

Announcing Tripwire Enterprise

Change Auditing software for enterprise IT organizations

SUMMARY:

On Monday, January 31, 2005, Tripwire will publicly announce and release Tripwire Enterprise, Tripwire's newest product for automated and independent change auditing of servers, desktops and network devices. Tripwire Enterprise detects both automated and manual changes, reconciles authorized and intended changes, and reports change activity to prove infrastructure integrity and process effectiveness.

Tripwire has already established itself as the world leader in change auditing solutions. Tripwire Enterprise combines and extends the best capabilities of Tripwire for Servers (TFS) and Tripwire for Network Devices (TND). For TND customers, Tripwire Enterprise provides a complete superset of features and is the follow-on version. For TFS customers, Tripwire Enterprise provides a migration path for advanced, enterprise-class capabilities. TFS will continue to be supported and enhanced, and continues to be a good solution for existing customers as well as new customers who do not require the advanced functionality of Tripwire Enterprise. Conversion kits are available to move from TFS to Tripwire Enterprise for a nominal cost. Key enhancements include:

- Auditing of changes to servers and network devices within a single product
- Comprehensive library of graphical reports and dashboards that display infrastructure-wide change activity in easy to use formats
- Web-based console and role-based permissions to support multiple users
- Scalable architecture designed to support up to 100,000 network devices and 10,000 file systems
- Extensible architecture to enable new monitoring capabilities in the future (e.g. data base monitoring in Q2)

With Tripwire Enterprise, customers can deploy the leading-edge change auditing solution to demonstrate compliance, increase availability and enhance security.

ABOUT THIS PRODUCT BULLETIN:

This document is provided to Tripwire field personnel and channel partners to assist in effectively selling new products and services. This product bulletin is for internal use only and should not be shared with customers. Please remember that all information on Tripwire Enterprise is confidential until the announcement date of January 31, 2005.

MARKET DESCRIPTION:

Over the past year enterprise infrastructure management technologies have increased in importance and visibility. This is being driven by a combination of concerns over compliance and security requirements plus the opportunities to improve availability, increase automation and reduce costs. These dynamics have created a renewed focus on Change and Configuration Management, because having a change process that is automated and in control is a prerequisite for the rest of the IT infrastructure to operate properly. And Change Auditing is the cornerstone of a controlled change management process.

Tripwire defines Change Auditing as the automated and independent detection, reconciliation and reporting of all changes across the breadth of the IT infrastructure. This means detecting both automated changes made by other tools as well as manual changes. This means reconciling authorized and intended changes from unexpected changes. And this means reporting changes in meaningful ways that allow for the quick identification of critical events.

Tripwire is the only company that provides true Change Auditing functionality in the marketplace today. These capabilities have already been available to users of Tripwire for Servers and Tripwire for Network Devices. Tripwire Enterprise now enhances and integrates these capabilities, taking Change Auditing to the next level.

BUSINESS BENEFITS:

Tripwire change auditing provides benefits in three primary areas – compliance, availability and security. Any of these areas by itself may be sufficient to justify purchase, and it is important to pitch the benefit area(s) that best match each customer's need.

Compliance: External regulations as well as good internal process controls require IT organizations to audit and demonstrate that their infrastructure is in its expected state and that the processes used to control infrastructure changes are performing effectively.

Tripwire Enterprise demonstrates compliance because:

- Tripwire Enterprise is a detective control that provides independent, verifiable evidence to prove the integrity of change management and security policies (process integrity) and demonstrate that systems operate in a known and trusted state (system integrity).
- Tripwire Enterprise's compliance reports document and categorize infrastructure changes, enabling managers to evaluate the effectiveness of change management processes.

Availability: Approximately 80% of outages are caused by people and process issues, including poor change management practices. Furthermore, when an outage occurs, approximately 80% of the remediation time is spent trying to determine what change caused the outage. Tripwire Enterprise increases availability because:

- Tripwire Enterprise detects and notifies users of undesired changes. Unauthorized and/or unintended changes are quickly identified allowing them to be investigated and remediated, often before a problem results.
- When a problem does occur, Tripwire speeds remediation by quickly answering the questions: What changed? When did it change? Who made the change? Was the change approved?

Security: Tripwire’s traditional “value proposition” is still an excellent reason to purchase Tripwire products, providing evidence that system integrity is intact and increasing confidence that perimeter security strategies are effective. Tripwire Enterprise enhances security because:

- If an unauthorized change is made to a critical server or network device, Tripwire will quickly detect it and notify responsible parties, allowing rapid investigation and remediation.
- Tripwire Enterprise captures change history describing exactly what changed, when it changed, how the change was made and by whom. This forensic information is archived in Tripwire’s database and is available for subsequent analysis.

PRODUCT DESCRIPTION:

Tripwire Enterprise provides a single point of control for independently auditing changes to servers, desktops and network devices to prove infrastructure integrity and process effectiveness. Tripwire Enterprise detects both automated and manual changes, reconciles authorized and intended changes, and documents activity with its library of reports and management dashboards.

Tripwire Enterprise functionality can be grouped into the following capabilities:

Change Detection: Tripwire Enterprise enables IT staff to better meet the needs of business users by validating changes across the breadth of IT infrastructure. Tripwire captures a baseline of file systems and network device configurations in a known-good state. Subsequent integrity checks automatically compare the current state against this baseline to discover any and all changes. Because Tripwire Enterprise is independent of changes made by manual actions, scripts or commercial tools that implement changes, it provides evidence that preventive controls are operating as expected and that changes made to production systems are under control. Key detection features include:

- Broad coverage of infrastructure elements including Windows desktops and multi-vendor servers, routers, switches, firewalls and load balancers.
- Extensible architecture to support additional monitored node types, e.g. database monitoring is planned for the Q2 release.
- Pre-packaged agents in native formats (e.g. Windows MSI) allow for quick deployment with existing software distribution tools; after initial installations, agents self-update as needed.

- Object-based, shared rules reduce administrative overhead and promote consistency across the enterprise.
- Complete change history is archived and available in Tripwire Enterprise's database, including attributes, permissions and has values.
- Version comparisons can be performed between two change histories, highlighting exactly what has been changed, added or deleted.
- Severity levels denote the relative significance of a change according to monitoring rules and can generate different response actions.
- When a questionable change has been detected, IT staff can be immediately notified via email, pages or through their change ticketing system.
- Command execution on either Tripwire Enterprise/Server or on monitored nodes enable automated responses to specific changes.

Change Reconciliation: Tripwire Enterprise provides the details essential to manually reconcile detected changes, plus provides multiple methods to automatically reconcile changes. Tripwire can cross check detected changes with manually documented change lists, with automatically generated lists created by software provisioning tools, or with a known-good reference system. Additionally, Tripwire Enterprise can query leading change ticketing systems to determine if an approved work order corresponds to the detected change. If the change matches an approved work order, Tripwire Enterprise can automatically update its baseline and annotate the work order with actual change information to validate the change. Key reconciliation features include:

- Baseline management and promotion, enabling users to designate only "known and trusted" configuration revisions as the point for subsequent version checking, and only promote new configurations that have been confirmed as desired.
- Detailed change information that captures, correlates, and records when a change occurred, who made the change and how the change was made, aiding in determining if a change should be promoted to be the new baseline or not.
- Automatic promotion of changes to current baselines when matching a pre-defined list of expected changes.
- Command Line Interface allows Tripwire Enterprise commands to be executed via command line or scripting to invoke a variety of program functions.
- Packaged integration are available for BMC Remedy AR System and (in Q2) HP OpenView Service Desk.
- Web-services and ODBC/JDBC interfaces are available for use with the assistance of Tripwire Professional Services.

Change Reporting: Tripwire Enterprise includes an extensive library of tailorable change audit reports and dashboards to demonstrate compliance, increase availability, and enhance security. Key reporting features include:

- Archived audit trail of all changes to specified assets including who made the changes, what changes were made, plus when and how the changes were made.
- Change status to help change and release managers validate approved changes.
- Real-time status of nodes supporting a specified service to help incident management determine outage root causes.
- Documented effectiveness of change management processes showing the number of unapproved changes, the overall compliance level to the change policy, and the occurrence of inconsistent changes across similar systems.
- Metrics to assist management as they improve their processes. For example, trending the quantity of unapproved changes or showing the change rate for a particular group of servers and/or network devices.
- Users can easily tailor reports and dashboards, schedule when they run, output them in PDF, HTML, or XML formats, and archive them for future reference.

Tripwire Enterprise has been specifically architected to be useable in the largest of IT environments. Key manageability features that make the product “enterprise class” are:

- Internal usage of a relational database for storing change data.
- Supports up to 100,000 network devices and 10,000 files systems.
- Supports an unlimited number of simultaneous, remote user sessions via its web-browser interface.
- Hierarchical groups manage large numbers of monitored nodes, rules, reports, and users. These groups are logical views allowing interaction with nodes, rules, etc. as user-defined collections.
- Utilizing secure protocols to communicate with monitored nodes and web browsers to ensure data communication is not compromised.
- User access controls to ensure users are authenticated and authorized to perform specific actions.

CONFIGURATION AND PRICING:

Tripwire Enterprise will be available for customer purchase on January 31, 2005. The product consists of the following component types:

1. **Tripwire Enterprise Server:** This is the core engine of the product, providing all management, administration and reporting functions, and includes the database, web server and access to the web-based console. This is a required component for a Tripwire Enterprise installation.
2. **Tripwire Enterprise Nodes:** Each node represents a monitored network system or device. There are initially three node types: server file systems (FS), desktop file systems (DT), and network devices (ND). A node license must be purchased for each monitored element and nodes may be purchased in any combination.

Pricing for Tripwire Enterprise is as follows:

Component	List Price
Tripwire Enterprise/Server – License	\$3,995
Tripwire Enterprise/FS-4 (1-4 processors) – License	\$595
Tripwire Enterprise/FS-16 (5-16 processors) – License	\$895
Tripwire Enterprise/FS-17 (17+ processors) – License	\$1,395
Tripwire Enterprise/DT – License	\$95
Tripwire Enterprise/ND – License	\$125

Because of the many possible combinations of different node licenses and quantities, rather than provide multi-tiered or packaged pricing, customers will receive a volume discount on the total license amount on the same Purchase Order, as follows:

Total Gross License Fees on PO	% Discount
\$1 – \$14,999	0%
\$15,000 - \$24,999	5%
\$25,000 – \$49,999	10%
\$50,000 – \$99,999	15%
\$100,000 – \$199,999	20%
\$200,000 – \$349,999	25%
\$350,000 – \$499,999	30%

One year of standard support is 20% of the total license price, after volume discount.

Pricing Example: As an example, the total price for a new customer ordering Tripwire Enterprise to monitor 50 single-processor systems, 25 eight-processor systems and 200 network devices, including support, would be computed as follows:

Example Price Calculation	Qty	List Price	Extended Price
Tripwire Enterprise/Server – License	1	\$3,995	\$3,995
Tripwire Enterprise/FS-4 – License	50	\$595	\$29,750
Tripwire Enterprise/FS-16 – License	25	\$895	\$22,375
Tripwire Enterprise/ND – License	200	\$125	\$25,000
Total Gross License Amount			\$81,120
Standard Discount		15%	(\$12,168)
Adjusted License Amount			\$68,952
Support (one-year standard)		20%	\$13,790
Total			\$82,742

Please refer to the official price list for a complete listing of Tripwire Enterprise products, services, packages, support and upgrade options, as well as for part numbers and channel pricing.

PRODUCT POSITIONING:

Tripwire Enterprise combines and extends the best capabilities of Tripwire for Servers (TFS) and Tripwire for Network Devices (TND). Since it incorporates significant aspects of the latest versions of both products (TFS 4.5 and TND 3.1), the initial offering of Tripwire Enterprise is designated version 5.0. This reinforces the point that Tripwire Enterprise is built on a solid foundation and offers a high level of product maturity and stability.

Although TND orders will continue to be accepted for at least the next 90 days, Tripwire Enterprise is meant to be the follow-on to the TND product line. Tripwire Enterprise is built on the same architecture as TND and provides a superset of TND's capabilities. The price of a Tripwire Enterprise product configured for monitoring network devices is approximately the same or less than the equivalent TND configuration.

Tripwire for Servers, on the other hand, will continue to be supported and enhanced. For new customers, TFS continues as Tripwire's product of choice for small-to-medium IT organizations whose change monitoring needs are limited to a moderate number of servers. At smaller configuration levels, TFS is also less expensive. (At larger configurations, the prices are approximately the same).

Tripwire Enterprise's OS support will initially be limited to Windows and Solaris. Customers needing broader support for server file monitoring or as a platform for running Tripwire Enterprise/Server should use TFS until subsequent Tripwire Enterprise releases provide the needed coverage (see TFS Migration Strategies below).

MIGRATION STRATEGIES – TND:

For TND customers, Tripwire Enterprise 5.0 is the version following TND 3.1. There is no charge for current TND customers on support to upgrade to Tripwire Enterprise, and all TND customers are encouraged to do so. TND license keys (certs) will work with Tripwire Enterprise.

Advantages of upgrading from TND to Tripwire Enterprise include:

- Tailorable reports and management dashboards
- Available server and desktop file system monitoring in the same product
- Network device firmware version tracking
- Expanded command line interface
- Available integration with BMC Remedy AR System and (in Q2) HP OpenView Network Node Manager

MIGRATION STRATEGIES – TFS:

Although Tripwire Enterprise provides a number of capabilities beyond TFS, it is not a complete superset. In addition, the method used for defining and managing policies within Tripwire Enterprise is different than TFS. Ultimately, it is more powerful and provides greater flexibility – but for current TFS customers, it is different and will require some conversion effort and training. This can be mitigated somewhat with an automated conversion tool available from Tripwire, but it will still require some manual review and learning a new interface.

Current TFS customers on support may exchange their licenses on a one-for-one basis to Tripwire Enterprise licenses. Advantages of upgrading from TFS to Tripwire Enterprise include:

- Tailorable reports and management dashboards
- Support for multiple, distributed console users
- Hierarchical groups for monitored nodes, rules, reports, and users
- Scalability to 100,000 network devices and 10,000 file systems
- Available network device monitoring in the same product
- Agent-less coverage for any POSIX compliant OS
- Interface options using Tripwire Professional Services for web-services and ODBC/JDBC interfaces

Despite these advantages, current TFS users may reasonably decide not to convert if their current implementation is meeting their needs, i.e. “if it ain’t broke, don’t fix it.”

In addition, there are a few features and platforms supported in TFS that will not be available in Tripwire Enterprise until later releases, specifically:

- Platform support for running Tripwire Enterprise/Server: Red Hat Linux (Q2)
- Server File Monitoring: Red Hat Linux (Q2), AIX (Q2), HP-UX (Q3)
- Registry Monitoring: Windows Registry (Q3)
- Integrations: HP OpenView Service Desk (Q2)

For those TFS users electing to delay or decline conversion to Tripwire Enterprise, TFS will continue to be supported and enhanced, with new releases planned for 2005.

The recommended progression for a TFS customer to decide whether to convert to Tripwire Enterprise is as follows:

1. View the Flash Presentation for a product overview
2. Use the Trial Kit to sample the new features and operation in a contained (single computer) environment
- 3a. Purchase the Conversion Kit
- 3b. Install the Evaluation Copy for in-depth evaluation and internal testing

The Conversion Kit is available for a one-time fee of \$1,995 and provides the customer with key conversion resources for a period of 90 days, specifically:

- Webcast training
- Access to the Conversion Desk for technical assistance
- Tripwire Manager to Tripwire Enterprise Conversion Utility

Customers can best assess their conversion effort by using the Conversion Kit in combination with the Tripwire Enterprise evaluation software. Customers not purchasing a Conversion Kit will be supported by their Systems Engineer, (not the Conversion Desk). Conversion assistance can also be purchased from Tripwire Professional Services.

When a customer is ready to cut-over, they sign a License Exchange Agreement and Tripwire will then provide them with new Tripwire Enterprise license keys (certs).

COMPETITIVE POSITIONING:

The renewed importance of Change and Configuration Management (CCM) creates a great opportunity for Tripwire, as the company is at the center of the CCM space. But at the same time it creates a more muddled competitive landscape, as more companies expand their offerings in this space. Many of these companies' products overlap, to some degree, with Tripwire Enterprise, as they have some ability to detect changes within their sphere of interest. But the other vendors all have as their primary focus some other area of CCM than Change Audit. These other areas, with a few example companies, include:

- **Enterprise Management Systems** (BMC, HP Service Desk, IBM Tivoli, Computer Associates, Mercury Interactive)
- **Provisioning and Patch Management** (BMC Marimba, HP Novadigm, Opsware, BladeLogic, Patchlink, Altiris, Ecora Patch Manager)
- **Application Services Discovery and Management** (Relicore, Cendura, Troux, Collation, mVallent)
- **Server Configuration Management** (Configuresoft ECM, Ecora Auditor)
- **Network Device Configuration Management** (AlterPoint, Intelliden, Rendition, Voyence, SMARTS)
- **Security** (Symantec ESM, CA eTrust, ISS System Scanner, Bindview by-Control, Pedestal SecurityExpressions, Configuresoft ECM)

Tripwire, by focusing on Change Auditing, is the only company that provides the automated and independent detection, reconciliation and reporting of all changes to the IT infrastructure. This is a prerequisite to having a change system that is “in control”.

Other vendor offerings have the following limitations, relative to Change Auditing:

- No independence – the same tool that makes the changes, reports the changes
- Limited detection capability – these tools will only detect changes within their own domains, e.g. only track and report back those elements they are managing or controlling
- Little or no ability to reconcile changes outside their own tool – their focus is on handling the change within their own tool set
- Simplistic change reporting – while these tools may provide great reporting within their domain-of-interest, they typically are not as good at providing detailed reporting useful for infrastructure-wide change management

As such, Tripwire Enterprise is at the core of any robust CCM system and complements the capabilities of these other vendors in this space. Unfortunately, the customer (and other vendor) may not always see it that way, and a competitive situation may be created when the degree of feature overlap is high, the level of organizational complexity is moderate and budget dollars are limited. In these cases, it is important to reinforce Tripwire’s unique value-adds:

- **Independence** – separate the process of making change from reporting change
- **Breadth of detection** – detects all changes, not just those changes made by the CCM tool, (e.g. manual changes), in both servers and network devices
- **Depth of detection** – detects changes to all types of files, attributes and directories (not just those tracked by the other CCM tool)
- **Reconciliation** – ties directly into change-ticketing and release management systems, plus provides detailed change information to assist with manual user reconciliation, (other CCM tools are often self-contained)
- **Better reporting** – provides a more robust and flexible set of reports, with a high degree of granularity, severity levels, hierarchical groupings, and more rigorous control over baselines

SALES SUPPORT MATERIALS:

The following Tripwire Enterprise sales materials will be available by January 31, 2005 to help with your selling process:

- Website update
- Product brochure
- Product presentation
- Flash demo
- Trial kit
- Users manual
- Price list
- Evaluation guide (available Feb. 15th)

SUMMARY:

Tripwire Enterprise provides automated and independent change auditing of IT infrastructure. The announcement of Tripwire Enterprise will further enhance Tripwire's leading position in providing Change Auditing solutions, and creates a great sales opportunity for all Tripwire direct sales and channel partners.

For additional information, contact the Tripwire Marketing Department.