Tripwire IP360 and the ForeScout Platform

Improve Real-time Visibility Over Known and Unknown Devices while Automating Network Access Control and Threat Response

Highlights

- **Identify**—Discover and profile all assets whether IT or automation environment in the cloud, on-premises or hybrid without an agent
- **Protect**—Enforce network access control by allowing, denying, or limiting access for assets lacking scans or insufficient hardening
- **Detect**—Continuously monitor for vulnerabilities and processes across your entire infrastructure with a scalable and performant solution in real-time
- **Respond**—Prioritize vulnerability response with precise risk scoring and automatic quarantining of assets
- **Recover**—Automate workflows and accelerate infrastructure wide response without human intervention

Vulnerability Assessment (VA) is considered a security best practice and is an important part of any modern security program. However, an increasingly mobile enterprise with a proliferation of transient devices, coupled with the speed of today's targeted attacks, creates new challenges for vulnerability management programs. Tripwire IP360 is a next-generation VA tool.

The Tripwire® IP360™ VM Plugin for ForeScout communicates with the Tripwire IP360 VnE, which is the centralized console for management and for viewing scan data. For organizations with large and complex networks, Tripwire IP360 performs enterprise-class vulnerability assessment.

Visibility—According to industry experts, the vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. However, most organizations are unaware of a significant percentage of the endpoints on their network because they are either not managed, Bring Your Own Device (BYOD), guest or Internet of Things (IoT) devices. Also, they may have disabled or broken agents, or are transient devices that aren't detected by periodic scans. As such, you are unaware of the attack surface with these devices.

Threat Detection—Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multi-vectored, stealthy and targeted, these attacks focus on acquiring sensitive personal information, intellectual property or insider information. Compromised endpoints and data breaches often remain undetected for weeks or months. To detect these advanced threats, zero-day attacks and infected endpoints, you need next-generation security controls that don't rely on signatures or known threats.

Response Automation—The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, create the perfect storm for IT security teams. Without an automated system to continuously monitor and mitigate endpoint security gaps, valuable time is lost performing these tasks manually. And without the ability to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyberthreats to propagate within your network and exfiltrate data.

How the Solution Works

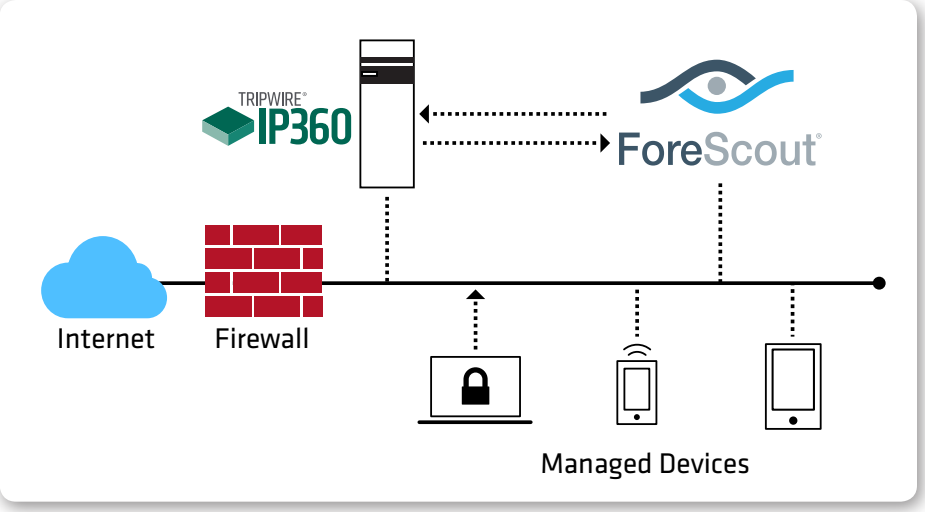
ForeScout is a network security solution that provides IT organizations with the unique ability to agentlessly discover and assess endpoints—including non-traditional devices—the instant

they connect to the network and while they are connected. ForeScout provides policy-based control of these devices to take such actions as control network access, initiate remediation of identified threats, and simple actions such as notifications. ForeScout also orchestrates information sharing and automates workflows among disparate security and IT management tools, including Tripwire IP360.

Tripwire IP360 is an enterprise-class vulnerability management solution designed for large, complex network environments. ForeScout communicates bi-directionally with Tripwire IP360 through the Tripwire IP360 VM Plugin for ForeScout, which is an extension of Tripwire IP360. ForeScout detects endpoints the moment they connect to the network and informs Tripwire IP360, which allows the operator to trigger scan requests based on network activity, as well as using ForeScout policies to monitor, manage, remediate and restrict endpoints based on Tripwire IP360 scan results.

For organizations interested in implementing best practice foundational controls in asset discovery and vulnerability management and who want to confirm an endpoint's health before it connects to the network, ForeScout is easily configured to automatically discover endpoints when they connect. This allows the endpoint to be put into an isolated network segment and have Tripwire IP360 scan the device. If the endpoint is considered safe, it is allowed onto the network. This function is particularly helpful when transient endpoints connect to the network, as they may have not been scanned in the routine scan performed by Tripwire IP360.

ForeScout can trigger a selected policy through Tripwire IP360 based on when



Bidirectional communication allows Tripwire IP360 scan requests to be triggered and ForeScout to monitor, manage, remediate and restrict endpoints

the last scan was done to provide a system scan, daily scan, or scan on connect. Once the scan is complete, ForeScout can review the results and take action, including automated remediation, in cases where vulnerabilities are found. Other capabilities include:

» Tripwire IP360 can trigger a policy in ForeScout to isolate vulnerable endpoints and remediate the vulnerabilities before being allowed back onto the network. ForeScout policies can be used to trigger a policy to launch a scan on endpoints that have not been scanned in a given number of days.

» If an endpoint is determined to have a particular vulnerability, or, a server has a vulnerable service, ForeScout policies can be created to only allow the endpoint access to low security network segments, or, in the case of the service, block access from the public network while allowing access from the private network.

» ForeScout can leverage Tripwire IP360 unique scoring algorithm to trigger a scan if the endpoint's vulnerability score is above an acceptable value, or if any monitored item has changed since the last scan. ForeScout can also use this information in policies that would trigger remediation for both of these instances.

» ForeScout can also retrieve information from Tripwire IP360 that indicates vulnerabilities and services found. This information can be used to create an inventory view that allows the admin to see devices with vulnerabilities and services and create reports that show endpoints with particular vulnerabilities or services or with specific vulnerability scores.

With the combination of Tripwire IP360, ForeScout and the Tripwire IP360 VM Plugin for ForeScout you gain comprehensive visibility and vulnerability management into all assets on your network. You also gain the ability to rapidly mitigate risks by controlling network access and automating remediation to increase your overall security posture.

About ForeScout

ForeScout Technologies is transforming security through visibility, providing continuous, agentless visibility and control of traditional and IoT/OT devices the instant they connect to the network. ForeScout technology works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. See devices. Control them. Orchestrate system-wide threat response. Learn how at www.forescout.com.

About Tripwire

Tripwire discovers every asset on an organization's network and delivers high fidelity visibility and deep intelligence about those endpoints. When combined with business context, this valuable information enables immediate detection of breach activity and identifies other changes that can impact security risk.

Tripwire solutions also deliver actionable reports and alerts and enable the integration of valuable endpoint intelligence into operational systems, such as change management databases, ticketing systems, patch management and security solutions including SIEMs, malware detection, and risk and analytics.

These integrations are part of our Technology Alliance Program and they ensure our customers have robust, accurate information to make their organizations more cyber-secure. Learn more at www.tripwire.com.

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at tripwire.com**

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » Watch us at youtube.com/TripwireInc

TAPTIPTFS1j 201804