Partner Solution Brief

ANOMALI®

Next Generation Security Solutions

Tripwire Enterprise

Industry
IT Security & Compliance

Website
www.Anomali.com

Company Overview
Tripwire is a provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to con idently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context and enable security automation through enterprise integration.

Product Overview
Tripwire Enterprise is a security con iguration management suite that provides fully integrated solutions for policy, file integrity and remediation management.

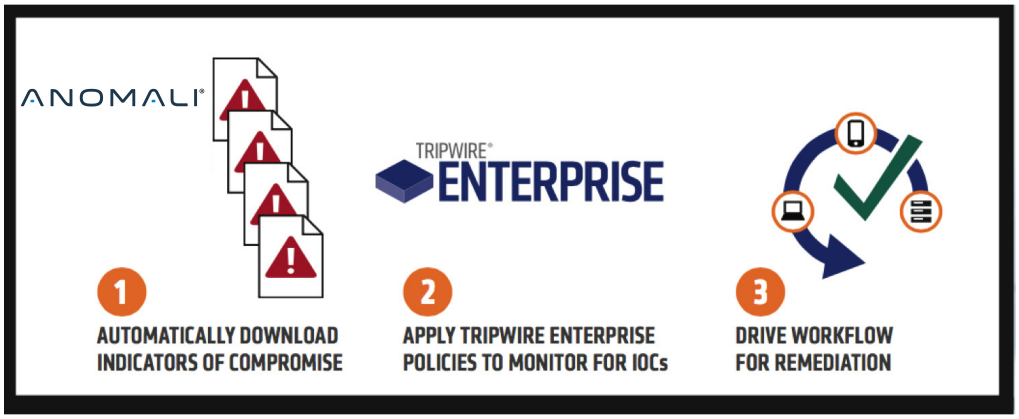
Solution Highlights
Protection from both known and unknown threats.

The threat landscape is continually expanding and organizations are under continuous attack and overwhelmed with alerts. Thousands of incidents occur each day and security professionals only have time to deal with dozens. This creates operational chaos. Security teams need next-generation security solutions to help them respond faster, defend proactively and invest smarter.

Just-in-time Intelligence

Tripwire® Enterprise can connect to a TAXII server and pull in real-time intelligence feeds that come from a variety of sources. We do two things with new intelligence as it arrives. First, we go back forensically through the history of change we have discovered. For most of our customers, Tripwire Enterprise is the most comprehensive forensics database of what has happened on their critical assets.

We can tell a customer if intelligence they receive today was something that happened to them very recently—or quite far in the past. We then incorporate that intelligence into the proactive monitoring of any future changes. If a change that maps to any of the indicators of compromise (IOC) received from a threat intelligence source is detected, the user is immediately alerted.



ANOMALI®

Benefits of Anomali

- Easy-to-use interface to view threat information received through STIX/TAXII feeds
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards
- Pinpoint IOCs - quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details
- Eliminate unnecessary, duplicative and irrelevant indicators - before they enter your infrastructure
- Identify and prioritize the events that matter now - without DIY scripting
- Machine-to-Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment

Benefits of Tripwire

- Proactive intelligence that monitors the assets and data that adversaries target
- Provides context into activities that require immediate attention to accelerate remediation
- Protects ahead of attacks, not while they are in progress—to have already occurred
- Stay up to date with the latest threats, no matter what the platform

Benefits of the Joint Offering

Tripwire Enterprise provides real-time endpoint and server monitoring and detection, and protection from advanced threats and attacks through integration with Anomali. The integration provides a comprehensive solution with unprecedented protection of both known and unknown threats.

Detect

Tripwire Enterprise's platform is trusted by over nine thousand customers on thirteen platforms to detect everything that is happening on mission critical systems.

- Automatic comparison of baselined, modified, and new files to IOCs
- Flag each file not only as known bad, but with metadata on why

Respond

Once the threat is identified what actions would you like to take?

- Tripwire Enterprise can be used to delete the file itself to surgically remove the issue
- Or actions can be triggered to monitor the file or host with increased scrutiny, to quarantine the host, or to simply alert on the threat to a SIEM

Prevent

Because Tripwire Enterprise possesses a robust business process engine attached to an excellent API there are numerous ways to integrate with other systems to adapt and prevent.

- Integrate with ticketing systems to provide patching of exploited vulnerability
- Integrate with network access controls
- Integrated with Next Generation Firewalls to block ports

About Anomali

Anomali is the leading provider of advanced threat intelligence solutions. Its award-winning platform provides organizations with the fastest way to find and respond to cyber threats. Anomali integrates real-time network activity with tens of millions of threat indicators, a wide range of threat feeds, forensic log data and externalcontext. This combination turns threat intelligence into a "cyber no-fly list" that customers spanning the private and public sectors use to identify and mitigate threats before they penetrate networks or cause material damage. www.anomali.com

About Tripwire

Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cyber security threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence.

ANOMALI®

808 Winslow Street, Redwood City, CA 94063 USA
1-844-4THREATS | support@anomali.com | www.anomali.com