tripwire by HelpSystems

SOLUTION BRIEF

Tripwire File Integrity Managment and Vulnerability Intelligence

Highlights

- Integrated view of enterprise security posture
- Continuous attack surface analysis
- Continuous security control automation
- Significant reduction in enterprise cyberthreat risk
- Improved security TCO and operational efficiency

There's not enough time in the day to investigate every system change and remediate every vulnerability. Ever-evolving capabilities of cyber adversaries—coupled with the dynamic nature of corporate networks—makes security prioritization increasingly difficult. With Tripwire® Enterprise and Tripwire IP360™ managed service offerings, you can minimize the amount of time you spend addressing high-risk vulnerabilities. And with clear-cut prioritization, you'll make sure you are tackling the vulnerabilities which introduce the biggest potential impact to your business.

To combat enterprise cyberthreats, you need instant access to the right information and expertise to quickly make informed decisions. Limited visibility into operational changes and the risk posture of your networked assets can slow reaction times. While capturing deep, rich system configuration information from assets improves visibility, it also produces a flood of additional data that can complicate prioritization. That problem only multiplies as asset coverage expands with the ever-increasing number of connected devices and endpoints.

The Tripwire ExpertOps℠ vulnerability management (VM) service provides a comprehensive managed service offering to maintain, advise, and lead your organization's VM security posture.

In short, you don't need more data to improve threat detection and response—you need timely and actionable information, and the expertise to make impactful decisions. You also need high-confidence context, or that information will have limited actionable value.

Tripwire Delivers Actionable FIM & Vulnerability Intelligence

You can solve this "big data" security problem with an integrated, automated and prioritized view of your enterprise security posture. Using the out-of-the-box integration between Tripwire Enterprise and Tripwire IP360, you can closely monitor integrity changes in your environment, automate remediation strategies, and tackle your most critical vulnerabilities from a unified reporting dashboard.

Continuous Security Control Automation

Now you can easily identify unauthorized changes occurring on your critical and highest-risk assets, enabling you to prioritize remediation based on vulnerability risk and change activity. Tripwire Enterprise leverages the vulnerability intelligence provided by Tripwire IP360 to provide insight into asset risk levels so that you can most effectively prioritize efforts. The Tripwire IP360 data is used to filter system file and configuration changes by vulnerability risk, while it enables automatic adjustment of monitoring and policy application within the ranges you specify.

An Integrated View of Enterprise Security Posture

Remediation is streamlined through a single, prioritized view of compliance findings and vulnerability risk. This reduces process-heavy communication and duplication of effort and data, while providing improved coordination and increased visibility between IT and Security functions. Clients are provided a dashboard to have catered views and reports generated, while Managed Service Engineers also provide scheduled status meetings and service performance reviews.

Security Coverage at Enterprise Scale

Important assets can be continuously monitored for change, and you'll know if—and where—coverage is missing. The device inventory provided by Tripwire

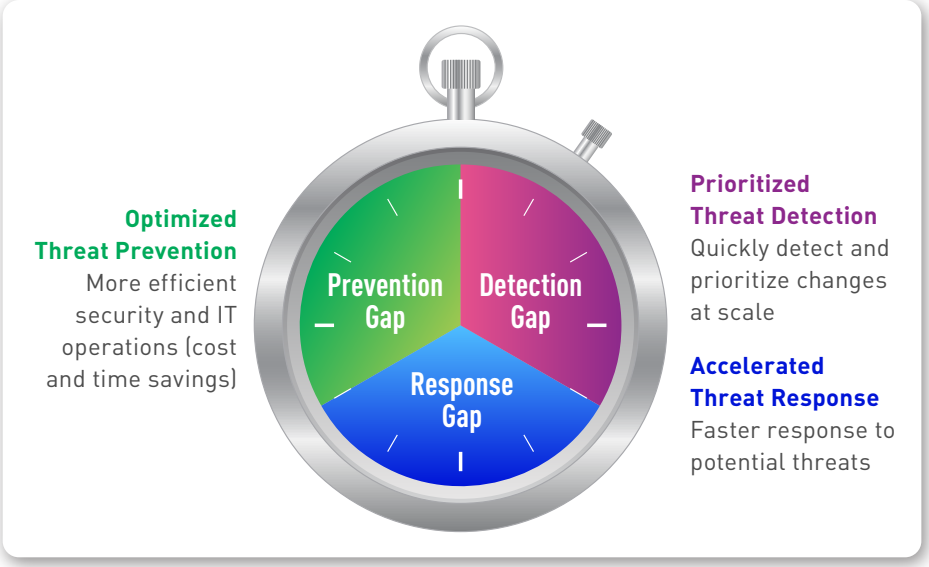

Fig. 1 Tripwire Enterprise leverages the Vulnerability Intelligence provided by Tripwire IP360 to automatically adjust security controls as the internal environment and threat landscape changes, prioritizing threat detection, accelerating threat response, and optimizing IT and security operations..

IP360 delivers an automated view of Tripwire Enterprise-managed versus unmanaged assets for a consistent view of enterprise-level security coverage. This gap analysis helps you identify all assets on your network, decide on additional coverage to improve your overall risk posture, and identify unknown devices that may be exposing your organization to greater risk. This prioritization is automatically updated in Tripwire Enterprise which enhances your ability to turn data into intelligent business insight.

The Value of FIM & Vulnerability Intelligence

Tripwire FIM and Vulnerability Intelligence provides valuable, up-to-date insights that reflect the state of your organization's network as changes are taking place:

Asset Discovery

Know what's on your network. Discover known and unknown assets that are not currently managed by Tripwire Enterprise, including on-premise and assets in the cloud. With a comprehensive view of network hosts, applications and services, you will have an up-to-date snapshot of devices which reside on your network and can react accordingly.

Asset Tag Rule Configuration

Tripwire Enterprise Asset Tags can be applied to the most critical assets so that changes can be tracked and, as vulnerabilities are remediated or subsequent scans are executed, tags are dynamically updated in Tripwire Enterprise to reflect your latest remediation efforts. These tags ensure that you can focus on important alerts first and prioritize your efforts to secure your important assets.

Network Risk

Combine vulnerability and change intelligence for a consolidated view of network risk. View reports and dashboards that filter and display security, threat and compliance information based on asset severity categories.

Vulnerability Risk

Identify the most critical security issues quickly using Tripwire's unique vulnerability scoring. Monitor high asset severity nodes for suspicious changes and configuration details.

Threat Watch List

Quickly identify and remediate specific vulnerabilities such as Log4J, ShellShock and Heartbleed from a

continually updated library capable of identifying over 317,000 conditions, including vulnerabilities, applications, and operating systems.

Application Watch List

Monitor for applications associated with threat indicators of compromise and data exfiltration, as well as applications (such as cloud sharing services) prohibited by policy.

Threat Skill Level

Filter vulnerable machines based on current threat information, including if exploit kits and automation tools are available to attackers, to closely monitor nodes with easily exploitable vulnerabilities.

Business Impact

Prioritize monitoring and response based on the business impact of a successful exploit. Automatically adjust monitoring based on the exposure, availability, and integrity impact of a successful exploit.

Scan Status

Ensure assets are continuously protected and in compliance. Automatically adjust monitoring and policy application based on time elapsed since the last vulnerability scan.

Managed Service Offerings

If you prefer a more hands-off approach to hardening your security posture or to gain the valuable insight from Tripwire's experts, managed service offerings can be leveraged for Tripwire Enterprise and Tripwire IP360 so that you spend less time configuring and more time remediating in your environment. Our skillful managed service engineers will track and remediate your console health, keep you up to date with regular status meetings, and help you establish or improve upon your existing vulnerability management program to keep your security posture at its best.

Fig. 2 Threat Monitoring that Adapts to Your Environment: Focus on what matters most. Prioritize monitoring and response based on the business impact of a successful exploit. Actionable data available from the Tripwire Connect platform, including the Vulnerability Count Risk Matrix.

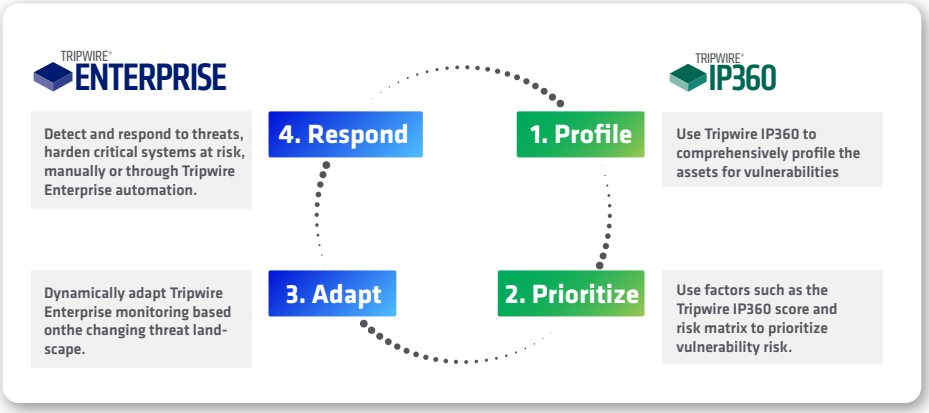

Fig. 3 Tripwire IP360 continuously analyzes your network attack surface to generate rich vulnerability intelligence based on prioritized vulnerability risk and ongoing coverage provided by the Tripwire Vulnerability and Exposures Research Team (VERT). Then Tripwire Enterprise leverages this vulnerability intelligence to automatically adjust security monitoring and policy application as the internal environment and threat landscape changes, prioritizing threat detection and accelerating remediation.

tripwire by HelpSystems

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