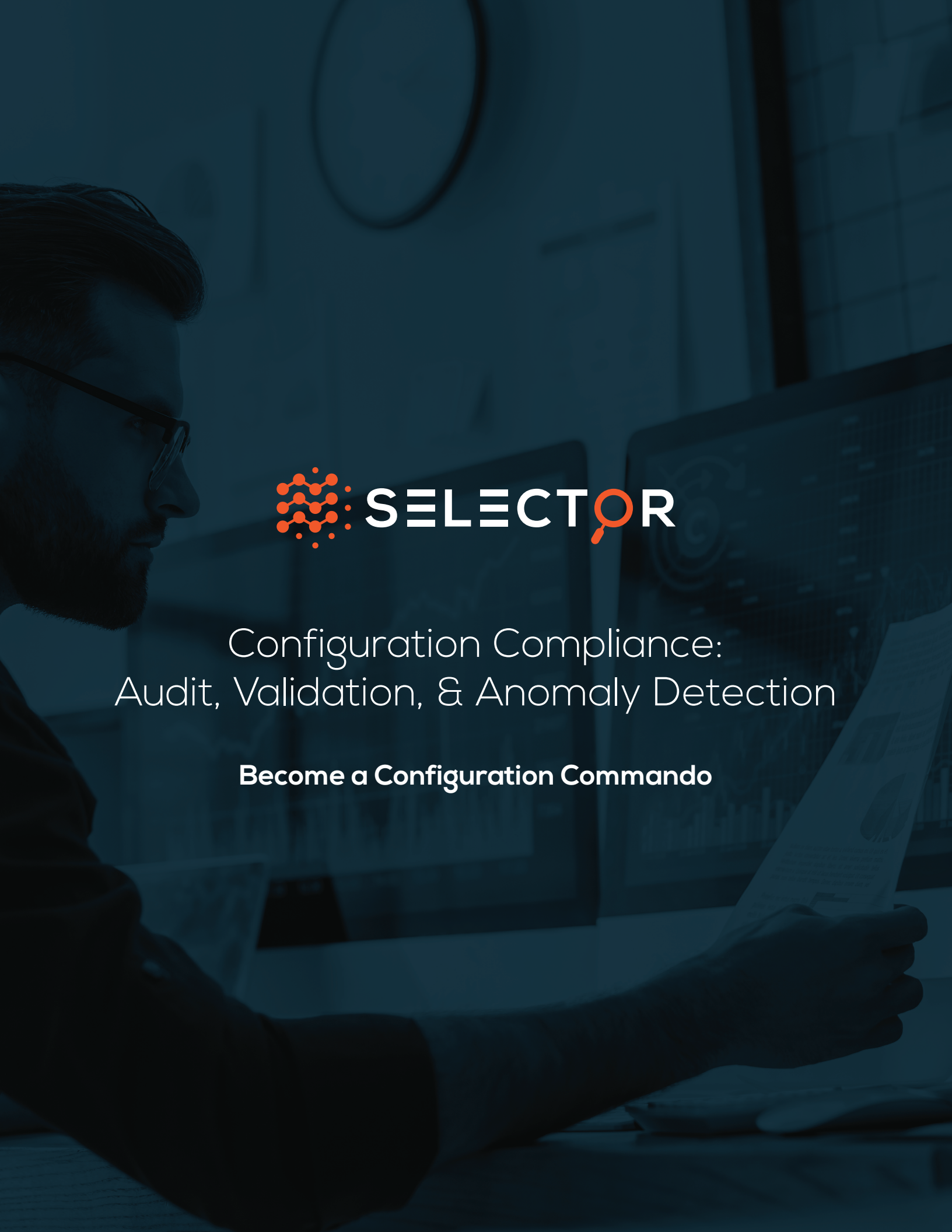


SELECTOR

Configuration Compliance: Audit, Validation, & Anomaly Detection

Become a Configuration Commando

Introduction

Observability tools have historically focused on logs and metrics, but not configuration information. This is surprising given how often configuration changes lead to outages as well as their potential to create security vulnerabilities.

Enter the Selector Configuration Compliance solution. Operations teams can now audit configuration changes, correlate configuration changes to anomalies, and search for the presence or absence of specific configuration statements. Operations teams can be configuration commandos, with an elite understanding of configuration changes, state, and consequences.

Anomaly Detection

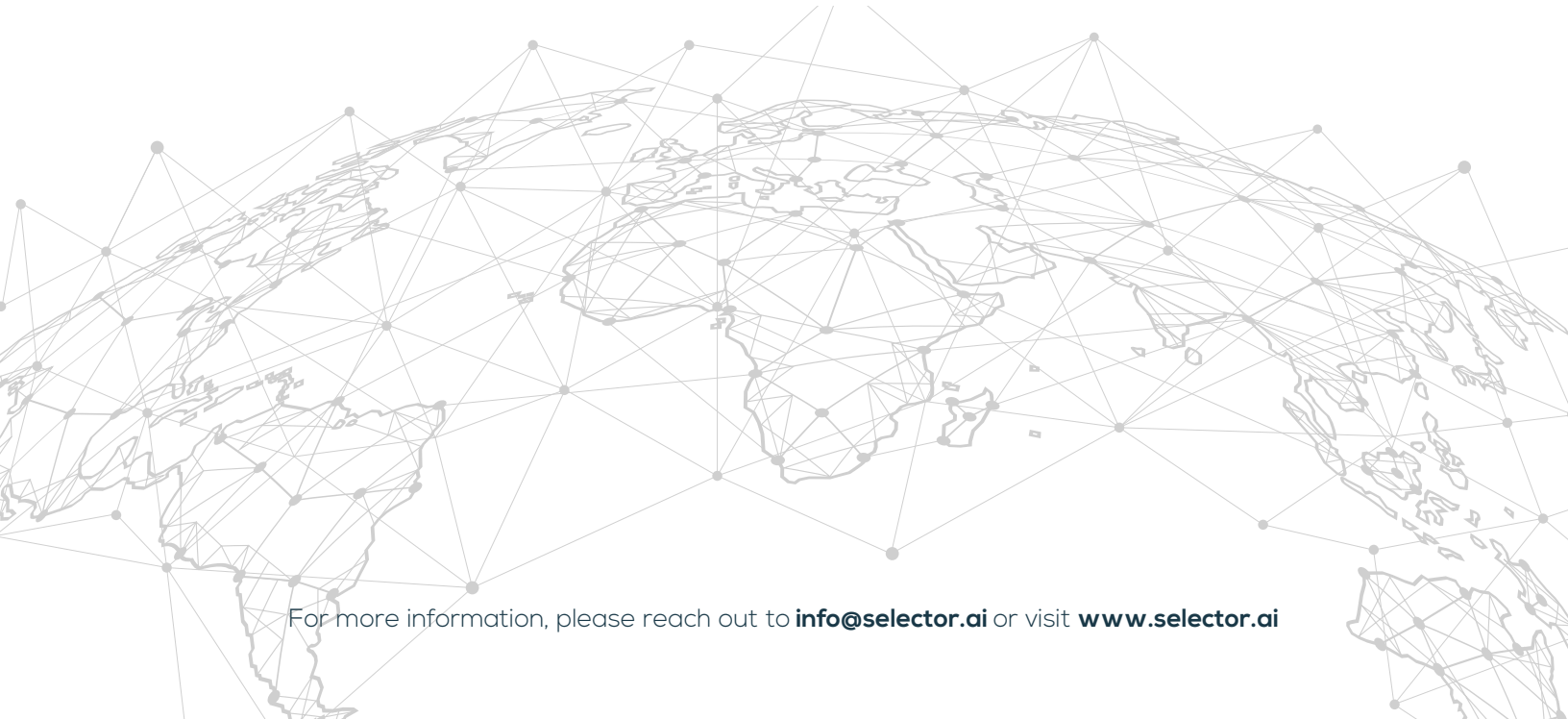
The Basic Workflow

- A configuration change occurs
- A syslog event monitor invokes an automation webhook, for example Rundeck/Ansible
- The entire configuration is retrieved from the affected device and stored in a repository
- The repository does a diff between the old config and the new config
- Selector Analytics stores both the diff and the new configuration
- Selector Analytics correlates the diff to any relevant anomalies
- Selector Analytics highlights the correlated incident to users
- Selector Analytics users can drill down on all correlated information including diff and whole configuration

Greater Clarity and Efficiency

Through this workflow, anomaly detection is much richer, and correlated to likely causes whether it is a fault in the network or a configuration change. Instead of operations teams having to guess at what are the likely sources of anomalies, there is greater clarity, more efficient triage, lower mean time to detect (MTTD), and lower mean time to repair (MTTR). With the impact of the configuration change identified, operations teams can rollback the change if needed, using an approved process.

This solution highlights the strength of the Selector Analytics architecture, capable of correlating any data source or data type, including configuration changes.



For more information, please reach out to **info@selector.ai** or visit **www.selector.ai**

Configuration Search / Validation

Be Prepared for Any Network Situation

Ever been in a situation where you are about to go live with a major new network segment and/or change, and wondered if every configuration was set the way it needed to be?

No problem, now you can do a configuration search for the absence or presence of any configuration element.

- Show me the devices that have this BGP statement.
- Show me the devices that do not have this ACL statement.

All with a natural language query. A Selector customer recently used this capability before going live with a major, highly visible media event, and were very pleased they did.

List all the devices that do or do not have a specific configuration statement.

Configuration Audit

Increase Performance and Security

As with many Selector analyzed events, a timeline is constructed so that Selector users can explore a timeline, see correlations, and do drill downs as needed.

With the Selector Configuration Change Timeline, operations teams can see when a change was made, what the change was, and who/what made the change. As automation becomes more prevalent, the frequency of changes are likely to increase. Buried in such changes may be configuration changes made by hackers that create significant security vulnerabilities. A configuration change trace / timeline is essential as configuration changes are among the most common sources of outage, performance degradation, and increasingly, security exposures.

Conclusion

While change management processes may provide a check on what planned changes occur, the outcome of a change is unpredictable.

There may be unwanted changes occurring outside of the change management process that operations teams need to know about. Importantly, if there is a correlation between a configuration change and outages / performance degradation, operations teams need to know about that as rapidly as possible, and then return to the desired KPIs as soon as possible.

Collect from Various Data Sources

Ingest variety of data sources in various formats

Correlate Metrics & Events

Machine Learning based data analytics for automated anomaly detection

Collaborate Across Boundaries

Instant actionable insights on collaborative platforms using Natural Language Queries (NLQ)

Technical Support

24x7 Product support

Low-Code Analytics

A fully interactive web portal with on-demand dashboards

Cloud-Native Deployment

Selector Analytics can be deployed in three possible modes - public, private, and cloud VPCs

For more information on any of our products or services please visit us on the web at **www.selector.ai**