

# Splunk for IT Operations

Get End-to-end Visibility Across the IT Infrastructure to Find and Fix Problems Faster

## Rising Complexity Impacts IT and the Business

Today's datacenter has evolved. It's become a very complex, layered group of siloed and interconnected technologies working in an environment without boundaries. When problems arise, finding the root cause or gaining visibility across the infrastructure to proactively identify and prevent outages is nearly impossible. Meanwhile, virtualization and cloud infrastructures introduce additional complexity and create an environment that is more difficult to control and manage.

## The Old Way

Traditional tools for managing and monitoring IT infrastructures are out of step with the constant change that is happening in today's datacenters. These systems are inflexible, cost too much and are not architected for the complexity of today's environments. Designed for a single function in IT, they do not work across multiple technologies to help solve problems. Further, their monitoring approaches are often based on filtering and summarizing. When problems arise they typically lack the ability to drill down and provide granular analysis of IT data.

Difficulties in getting access to the system data adds to the problem. Developer teams responsible for finding and fixing issues require secure access to system data. Getting them the proper security access can be a time consuming and manual task.

Linking the various causes of performance issues and outages is extremely challenging because traditional tools are siloed and can't access and analyze all the relevant events across the IT landscape.

## The Splunk Way

Splunk Enterprise is a highly versatile and scalable data engine for the machine data generated by your IT infrastructure. It collects, indexes and harnesses live data generated from virtually any source, format or location including your packaged and custom applications, app servers, web servers, databases, networks, virtual machines, hypervisors, operating systems and more—without requiring custom parsers, adapters or a database on the backend.

Use Splunk to gain operational visibility into the layers of your environment. Turn the silos of machine data generated in your datacenter into integrated and actionable information. Reduce your mean-time-to-investigate (MTTI) and mean-time-to-recovery (MTTR) and keep your critical services running. Find and fix problems faster than ever before.

Proactively monitor key IT KPIs and end-to-end service levels to detect anomalies and prevent problems in real time. Get instant drilldown into highly granular source data without needing to access individual servers or devices.

Use Splunk's role-based access controls to provide access to the data without compromising your production systems. Provide the Tier 1 service desk with secure views into your data so they can diagnose and resolve issues.

Use Splunk to examine data and to correlate issues relating to the performance or availability of services across all tiers of your information architecture. Monitor your environment for changes that could cause security or operational issues. Combine real-time data analysis with terabytes of historical data correlation to detect patterns that can help predict and prevent issues and outages.

Splunk runs in physical, virtual and cloud infrastructures and scales from a single server to the largest distributed environments. Regardless of the deployment, Splunk helps reduce monitoring costs and downtime and supports strategic initiatives such as datacenter optimization and tool consolidation.

## Using Splunk for IT Operations

### Applications

Complex distributed applications can introduce many points of failure. Problems are hard to find and fix, delaying incident response and creating costly escalations. Application developers and administrators don't have direct access to the machine data they need. Splunk enables rapid problem investigation from a central location. Splunk also provides developers access to the data they need and offers rapid problem resolution.



**"Thanks to Splunk, our application issues are identified and resolved before they become problems that affect our systems, transactions and customers."**

Robert Reilly, Sr. Manager Systems Engineer,  
FreshDirect

### Virtualization

Virtualization brings more complexity and dynamic behavior to an already challenging IT landscape. Guest sessions fight for resources on the same physical hosts and system performance can be unpredictable. Existing management tools can't keep up.

Splunk provides visibility across the virtual stack. Search transactions spanning virtual and physical components from one place; get fast event correlation across virtual and physical resources. Splunk brings it all together for root cause analysis, security and compliance investigations.



**“Splunk delivers critical visibility of our virtual infrastructure, helping diagnose when things go wrong!”**

Joseph Rinckey, VMware Systems Engineer  
Leading Managed Healthcare Provider

## Service Desk

Tier 1 service desk teams are the first to know of issues but existing tools provide them limited information to diagnose and pinpoint root cause. Splunk empowers your service desk with secure access to pertinent data across your infrastructure, significantly reducing escalations.

The Splunk customizable interface and integration with Active Directory gives role-based access to support professionals as well as developers. This enables a faster root cause analysis and resolution while still maintaining compliance.



**“Splunk reduced our escalations by 90% and our problem resolution time by 67%. ”**

Paulo Carvalho, Director Operations, Vodafone

## Monitor Cloud Environments

The rise of hybrid infrastructures have presented IT organizations with another new challenge—accountability for infrastructures outside of their direct control. With its ability to universally index data from virtually any source or format, Splunk enables visibility into hybrid environments, regardless of the cloud provider.

In addition to providing operational visibility into cloud environments, Splunk can uncover additional insights such as customer usage, asset utilization and capacity planning, which support decisions around vendor pricing, account management and operational planning.



**“Our high performance cloud computing offering has Splunk integrated from the ground up. It is the go-to solution for every type of question – it helps in decision making at every level from DevOps to account management, product management and pricing.”**

Principal Engineer, RiskMetrics Group

## Messaging Systems

The complexity of messaging systems is massive. From tracing email messages and troubleshooting delivery problems, to managing compliance and analyzing spam and phishing attacks; the infrastructure is complex and resource intensive. Splunk helps you search messaging transactions in real time across your infrastructure.



**“Splunk empowers our frontline IT staff to instantly trace the path of lost messages across our Sendmail and Exchange infrastructures. ”**

Yonas Hambissa, System Administrator, Interwoven

## Servers

Server management costs are being driven sky high. Central server management is challenging, requiring many agents to grab data from the same server. Identifying and diagnosing server problems involves direct access and interfering with running systems.

Splunk integrates logs, configurations, messages, traps and metrics all in one place. Search, alert and report across your servers in seconds—troubleshoot problems, outages and chronic failures quickly. Integrate Splunk with existing server monitoring and provisioning tools for one-click granular data analysis.



**“Splunk cuts down on the time to identify and investigate our server problems and outages by providing central access to all our IT data from a single interface.”**

Andre Kocher, Sr. Systems Engineer,  
Swiss Post Finance

## Networks

In today's converged network infrastructures many network issues go undetected until it's too late. Errors and warnings that are buried in logs are often ignored or overlooked because it is too difficult to keep track of all the data. Writing a script to analyze raw data is difficult and brittle as verbosity levels and data formats change.

Splunk lets you search, alert and report on network in real time on network events and transactions across the complete network stack. Navigate from symptom to root cause quickly with syslog, SNMP trap, configuration and netflow data all in one place. Find early warning signs of problems that go undetected with component monitoring and integrate Splunk into existing network monitoring consoles for one-click investigations.



**“Splunk gives our customer service, NOC staff and network engineers comprehensive real-time event data for incident response, chronic problem identification and optimization.”**

Dave McCallum, Network Platform Architect,  
BT Design

## 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](mailto:sales@splunk.com).