DATASHEET

Keep Pace with Continually Changing Security Configurations

With Tripwire and Splunk

Highlights

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

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 Tripwire® Enterprise provides the ability to easily visualize the overall health of the IT environment. Tripwire Enterprise provides an endpoint detective, corrective, and preventative control, 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 a security configuration 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 at tripwire.com/products/tripwire-ip360/ip360-splunk-app-register. It pulls in data from Tripwire Enterprise and offers built-in 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 Splunk Enterprise visualizes in out-of-the-box dashboards examples 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.

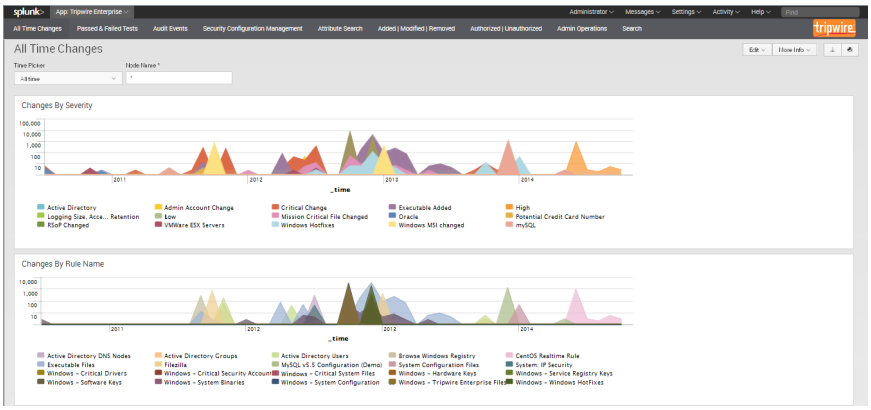
Reports, Dashboards and Workflows in the Tripwire Enterprise App for Splunk Enterprise include:

» **Host Change Overview—**Comparison of two or more nodes
- Types of over time by Node A
- Types of over time by Node B

» **Tripwire Enterprise Added/Modified/Removed—**With drilldown

» **Tripwire Enterprise Admin Operations**
- Activity Categories—Audit of Tripwire Enterprise console
- Recent Check Activities—Node, Rule, Duration
- Activity Over Time
- Activity Last 24 Hours
- TE Console Activity Seen
- Failed Logons to TE Console
- Administrative Changes
- TE Console Session History—Visualized length in minutes

» **Tripwire Enterprise Attributes Search**
- Time, Rule, Hash Value, Filename, Hostname, Users



Sample Dashboard from the Tripwire Enterprise App for Splunk Enterprise

» **Tripwire Enterprise All Time Changes**
- Changes by Severity
- Changes by Rule Name
- Change Types
- Change Type by Node Name
- Most Changed Element By Host—With count and sparkline
- Top Windows System Binary Changes—Count and sparkline
- Changes by File and User—Counts per Node

» **Tripwire Enterprise Audit Events**
- Audit Event Overview—Programs responsible for changes with sparkline
- Audit Event Rate—"counting the haystacks"
- Audit Event Details—With easy to use program dropdown selection

» **Tripwire Enterprise Passed & Failed Tests**—Chart and selectable policy dropdown

» **Reports**
- Added, Modified, Removed
- Hashes—Expected and Observed
- Nodes with Failures
- Tripwire Enterprise Parent Test Group

» **Tripwire Enterprise Report Panels—**Pick and Choose, Reuse
- Authorized vs. Unauthorized Changes = Change Process Compliance
- Test Result Summary
- Frequently Changed Elements
- Frequently Changed Nodes
- Scoring History

» **Tripwire Security Configuration Management**
- Nodes with Failures (policy)
- Policy Test Groups

» **Workflow Actions**
- Launch Tripwire Enterprise in Context on Policy Failures using name of policy and node
- Launch Tripwire Enterprise in Context on ElementID to present side-by-side difference viewer of element changes on node
- Launch Tripwire Enterprise in Context on Node to further enrich investigations

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook