

# Splunk® for Windows®

End-to-End Real-time Visibility of Your Windows Environment

## HIGHLIGHTS

- Monitor key Microsoft workloads and applications in real time
- Identify and resolve issues faster and greatly reduce costly escalations
- Manage your heterogeneous Windows, Unix and Linux environments with a single, integrated console
- Deploy on an extendable platform that covers the full Microsoft install base

Microsoft Windows environments are a complex but crucial component of an IT organization's infrastructure. When you add heterogeneous connectivity to Linux- and Unix-based systems and factor in virtualized and cloud-based instances, you have a mission critical infrastructure that runs a business, yet this infrastructure poses a significant management challenge. To proactively manage these systems, IT organizations need information about their environment, from operating systems running onsite to applications in the cloud. The information organization need to make decisions and manage their infrastructure can be found in the machine data generated by servers, applications and network devices. By monitoring and analyzing everything from clickstreams and transactions to network activity and application source data, Splunk software turns machine data into valuable real-time insights you need to make informed decisions.

## Product Overview

Splunk is the engine for machine data. It collects, indexes and harnesses the machine data generated by all your Windows Server systems and Microsoft infrastructure—physical, virtual and in the cloud. Machine data is one of the fastest growing, most complex segments of data in your organization. It's also one of the most valuable, containing a definitive record of user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. Splunk for Windows collects machine data securely and reliably from wherever it's generated. It stores and indexes the data in real time in a centralized location and protects it with role-based access controls. Splunk lets you search, monitor, report and analyze your real-time and historical data. Now you have the ability to quickly visualize and share your data, no matter how unstructured, large or diverse it may be. Troubleshoot

application problems and investigate security incidents in minutes instead of hours or days, avoid service degradation or outages, deliver compliance at lower cost and gain new business insights. With Splunk you can gain rapid visibility, insights and intelligence for IT and business.

Use Splunk software and monitor your entire Windows infrastructure from one place in real-time—from operating system environment to business critical application.

## Splunk Features for Windows

Splunk provides several specialized features to monitor Windows data, including:

- **Windows Event Logs:** Monitor logs generated by the Windows Event Log service on any event log channel that is available on a machine
- **Performance monitoring:** Collect performance data on Windows machines with Splunk software and then alert or report on that data. Any performance counter that is available in Performance Monitor is also available to Splunk
- **Remote monitoring over WMI:** Use WMI to access event log and performance data on remote machines.
- **Registry monitoring:** Monitor changes to the local Windows Registry using Splunk's built-in registry monitoring capabilities
- **Active Directory monitoring:** Audit any changes to the Active Directory, including changes to user, group, machine and group policy objects

## Splunk Apps for Windows

Splunk software is an enterprise platform that allows you to scale to meet the demands of the business. With supported App extensions that cover the full install base of a Windows Server infrastructure, Splunk Apps for Windows deliver a defined user experience with pre-built dashboards and views that extend the Splunk-for-Windows experience, delivering deeper insight to key workloads.

## Splunk Apps for the Microsoft Windows Infrastructure

### Security

The Splunk App for Enterprise Security supports SIEM capabilities and watches for known threats and monitors key security metrics.

## Virtualization (BETA)

The Splunk App for VMware collects and harnesses data from the virtualization layer to enable true end-to-end visibility in virtualized environments.

## Web Traffic

Splunk App for Web Intelligence provides insight into your web traffic for both IT and business. Use it to track real-time visitor metrics, perform ad hoc analyses on your data and view historical trending and reporting.

## Infrastructure

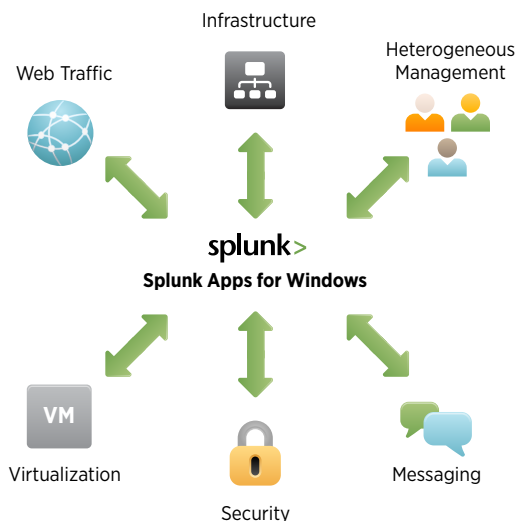
The Splunk App for Windows provides pre-built data inputs, searches, reports, alerts and dashboards for Windows server and desktop management that allow you to monitor, manage and troubleshoot Windows operating systems.

## Heterogeneous Management

The Splunk App for Unix and Linux provides pre-built data inputs, searches, reports, alerts and dashboards for Linux and Unix management that allow you to monitor, manage and troubleshoot \*nix operating systems.

## Messaging

The Splunk App for Microsoft Exchange consumes logs from your Microsoft Exchange systems to give you deep visibility into the health and performance of your Microsoft Exchange environment, from Edge and Hub Transport servers to the Client Access servers and the Mailbox Store itself.



## Dashboard View of the Splunk App for Microsoft Exchange

Splunk Apps for Windows are developed by and supported by Splunk. To extend the platform further, apps created by Splunk partners and the Splunk user community are available to extend Splunk on Windows further to deliver a complete end-to-end solution.

## Splunk Partner and Community App Examples

<b>Security</b>	Window Security Operations Center
<b>Networking</b>	Splunk App for F5 Networks
<b>VDI</b>	Splunk App for Xen Desktops
<b>Identity</b>	Splunk App for Centrify Insight
<b>Database</b>	Oracle Audit Trail
<b>Management</b>	Systems Center Operations Manager Integration

**It's Software; Download it and Install it in Minutes.** Splunk is enterprise software made easy. Try Splunk on your laptop and then deploy it to one or more datacenters. You're up and running with a web interface for users and a powerful engine for indexing your machine data.

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Unlimited (based on license)
Universal, real-time indexing	•	•
Real-time and historical search	•	•
Reporting	•	•
Knowledge mapping	•	•
Dashboards	•	•
Monitoring and alerting		•
Distributed search		•
Data forwarding and receiving	•	•
Role-based access controls		•
Single sign-on		•
Developer APIs	•	•
Community Apps	•	•
Enterprise Apps		•
Standard support	•	
Enterprise support		•

## 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. You can convert to a perpetual Free license or purchase an Enterprise license by contacting [sales@splunk.com](mailto:sales@splunk.com).