DEPARTMENT OF DEFENSE OVERVIEW

INTEGRATED SECURITY CONTROLS TO PROTECT YOUR ORGANIZATION

◆ Tripwire solutions solve the File Integrity Monitoring, Security Configuration Management, Continuous Monitoring and Incident Detection challenges facing organizations. ◆

TRIPWIRE PRODUCT INFORMATION LINKS

TRIPWIRE ENTERPRISE (FIM, SCM, CDM)

TRIPWIRE IP360 (VULNERABILITY MANAGEMENT)

TRIPWIRE LOG CENTER (LOG INTELLIGENCE)

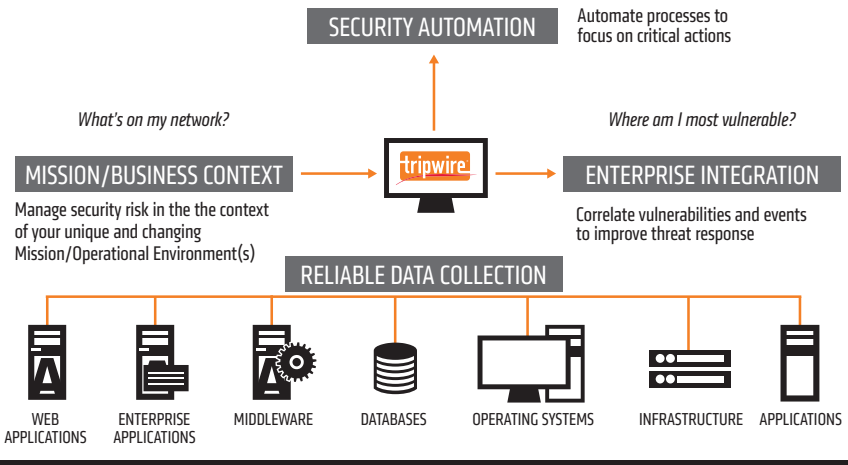
TRIPWIRE FOR SERVERS (FIM)

TRIPWIRE TECHNOLOGY ALLIANCE PARTNERS

Tripwire provides an integrated suite of solutions to help solve security challenges facing organizations within today's Department of Defense. Tripwire tools have been used within government and military organizations in both tactical and non-tactical environments to ensure system hardening through security configuration management, real-time threat detection with continuous monitoring, and data storage and analytics for faster incident response. Tripwire helps reduce cybersecurity risks while maintaining government compliance standards through continuous discovery, profiling, assessment, monitoring and mitigation of their IT infrastructure.

Tripwire enables organizations to reduce IT security risks while maintaining compliance with industry and/or government regulations through continuous discovery, profiling, assessment, monitoring and mitigation of their IT infrastructure. Tripwire products align with Best Practice Frameworks enabling the customer to follow widely-accepted process or control frameworks such as SANS 20 CSC, TIL, NIST RMF (800-37), NIST 800-53, DISA Polices/ STIGs, PCI and SCAP and more. Tripwire has obtained Army CoNs and ATOs in the Air Force and NSA. In addition, Tripwire monitors and protects systems in major Army commands, and is installed in every major cabinet level civilian agency. Tripwire has also developed custom policies that monitor and detect vulnerabilities in the active cyber defense (ACD) initiative. Cyber Protection Organizations require timely and actionable information. It requires operational context that is prioritized for quick response, or that information will have limited actionable value.

Tripwire delivers unprecedented risk visibility, mission/operational context and security business intelligence. We enable enterprises to protect sensitive data and assets from breaches, vulnerabilities and threats through our trusted portfolio of high priority security control solutions that include:



◆ **FIG. 2** *Focus on top actions to close your threat gaps.*

- Security Configuration Management (SCM)
- Vulnerability Intelligence
- File Integrity Monitoring (FIM)
- Automated Continuous Diagnostics and Mitigation (CDM)
- Log Intelligence
- Granular Vulnerability Scoring and Prioritization
- Real Time Change Detection
- Advanced Analytics and Reporting

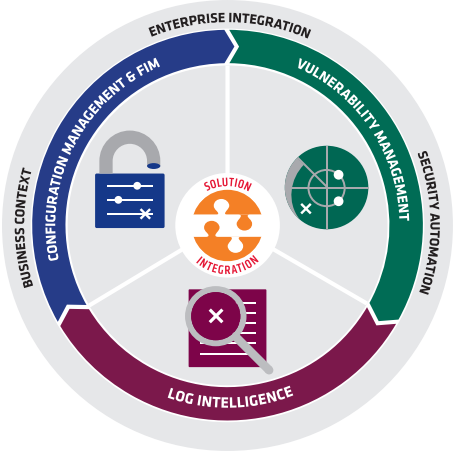
The Tripwire security suite can monitor over 125 operating systems and applications for change including Window, Mac OS, Linux, virtual infrastructures, databases and network devices. This enables Tripwire to detect leading indicators of breach activity across the enterprise, dynamically protect mission critical systems, and make security efforts visible, measurable and action-able. Tripwire has a portfolio of solutions that are unique in delivering cyberthreat security that provide:

- Detection indicators of breach, compromise and vulnerability
- Relevant operational context connecting security efforts to mission and operational goals and minimizing risks
- Automation with applied intelligence to deliver more effective operations
- Enterprise integration across the Tripwire portfolio, as well as with

MISSION/OPERATIONS CONTEXT
Connect your security efforts to what matters to your business

SECURITY AUTOMATION
Apply intelligence and drive automation for more effective operations

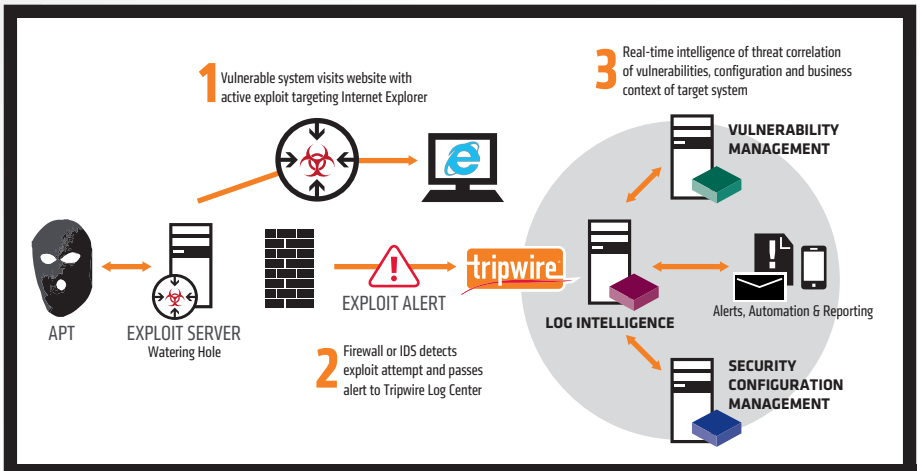
ENTERPRISE INTEGRATION
Across our portfolio and also with other security ecosystem partner solutions



PROVIDING SECURITY INTELLIGENCE

- Which systems are vulnerable?
- Which systems are being attacked?
- Which systems have already been compromised?
- Which systems should we fix first?
- Have we seen this before?
- When was it last in a trusted state?

◆ **FIG. 1** *Tripwire;s cyberthreat security portfolio detects vulnerabilities, compromises, and indicators of breach.*



◆ **FIG. 3** *Detect and prevent IE zero-day threats with Tripwire. CVE-2014-1776*

your existing and future security ecosystem

With Tripwire's combined set of security controls you can monitor your environment for events of interest in real-time, track configuration changes and identify vulnerabilities before they are exploited.

Tripwire provides practical Security Information and Event Management (SIEM) in a tactical or non-tactical environment through Operational and System Architectures implemented throughout an organization's Cyberspace/Battlespace.

The Tripwire suite provides operators with deep security intelligence, providing visibility into otherwise overwhelming and disjointed data from siloed security controls. Tripwire adds rich context to security events and decreases the time and effort required to identify and respond to security incidents.

Tripwire's Security Configuration Management provides leading indicators of breach activity by being aware of the state of systems, how they're configured and whether they're configured according to current policy. Once a known and trusted state is achieved, Tripwire continuously monitors for changes and deviations from your baseline. Tripwire's Event Integration Framework overlays log intelligence and event data to detect suspicious events and enables security context and prioritization.

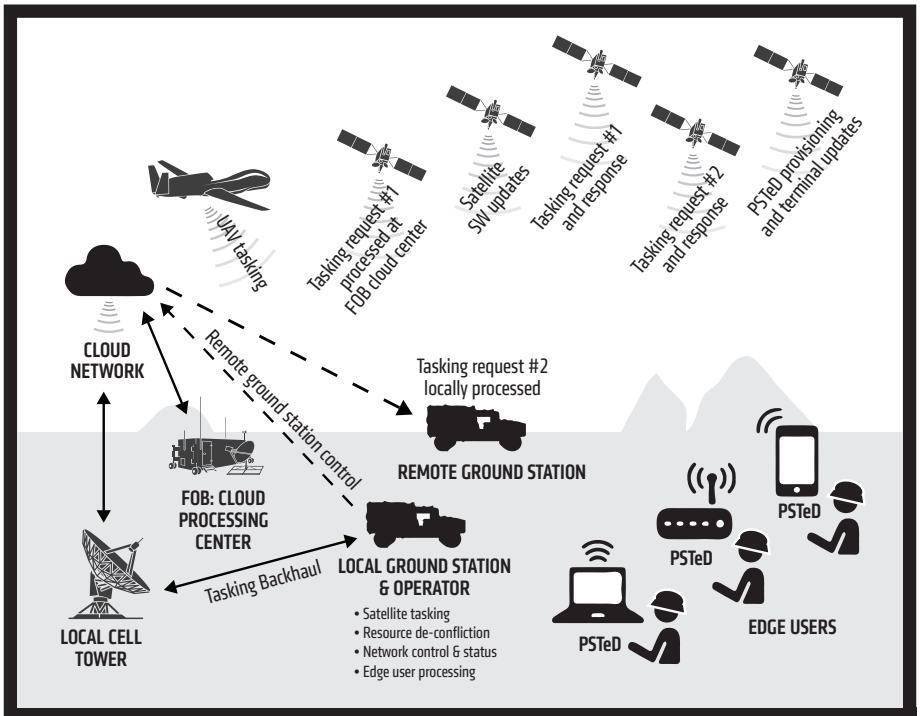
INSIDER THREATS

Managing the risks an insider threat poses to an organization requires a combination of people, process and technology. Although it may seem like an impossible task to mitigate damage caused by insider, there are usually indicators that can identify potential risk before an incident occurs. By aligning communication and policies between Human Resources and your IT department you can implement controls to reduce risk and detect incidents before they cause damage.

A FIPS 140-1 AND 140-2 VENDOR

The page csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm provides a list of all vendors with a validated FIPS 140-1 and FIPS 140-2 cryptographic module. Beside each vendor name is the validation certificate number(s) for the vendor's module(s) including the module name. Here is the section pertaining to Tripwire's FIPS 140-2 Certification:

Vendor	Validation Certificate #s with Module Names
Tripwire	1346 - Tripwire Cryptographic Module 2218 - Tripwire Cryptographic Module



◆ **FIG. 4** *Tactical environment notional operational view.*

◆ 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 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. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

SBDOD1a 201506