FORTRA®

DATASHEET (TRIPWIRE)

Tripwire Enterprise App for Splunk Enterprise

Keep Pace with Continually Changing Security Configurations

Defending business-critical systems, data, and applications against potential threats requires that you know what is — and is not — normal behavior. Security teams collect large quantities of data for security intelligence, but gaining valuable insights from this data can be very challenging given the volume, velocity, and variety of that data. The challenge is getting high quality information with the necessary business context to make good decisions in time.

Integrating Splunk Enterprise with Fortra's Tripwire® Enterprise provides the ability to easily visualize the overall health of the IT environment. Tripwire Enterprise provides an endpoint detective, corrective, and preventative controls, driving real-time intelligence into Splunk's analytics engine. This enables the visualization of data in easy-to-implement dashboards to help reduce the cycle-time of identifying not only vulnerabilities and security violations, but also reducing mean time to identify and repair IT systems and remediate risks.

The Complete Solution for Security Intelligence

Tripwire Enterprise is an integrity management suite that provides fully integrated solutions for policy, file integrity and remediation management. With Tripwire Enterprise, IT security professionals rapidly achieve a foundational level of security throughout the IT infrastructure and can easily demonstrate that assets, services, and initiatives are protected. Tripwire Enterprise then continually maintains that level — in spite of the patches, updates, fixes, and application and configuration changes that tend to destabilize security configurations and whittle away at overall organizational security.

Splunk Enterprise is a security intelligence platform that collects, indexes, and harnesses machine-generated big data coming from websites, applications, servers, networks, and security solutions such as Tripwire Enterprise. Splunk Enterprise is often used as a big data platform for incident investigations and forensics, security reporting and visualization, and security information and event management (SIEM) threat correlation.

The Tripwire Enterprise App for Splunk Enterprise

The Tripwire Enterprise App for Splunk Enterprise is freely available on Splunkbase. It pulls in data from Tripwire Enterprise and offers built-in

PRODUCT HIGHLIGHTS

- Real-time dashboards and panels
- Easily view system state and vulnerability data from Tripwire Enterprise
- Fast reporting and drill-down over large amounts of data
- Quickly detect, prioritize and investigate risk

Key Features

- **Direct Data Integration:** Uses direct data collection through the Tripwire Splunk App Data Adapter, simplifying setup and improving performance
- **Asset View Data:** Captures detailed asset information, including tags and tagsets, which provides a more nuanced view of asset characteristics and relationships
- **SCM Data Flow:** Continuous access to compliance and security testing information through detailed datasets rather than mere snapshots
- **Waivers and Device Inventory:** Insights into compliance waivers and enhanced inventory visibility with detailed asset and test characteristics
- **Advanced FIM:** Enhanced file integrity monitoring (FIM) to distinguish between approved and unapproved changes

dashboards, reports, and fast access to critical system and application data through workflow actions. Tripwire Enterprise provides the unique high-fidelity security data, controls, and policies, which the app visualizes in out-of-the-box dashboards to help reduce the cycle time of identifying vulnerabilities or security violations.

In addition, the app provides the ability to drill into client logs to easily identify assets that may have vulnerabilities or security violations. Finally, you can use these sample searches to build your own customizations on the data Tripwire Enterprise provides.

Risk-based approaches to incident detection and response must focus efforts on detective controls, with the most attention given to critical assets where the data lives. While we would all like to stop every attack at the firewall, that conventional outlook is a losing proposition. Attackers sometimes get in, but Tripwire Enterprise is deployed on critical assets to detect not just the tools but the techniques that they've used.

Once the Tripwire Enterprise data is collected, it's easily correlated with other data in Splunk Enterprise to uncover the presence of advanced threats that may hide behind credentials or have employed other stealthy methods to evade detection by traditional stand-alone security products.

Sampling of Reports, Dashboards, and Workflows in the Tripwire Enterprise App for Splunk Enterprise

Assets

Asset Inventory: Easily track and manage your systems by filtering data sources, tags, versions, and more. See system health, licensing, and agent versions through clear visualizations and a comprehensive asset table for fast and informed decisions.

Compliance

SCM - Security Configuration Management: View a snapshot of security configuration tests across your systems and monitor the health of your nodes by showing which have had test failures. Assess test performance with group trends and a detailed result table.

SCM - Passed & Failed Tests: This dashboard provides a real-time overview of SCM test results across various assets. Receive a quick visual summary through a pie chart distinguishing between passed and failed tests and a trend line graph depicting the pattern of these results over time.

SCM - Test Results by Asset: See a summary of test results for a selected group of assets. This report can be used to easily identify which assets have the lowest compliance percentage.

SCM - Waiver Details: Use this dashboard to track and manage waivers to internal security policies. Quickly see how many sources, assets, policies, and tests are currently operating under exceptions.

Change Intelligence

FIM - Added | Modified | Removed: Track file integrity monitoring (FIM) changes across your systems with drill-down functionality. This dashboard provides a clear view of all added, modified, or removed files, enabling quick identification of changes that could indicate security concerns.

FIM - All Time Changes: Get a snapshot of FIM data across your systems to track trends in file modifications over time. It categorizes data by severity, rule name, and change type, providing detailed views on modifications per asset.

FIM - Attribute Search: Search and monitor FIM events across a specified time range and filter by attributes like hash value, filename, rule, or user, providing detailed visibility into the changes occurring across monitored assets. This dashboard presents details about modifications to files or elements on monitored servers.

FIM - Authorized | Unauthorized: See a comprehensive overview of authorized and unauthorized changes within monitored systems. Identify unauthorized changes, analyze trends by user, and track frequently changed elements to ensure compliance and detect unauthorized activities. The insights gathered here are crucial for identifying potential security threats.

THE TRIPWIRE ENTERPRISE SPLUNK APP

The Tripwire Enterprise App for Splunk Enterprise is freely available at https://splunkbase.splunk.com/app/6928. To get started, install the app on the Universal Forwarder of your Tripwire console and the Splunk Search Head. Next, enable the Tripwire Enterprise Data Adapter for best performance.

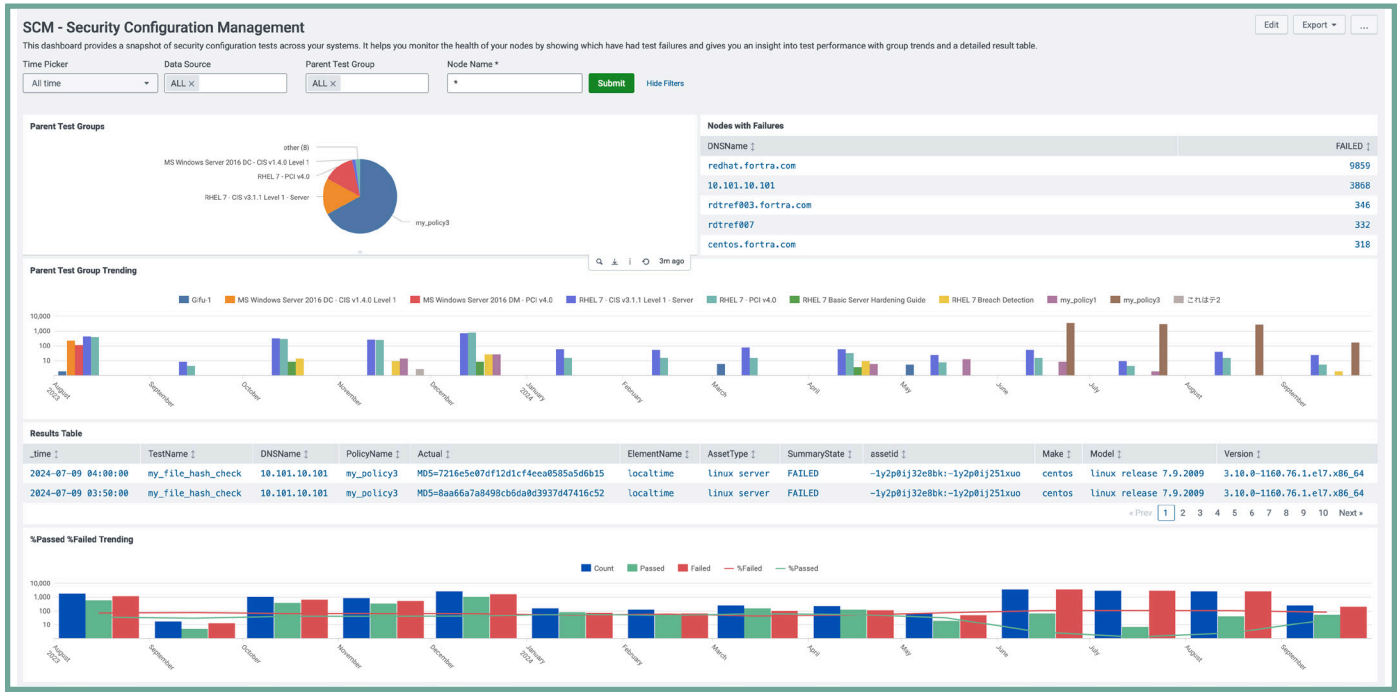
FIM – Change Summary by Asset: Summarizes the number of changes for each asset, including added, modified, and removed elements. It highlights assets with the highest unauthorized change percentage, enabling users to prioritize monitoring and manage compliance effectively.

System

System – Dashboards, Jobs, and Data Performance: This all-encompassing dashboard offers a deep dive into your system's operational health, displaying real-time metrics and historical data on dashboard performance, job execution, data ingestion, and TE server functionality. It's designed to streamline troubleshooting, optimize system maintenance, and enhance performance.

TE SysLogs

Admin Operations Audit Events: See recent activity based on nodes, rules, and duration, as well as activity over time (e.g. last 24 hours). View failed console logins, administrative changes, console session history, and event details.



Sample report from the Tripwire Enterprise App for Splunk Enterprise

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.