

Splunk for Business Analytics

Harness Your IT Data to Gain Valuable Real-time Insight for IT and the Business

The IT Data Opportunity

Business intelligence tools and data warehouses have a long history of giving businesses the information they need to optimize their operations and make critical decisions. They are designed with specific questions in mind and are defined by database schemas, business rules, industry standards, laws and regulations.

Now a new class of data is being generated by a huge array of sources such as web servers, machines and systems of all types. This machine-generated IT data includes click streams, call logs, social media, RSS feeds, GPS readings, weather data, fleet locators and more. It contains a definitive record of all customer behavior, user transactions, machine behavior, security threats, fraudulent activities and much more.

This data is an incredibly valuable resource but organizations rarely get the value they need from it. Existing business intelligence tools and data warehouses are simply not engineered to handle this type of high-volume, variable and dynamic data.

Splunk and Operational Intelligence

Splunk Enterprise is a massively scalable data engine for machine-generated data. It collects, indexes and harnesses IT data across your infrastructure in real time. Splunk has the unique ability to make sense of virtually all types of machine data. Whether it is structured or unstructured data, Splunk can mash it up with other business data for complete real-time visibility and Operational Intelligence. From your customer behavior and usage statistics to security readiness and operational analytics, Splunk makes IT data accessible, usable and valuable and provides new levels of visibility and insight for IT and the business.

Use Splunk and your IT data to make better-informed business decisions—understand trends, patterns and gain Operational Intelligence. Monitor the success of new online services in real time, reconcile third-party service provider fees against actual use, find your heaviest users and heaviest abusers and more. Your IT data captures virtually every behavior, so the possibilities are game changing. With Splunk you can get this intelligence dramatically faster—measured in just hours or days instead of many months.

Splunk delivers a real-time understanding of what is happening and deep analysis of what has happened across your organization.

The following unique capabilities of Splunk are fundamental to harnessing your IT data:

- Real-time visibility—search, correlate and monitor live events in real time as they occur across your IT environment.
- High-performance search and navigation—find what you're looking for anywhere in your environment quickly and easily. Search across billions of events in seconds on a single commodity server. Splunk scales to the largest of data volumes.
- Powerful historical analytics—analyze important trends, statistics and metrics about nearly any aspect of behavior. Custom dashboards help you to analyze the behavior of your customers, users, transactions, applications, web servers, app servers and networks.

Splunk captures a full scope of your IT data so you can focus on what's important. Here are but a few examples of how customers are using Splunk to gain unprecedented visibility and insight for your organization.

Revenue Optimization

Splunk has the unique ability to make sense of machine data and combine it with other traditional business data. A leading US-based flat rate wireless provider with 6.6 million subscribers deployed Splunk to provide better intelligence on wireless usage and revenue per user and to also optimize their partner carrier charges. Since their customers were charged a flat rate fee per month, determining the lowest-cost route for calls, translated directly to higher margins and profits. Before Splunk, they evaluated a number of conventional packaged solutions, all of which were costly and required 6 months or more to implement.

Using Splunk they began gathering data immediately and deployed their entire solution in a few weeks. Now they use Splunk to combine call duration in the CDR with their tariff database to report on revenue per user. Splunk also calculates the best rate and most cost-effective telecoms partner. This makes it easy to ensure that lowest-cost partners are being used in all cases.

Comprehensive Web Analytics

Splunk requires no instrumentation, lets you analyze real-time and historical data and creates dashboards and views quickly so you can visualize your data.

A large US-based public media company with nearly 10 million online subscribers had no way to measure the popularity of their streaming web programs. The company needed to answer questions like: “When were different assets streamed?” and “How many were concurrent?” They deployed Splunk and achieved comprehensive visibility and intelligence beyond just their websites. For the first time they were able to gain a deeper understanding of their assets and reconcile their royalty payments and measure their abandonment rates.



“After 6 months of effort with a leading web analytics company, we turned to Splunk to give us the business reports about our web-based digital assets that we needed.”

Sondra Russell

Sr. Digital Analyst, National Public Radio

Trending Analysis

Edmunds Inc. publishes four websites that empower, engage and educate automotive consumers, enthusiasts and insiders. They were however spending way too much effort on disparate analysis and not enough answering questions that could impact the business. They had limited visibility across their website properties. Each property included its own tools, great for single point analysis, but lacking a holistic view. Edmunds deployed Splunk to deliver operational insights for investigating root cause analysis and to enhance troubleshooting. They now also use Splunk and their IT data to analyze longer-term trends and capture and identify new customer behavior.



“Our Splunk dashboards provide both real-time and historical trending data we use to make the decisions that impact revenue.”

John Martin

Senior Director, Application Operations

End-to-end Visibility

Splunk was developed to solve a major IT data problem and provide end-to-end visibility across the entire IT environment—including all the systems that run the business and drive customer experience. The team at Macy’s.com manages some of the world’s highest-grossing retail websites, with online sales in excess of \$1/billion per year. After experiencing outages for 6 consecutive holiday seasons Macy’s turned to Splunk.



“The money we’ve spent on licensing Splunk, we’ve captured back over and over again. We’ll spend two or three minutes using Splunk, versus five or six hours before.”

Camille Bali,

Senior Analyst, Architecture Team

Macy’s subsequently achieved end-to-end real-time visibility across their online properties and delivered a premier customer experience—including the speed and availability of purchasing transactions. Not only has Macy’s seen no holiday downtime since introducing Splunk (in spite of a 50% increase in site traffic), they can provide new levels of operational visibility for IT and the business.

The world’s largest telecoms, social networking companies, retailers and banks rely on Splunk and their machine-generated IT data to move their businesses forward. Web analytics drives new business offerings. Click-stream analysis and user behaviors impacts product design. Fraud detection and abuse monitoring protects the business. Trending reports and data drill-down capabilities help them to optimize their IT infrastructure performance.

Splunk makes your IT data accessible, useful and valuable to everyone in your organization. Use Splunk to provide real-time insights into the trends and behaviors of your customers, services and systems.

Splunk Capabilities

Index All Types of Data Formats: Splunk indexes virtually any data and data format across your infrastructure in real time.

Ad hoc Search and Investigate: Search terabytes of historical data and live streaming data using the powerful Splunk search language.

Monitor and Alert: Monitor your data for patterns, breakout trends or specific events and turn these into proactive alerts.

Report and Analysis: Build powerful reports in minutes, visualize your data, perform statistical analysis, spot trends and share your reports.

Custom Dashboards: Create custom dashboards in a few clicks, integrate multiple charts and views of your data for needs of different users.

Advanced Visualization: Integrate maps and more complex visualizations within Splunk dashboards.

Role-based Access: Provide secure, role-based access controls to anyone in your organization.

External Lookups: Enrich your results by performing lookups to external databases and other systems.

Massive, Linear Scalability: Scale Splunk linearly across commodity servers to support the largest of data volumes.

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. 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.