DATASHEET

Tripwire ExpertOps Proxy Appliance Security Hardening

The Tripwire® ExpertOps℠ Proxy Appliance is a secure and hardened platform that eliminates the need for customers to perform any type of operating system management. Tripwire's appliance-based approach reduces the level of effort and skills needed to maintain and operate network connections to Tripwire ExpertOps, all while maintaining a low-risk footprint.

Secured, For Your Peace of Mind

Only software that has been developed and/or validated by Tripwire is executed on the Tripwire ExpertOps Proxy Appliance. All software upgrades are transmitted via transport layer security (TLS), and only upgrades that have been signed by Tripwire can be installed.

General System Overview

The Tripwire ExpertOps Proxy Appliance allows communication from Tripwire Enterprise agents or Tripwire IP360™ Device Profilers to communicate back to the hosted Tripwire Enterprise console or Tripwire IP360 VnE Manager.

The appliance has:

- A VPN client for secure communication
- A SOCKS5 proxy to route agent communication
- Tripwire Enterprise apps for integrations
- An agent to monitor the appliance itself

The proxy appliance allows a single source to proxy agent communication, and the VPN ensures the agent communication back to the console is secure and encrypted. Additionally, the app integrations need to reside in the customer network to avoid unnecessary holes in the firewall; this gives the customer much more control and flexibility when integrating with ITSM tools (such as ServiceNow) and sending event data to their SIEMs via Event Sender.

The Tripwire ExpertOps Proxy Appliance can be accessed by the user through a secure shell (SSH) interface to access a restricted command line interface that only allows users to perform specific configuration and maintenance tasks on the appliance. The SSH interface doesn't allow root to log in, nor does it permit any interactive remote access.

Tripwire ExpertOps Proxy Hardening

The Tripwire ExpertOps Proxy Appliance includes, but is not limited to, the following configuration settings to enable only the system capabilities needed to facilitate secure communication between the customer environment and Tripwire ExpertOps:

- Updating and package auditing of the Linux operating system
- OS hardening and configuration
- Updating and auditing of third-party software and security patches
- Configuring third-party software to run at the minimum privilege level required
- Disabling unnecessary services
- Disabling all unneeded ports
- Checking all file permissions, including permissions for key files
- Removal of all unneeded accounts
- Limiting root access to the system (requires using sudo as much as possible)
- Not allowing root access to cron

- Ensuring the warning banner is not bypassable
- Checking remote access and SSH security settings; unsecure communication software (e.g. Telnet) is not allowed/used in the appliance
- Use of Linux firewall
- System event logging

Tripwire periodically conducts security reviews and internal penetration-style testing on the appliance.

Secure Data Storage on the Tripwire ExpertOps Proxy Appliance

All credentials used for access to the appliance are stored in an encrypted form and are not displayed or recoverable through the user interface. All communication with the appliance is secure and uses OpenSSL for TLS support.

Secure Software Delivery

Software is delivered through Tripwire's software update manager, which the customer's Tripwire ExpertOps Proxy Appliances connect to via a secure TLS connection. The appliance installation packages are signed by Tripwire using standard public cryptography techniques. Only updates that have been signed by Tripwire can be installed. Unsigned updates or updates that have invalid signatures are rejected by the appliances. The update process is typically initiated by the Tripwire ExpertOps managed services engineer, in coordination with the customer.

Software Lifecycle Support Assurance Requirements and Methodology

Configuration Management

Tripwire uses source control to track changes that are made to the Tripwire ExpertOps Proxy Appliance. This includes details on which changes are made and how potential changes are incorporated. Tripwire uses a revision control and source code management system for software and documentation configuration management. The revision control system allows Tripwire to maintain and archive who modified a file, what changes were made, and the time, date, and version.

Tripwire uses agile as their development lifecycle model (primarily Kanban, augmented with best practices from several other agile development methodologies), along with an agile management tool to manage and document their software development process.

Tripwire has a well-defined code review process. All code written for the Tripwire ExpertOps Proxy Appliance is required to be reviewed by at least one other person before being accepted. Tripwire uses a collaborative code review tool to manage, document, and archive the code review process.

Internal and External Security Validation

Tripwire reviews the architecture and features of its products from a security perspective on a periodic basis to include conducting internal penetration testing. Tripwire has a program of regular third-party security testing of its services, which includes the Tripwire ExpertOps Proxy Appliance.

Tripwire uses its own products (i.e. Tripwire IP360 and Tripwire Enterprise) to scan and detect vulnerabilities in its own systems, and both products are used to assess the Tripwire ExpertOps Proxy Appliance. Priority is given to correcting or mitigating known vulnerabilities.

Schedule Your Demo Today

Let us take you through a demo and answer any of your questions. Visit tripwire.com/contact/request-demo

tripwire®

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

TXOPASHDS1a 2101