

# Splunk App for Citrix NetScaler with AppFlow

Enhanced Visibility and Analytics for Application Performance and Security

## Citrix® NetScaler

Citrix NetScaler makes apps and cloud-based services run five times better by offloading app and database servers, accelerating app and service performance and integrating security. Deployed in front of web and database servers, NetScaler combines high-speed load balancing and content switching, data compression, content caching, SSL acceleration, network optimization, application visibility and application security on a single, comprehensive platform.

## Solving the Customer Experience Riddle with AppFlow

As more and more business becomes web-based, monitoring speed, latency and response times of web applications becomes a critical customer service metric. New to Citrix NetScaler version 9.3, AppFlow is an open standard that extends the Internet Protocol Flow Information eXport (IPFIX) format with application transaction flow data. With the addition of AppFlow, Netscaler solves an important problem of connecting application transactions to the underlying network without the use of costly taps or span ports. AppFlow is inherently cloud-ready since virtualized infrastructure such as the NetScaler VPX can generate this flow data as part of normal operations.

Similar to conventional flow data, AppFlow provides visibility at the transaction level for HTTP, SSL, TCP, and SSL\_TCP flows. This data can provide valuable visibility into user experience, latency and response times as user data traverses client and server for web-based transactions.

AppFlow records contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of flow, packet and byte counts. AppFlow records also contain application-level information, such as HTTP URLs, HTTP request methods and response status codes, server response times and latency.

Once AppFlow data is harnessed, it can be used to:

- Identify bottlenecks in user experience for online transactions
- Detect transaction time SLA violations proactively to prevent large scale issues from impacting users
- Identify how changes to the environment impact the application
- Identifying whether performance issues are client side or server side
- Point in time Top-N reports (a-la Unix top) for hot URLs, netblocks, servers, etc.
- Monitoring client server activities for attacks at the HTTP protocol level such as slow denial of service attacks (Slow DoS)
- Monitoring abnormal client-server behavior based on packet counts, byte counts and server response times

## Why Splunk?

Splunk Enterprise is the scalable and versatile data engine for IT with a unique approach to solving difficult problems in complex application environments. Splunk collects, indexes and harnesses the power of your machine-generated IT data from virtually every component of your large scale, multi-tiered application infrastructure.

Using Splunk's central console, you can not only gain deep visibility across your entire application environment, you can also utilize untapped operational data to enrich business level decision making.

Splunk integrates data from technology across the IT infrastructure, including data from applications, servers, network devices, firewalls, load balancers, virtualization layers and operating systems to provide cross-tier visibility. Splunk's powerful search language and statistical analysis commands link events or transactions across technology tiers, allowing you to understand real service levels, detect anomalies and deliver actual service-level reporting. Splunk customers gain the ability to trace transactions across a heterogeneous infrastructure in seconds, dramatically improving customer service.

## Splunk App for NetScaler

Splunk can index and harness any text data. The Splunk App for NetScaler with AppFlow translates binary AppFlow data to time-stamped ASCII text, so Splunk can utilize it and put it in context of all other data in the environment such as custom application log data, logs and metrics data of application components such as web servers, application servers, databases, firewalls, hypervisors and more. With added visibility into NetScaler and Appflow data, systems administrators and application support professionals are able to get central visibility into their entire environment and are able to correctly identify performance bottlenecks that lead to user experience issues. In addition to being able to detect and troubleshoot application performance issues faster, administrators can also visualize baselines, trends and other analytics that can help them plan capacity and make transactions more efficient for a better customer experience.

Splunk's powerful visualization provides real-time views and role-appropriate dashboards on the state of key application performance and availability metrics. The flexibility and universality of Splunk allows you to put your operational data in a business context to allow richer, more informed business decision making. It also allows you to integrate in non-IT data to provide value added analysis that support the organization's business objectives.

## Splunk App for NetScaler with AppFlow— Dashboards and Reports

The Splunk App for NetScaler with AppFlow contains over 30 reports for situational awareness and dashboards supporting key business and security performance indicators (KPIs). Key reports available include:

**HTTP user agents:** shows you which platforms are most commonly used to access your web application

**Most requested URLs:** allows you to prioritize your response time optimization

**Source and destination IPs and ports:** gives you real time insight into the origins of your traffic

**Average transaction times and round trip response times:** allows you to monitor end user service levels

**Traffic analysis by applications/servers:** includes analysis of latencies and bandwidth usage

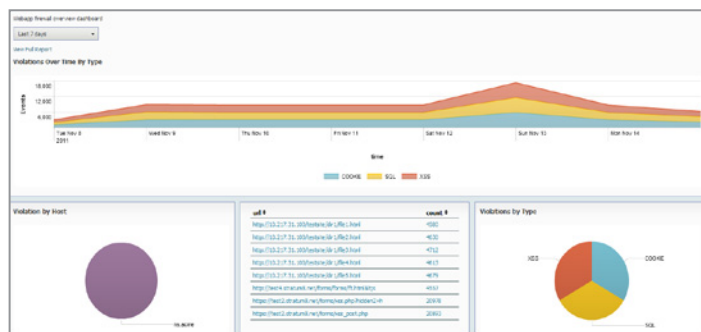
**Load balancing dashboard:** provides views of total bytes transferred by source destination and protocol

**Web application firewall dashboard:** shows violations by type over time, violations by IP address and the URL of the web page attacked.

**SSL-VPN dashboard Critical Statistics dashboard:** indicates the number of HTTP transactions URI, virtual server, user and host trended over time.

**System Audit dashboard:** depicts system console events and tracking commands/changes by user.

Reports from Splunk can be downloaded in PDF or Excel format and data ranges are fully supported. Reports can also be scheduled for delivery to individuals as PDFs. The Splunk App for Citrix NetScaler supports core Splunk functionality such as the ability to drill-down into raw log data from graphical elements and robust role-based access control.



### 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).