

Splunk Integration with the Pensando Distributed Services Card

Integration Overview

Pensando ensures that any customer can easily build on the power of their existing Splunk environment by providing integrated access to data available from the Pensando Distributed Services Platform. Pensando/Splunk integration supports the ingestion of IPFIX and Syslog records gathered by the platform from every host deployed with a Pensando Distributed Services Card (DSC). New use-case-specific visualizations simplify each operations teams' ability to leverage this information at any time.

Pensando/Splunk integration aids Network and Security Operations in one of their most fundamental tasks: identifying issues as early as possible, before they grow into major problems.

DSCs track network data at the compute edge in every server, enabling previously-unavailable data insights—exposing flow data between the workloads on each server and even between workloads on the same server—with a simplified visual representation designed to highlight anomalous behavior.

The net result: **Operations can immediately uncover workload and workload connection issues and begin remediation in real time.**

Pensando has designed views to support the NOC team as well as the SOC team, showing contextual information from the platform's integrated firewall and IPFIX/NetFlow services, based on aggregated DSC data.

Use Cases Supported

- **Application Performance Optimization.** Analyze each application's communication traffic, and find any instances of network congestion, server congestion, or intermittent drops that require action. This also helps to quickly determine if the issue requires a network team or a server team response.
- **Network Design and Management.** Determine network path issues by getting detailed application-level feedback. Instead of having to track link by link, get an end-to-end view to determine where issues are appearing.
- **Security Threat Management.** Gain rapid insight into firewall policy violations and find applications that are behaving contrary to the policies they are mapped to. Quickly determine if there is a rule issue, an application communication issue, or an actual break/infection that needs to be addressed.
- **Identify Unmanaged/Underutilized Resources.** Quickly find underutilized servers hosting “dead” applications or improperly functioning workloads. Simplify workload hosting optimization with the ability to map overall application communication, as well as concurrent workloads hosted.

