

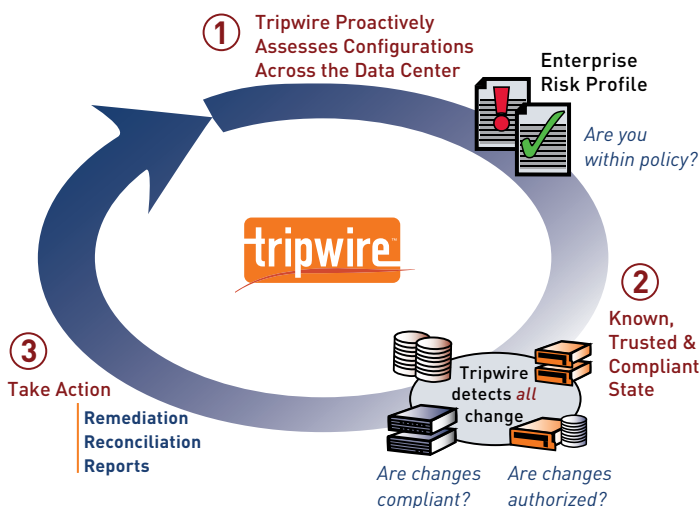
Configuration Assessment

Automated, Continuous Compliance with Tripwire Enterprise

One of the leading causes of security breaches, loss of data, and regulatory non-compliance are improperly configured systems. That's why it is so important to keep IT systems in a known, trusted and compliant state. But given today's complex infrastructure, a compliant state is beyond the capabilities of manual change control solutions. It requires a solution that can automatically audit change and manage the assessments of configurations across the data center, determining the degree of risk for operational, regulatory and security vulnerabilities. To be truly effective, controls must cover the entire enterprise, monitoring activity occurring on servers, network devices, databases, directories, virtual environments, and—for retail organizations—points of sale.

AUTHORIZED, WITHIN POLICY AND COMPLIANT

Tripwire® Enterprise is the first solution to effectively combine configuration audit and control with configuration assessment, enabling automatic evaluation of configuration changes against policies that address three critical concerns: Is the change authorized, within policy, and compliant? Tripwire's process delivers a known, trusted and compliant state:



- Tripwire Enterprise scans the entire IT infrastructure's configuration settings, providing a baseline configuration known state.
- It then analyzes all configuration settings and identifies the difference between the current state and an established known good or compliant state, then provides an enterprise risk profile.
- Using policy-driven capabilities, Tripwire Enterprise detects all change as it occurs, no matter the source, and without the need to re-scan the entire system. Those changes are then assessed for policy and process compliance.
- Changes that put the system out of policy compliance are automatically escalated so immediate action can be taken.

Tripwire proactively assesses such system settings as startup procedures, auditing policies, account policies, security settings, user rights, and file and registry permissions. In all, Tripwire runs thousands of tests throughout the data center. Although audits are periodic, risks must be controlled continuously, so Tripwire utilizes remediation, reconciliation and reporting techniques to alert you when non-compliance is detected. Tripwire's unique and comprehensive approach ensures your systems achieve and maintain a known, trusted and compliant state.

TRIPWIRE LEVERAGES INDUSTRY STANDARD BENCHMARKS

Tripwire's powerful approach leverages industry standards, specifically benchmarks from The Center for Internet Security (CIS). Highly recommended by SANS (the SysAdmin, Audit, Network, Security Institute), analysts and customers, CIS uses team-developed consensus benchmarks for system configurations, and acts as a certifying agency. CIS benchmarks include tens of thousands of configuration assessments for operational, regulatory and security policy compliance, enabling automatic, out-of-the-box policy compliance testing for PCI, SOX, COBIT, FISMA, and many other data center-specific standards

TRIPWIRE'S POLICY MANAGER PROVIDES FLEXIBILITY

Within the Tripwire Enterprise configuration assessment capability is the Policy Manager function. This allows customization of policy assessment, providing the flexibility to modify out-of-the-box policies, or create a custom policy to meet specific business needs. Configuration assessment policies can be downloaded from Tripwire's Customer Support Center.

CURRENTLY AVAILABLE POLICIES *(New policies are continuously under development and made available for download)*

SOURCE	POLICIES	PLATFORMS
CIS	24	AIX, Cisco, HP-UX, Oracle, Linux (Red Hat and SUSE), Solaris, Windows, SQL Server, Exchange and IIS
PCI	20	AIX, Cisco, HP-UX, Oracle, Linux (Red Hat and SUSE), Solaris, Windows, SQL Server, Exchange and IIS
TW	17	AIX, Cisco, HP-UX, Oracle, Linux, Solaris, Windows, SQL Server, Exchange and IIS
DISA	5	Solaris, Linux (Red Hat), Windows
NIST	5	Solaris, Linux (Red Hat), Windows
FISMA	2	Solaris, Windows

COMPLIANCE REPORTING

Tripwire's pre-defined, out-of-the-box reports provide holistic views of configuration assessment and change auditing activities. Users can easily develop custom reports to capture and view the information most critical to their business. Tripwire Enterprise reports also include drill-down capabilities so IT can quickly pinpoint and correct the cause of a problem generated by out-of-policy or unauthorized change.

BENEFITS OF TRIPWIRE ENTERPRISE CONFIGURATION ASSESSMENT

Automated continuous compliance with demonstrable proof	The combination of change auditing and configuration assessment gives organizations an automated method for proving integrity of all systems and applications, providing auditors with reports that satisfy the audit process.
Out-of-box policies based on industry benchmarks, and Policy Manager for customization	Tripwire Enterprise comes with extensive sets of policies that can be deployed as is, adjusted to suit an organization's needs, or completely customized for specific internal operations
"Hardened" IT infrastructure based on industry benchmarks	Tripwire's inclusions of CIS policies enable an organization to test their IT environment against industry best practice benchmarks.
Breadth and depth of coverage	Tripwire offers comprehensive, out-of-box policies to address numerous regulatory standards, and tracks change across the entire IT infrastructure (e.g. servers, network devices, databases, Active Directories, virtual environments, POS, etc.)
Maintain a known, trusted and compliant state across the data center	By evaluating every change as authorized, within policy and compliant, and alerting IT to the changes that do not meet criteria, systems remain in a stable and known state that is continuously compliant.



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