

SOLUTION BRIEF

Tripwire Enterprise Configuration Audit & Control for Microsoft Applications



"Ensuring the consistent availability of our website and email is of the highest priority because they are our primary communication channels to schools, students and employees. That is why we are employing Tripwire to help monitor these systems for unauthorized and unintended changes, further hardening our services, and operationalizing our ability to meet business demands."

— Chad Plemons
VP Information Technology
EdFinancial Services

➔ Change is a challenge in any IT environment, but change can be particularly risky on application servers as it can have the most immediate affect on business. While widely used applications such as Microsoft Exchange and Microsoft IIS have grown more stable, the sheer number of changes that can create a disruption in service has also grown more complex. A single unauthorized or non-compliant change can result in serious service impacts if one of these systems slows or fails. That's why it is important to achieve and maintain the integrity of the IT configurations of these mission-critical applications.

Tripwire helps over 6,000 customers worldwide achieve and maintain a known and trusted state. Tripwire Enterprise's application monitoring includes:

- A collection of critical change auditing rules for business-critical applications, enabling the detection of all changes across the data center;
- Out-of-the-box library of security, regulatory and operational policies;

- Performance assessment policies for business-critical applications designed by industry experts to analyze an application's implementation, and evaluate configured settings against best practices for maximum performance; and
- Comprehensive, actionable reports and dashboards to demonstrate a known, trusted state.

Tripwire Enterprise's out-of-the-box coverage of applications provides a single point of configuration control for ensuring the rapid discovery of all service-affecting changes, and that all unauthorized changes are immediately detected and investigated. Tripwire can be customized to reduce the "noise" of business-as-usual changes, and instead concentrate on changes—authorized or not—that are most critical to operations. Tripwire also provides these same assurances for non-Microsoft platforms, giving you a single point of control over the entire data center. With Tripwire's core capabilities, IT organizations can achieve and maintain a known and trusted efficiently and effectively.



Tripwire detects change across your entire ecosystem, including Windows, Microsoft applications (such as Exchange and IIS), Active Directory and SQL. It seamlessly integrates into any environment, bringing immediate value to your business.

Configuration Audit and Control for the Microsoft Environment

The ability to know exactly what changed—and who made the change—is powerful in ensuring the quality, advanced security and predictability of services. Tripwire Enterprise detects change across your entire ecosystem, including Windows, Microsoft applications (such as Exchange and IIS), Active Directory and SQL. It seamlessly integrates into any environment, bringing immediate value to your business with these out-of-the-box capabilities:

Configuration and Risk Assessment

Achieving a known and trusted state across the entire data center is a challenging task for even the most technically adept and process-focused organizations. Tripwire Enterprise proactively captures detailed configuration information from across your data center and automatically compares this configuration data against Tripwire's unparalleled library of security, regulatory and operational policies. Tripwire Enterprise reduces an organization's exposure to risk, decreases unplanned work, and ensures you can demonstrate the state of your data center.

Change Auditing

Tripwire delivers real-time, tunable change detection to the Microsoft infrastructure, improving the integrity and availability of the entire ecosystem, and minimizes risks from unknown and unmanaged changes.

Comprehensive Alerting and Reporting

Tripwire provides immediate alerting to unauthorized change, and comprehensive reporting to proactively take action through reconciliation, remediation and reporting techniques.

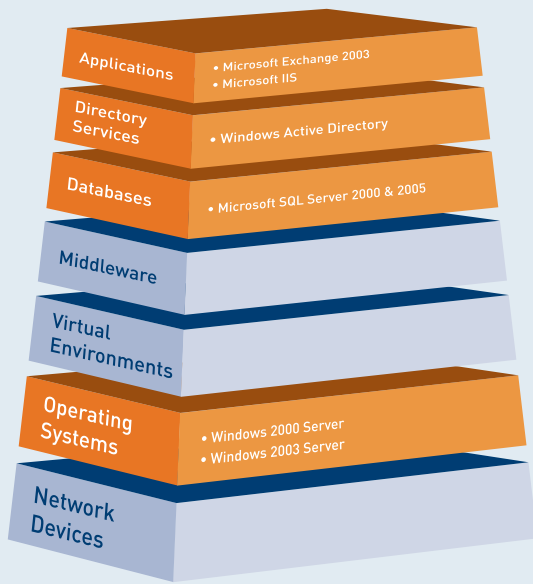
Reconciliation

Tripwire categorizes changes that pose potential risk to the business, providing the flexibility to quickly and easily reconcile changes that are unauthorized, and effectively resolve and restore business services and bring systems back to a known and trusted state.

Managing Microsoft Applications: A Single Point of Control

A workday without email is nowadays unimaginable. Businesses rely so heavily on applications such as Microsoft Exchange that a disruption in service can put an abrupt halt to business-critical transactions and greatly reduce productivity. And Microsoft Exchange is not just about email; it's also about calendars, contacts, and collaboration between colleagues and customers—each and every day. Any IT organization focused on servicing its business customers implicitly understands the importance of ensuring 100% availability, integrity and security of its email application. Similarly, with Microsoft IIS serving over one third of all corporate Web sites, it is critical to ensure its reliability and security.

Tripwire provides compliance, security and operational solutions for Microsoft applications. For compliance purposes, Tripwire helps achieve and maintain regulatory compliance and demonstrate proof of compliance across the entire Microsoft platform. For security concerns, Tripwire helps reduce business risks by guarding against unauthorized change and assessing systems against leading security standards. And for IT operations, Tripwire increases operational efficiency improving service availability and speeding the recovery of service outages caused by unauthorized change.



Tripwire Enterprise Microsoft Configuration Audit and Control in the IT Infrastructure

Tripwire's configuration audit and control capabilities cover the entire Microsoft environment, offering a single point of visibility and change control for Security, Compliance and IT Operations.

Many IT organizations desiring to increase service levels, decrease costs and improve security look to the ITIL framework for guidance. ITIL® (the IT Infrastructure Library), is widely accepted as the world's leading compilation of IT best practices. Similarly, the Microsoft Operations Framework (MOF) is a collection of best practices, principles, and models that provide comprehensive technical guidance for achieving mission critical production system reliability, availability, supportability, and manageability for solutions and services built on Microsoft products and technologies. Tripwire strongly supports and accelerates the adoption of ITIL and the Microsoft Operations Framework.

Release Processes

Tripwire captures a known, good state in preproduction, and then captures production changes that need to be included into the build.

Resolution Processes

Tripwire enforces the change process, ruling out change as early as possible in the repair cycle.

Control Processes

Tripwire protects high-risk systems from inappropriate change, enforcing a change freeze and preventing configuration drift (inaccuracies from a known state).

ENSURING SECURITY AND PERFORMANCE IN MICROSOFT EXCHANGE AND IIS

Tripwire delivers a comprehensive set of configuration and control capabilities to ensure that Microsoft Exchange and IIS applications operate at peak security and performance.

- Change auditing rules that support Microsoft policies.
- Center for Internet Security (CIS) configuration assessment policies, an industry best practices security standard. CIS benchmarks contains information for securing Exchange capabilities, such as logging, services (IMAP4 Server, POP3 Server, SMTP Server), and features (Outlook Mobile Access, ActiveSync, Outlook Web Access and Public Folders).
- Payment Card Industry Data Security Standard (PCI DSS) compliance policies for web-enabled applications that store cardholder information, and to protect against security attacks.
- Tripwire performance assessment policy for analyzing configuration settings against best practices for maximum performance.

Key Features and Benefits

As the recognized leader in Configuration Audit and Control, Tripwire helps you achieve and maintain compliance, mitigate business risk, and increase operational efficiency, whether your application environment is mostly Microsoft, or a mix, as well as the unique heterogeneous system of various network devices, operating systems, virtual environments, and middleware that make up the rest of your IT infrastructure.

Detect All Change

- Minimize manual efforts—Tripwire Enterprise's detective controls alert you to unauthorized changes made throughout business-critical applications. Tripwire detects all change across the data center, real-time within the Microsoft environment, including Exchange, IIS, Active Directory, Windows and SQL Server.

Availability and Integrity of Core Business Applications

- Minimize types of changes that cause disruption, discovering unauthorized changes and configurations before they create critical issues
- Gain valuable insights into the root cause of service outages or degradations
- Validate applied patches

Reliable, Scalable, Predictable Enterprise Applications

- Maintain a known and trusted state by reducing business risk associated with change
- Reduce service level agreement penalties by decreasing the unscheduled downtime that can violate service level agreements

Process Enforcement

- Promote broader use of automated tools through increased visibility and control of their circumvention

Tripwire Specifications for the Microsoft Environment

Tripwire supports and seamlessly integrates into Microsoft Applications and Windows operating systems, up and down the service stack. Tripwire Enterprise coverage of the Microsoft infrastructure includes:

Microsoft Exchange 2003

- Binary and executable files
- Registry
- Patch levels
- Versions
- Mailbox settings in AD
- Configuration files
- Settings
- DLL
- Directories

Microsoft IIS

- Windows File Systems
- Windows Registry

Windows Active Directory

- Password settings
- User permissions
- Network settings
- Group updates
- Security policies

Microsoft SQL Server 2000 & 2005

- Security privileges
- Access settings
- Schema objects
- Configuration parameters
- User roles and permissions

Windows system properties

- File adds, deletes, modifications
- Registry keys and values
- Event tracking
- Installation package data
- Flags: archive, hidden, offline, temporary, system, compressed
- Access, write and create time
- File and directory type, and file size
- Owner, Group, DACL, SACL, read-only
- Number and hashes of alternate data streams
- Growing attribute

Microsoft Windows

- Windows NT 4.0
- Windows 2000 Server
- Windows Server 2003 (incl. x64 Editions)
- Windows XP Professional
- Windows 2000 Professional

About Tripwire

Tripwire, Inc. is the recognized leader of configuration audit and control solutions, serving over 6,000 enterprises worldwide. As the first in the industry to combine configuration assessment with configuration change auditing, Tripwire helps IT organizations automate compliance across the data center, reducing risk and increasing operational efficiency. Tripwire ensures the organization achieves continuous operational, regulatory and security compliance, helping IT achieve and maintain a known, trusted and compliant system state. Tripwire is headquartered in Portland, Oregon. with offices worldwide. For more information visit www.tripwire.com.



www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA