SteelCloud

DATA SHEET

Monitor Your Infrastructure Compliance with ConfigOS DashView

Dramatically reduce the time spent monitoring, detecting, and maintaining the enterprise's DISA STIG or CIS infrastructure compliance.

ConfigOS DashView is revolutionizing the way organizations monitor and maintain their infrastructure hardening compliance. Maintaining risk awareness; performing compliance trend analysis; discovering and correcting endpoint hardening drift is usually a cumbersome, time-consuming manual process. ConfigOS DashView leverages Splunk's Big Data platforms to automate these processes and provide the organization with near real time awareness.

ConfigOS hardens an endpoint's unique application stack per the DISA STIG or CIS Benchmark hardening standards. ConfigOS generates a job report each time an endpoint is scanned, remediated, or rolled back. An enterprise that remediates 100K endpoints once a day will generate 10M reports in a little more than 3 months!

Enterprises that currently use ConfigOS can deploy the ConfigOS DashView App to their existing Splunk Enterprise or Splunk Cloud platform. Splunk ingests the ConfigOS job reports while the ConfigOS DashView App displays key metrics and can be configured to send automated notifications. With ConfigOS DashView, enterprises will gain immediate visibility into their enterprise infrastructure compliance and yield additional value from their existing Splunk and ConfigOS investments.

Insights and Actionable Intel That Matters

- ✓ Report the enterprise's infrastructure compliance over time.
- ✓ Monitor and manage the enterprise's infrastructure risk.
- ✓ Generate a trouble ticket or notify a System Administrator if an endpoint's compliance falls below a minimum threshold.
- ✓ If an endpoint falls out of compliance ("drifts"), immediately identify the specific security controls that have changed. Investigate to determine which IT process, security process, or GPO conflict(s) caused the drift.
- ✓ Identify endpoints that have not been hardened within the enterprise's minimum remediation interval.
- ✓ Detect situations where there is a significant compliance difference between endpoints that are managed by different groups, remote sites, etc.
- ✓ Manage security compliance by location, time, operating system, or individual policy.
- ✓ Manage security control waivers across your enterprise.
- ✓ Know which controls are currently waived at various levels: enterprise wide; platform type; or endpoint.
- ✓ Know which CIS Benchmarks or DISA STIGs are currently deployed and being enforced throughout the enterprise.

ConfigOS DashView Organization

The ConfigOS DashView App is organized as a set of five, linked, intuitive dashboards:

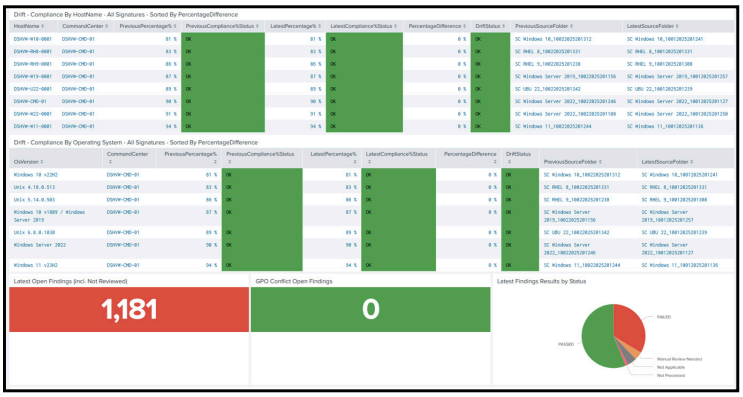
- ✓ Enterprise Compliance
- ✓ Risk Insights
- ✓ Operating System Insights
- ✓ Endpoint Insights
- ✓ Control Insights

Each dashboard includes multiple filters to perform specific analyses and generate desired reports.

Enterprise Compliance Dashboard

Information Security Managers will use this top-level dashboard. It provides visibility into your enterprise's infrastructure compliance at any point in time, or trend analysis over a time period. It also provides visibility into the enterprise infrastructure compliance at multiple levels:

- ✓ Enterprise/Agency
- ✓ Command Center
- ✓ Signature Container
- ✓ Security Policy
- ✓ Platform Type
- ✓ Endpoint
- ✓ Security Control



Risk Insights Dashboard

Information Security Managers will use this dashboard. The enterprise's risk score is calculated as a function of failed security controls (Category 1, Category 2, Category 3).

Operating System Insights Dashboard

Information Security Managers, System Directors, and Windows & Linux Managers/Administrators will use this dashboard. The security compliance for the various operating system platforms deployed within the enterprise is reported. For a specific operating system, a report on the percentage of endpoints that have drifted; and, for Windows, the "GPO Conflict Count" are reported.

Endpoint & Control Insights

Windows & Linux Administrators, Security Engineers, Information Security Managers, and ConfigOS Administrators will use this dashboard to:

- ✓ See specific endpoint reports, specific operating system platform reports, and application stack-specific security policies.
- ✓ View scan and remediation compliance percentages.
- ✓ Monitor drift status at the security container, security policy, and security control levels.
- ✓ Review the CIS Benchmark or DISA STIG control descriptions and waived or ignored controls.

Rapid Setup

Because ConfigOS DashView leverages the enterprise's existing Splunk and ConfigOS assets, set up is easy.

- ✓ The ConfigOS Command Center and MPO Commander publishes the endpoint compliance status JSON files to the configured directory monitored by the Splunk "Forwarder" component.
- ✓ Deploy the ConfigOS DashView App to the Splunk Enterprise or Splunk Cloud platform.

System Requirements

- ✓ ConfigOS 2.8.0+
- ✓ ConfigOS MPO Suite
- ✓ Splunk Enterprise v8.1+
- ✓ Splunk Cloud

Application Support

The SteelCloud support team is available to assist you with understanding, deploying, configuring, using, and maintaining ConfigOS DashView.

For more information on any SteelCloud products or services, please visit us at steelcloud.com

SteelCloud
20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**