

# Splunk App for Palo Alto Networks

Maximizing Network and Application Security, Visibility and Control

## Palo Alto Networks

Palo Alto Networks next-generation firewalls enhance network security and enable enterprises to look beyond IP addresses and packets. These innovative firewalls let you see and control applications, user behaviors and content using three unique identification technologies: App-ID, User-ID, and Content-ID. The Palo Alto identification technologies enable you to create business-relevant and application-based security policies. This approach goes beyond the traditional “all-or-nothing” method offered by traditional port-blocking firewalls used in many security infrastructures.

Palo Alto firewalls integrate IPS and firewall capabilities and use signature heuristics to identify particular application risks and threats. They also integrate with LDAP or Active Directory and can dynamically link IP addresses to users and groups accessing your network.

## Why Splunk for Palo Alto?

Splunk Enterprise offers Palo Alto firewall users a massively scalable real-time IT data engine. The Splunk App for Palo Alto Networks gives you pre-defined content with key performance indicators (KPIs) and long-term trending. In addition to robust reporting, Splunk supports the collection of terabytes of data per day in real time.

Splunk extends Palo Alto’s situational awareness capabilities with real-time continuous monitoring and trending. While Palo Alto can detect users that are running peer-to-peer applications that add security risk to the enterprise, Splunk can monitor for repeat offenders. Using Palo Alto data, Splunk can be set for a specific risk threshold and monitor for variances based on time-of-day, day-of-the week or over a year’s worth of data. Palo Alto’s URL filtering capabilities are enhanced by Splunk’s ability to perform long-term trending and provide business-level reports as needed. Human resource departments, for example, can leverage these reports to track security compliance.

Splunk’s ability to accept multi-line application data can help to define the difference between a misconfigured application behaving like a malicious application or a real security threat. Security administrators can drill down into Palo Alto data in one or two clicks. This enables security teams to investigate incidents in minutes instead of hours or days. Security-relevant data can be searched and analyzed from one place—catching attackers and malicious insiders who may have previously gone undetected. Splunk can be deployed without requiring custom parsers or connectors and the Splunk for Palo Alto content and app are available at no additional cost. You can extend this Splunk app by creating your own dashboards, visualizations and alerts to match the specific use case as needed.

Splunk provides additional context for Palo Alto data through the use of its “look-up” feature. This feature allows Splunk to communicate with asset databases to collect and add additional context to dashboards and reports containing Palo Alto data.

## Palo Alto Next-Generation Firewall & Splunk

The App Splunk for Palo Alto Networks app delivers advanced security reporting and analysis. Security analysts, network administrators and architects can now leverage application and user visibility at an unprecedented scale and rate.

The following visualizations and reports are available in this version of the Splunk App for Palo Alto Networks. Each visualization or report can be clicked on to drill down into the Palo Alto data fueling the dashboard graphic.

### Threat Dashboard

Assess security threats quickly via the Threat Dashboard. Out-of-the box visualizations and reports include:

**Threats over Time by Subtype:** monitors and tracks real-time or historic data from Palo Alto by threat sub-type. You can view threats by sub-type, vulnerability, virus or Spyware

**Threats over Time by Risk:** monitors and tracks real-time or historic data from Palo Alto using Palo Alto’s risk scoring data for risk trending

**Top Threat IDs:** uses Splunk’s look-up capability to show the actual or “plain English” meaning of a threat ID. It displays the ID number along with how many times the threat has been seen by the firewall

**Threats by Application:** shows which applications are being seen by Palo Alto as a threat

**Threats by Destination Category:** indicates which business category of hosts is being threatened

**Top Source IP:** shows the top source IPs by the number of attempts to access the network

**Threats by Severity:** uses Palo Alto threat category classifications to graphically represent the number threats seen by application

**Top Destination IP:** shows the top destination IPs by the number of attempts

## Traffic Statistics Dashboard

Assess network traffic statistics at a glance with the Traffic Statistics Dashboard, which includes the following reports:

**Bytes Transferred over Time:** watches for spikes in traffic and allows for drill-down into specific time periods to view anomalous behavior

**Top App by Bytes Transferred:** records the app transferring the most data in or out of the network

**Top App by Request:** monitors the use of app requests and classifies them using Palo Alto categories

**Top Source IP:** presents a view of inbound traffic by IP address

**Top Destination Port:** presents a view of the traffic through the firewall by common port.number

**Top Destination IP:** indicates what IPs are being accessed outside of the network

**Top Destination User:** indicates which users are making the most connections to an external website

## 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).