FORTRA®

DATASHEET (TRIPWIRE)

Enterprise-wide Vulnerability and Risk Visualization for Advanced Threat Protection

With Tripwire IP360 and Splunk Enterprise

Defending against attacks in today's threat landscape is becoming increasingly difficult given the high rate of change on enterprise networks, the constantly evolving threat environment and the increased focus on internal and regulatory compliance. Organizations require a comprehensive view of security risk across the global enterprise network. While large quantities of data for security intelligence are collected every day, gaining valuable insights is hindered by its volume, velocity and variety.

Integrating Tripwire® IP360™ with Splunk Enterprise enables you to visualize security vulnerability risk data so you can easily measure and manage your security risk posture. Tripwire IP360 provides vulnerability and risk assessment, scoring and profiling intelligence to Splunk's analytics engine where, in easy to implement dashboards, you can easily discover every system on your network and reduce the time spent investigating security incidents.

Complete Solution for Security Intelligence

Tripwire IP360 is a leading vulnerability and security risk management solution that delivers comprehensive discovery and profiling of network assets. IT security professionals leverage the advanced prioritization metrics that combine asset value and vulnerability scores to place security risk in the context of the business. Tripwire's industry-leading Vulnerability and Exposure Research Team (VERT) keeps Tripwire IP360 up to date with accurate, non-intrusive discovery signatures that are current and relevant to large enterprises.

Spunk 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 IP360. Splunk 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.

PRODUCT HIGHLIGHTS

- Real-time dashboards for risk assessment and incident investigation
- Easily view when critical vulnerabilities are increasing or decreasing over time
- Fast reporting and drill-down over large amounts of data
- Quickly and effectively reduce overall network risk

KEY BENEFITS

- Continuous risk assessment and incident investigation
- Visualize security risk and vulnerability intelligence from Tripwire IP360
- Measure to see if critical vulnerabilities are increasing or decreasing over time
- Profile all assets across your network
- Correlate vulnerability information with other security/data sources

Tripwire IP360 App for Splunk Enterprise

The Tripwire IP360 App for Splunk Enterprise is a free app available on Splunkbase It pulls in data from Tripwire IP360 and offers out of the box dashboards, reports and fast access to critical system and application data. Tripwire IP360 provides CIM-compliant security vulnerability risk data, which Splunk visualizes in out of the box dashboards examples. This enables real-time risk assessment and incident investigation, and easily correlates with other data sources.

Adaptive Threat Protection

Tripwire also offers integrations between Tripwire Enterprise and Splunk Enterprise. Tripwire Enterprise provides enterprise-wide security configuration and policy management with endpoint detection, response and prevention controls. Combining Tripwire Enterprise with Tripwire IP360 enables Adaptive Threat Protection™ by continuously monitoring the threat landscape in an automated way and reducing the manual effort of prioritizing risk. By combining Adaptive Threat Protection with Spunk Enterprise you get unprecedented IT and security visibility for faster threat detection and prevention.

Fig. 1 Sample Dashboard from the Tripwire IP360 App for Splunk Enterprise

Dashboards in the Tripwire IP360 App for Splunk Enterprise

Summary Overview

- Average Host Score
- Average Tripwire IP360 Vulnerability Score
- Average CVSS Score
- Host Count
- Total Vulnerabilities per Host
- Host Score Trend
- Host Score by Network
- Host Score by OS Group
- Trend of Host Scores by Strategy

Vulnerabilities

- Accessibility Type
- Skill to Exploit
- Exploitation Strategy
- IP Address, DNS Name, NetBIOS Name
- Vulnerability Name

Top Ten – Percentage of Risk by:

- Network group
- Network name
- Operating System
- Vulnerability Category
- Host Name
- Vulnerability Name

Audit Trending

- Risk over Time
- Tripwire IP360 Score Distribution
- Risk Score over OS Distribution

Audit Status

- Overall Scan Status
- Scan Status By Network

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.