CONFIDENCE: SECURED

TRIPWIRE: ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

TODAY'S REALITY

Cyberthreats are coming at organizations faster than most can keep up with—2014 saw the introduction of 140 million new pieces of malware. Confronted with over 390,000 new malicious programs every day, legacy security solutions simply cannot be effective.

The typical gap between a successful breach and its detection provides cybercriminals plenty of time to compromise enterprise systems, and we read news of their actions on a daily basis. Loss of data, damage to the brand, costs associated with notifications and fines, and loss of customer confidence are all part of the aftermath. The Center for Strategic and International Studies estimates that global losses to cybercrime have hit $445 billion annually, with organizations rather than individuals taking most of that hit.

Over 390,000 malicious programs are discovered every day
—AV-Test.org

On day 0, only 51% of AV scanners detected new malware samples
—Lastline Labs

>390K

51%

85%

94%

85% of breaches could be prevented by remediating known vulnerabilities
—US-CERT

Percentage of unauthorized data access that came through compromised servers
—Verizon DBIR

TODAY'S CHALLENGE: THE ENTERPRISE CYBERTHREAT GAP

This cyberthreat landscape means enterprises need to operate as though they are in a continuous state of compromise. One frequently hears, "It's not a question of if you'll be breached, but when," which raises the question, how much damage will result from each breach?

THE DETECTION GAP

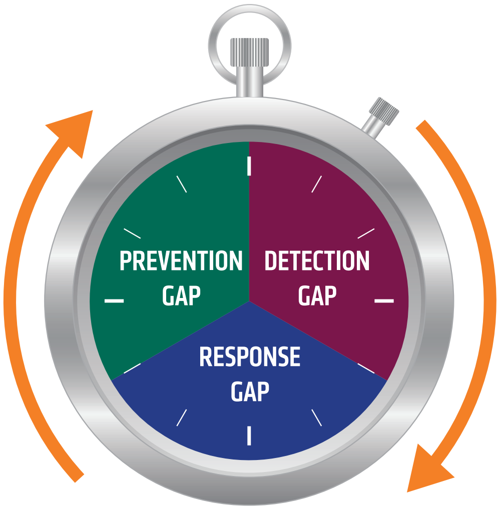
The amount of time it takes to discover a compromise and identify its nature. Reports show this often takes five to 18 months.

THE RESPONSE GAP

The amount of time it takes to identify the full scope of the breach and limit its damage. Research indicates this typically takes over four months.

THE PREVENTION GAP

The time it takes to implement measures to avoid a repeat (or similar) attack.



◆ **THE TIME** *between breach, discovery and full remediation is a model we call the Enterprise Cyberthreat Gap, to illustrate the different phases of this challenge.*

In this environment, time is of the essence. It's critical to be able to quickly detect if your organization has been breached and, if so, its extent—then take effective steps to mitigate the damage and ensure it doesn't happen again.

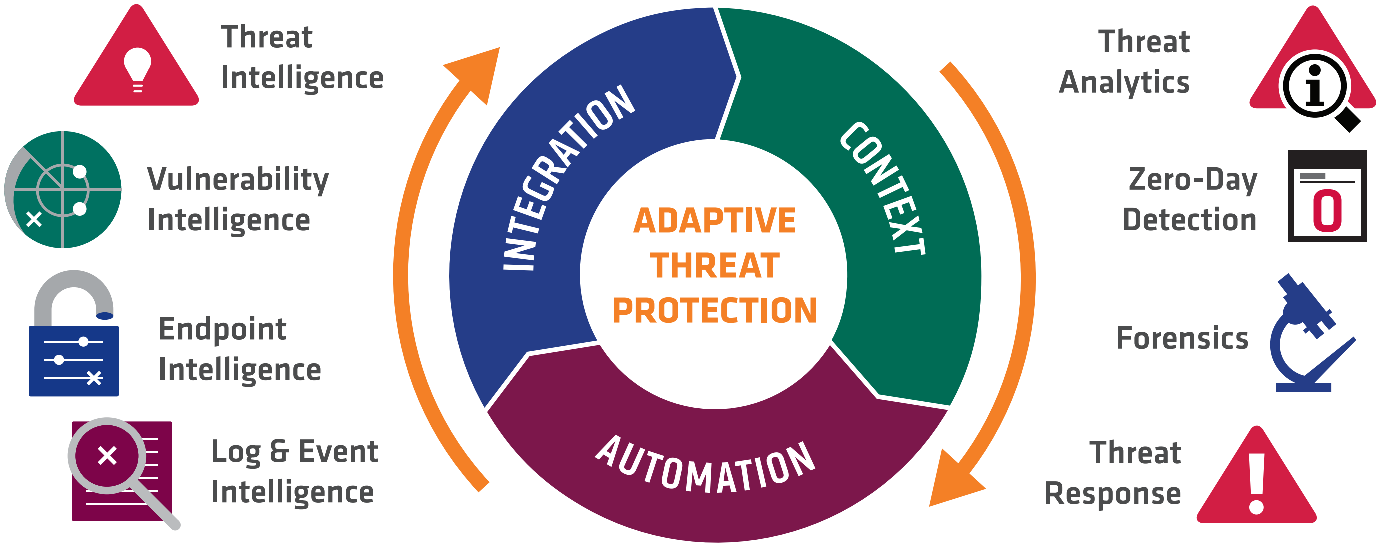
With advanced zero-day and targeted attacks, it's even more difficult to quickly detect and respond in time. And no one has enough resources to address the large number of malicious incidents. Beyond the sheer number of attack vectors, there's the problem of scale—how do you effectively focus your resources on the greatest risks to your most critical assets?

Organizations have installed untold millions of dollars of security tools, but they still lack depth and context, and the data they generate is fragmented and siloed. Security professionals don't need more data, they need high-confidence actionable information with business context about risks and impacted assets, a prioritized view into enterprise vulnerabilities, and to know if additional malware or vulnerabilities are associated with each threat.

TRIPWIRE—WHAT WE DO

The solution to this cybersecurity problem that business and government organizations face is what Tripwire calls Adaptive Threat Protection™, which provides dynamic threat and asset context along with integration and automation. Adaptive Threat Protection is Tripwire's next-generation innovative solution architecture to reduce the cyberthreat gap—enabling our customers to respond faster and with more precision to threats and vulnerabilities.

Adaptive Threat Protection is based on real-time security intelligence and analysis that includes log and event intelligence, deep endpoint intelligence, and combined vulnerability and threat intelligence. This threat protection solution enables highly granular threat analytics and forensics capability, while at the same time the ability to detect and respond adaptively to zero-day and today's advanced threats.



KEY SECURITY PROBLEMS ORGANIZATIONS NEED TO SOLVE—TRIPWIRE PROVIDES A BREADTH OF CAPABILITY

ASSET DISCOVERY

A foundational control for security is identifying all the hardware and software running in your environment—you can't secure what you don't know you have. Tripwire continuously discovers all assets to deliver a complete picture of your IT environment.

CONTINUOUS MONITORING

Continuous monitoring is critical to both good security and compliance, so there aren't gaps that attackers can find or your auditors will question. Tripwire operates continuously and in real-time to detect changes, risks and threats.

CONFIGURE AND HARDEN SYSTEMS

With over 90% of unauthorized data access coming through compromised servers, continuous system hardening is critical to protect valuable IT assets. Tripwire knows your assets—file servers, databases, active directory, network devices and endpoints—and how they're configured to provide you both security and compliance.

VULNERABILITY AND RISK MANAGEMENT

The vulnerability environment changes every day. Tripwire identifies and uniquely prioritizes vulnerabilities based on their level of risk to your organization, so you can deploy your resources most effectively to reduce overall risk.

INTEGRITY MONITORING

Automatic change detection is the best early indicator for advanced threats. Tripwire is the gold standard in integrity monitoring, identifying changes to files and systems and determining low- from high-risk change, as part of real-time assessment, prioritization and reconciliation of detected change.

CLOUD SECURITY

Today's agile IT organizations need security solutions that work in their physical, virtual and cloud environments. Tripwire delivers security and compliance solutions that work on-premise and in virtual, private and hybrid cloud environments—and with less overhead.

COMPLIANCE AND POLICY MANAGEMENT

Every organization has internal security policies and external compliance requirements. Tripwire delivers advanced policy and compliance assessment that pinpoints non-compliance, making policy status and configuration weakness not only visible, but actionable. Keep industry-current with the largest library of integrated compliance policies available.

INCIDENT DETECTION AND FORENSICS

Cyberthreats have become sophisticated, side-stepping outdated detection methods and requiring quick discovery to contain damage and protect sensitive data. Tripwire reacts to threats in real time while securely collecting and archiving data, giving you dynamic security analytics for rapid forensics, identification of historical indicators of risk and threat patterns, and enabling you to quickly restore systems to a known, trusted and operational state.

INSIDER THREAT

Your organization's greatest asset can also be its greatest threat, as the people you trust to make your organization successful can also cause the most damage. Tripwire's combined security controls not only help detect threats from outside your network, but also from within, identifying key risk indicators and detecting malicious insiders before sensitive data is exfiltrated and containing the potential damage.

TRIPWIRE'S THREAT PROTECTION SOLUTIONS

Tripwire delivers a portfolio of products all built on the same foundation—delivering business context, security automation and enterprise integration, critical components to an effective security ecosystem. Having relevant business context is the only way to connect your security efforts to what matters to your business and to identify the risks that you need to minimize. Automation is required to operate at the machine speed that is being used by your adversaries, and enterprise integration across our portfolio—and with other security ecosystem solutions—delivers the best results for your security investments.

SECURITY CONFIGURATION MANAGEMENT

Tripwire® Enterprise and Tripwire Configuration Compliance Manager™ provide unequalled depth and granularity of continuous endpoint intelligence, including system state and integrity monitoring data, across a broad range of endpoint, server and network platforms. It's built on one of industry's most robust, proven change detection technologies, with capabilities to definitively detect anomalous system and file changes, and to provide early indicators of threat and breaches—including endpoint data exfiltration. During a targeted attack, Tripwire detects changes in real time by leveraging out-of-the-box Cybercrime Controls. Finally, Tripwire maintains a complete state history for investigation and forensics, and can answer with confidence if a critical system has or has not been breached, when it happened and what changed.

VULNERABILITY INTELLIGENCE

Tripwire IP360™, with its unique integration of vulnerability risk information and configuration management, helps focus remediation efforts on the greatest risks to the most critical assets. The solution is built on an enterprise-class vulnerability management technology that includes the industry's most comprehensive vulnerability and risk scoring. With the combination of vulnerability and endpoint intelligence, customers can now quickly investigate and unravel the critical threat context they need to confidently respond to advanced threats. Vulnerability intelligence helps security analysts quickly detect and respond to potential threats and harden at-risk critical systems through endpoint configuration management. They can now continuously reduce their attack surface to protect from both known and new advanced attacks.

LOG AND EVENT INTELLIGENCE

Organizations need to detect incidents and respond to threats immediately. They also need to prove compliance with standards and regulations. Tripwire Log Center®, powered by the new Advanced Log Collector, reliably and securely collects, analyzes and correlates log data from devices, servers, applications and automated security processes to improve security for analytics and forensics while dramatically simplifying compliance. Collected data is analyzed and filtered so only actionable and relevant events are sent to IT security teams or forwarded to a SIEM. Log and Event Intelligence provided by Tripwire Log Center is a critical part of any threat protection deployment, and includes both network and endpoint security information and analysis.

THREAT INTELLIGENCE

Tripwire's open integration architecture is built to allow customers to select from a broad choice of threat intelligence and other security solution vendors that fit their industry and organization needs—delivering the best value at the best terms. With the industry's best threat intelligence partner integrations, Tripwire helps customers detect, analyze and verify zero-day exploits and advanced persistent threats. Our solution is designed to support both on-premise and cloud-based threat intelligence platforms, giving customers full flexibility that includes customization and open source integration. Future direction of this technology points to a potential asymmetric advantage for security analysts against hackers, as a result of the real-time sharing of malware and IOCs across a wide variety of endpoints and network enforcement platforms, both within the enterprise and the public cloud.

YOU’RE IN GOOD COMPANY

Tripwire is committed to sharing our unique endpoint, vulnerability and log intelligence with our Technology Alliance Partners to help make our customers’ entire security ecosystems more resilient. Tripwire integrates with a breadth of security partners including Threat Intelligence, Security Information and Event Management (SIEM), Change Management, Security Analytics, Platform, and Security Community partners. This ensures that our customers have the best possible security intelligence for threat analytics, forensics and investigation for a complete advanced cyberthreat protection solution.

THREAT INTELLIGENCE PROVIDERS

CISCO
paloalto networks
lastline
Check Point SOFTWARE TECHNOLOGIES LTD.
iSIGHTPARTNERS
CROWDSTRIKE
SOLTRA

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

RSA
hp
splunk>
Q1Labs
Symantec
NetIQ

CHANGE MANAGEMENT

ca
hp
bmcsoftware

PLATFORM PARTNERS

IBM
Microsoft
CISCO
hp
vmware
f5
ORACLE
SUSE
redhat
Novell
NetApp

SECURITY ANALYTICS

RSA
hp
splunk>
brinqa
Agiliance
Risk I/O
LockPath
FIREMON

SECURITY COMMUNITY PARTNERS

NIST
INTERNET SECURITY ALLIANCE
CENTER FOR INTERNET SECURITY
CSA cloud security alliance
ICS-ISAC

TRIPWIRE—A HISTORY OF INNOVATION, A TRACK RECORD OF SATISFIED CUSTOMERS

Tripwire is built on a foundation of innovation and deep security expertise—and our success has gained attention worldwide. Over 9,000 organizations, including over half of the Fortune 500, trust us with their security and compliance needs. Tripwire solutions protect many of the largest, most sensitive networks, including nine of the top 10 utilities in the U.S., eight out of the top 10 global retailers, and seven of the top 10 global telecommunications firms. Tripwire enables enterprises, service providers and government agencies around the world to detect, prevent and respond to their most challenging cybersecurity threats.

Tripwire is the leader in both the security configuration management and the security and vulnerability management markets, and is the largest "pure-play" company focused exclusively on these markets. The International Data Corporation (IDC) annual "*Worldwide Security and Vulnerability Management 2014-2018 Forecast and 2013 Vendor Shares*" report shows Tripwire is now the second largest vendor in the policy and compliance category. With 10.3 percent market share in this category, Tripwire's market presence now exceeds Symantec's, and is second only to IBM.

In January 2015, Belden Inc., a global leader in signal transmission solutions for mission-critical applications, acquired Tripwire, adding an important strategic element to Belden's portfolio. Together, the companies will work to deliver the next generation of cybersecurity solutions that will be used secure the enterprise and industrial Internet of Things.

> *"We were able to increase the overall security posture of the university in being able to detect, stop and disable 'break-in' attempts on our systems and infrastructure."*
>
> —NAVENN SHARMA,
> MANAGER OF THE OFFICE OF THE DIRECTOR, IS,
> GRIFFITH UNIVERSITY

> *"We chose Tripwire not only because it is a proven brand, but also for its proficiency in addressing a broad range of regulations and policies our customers face in their respective industries. Tripwire gave us immediate credibility when we launched our PCI services."*
>
> —TIM IRVINE, SALES DIRECTOR,
> INETU

> *"The Tripwire team and people from reseller PointGroup have an enormous amount of product expertise. They really know what they are talking about, and that inspires trust."*
>
> —WARD DEWERCHIN,
> HOST SERVICES & DATA COMMUNICATION MANAGER,
> TOKHEIM

RECENT AWARDS

SC MAGAZINE AWARDS 2014 WINNER Honored in the U.S.

SC MAGAZINE AWARDS 2014 FINALIST Honored in the U.S.

Info Security Products Guide 2014 GLOBAL EXCELLENCE GRAND

Info Security Products Guide 2014 GLOBAL EXCELLENCE GOLD

THE GOLDEN BRIDGE AWARDS GOLD BEST 2014 BUSINESS WORLD

THE GOLDEN BRIDGE AWARDS GOLD BEST 2013 BUSINESS WORLD

Security Bloggers Network All the security news fit to print

CONFIDENCE: **SECURED**

WWW.TRIPWIRE.COM

***THE STATE OF SECURITY*: SECURITY STORIES, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC**