Tripwire IP360 Commander

Powerful Integration and Workflow Automation

Maximize the value of Tripwire® IP360™ by adding additional leverage to your valuable strategic business solution, and extend Tripwire IP360 to achieve better, faster and more cost effective vulnerability risk management and compliance.

Many enterprise applications lack a native command line interface. This can be a challenge if you want to automate and integrate basic operations, which is a necessary function in most enterprise IT environments.

Organizations have continually found new ways to unlock the value of Tripwire products, adding additional leverage to valuable strategic business solutions. And now you can extend Tripwire IP360 to achieve better, faster and more cost effective cyberthreat protection and compliance.

Tripwire apps are available to all customers, and new ones are constantly under development. Our apps can help you achieve a new level of scale and workflow efficiency with your Tripwire installation. Visit tripwire.com/it-security-software/tripwire-apps/ to see other available apps.u

Maximize the value of Tripwire® IP360™ by adding additional leverage to your valuable strategic business solution, and extend Tripwire IP360 to achieve better, faster and more cost effective vulnerability risk management and compliance.

Many enterprise applications lack a native command line interface. This can be a challenge if you want to automate and integrate basic operations, which is a necessary function in most enterprise IT environments.

Organizations using Tripwire IP360 can use Tripwire IP360 Commander as a powerful yet simple way to integrate and automate many of the complex systems and enterprise applications needed for business. Tripwire IP360 Commander is a cross-platform command line interface (CLI) for Tripwire IP360 that allows unlimited integration and workflow possibilities. It offers a consistent, flexible and reliable way to retrieve rich information from Tripwire IP360.

Tripwire IP360 Commander automates management of vulnerability assessment workflows on large networks, including:

- Batch apply network, scan profile, and other configurations across hundreds of networks at once
- Automate export of multiple scan results into a single CSV/XML file
- Automatically create assessment target networks based on a list target hostnames
- Quickly back up and restore portions of the vulnerability management console configurations for more control and to ensure stability
- Protect the integrity and confidentiality of your vulnerability management solution by monitoring console system changes, events and scan status in SIEMs and third party tools

Tripwire IP360 Commander exposes additional functionality to and from Tripwire IP360 through the CLI, including the following commands and more:

- Run a scan on demand
- Create a network
- List all scan configurations
- Add IP addresses to a network by ID
- Add IP addresses to a network by Name
- List all networks and included/excluded IP addresses
- List all networks but only IDs and Names
- List all active networks but only IDs, Names and included IP addresses
- List IP addresses of Device Profilers
- Show running scans for a Device Profiler
- List all credential types
- List all SMB credentials
- Retrieve Cyberscope report for an audit
- Count number of persistent hosts
- Batch import command parameters from an Excel spreadsheet

Common Use Cases For Tripwire IP360 Commander Include

CMDB Integration

- Assign ownership information based on ServiceNow data
- Create tickets for vulnerability remediation

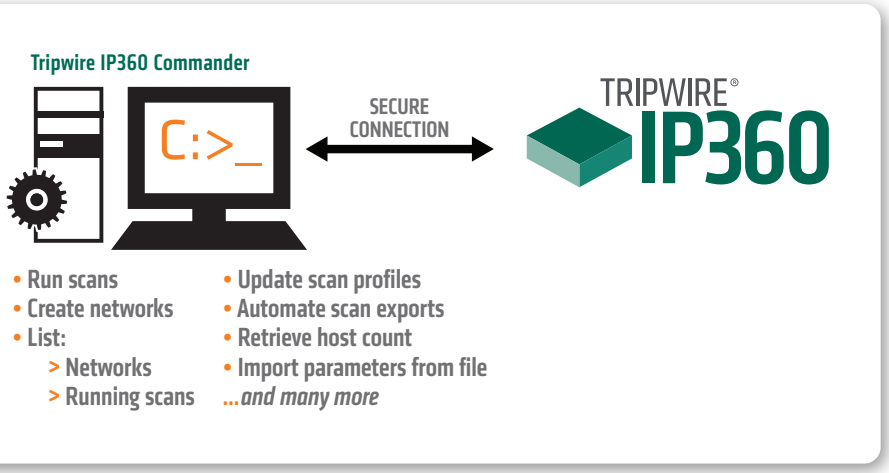

Fig. 1 Tripwire IP360 Commander, the cross-platform command line interface for Tripwire IP360, allows unlimited integration and workflow possibilities. This facility delivers the greatest flexibility and customization to our customers.

High-risk Vulnerability Alerting

- Report (via syslog) to an external SIEM for detected high risk vulnerabilities
- Email owners for detected high risk vulnerabilities

User Auditing

- Audit administrative activity in Tripwire IP360
- Audit failed logins

New Host Alerting

- Report (via syslog) to an external SIEM for new hosts detected
- Email owners for new hosts detected

Credential Configuration Automation

- Sync credentials with an external PAM system
- Configure per IP credentials

Scan Configuration Automation

- Audit scans to ensure all networks are being scanned monthly
- Configure new networks to be scanned in a timely manner

Network Configuration Automation

- Transfer IP range configuration from a testing to a production environment
- Configure or compare IP coverage to an external CMDB

On-demand Scanning

- Create scan profiles for on-demand scanning for vulnerabilities that match a custom criteria (newly released vulnerabilities, high risk vulnerabilities, vendor-only vulnerabilities, etc.)
- Run on-demand scans against all networks in a network group

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

TAPPTIPTC2k 201608