

Tripwire Connect Actionable Reporting Made Simple

Rich, visual analytics and reports help security teams translate their tools' data into the strategic remediation activities that best reduce cyber risk. While Fortra's Tripwire solutions provide you with an abundance of invaluable security and compliance data, Tripwire® Connect 4.6 extends the value of that data even further by combining information from multiple sources and presenting it in a unified way.

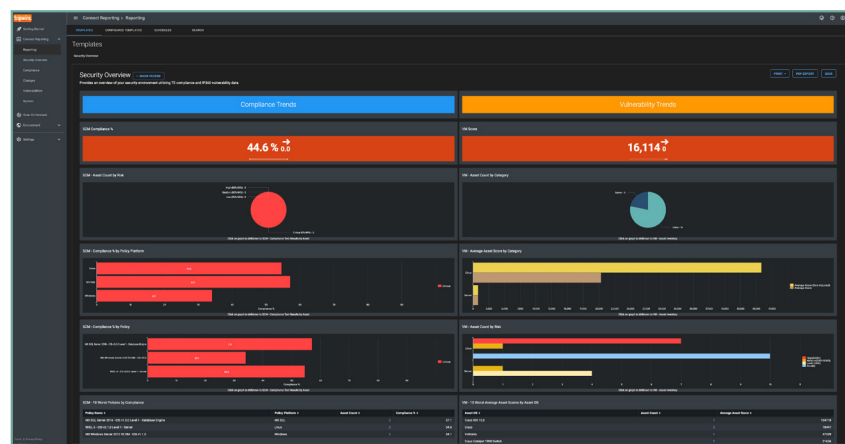
Tripwire Connect is a highly customizable analytics, reporting, integration and management platform for Tripwire® Enterprise and Tripwire IP360™ that can be deployed and scaled according to your organization's needs.

Clear, Actionable Reports and Dashboards

Dashboards provide clear, actionable insights so you can address the most urgent concerns first. Incremental transmission for all data in Tripwire Enterprise enables real-time reporting, and the ability to aggregate deltas of change data reduces network bandwidth and speeds analysis. In addition, high-demand data fields bolster compliance and file integrity reports.

Reporting details include:

- Vulnerability reports and scores, including remediation guidance
- SCM/FIM reports and scores with Tripwire Enterprise element content



Tripwire Connect Security Overview dashboard

KEY BENEFITS

- **Ready out of the box:** Use pre-built dashboards and reports
- **Flexible:** Choose on-prem or SaaS deployment
- **Scalable:** Architecture that scales with your needs, reporting on up to 100,000 nodes
- **In-depth:** View granular change and vulnerability reporting, including historical trend data
- **Visual:** Graphs, charts and widgets help you visualize your data
- **User-friendly:** Enhanced user interface and workflows ease navigation and display
- **Tracking:** Tag assets across multiple cybersecurity tools
- **Unified:** A single UI for your Tripwire products
- **Customizable:** Create custom reports and templates to suit your cybersecurity needs

- Application inventory
- Historical and trend data
- Assets out of compliance
- Policy test failures
- List of impacted assets and remediation options
- List of assets scoped by tag on both SCM and VM
- Correlated asset data from multiple sources

For a deeper look at reports, refer to the Tripwire Connect Report Catalog.

Customized Reports for Specific Audiences

Tripwire Connect provides audience-specific reporting and analytics for security, configuration, and compliance stakeholders, enabling you to measure and track improvements over time. Customizable report templates provide at-a-glance information on the status of the enterprise's state of cybersecurity health and ongoing initiatives.

Tripwire Connect reports address a range of enterprise audiences:

- CEO/Board of Directors: Trending reports on your cyberthreat and policy compliance posture
- CISO/CSO: Report on your current security posture including enterprise, business unit and department comparison reports
- Policy Compliance Management: View updates on current compliance and IT security policies
- IT Operations: Understand which critical assets are monitored by Tripwire Enterprise
- IT Security: View and identify configuration drift and assets that are vulnerable due to missed patch updates

See Your SCM and VM Data Side by Side

Tripwire Connect consolidates data from multiple Tripwire consoles to present a unified picture of your security posture. By viewing your Tripwire Enterprise and Tripwire IP360 data side by side, you can evaluate both the changes and the vulnerabilities discovered in your environment simultaneously.

FIVE ESSENTIAL TRIPWIRE CONNECT DASHBOARDS

1. **Security Overview:** A high-level overview of vulnerabilities and applications present in your organization, with side-by-side VM and SCM data
2. **Change Summary:** An overview of change across your organization to identify areas that have a higher change rate than others
3. **Vulnerability Management Summary:** A high-level view of your organization's vulnerability posture
4. **Compliance Detailed Test Results:** Detailed policy test results including element content for use in an audit or to identify failing policy tests on specific assets
5. **Vulnerability Asset Details:** List of the vulnerabilities present on a specific asset along with the associated application asset configuration data, remediation details, the method of detection, and evidence of how the vulnerability was detected

Flexible Deployment

Tripwire Connect is available either on-prem or as a SaaS to match your deployment needs. Both versions provide the same functionality.

Minimum and recommend requirements are provided below. Contact Tripwire for recommended resource allocations based on your environment.

Summary

Tripwire Connect is a highly-customizable analytics, reporting, integration and management platform for Tripwire products that can deploy and scale according to your organization's needs. It maximizes the power of your Tripwire Enterprise and Tripwire IP360 data, providing you multi-level, unified views of all your Tripwire data across the organization.

Platform Support and Specifications

Client Software Requirements

- Microsoft Edge 91 and later
 - Mozilla Firefox 78 and later
 - Google Chrome 90 and later
-

System Requirements for Tripwire Enterprise Integration to Tripwire Connect

- Supporting Tripwire Enterprise 8.8.2 or later, patch forward versions will be compatible
 - Tripwire Supporting Java 1.8, 64 bit
 - Tripwire Enterprise Console running based on Windows Server 2012 R2, RHEL 7, or other Tripwire Enterprise supported consoles
 - Tripwire Enterprise Console, Minimal Enterprise Console system specification
 - Gigabit interconnect, network connection to Connect appliance
 - Network port 443 (outbound)
-

System Requirements for Tripwire IP360 Integration to Tripwire Connect

- Supporting Tripwire IP360 9.0, patch forward versions will be compatible
 - Gigabit interconnect, network connection to Connect appliance
 - Network port 443 (outbound)
-

Tripwire Connect Requirements

- Tripwire Enterprise 8.8.2 or later, or Tripwire IP360 9.0 or later (see product specific requirements below for details)
 - Installation of product-specific Tripwire Connect Data Adapter on Tripwire Enterprise console or Tripwire IP360 VnE
-

Tripwire Connect Forwarder Virtual Machine – Minimum and Recommended Requirements

- Virtual instance
 - Valid IP address and network connectivity supplied via VMware network
 - vCPU: 4 cores
 - RAM: Minimum 16GB, Recommended 32GB
 - Disk space: 24GB for install, plus minimum 40GB/500GB recommended for data partition
 - Firewall allowing access to Port 443, 22, and 5432
 - Verify that the FQDN is resolvable
 - To install or upgrade the Tripwire Connect Forwarder appliance, like any other network server, on a virtual machine with a fixed IP address and well-known DNS name, so that clients can reliably access the service
-

Tripwire Connect Reporting, Analytics, and Visualization (RAV) Virtual Machine – Minimum and Recommended Requirements

- Virtual instance
 - Valid IP address and network connectivity supplied via VMware network
 - vCPU: 12 Cores
 - RAM: Minimum 16GB, Recommended 32GB
 - Disk space: 24GB for install, plus minimum 40GB/500GB recommended for data partition
 - IOPS: 800
 - Firewall allowing access to Port 443, 22, 8088, and 8089
 - Verify that the FQDN is resolvable
 - To install or upgrade the Tripwire Connect Forwarder appliance Server, like any other network server, on a virtual machine with a fixed IP address and well-known DNS name, so that clients can reliably access the service
-

System Requirements for Tripwire Connect on VMware

- Host system with VMware version ESXi-6.0.0 update 1 or newer
 - VMware virtual machine support capable of running CentOS 7, 64 bit
 - OVA load, execution permissions allowing configuration for Network, HA, DRS
 - External hard drive SAN/NAS connections
 - Gigabit Ethernet
-

System Requirements for Tripwire Connect on Microsoft Hyper-V

- Host system with Hyper-V Manager version 10.0.14393.0 or newer
- Generation 1 virtual machine capable of running CentOS 7, 64 bit
- Gigabit Ethernet



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.