Cisco AMP Threat Grid and Tripwire Enterprise

Advanced Protection to Combat Malware and Advanced Threats

Highlights

- » Quickly detect divergences from expected, secure configuration standards and guidelines
- » Rapidly determine risk to endpoints with automated malware analysis
- » Enable zero-day exploit response and remediation
- » Leverage real-time global threat intelligence to automatically block known advanced threats
- » Ensure all endpoint systems and networks are protected against known and new attacks

Overview

There is mounting concern at the senior executive and board level regarding cybersecurity, driven by highly visible advanced targeted attacks. These attacks threaten precious IP, valuable customer information, company valuation and trade secrets. To truly protect valuable resources, organizations have to accept the nature of modern networked environments and devices, and start defending them by understanding how attackers think and what is required to keep ahead of attackers' abilities in order to secure the infrastructure.

Tripwire® Enterprise provides real-time endpoint and server monitoring and detection. Cisco AMP Threat Grid offers dynamic malware analysis, which correlates the results of hundreds of millions of analyzed malware samples and related artifacts to provide a global view of malware attacks. The integration provides a comprehensive end-to-end solution with unprecedented protection from both known and unknown threats.

How the Joint Solution Works

Tripwire Enterprise continuously captures, monitors and records system and file change data on a broad range of enterprise servers and endpoint platforms. When Tripwire Enterprise discovers a suspicious, unknown threat, it sends the file to Threat Grid for further analysis.

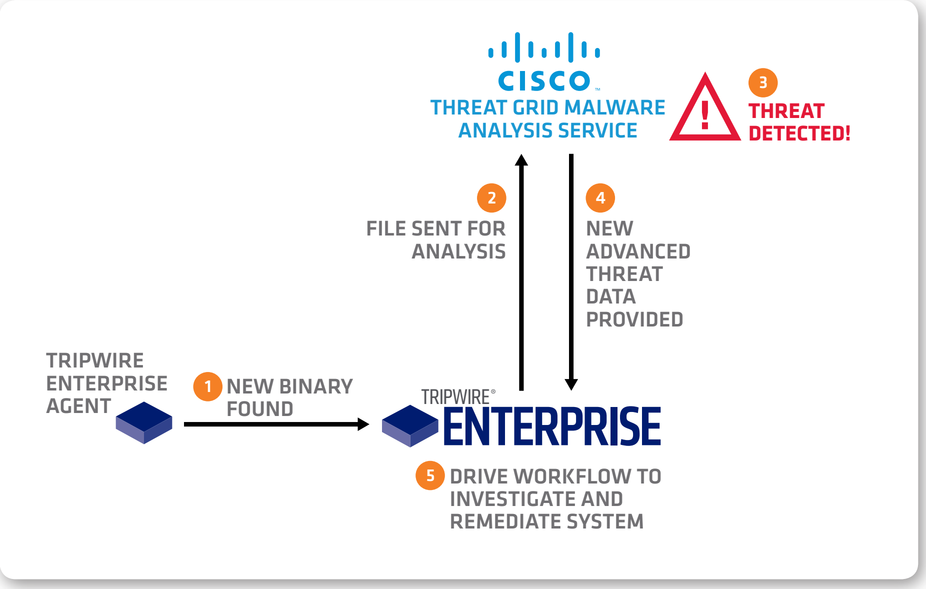
CISCO
THREAT GRID MALWARE ANALYSIS SERVICE
3 THREAT DETECTED!
2 FILE SENT FOR ANALYSIS
4 NEW ADVANCED THREAT DATA PROVIDED
TRIPWIRE ENTERPRISE AGENT
1 NEW BINARY FOUND
TRIPWIRE® ENTERPRISE
5 DRIVE WORKFLOW TO INVESTIGATE AND REMEDIATE SYSTEM

Fig. 1 AMP Threat Grid and Tripwire Enterprise together provide enhanced protection from advanced threats.

AMP Threat Grid's content-driven security analytics dynamically and statically analyzes all submitted files, examines the behavior of the samples, and correlates the results with hundreds of millions of other analyzed malware artifacts. Within minutes, Threat Grid reports back and Tripwire Enterprise tags the file with the result. This enables Tripwire Enterprise customers to prioritize actions for changes on systems with threats identified by Threat Grid and initiate workflow actions for quick remediation.

Cisco automatically and continuously updates its threat intelligence database, creating protections for all newly-discovered threats and sharing them with Threat Grid subscribers worldwide in minutes. Malicious binaries detected by Tripwire Enterprise are tagged as malicious, enabling prioritization of actions for changes on endpoint systems as well as blocking these binaries within minutes at the network level, preventing further infection.

Together, Cisco and Tripwire reduce the time to accurately detect and protect against advanced threats from endpoint systems to the network edge.

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolio of solutions across the broadest set of attack vectors. Cisco's threat–centric and operationalized approach to security reduces complexity while providing unmatched visibility, consistent control, and advanced threat protection before, during, and after an attack. For more information visit cisco.com/go/security

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **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