



The Tripwire VIA Suite

IT SECURITY AND COMPLIANCE AUTOMATION WITH TRIPWIRE



Breach-to-Detection Gap Leaves Organizations Exposed and Vulnerable

- Breaches go undiscovered and uncontained for weeks or months in 75 percent of cases

– *Verizon Business, 2009*

- The average time between a breach and its detection: 156 days (5.2 months)

– *Help Net Security, February 2010*

- Breaches that targeted stored data averaged 686 days before detection (almost 2 years)

– *Trustwave, 2010*

The stream of news reports on IT security breaches reveals a critical IT security challenge: the breach-to-detection gap, the time that it takes from the moment a system is breached to the point it is discovered, is far too long. When breaches occur, it might take weeks, months, or even years to detect them. By then, significant damage to reputation and systems has been done, and the costs of recovery can run into the millions—if not *billions*—of dollars.

The way security tools have evolved in isolated silos presents a second challenge: IT staff monitoring one security point system have an incomplete security picture around suspicious events. To complete that picture they must ask other security analysts monitoring other systems for data related to a suspicious event. With up to billions of events occurring each and every day, these requests add up, placing overwhelming demands on IT without gaining effective insight into the true state of security.

The new Tripwire® VIA™ suite tackles these IT security challenges head on. Tripwire VIA solutions work together to provide the visibility, intelligence and automation IT security needs to narrow the breach-to-detection gap from weeks, months, or years to minutes. And they do this while keeping a pulse on the billions of log and change events being tracked by different security point solutions across the IT infrastructure every day. Tripwire VIA provides real value by combining information from each solution in a way

that rapidly identifies vulnerabilities from non-secure or non-compliant configurations and any breaches that have taken advantage of them.

Tripwire VIA solutions integrate out of the box to address the issue of siloed security tools and the vast quantities of data they produce. By automatically correlating change and configuration data from one solution with log and event data from another, Tripwire VIA provides IT security teams visibility across silos of data that independent solutions cannot

SOLUTION BRIEF

Simplify the Approach to Security

“CISOs needed to focus on efficiency, automating processes, standardizing, and centralizing wherever possible.”

– Paul Dorey, Director, Security Faculty, and former CISO, BP, speaking to CISOs and CSOs at the Forrester EMEA Security Forum in London, April 2009

match. Plus, customers of Tripwire VIA solutions gain these benefits without the complexity and bloat associated with traditional security tools.

TRIPWIRE VIA SOLUTIONS DELIVER IT SECURITY AND COMPLIANCE

Tripwire VIA solutions deliver actionable intelligence to help IT staff prioritize threats so they can focus on the most critical ones. This intelligence offers security—and easily proven compliance as a natural byproduct of that security—by providing complete visibility to all events of interest, from log and change events to other security events.

Proactive alerts, along with reports and dashboards that combine this information in meaningful ways, let IT identify threatening patterns as they occur, so they can forestall attacks and rapidly remediate vulnerability issues. Out-of-the-box reports and dashboards also provide evidence of compliance status and how IT has addressed any compliance issues. With these capabilities, critical data stays protected and IT has proof that security controls are in place to meet required compliance standards.

Specifically, the Tripwire VIA suite:

- Combines log and event data with real-time change data to immediately reveal events of interest that impact policy or threaten security;
- Supports incident investigation by providing access from a Tripwire console to log and event data related to a file or configuration change;
- Offers global search capabilities to identify patterns and threats that might relate to specific changes;
- Provides visibility to downstream impacts of a given change, such as all

changes or events associated with the addition of unauthorized users; and

- Enables instant audit logging across Tripwire Enterprise-monitored infrastructure without installing additional code on individual systems.

AVAILABLE TRIPWIRE VIA SOLUTIONS

The Tripwire VIA suite includes Tripwire® Log Center for next-generation security information and event management (SIEM), and Tripwire® Enterprise, the industry-recognized solution for configuration control. By design, Tripwire VIA solutions integrate out of the box to offer visibility to the entire IT infrastructure, intelligence to make better decisions faster, and automation to reduce manual, repetitive tasks.

COMBINE TRIPWIRE VIA SOLUTIONS AND TAKE CONTROL

For IT security, Tripwire VIA solutions forever change how they address the security and compliance needs of IT infrastructure. The out-of-the-box integration of these solutions helps IT narrow the breach-to-detection gap, reducing the financial costs and loss of reputation and customer trust associated with breaches that go undetected for long periods of time. The integration also eliminates the issue of siloed IT security tools that produce unmanageable amounts of uncorrelated data.

When used together, Tripwire VIA gives IT security unparalleled visibility to the change, log and event data generated across the IT infrastructure, and therefore a clearer view of the activities that impact policy and threaten security. With Tripwire VIA, IT can take control of threats, reduce the breach-to-detection gap, generate proof of compliance, and gain greater visibility over to the entire IT infrastructure.

TRIPWIRE VIA FOR TRIPWIRE LOG CENTER USERS

The Tripwire VIA suite lets Tripwire Log Center users immediately respond to events of interest. Designed and built from the ground up as a complete log and event management solution, Tripwire Log Center avoids the complexity and high cost of ownership associated with traditional SIEM tools.

Tripwire Log Center includes:

- High-speed log archiving
- Google-like log indexing for fast log data searching
- Intelligent reporting
- Immediate visibility to events of interest
- Automated Correlation of log and change event data
- Threat pattern identification

TRIPWIRE VIA AT WORK THROUGH TRIPWIRE LOG CENTER

Tripwire VIA helps Tripwire Log Center users identify events of interest that impact policy and threaten security. For example, a security analyst reviews logs and discovers an unauthorized user has accessed a given system. Using the suite, a security analyst not only detects this activity, but also sees that the unauthorized user changed a file containing user account information for the system—a combination of events that warrants further investigation.

TRIPWIRE VIA FOR TRIPWIRE ENTERPRISE USERS

The Tripwire VIA suite provides equally powerful benefits to Tripwire Enterprise users, letting them discover the root cause of detected changes, identify suspicious activities that preceded or followed the change, and determine whether changes that occurred after it were caused by the same user or IP address.

Tripwire Enterprise offers:

- File integrity monitoring
- Compliance policy management
- Real-time analysis of change
- Remediation advice for changes that introduce risk or non-compliance

TRIPWIRE VIA AT WORK THROUGH TRIPWIRE ENTERPRISE

Tripwire VIA lets Tripwire Enterprise users correlate change data with event data in a single, intelligent, automated solution. For example, a user notes that a specific change caused a node to fail a PCI compliance policy test. With Tripwire VIA, the user gains access to log data related to the change. This data can help assure it was a business-as-usual change, or may reveal the seeds of a malicious attack by noting that numerous failed login attempts and one successful one preceded the change.

ABOUT TRIPWIRE

Tripwire is the leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Over 7,000 customers in more than 86 countries rely on Tripwire's integrated solutions. Tripwire VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and event management solutions, is the way organizations proactively prove continuous compliance, mitigate risk, and achieve operational control through Visibility, Intelligence and Automation. Learn more at tripwire.com.

