. Zoom in and out on a time line of your results to quickly reveal trends, spikes and anomalies. Click to drill down into your results to get to the needle in the haystack. Whether you're troubleshooting a customer problem or investigating a security alert, **Splunk 4** will get you to the answer in seconds or minutes rather than hours or days.

Add Knowledge

Splunk 4 automatically extracts knowledge from your IT data to help you better harness that information. You can also add your own knowledge on-the-fly to enrich the IT data further and make the system smarter for all users - especially non-technical users. This includes knowledge about events, fields, transactions, patterns and statistics, allowing you to identify, name and tag fields. In addition, **Splunk 4** lets you enrich your IT data with information from external asset management databases, configuration management systems and user directories providing added context and depth.

Monitor and Alert Proactively

With **Splunk 4** any search can be saved, shared and scheduled for continual monitoring and can trigger alerts via email or RSS. You can even kick off a script to take remedial actions, send an SNMP trap to your system management console or generate a ticket at a service desk. Alerts can be based on a variety of threshold and trend-based conditions. And **Splunk 4** improvements to the search language let you go beyond simple Boolean searches into fielded searches, statistical searches and sub-searches; you can correlate on anything you want and alert on complex patterns such as abandoned shopping carts, brute force attacks and fraud scenarios.

Report and Analyze On-the-fly

If you've ever wanted to generate a report on-the-fly, you'll love Splunk. The **Splunk 4** Report Builder helps you easily build advanced graphs and charts and visualize important trends, see highs and lows, summarize top values and report on the most and least frequent types of conditions. You can create robust, information-rich reports from scratch without an advanced knowledge of search commands. You can save reports, integrate them into dashboards and share them with colleagues in secure, read-only formats such as PDF.

Create Custom Dashboards

The **Splunk 4** dashboard editor lets you create dashboards in less than five clicks. Create custom dashboards in minutes to automatically monitor the information most relevant to your role. Easily create custom dashboards for management, security analysts, auditors, developers and sysadmins.

Build and Deploy IT Apps

Apps let you do even more with Splunk. **Splunk 4** makes it easy for customers, partners and the community to innovate on Splunk and build, package and deploy their own Apps. You can also add Apps directly from Splunk for different platforms, such as Windows, Linux and Unix; for different use cases, such as for security, PCI compliance and change monitoring. Once installed, you can easily apply role-based access controls launch Apps from the App launcher screen.

Scale from Single Server to Datacenter

Splunk scales from a single commodity server to the largest infrastructures with multiple datacenters and geographies. We've invested 18 months perfecting the **Splunk 4** architecture so it can massively scale to multi-terabytes of IT data per day. When you needs grow you can easily add more index servers to scale your deployment. Users can see all these servers as a single logical datastore thanks to distributed search.

Secure Data Access and Archiving

Once your IT data is indexed, you're in control of it. Integrate with LDAP and AD and map groups to Splunk roles. Filter what data users see by role. Set up an archiving policy based on datastore size or age. And because all the data needed to troubleshoot, investigate security incidents and demonstrate compliance is persisted in Splunk, you can restrict access on sensitive production servers.

It's Software. Download and Install It in Minutes.

Splunk is a self-contained software package that runs on all the leading operating systems. Just pick your platform, download and install. You're up and running with a Web interface for users and a datastore to index your data.

Free Download

The free download automatically includes all the Splunk 4 Enterprise features for 60 days and lets users index 500MB of data per day. After 60 days, or anytime before then, users can convert to a Splunk 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	✓	✓
Ad-hoc search and investigation	✓	✓
Reporting	✓	✓
Knowledge mapping	✓	✓
Personal dashboards	✓	✓
Enterprise dashboards		✓
Monitoring and alerting		✓
Distributed deployments		✓
Forwarding and receiving	✓	✓
Access controls		✓
Developer APIs	✓	✓
Works with Free Apps	✓	✓
Works with Splunk and Partner Apps		✓
Community 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 !

- **Free Splunk 4 Download:** www.splunk.com/download