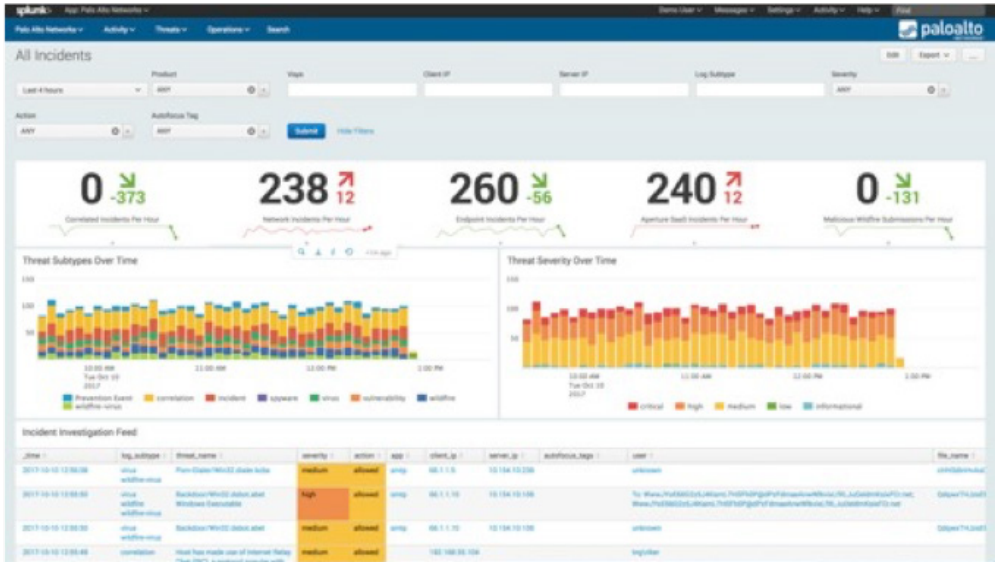
AT A GLANCE
PALO ALTO NETWORKS AND SPLUNK PARTNERSHIP

Palo Alto Networks® and Splunk® have partnered to deliver innovation to customers by pioneering bidirectional integration that protects critical resources and prevents successful attacks. The Palo Alto Networks Security Operating Platform fuels the Splunk data engine with invaluable network and endpoint traffic data, including details of the applications, users, content and threats responsible for and contained within each session. This serves to increase visibility and improve Splunk's analysis results.

The integrated offering combines several approaches for identifying advanced threats, including static and dynamic sandbox analysis, statistical anomaly detection, and infrastructure-wide event correlation, in addition to enabling administrators to expedite incident response through automated blocking of malicious sources and quarantine of compromised devices.



Key Benefits of the Partnership

- 4,000 customers and more than 40,000 downloads
- Advanced analytics and reporting with Palo Alto Networks app for Splunk
- Unique, rich data on applications, users and more from Palo Alto Networks
- Security Operating Platform integrated with Splunk Adaptive Response
- Top downloaded third-party vendor app on Splunkbase
- Partnership between Gartner Magic Quadrant® Leaders

Example Use Cases

- How can I automatically contain infected endpoints?
- Is this traffic/activity normal for this application server?
- How do I aggregate all my threat intelligence feeds in one place and make them actionable?
- How can I visualize our security posture against the latest malware outbreaks for our management team, partners, customers and board?
- How can I report on the number of blocked IPs during peak season last year versus this year?

A Single-Pane-of-Glass View

Robust analysis takes advantage of threat intelligence sharing between vendors to turn unknown threats into known threats, in turn reducing your attack surface.

Palo Alto Networks and Splunk technology work seamlessly to give you visibility and a contextual view across your data center, endpoints and clouds, mitigating overall risk to your infrastructure. Enhanced dashboards enable you to correlate the threat profile of your adversary landscape across your entire environment.

For more information about the integration, visit our Splunk strategic partnership page.