FORTRA™

WHITE PAPER (TRIPWIRE)

Sustaining SOX Compliance

Best Practices to Mitigate Risk, Automate Compliance, and Reduce Costs

The passage of information security and technology laws and rules since the early 2000s has affected nearly every industry and organization. In response to these laws, management must be more accountable and aware of the need for a continuous and proactive operational risk management environment that recognizes the links between its technology infrastructure, business processes, reputation, compliance and internal controls. This era of heightened compliance is driving major corporate initiatives for greater transparency, governance, accuracy and accountability throughout the enterprise. Each company must identify, track and validate all business processes to ensure that its operations are compliant. In many cases the controls required by many of these regulations and standards, such as Sarbanes-Oxley, must be implemented worldwide for affected companies, which may prove challenging for some organizations given cultural and legal differences overseas.

However, recent trends indicate that the initial cloud of heightened compliance is now yielding a silver lining. This comes in the form of financial benefits (stability in share prices) for compliant companies, and lower costs, increased efficiency and lower risk of having to disclose a material weakness in controls for companies that choose automation of internal controls.

Sustaining SOX Compliance

Efforts Must be Sustainable

The Sarbanes-Oxley Act (SOX) has significant information security implications for companies governed by the regulation. Sections 302, 404 and 409 of SOX, and corresponding SEC Rules and Regulations, have tremendous ramifications for information technology (IT) in the areas of control (internal controls), evaluation (governance, measurement and record keeping), and disclosure (reporting and certification). Perhaps the most talked-about requirements of SOX are the ones related to internal control over financial reporting. Section 302 of SOX and the SEC Regulations that were passed to implement it require corporations to adopt internal controls over financial reporting and operations.

Specifically, sections 302(a)(4)(A) and (B) of SOX require a company's chief financial officer and chief executive to certify in quarterly and annual reports to the SEC that they:

1. are responsible for establishing and maintaining internal controls;
2. have designed such internal controls to ensure that material information [about the company and its subsidiaries] is made known to such officers by others within those entities…

Staff guidance from the SEC in 2007 states that these internal controls must not only be implemented over IT systems directly related to financial reporting, but also those general IT controls that would affect such systems. In other words, the controls must be broad enough to prevent not only "gaming the system" on those applications and systems directly used in financial reporting, but also general systems and applications that could impact the financial reporting applications and systems.

These "control, evaluate and disclose" elements must therefore work together as integral parts of the SOX compliance process. To meet the challenges of SOX compliance, companies need to adopt changes to corporate governance and implement a configuration audit and control solution such as Fortra's Tripwire® Enterprise. The Tripwire solution continually collects information to generate needed reports and evidence of SOX compliance, making audits a quick task instead of a lengthy manual project.

Efforts Must be Cost Effective, Risk-Based, Business Driven

An organization's SOX compliance efforts must meet the requirements of the Act and the rules set by the SEC and PCAOB. The SOX program must also be driven by management and the board (not the external auditor) and reflect the risks facing the organization.

That is, SOX efforts should reflect the organization's strategic goals and objectives, as well as ensure accurate financial reporting, and transparent and timely disclosures.

Many "lessons learned" resulted from the first few years' implementation of SOX. Numerous public round tables were held, such as ones held by the SEC and PCAOB (see their web sites for summaries of this extensive public debate). Many webcasts and other public events by FEI, NACD, IIA, and numerous other organizations have featured extensive debate on enhancing the SOX implementation on a go-forward basis. Furthermore, the SEC released additional guidance in 2007 aimed at smaller companies, and the PCAOB issued Audit Standard 5 the same year.

One of the first studies released was an IIA research study entitled Sarbanes-Oxley Section 404 Work — Looking at the Benefits (www.theiia.org/download.cfm?file=343, gated) provides an extensive summary of some of the key benefits from SOX implementations, along with extensive discussion regarding the high first year costs involved in meeting the requirements of the Act and its related SEC rules.

The IIA research study presented three major themes, most of which have been borne out by later studies and SEC guidance:

First, while compliance costs have been high (especially for small caps), there are significant benefits associated with the control identification, documentation, and testing process. The evaluation process has led to improvements in basic internal controls such as reconciliations and segregation of duties. Substantial improvements in the control environment have resulted from the process. Many companies have recognized that they have vulnerabilities in the information technology (IT) area and will be devoting more resources to improving and evaluating IT controls as they move forward. Companies are gaining more confidence in their control structure and are evaluating accounting risks, which should enable investors to have more confidence in the reliability of unaudited data furnished to the securities market.

An article in the Journal of Economics and Business that looked at six years of SOX implementation (from 2001–2007) identified the high costs of compliance. It noted that the total audit fees for large caps (over $75 million) were up 189% from 2001 to 2006, while the total audit fees for small caps was up 311% for the same period. It also noted that compliance has resulted in lost investor opportunity (38% of all 13E-1, or "go private" filings have cited compliance costs), and weaker returns for a company's stock on the day a material weakness in ICFR was disclosed.

The same article tempered the impact of these costs, however, with a discussion of the benefits of compliance. It noted that the "bid/ask" spread decreased for companies after 302 certification, and that such companies generally experienced an increase in market liquidity. Furthermore, SEC enforcement releases have shown a vast decline in fraud incidences during that period, and private companies are now adopting SOX-like controls "to gain value through operational and control efficiencies."

> *"Good controls and auditing processes have operational and organizational benefits. Tripwire gives us the confidence now that our staff, systems and policies will be able to support our growing business."*
>
> — **Chad Plemons, Vice President of Information Technology, EdFinancial**

Second, the prognosis is that the future costs associated with Section 404 will decrease substantially as we look forward three years, especially for companies that embrace automated controls. Much of the initial cost came about because controls had not been systematically documented or evaluated prior to the Section 404 requirements. Chief Audit Executives (CAEs) see the process as becoming more systematized. The authors believe companies will see significant efficiencies as they fully implement the information, communication and monitoring concepts embedded in COSO's Internal Control Integrated Framework.

In this regard, one of the best compliance values from a cost and efficiency standpoint is to choose automated controls whenever possible. Both the SEC June 2007 Guidance Regarding Management's Report on Internal Control Over Financial Reporting and the May 2007 PCAOB Audit Standard 5 emphasize the benefits of automation. The SEC noted in its June 2007 guidance that:

> [W]hen adequate [IT] general controls exist and management has determined that the operation of such controls is effective, management may determine that automated controls are more efficient to evaluate than manual controls.

This is especially true for smaller companies, who bear compliance costs that are disproportionately greater than large ones. Besides the fact that automation of controls is more efficient and cost effective because it typically replaces costlier manual controls, the SEC identified a more compelling reason for implementing technology that facilitates automated controls, namely, less risk of noncompliance:

> [A] financial reporting element… may require a combination of automated controls that accumulate source data and manual controls…. In this case, the automated controls may be subject to a system that is

stable… and is supported by effective IT general controls and are therefore assessed as lower risk, whereas the manual controls would be assessed as higher risk.

Third, there is uncertainty about the future role of internal auditing with respect to Section 404 work. The majority of CAEs want to maintain a strong presence in the risk and control arena. They recognize the need to perform more operational auditing and that it continues to add value to the organization. The majority of the respondents recognize a need to invest resources in IT auditing. Most CAEs see themselves playing a major role in ongoing monitoring and testing activities associated with Section 404 work.

Tripwire as Part of Your SOX Sustainability Strategy

To successfully sustain compliance, organizations must implement best practices to ensure that IT systems not only achieve a known and trusted state but they also maintain that state. This must address the control, evaluation, and disclosure elements of SOX Sections 302, 404, and 409. To do so, many organizations are adopting a standard framework, such as the Committee of Sponsoring Organizations of the Treadway commission (COSO). The U.S. Securities and Exchange Commission (SEC) recognizes COSO as the official framework for establishing Internal controls over financial reporting. The IT-specific aspect of the COSO framework Is known as Control Objectives for Information and Related Technology, or COBIT.

Tripwire security configuration management (SCM) solutions support many elements of the Acquire and Implement (AI) and Delivery and Support (DS) guidelines of COBIT. Tripwire® Enterprise can help address these guidelines right out of the box with change audit reporting and a library of COBIT configuration assessment tests.

Tripwire has also developed a comprehensive set of rules for the systems we monitor and the many applications our customers use. Our level of experience and knowledge makes creating rules for custom applications simple. That is why many organizations rely upon Tripwire solutions as an integral element of their sustained compliance initiatives.

> *"Without Tripwire, Cascade Microtech would have had to undergo an extensive and time-consuming sampling exercise, costing time and money to request, gather and compare change request logs. Tripwire's ROI is there several times over."*
>
> —Protiviti On-site Auditor

Benefits Well Beyond Compliance

Tripwire Enterprise can leverage industry standards and benchmarks to automatically assess configurations, determining the degree of risk for operational, regulatory and security vulnerabilities. Tripwire Enterprise also helps to continuously maintain a known and trusted state by establishing a secure baseline to measure change against, then monitor against that baseline, resulting in a controlled approach to maintaining system and application security, greater system uptime, and confidence that critical data is secure.

Tripwire and COBIT

The tables on the following pages provide key Tripwire Enterprise capabilities against specific COBIT guidelines in the Acquire and Implement (AI) and Deliver and Support (DS) domains.

Acquire and Implement

The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the organizations current business process. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components.

Delivery and Support

The Delivery and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as, the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training.

Acquire and Implement (AI)	Control Definition	How Tripwire Addresses the Control
COBIT AI2: Acquire and Maintain Application Software — Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration In line with standards. This allows organizations to properly support business operations with the correct automated applications.		
AI2.3: Application Control and Auditability	Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorized and auditable.	With Configuration Assessment, Tripwire Enterprise will capture failed login attempt messages if the file exists. Through kernel-level auditing, Tripwire provides information on commands and system calls which are executed on the local system. This logs "interesting" system events without consuming excessive amounts of resources logging "significant but usually uninteresting" system calls.
COBIT AI3: Acquire and Maintain Technology Infrastructure — Organizations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.		
AI3.2: Infrastructure Resource Protection and Availability	Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	Tripwire provides security and auditability measures during configuration, integration and maintenance of infrastructure software. Specifically, Tripwire Enterprise can compare configurations of systems to "golden systems" and report variance from the "golden system". (See Figure 1) Additionally, Tripwire Enterprise can analyze configurations of servers, applications, DBMSs, directory services, network devices, and virtual hypervisors and compare those configurations to multiple standards, including custom standards and those published by the Center for Internet Security (CIS) and the Defense Information Systems Agency (DISA). Variance from these standards is clearly reported, including the percent of platforms that are not in line with defined IT standards. Tripwire reports the number percent of systems that are not in line with defined IT standards. (See Figure 2)
AI3.3: Infrastructure Maintenance	Develop a strategy and plan for infrastructure maintenance, and ensure that changes are controlled in line with the organization's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements.	Tripwire ensures that changes are controlled in line with the organization's change management procedure. Tripwire Enterprise identifies changes to across the entire IT infrastructure, then compares detected changes to changes that were authorized by the organization's change management procedure and reports on unauthorized changes. These reports can document the percent of changes that are unauthorized. (See Figure 3)
COBIT AI6: Manage Changes — All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.		
AI6.2: Impact Assessment, Prioritization and Authorization	Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorized, prioritized and authorized.	Tripwire Enterprise audits changes to the entire IT infrastructure to identify unauthorized changes. Tripwire then compares detected changes to changes that were authorized by the organization's change management procedure and reports on unauthorized changes. Reports can document the percent of changes that are unauthorized. (See Figure 4)

Acquire and Implement (AI)	Control Definition	How Tripwire Addresses the Control
AI6.3: Emergency Changes	Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process.	Tripwire can help document emergency changes by flagging changes that were not made in accordance with procedures for standard changes. Tripwire Enterprise can open an incident for these changes causing them to be investigates. Changes that are found to be emergency changes can then be designated as such and change authorization IDs can be applied after the fact. (See Figure 5)
AI6.4: Change Status Tracking and Reporting	Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.	Tripwire Enterprise helps make certain approved changes were implemented as planned. Tripwire can report on changes that were expected but not made at all. Additionally, Tripwire Enterprise can compare actual change details to expected change details and identify changes that were not made as expected. The report in Figure 6 identifies all elements for which Tripwire Enterprise did not detect a change in the specified time range. (See Figure 6) Furthermore, Tripwire integrates with Remedy, HP OpenView, and other similar systems to provide validation and documentation of planned changes, as well as automatable storage of "before and after" snapshots of systems, which can be appended to work orders.
COBIT AI7: Install and Accredit Solutions and Changes — New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with agreed-upon expectations and outcomes.		
AI7.6: Testing of Changes	Test changes independently in accordance with the defined test plan prior to migration to the operational environment. Ensure that the plan considers security and performance.	Tripwire Enterprise audits changes to test systems and records that the changes were deployed as expected to those test systems. A record of the change can be included in the test report to verify that the change was made to the test system. Tripwire can also identify authorized and unauthorized changes to elements over specified time intervals. Authorized changes are associated with a valid change request ticket ID to validate that changes are tested in adherence to change process controls. (See Figure 7)
AI7.9: Post-implementation Review	Establish procedures in line with the organizational change management standards to require a post-implementation review as set out in the implementation plan.	Tripwire Enterprise can validate changes made to production systems match changes made to test systems. If the changes in production match the changes in test, Tripwire Enterprise reports such status. If variances occur between test and production they are documented in a Detailed Changes report. (See Figure 8)

Delivery and Support (DS)	Control Definition	How Tripwire Addresses the Control
COBIT DS4: Ensure Continuous Service — The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing off-site backup storage and providing periodic continuity plan training. An effective continuous service process minimizes the probability and impact of a major IT service interruption on key business functions and processes.		
DS4.5: Testing of the IT Continuity Plan	Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.	Tripwire Enterprise can compare production systems to their disaster recovery counterparts and identify differences showing that the two environments are out of synch. Tripwire's baseline information can be used to test disaster recovery capability to validate that systems reproduced from disaster recovery procedures actually match the current production systems they were meant to replicate. Should an actual emergency or disaster occur, archived Tripwire baseline information can be used to validate that the deployed systems actually correspond to the pre-emergency state of the systems. (See Figure 9)
DS4.8: IT Services Recovery and Resumption	Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understand IT recovery times and the necessary technology investments to support business recovery and resumption needs.	Tripwire speeds recovery from outages by answering the question, "What changed?" As reported by Gartner, 80% of outages are caused by IT staff actions, and 80% of the time to recover is spent just trying to identify the change. (See Figure 10)
COBIT DS5: Ensure Systems Security — The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents.		
DS5.3: Identity Management	Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms.	Tripwire Enterprise monitors user accounts maintained in LDAP directory services, such as Active Directory, and detect additions, deletions, and changes. Tripwire then compares detected changes to changes that were authorized by the organization's identity
	Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.	Tripwire Enterprise monitors user accounts maintained in LDAP directory services, such as Active Directory, and detect additions, deletions, and changes. Tripwire then compares detected changes to changes that were authorized by the organization's identity management procedure and reports on unauthorized changes. Reports can document the percent of changes that are unauthorized. With Configuration Assessment, Tripwire Enterprise helps to enforce the default owners and access permissions for critical files and prevents users from subverting the system's normal access control mechanisms. (See Figure 11)

Delivery and Support (DS)	Control Definition	How Tripwire Addresses the Control
DS5.4: User Account Management	Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.	Tripwire Enterprise monitors user accounts maintained in LDAP directory services, such as Active Directory, and detect additions, deletions, and changes. Configuration Assessment policies from Tripwire tests parameters of the number of failed login attempts a user is allowed before being disconnected from the system and forced to reconnect. Setting such values helps discourage brute force password guessing attacks.
DS5.5: Security Testing, Surveillance and Monitoring	Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.	With Configuration Assessment, Tripwire Enterprise can test to ensure systems only enable the GUI if there is a business need for one.
DS5.7: Protection of Security Technology	Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	With Tripwire Enterprise, the user model provides segregation of duty for Tripwire users so users only can perform tasks consistent with their role. Furthermore, Tripwire Enterprise uses secure communications and user access controls.
COBIT DS5: Ensure Systems Security — The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents.		
		Tripwire also is commonly used to "guard the guard" and monitor the configuration, application, and underlying OS of security software and appliances. In this way, Tripwire provides 3rd party validation that security applications and their configurations have not been tampered with or compromised without your knowledge. Tripwire also monitors and cryptographically protects its own files to protect itself from compromise. (See Figure 10)
DS5.9: Malicious Software Prevention, Detection and Correction	Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	Buffer overflow exploits have been the basis for many of the recent highly publicized compromises and defacements of large numbers of Internet connected systems. With Configuration Assessment, Tripwire policies test for enabled stack protection. This prevents certain classes of buffer overflow attacks and is a significant security enhancement. Also, the change auditing capabilities in Tripwire Enterprise detect changes resulting from the installation of malicious software, such as root kits, viruses, etc.

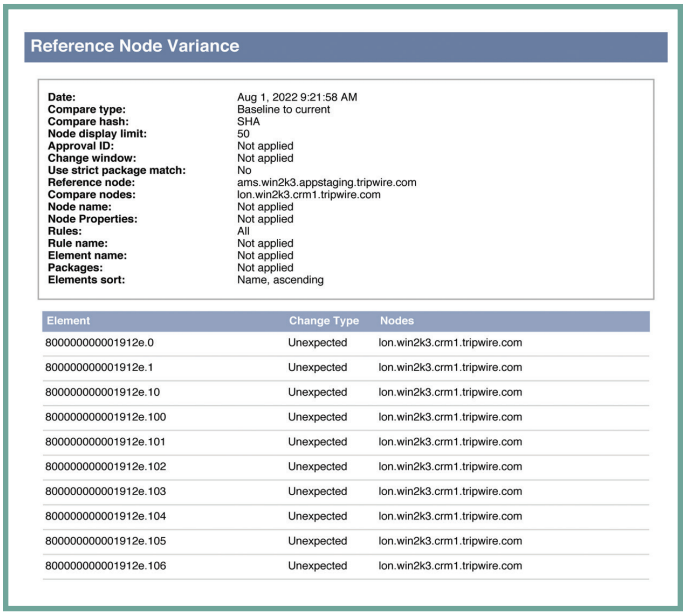
Delivery and Support (DS)	Control Definition	How Tripwire Addresses the Control
DS5.4: User Account Management	Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.	Tripwire Enterprise monitors user accounts maintained in LDAP directory services, such as Active Directory, and detect additions, deletions, and changes. Configuration Assessment policies from Tripwire tests parameters of the number of failed login attempts a user is allowed before being disconnected from the system and forced to reconnect. Setting such values helps discourage brute force password guessing attacks.
DS5.5: Security Testing, Surveillance and Monitoring	Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.	With Configuration Assessment, Tripwire Enterprise can test to ensure systems only enable the GUI if there is a business need for one.
DS5.7: Protection of Security Technology	Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.	With Tripwire Enterprise, the user model provides segregation of duty for Tripwire users so users only can perform tasks consistent with their role. Furthermore, Tripwire Enterprise uses secure communications and user access controls.
COBIT DS5: Ensure Systems Security — The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents.		
		Tripwire also is commonly used to "guard the guard" and monitor the configuration, application, and underlying OS of security software and appliances. In this way, Tripwire provides 3rd party validation that security applications and their configurations have not been tampered with or compromised without your knowledge. Tripwire also monitors and cryptographically protects its own files to protect itself from compromise. (See Figure 10)
DS5.9: Malicious Software Prevention, Detection and Correction	Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	Buffer overflow exploits have been the basis for many of the recent highly publicized compromises and defacements of large numbers of Internet connected systems. With Configuration Assessment, Tripwire policies test for enabled stack protection. This prevents certain classes of buffer overflow attacks and is a significant security enhancement. Also, the change auditing capabilities in Tripwire Enterprise detect changes resulting from the installation of malicious software, such as root kits, viruses, etc.

Delivery and Support (DS)	Control Definition	How Tripwire Addresses the Control
DS5.10: Network Security	Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.	Tripwire Enterprise can analyze firewalls, security appliances, etc. according to custom or proprietary security standards to ensure these devices are configured in accordance with security best practices. Furthermore, Tripwire can detect configuration changes to such devices ensuring that unauthorized changes that may result from malicious activity to be investigated. Tripwire Enterprise can elevate the severity of changes made to critical security devices, such as firewalls and edge routers to expedite investigation of unauthorized change.
DS5.11: Exchange of Sensitive Data	Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.	When a domain member workstation or server boots up, it creates an encrypted tunnel with a domain controller to pass sensitive information. Tripwire Enterprise Configuration Assessment will test to ensure Encrypt Secure Data Channel is enabled. Also, Tripwire will test to ensure the client or server may close the connection to conserve resources after 15 minutes of inactivity. (See Figure 12)
COBIT DS9: Manage the Configuration — Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimizes production issues and resolves issues more quickly.		
DS9.1: Configuration Repository and Baseline	Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.	Tripwire Enterprise maintains significant configuration, attribute, and baseline information for configuration items. It also detects changes to this information, keeping it up to date. Tripwire assesses and audits detailed software configurations for OSes, applications, DBMSs, directory services, and network devices. Assessment evaluates configuration relative to published security and best practice standards. Auditing includes managing a baseline representation of their known and trusted state. These baselines are monitored for change, and all changes are recorded. Below are examples mentioned above: File Systems: • File or directory permissions; password strength • Available Network Services — many network services should be disabled per CIS (companies typically open up these services only when absolutely needed) such as FTP, TFTP, Print Server, File Replication, Fax Service, Messenger, RPC Locator, etc. • Boot services such as email servers, web servers, Kerberos Server Daemons, RPC-based services, NFS client process, login prompts on serial ports should be disabled unless necessary Databases: • Permissions • Privileges • Failed login attempts, password strength • Configurations in init.ora that prevent spoofing, unauthorized connections to the database, and set user permissions • Configurations in init.ora that ensure segregation of duties • Configurations that allow access to specific tablespaces (Continues next page)

Delivery and Support (DS)	Control Definition	How Tripwire Addresses the Control
		Network Devices: • User authentication • SNMP configuration • Disable unneeded management and control services • Network Time Protocol (NTP) configuration • System logging Directory Services: • Audit event policies • Account policies, e.g. password strength • Logging policies ESX Server: • Firewalls for VM service layer ports • Communications encryption • Time synchronization • Disabling unneeded features e.g. screen savers • Auditing
DS9.2: Identification and Maintenance of Configuration Items	Establish procedures in line with the organizational change management standards to require a post-implementation review as set out in the implementation plan.	Tripwire Enterprise goes beyond logging all changes to the configuration repository and logs all changes to the configurations themselves.
DS9.3: Configuration Integrity Review	Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.	Tripwire Enterprise frequently compares the "as expected" state recorded in the Tripwire Enterprise database to the "as is" state of configurations. Tripwire reports any deviations and can utilize any of a number of notification mechanisms, including SNMP and email.
COBIT DS11: Manage Data — Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimizes production issues and resolves issues more quickly.		
DS11.6: Security Requirements for Data Management	Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organization's security policy and regulatory requirements.	Using Configuration Assessment, Tripwire can test to ensure all media volumes are formatted using the NTFS file system.
COBIT DS13: Manage Operations — Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.		
DS13.3: IT Infrastructure Monitoring	Define and implement procedures to monitor the IT infrastructure and related events. Ensure that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.	With Configuration Assessment, Tripwire can test systems to ensure maximum application event log size. The default size of each event log is 512k. This has been standard since the days of Windows NT 3.5, when hard drives were typically less than 2 Gigabytes (GB) in size. However, recent hardware capacity improvements should leave ample storage space for an 80MB event log. (See Figure 13)

Delivery and Support (DS)	Control Definition	How Tripwire Addresses the Control
DS13.4: Sensitive Documents and Output Devices	Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special purpose printers or security tokens.	With Configuration Assessment, Tripwire can test to ensure printer daemons are disabled if a particular server isn't a print server. If users will never print files from a particular machine and the system will never be used as a print server by other hosts on the network, then it is safe to disable these services. (See Figure 13)
DS13.5: Preventive Maintenance for Hardware	Define and implement procedures to ensure timely maintenance of infrastructure to reduce the frequency and impact of failures or performance degradation.	Tripwire's Configuration Assessment tests to protect systems from users loading printer drivers into protected kernel space. Without protecting these systems, malicious user could choose to install an invalid or Trojan Horse print driver to gain control on the system.

Tripwire Enterprise Reports and Screenshots Referenced Above



Reference Node Variance

Date:	Aug 1, 2022 9:21:58 AM
Compare type:	Baseline to current
Compare hash:	SHA
Node display limit:	50
Approval ID:	Not applied
Change window:	Not applied
Use strict package match:	No
Reference node:	ams.win2k3.appstaging.tripwire.com
Compare nodes:	lon.win2k3.crm1.tripwire.com
Node name:	Not applied
Node Properties:	Not applied
Rules:	All
Rule name:	Not applied
Element name:	Not applied
Packages:	Not applied
Elements sort:	Name, ascending

Element	Change Type	Nodes
8000000000001912e.0	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.1	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.10	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.100	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.101	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.102	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.103	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.104	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.105	Unexpected	lon.win2k3.crm1.tripwire.com
8000000000001912e.106	Unexpected	lon.win2k3.crm1.tripwire.com

Fig. 1 Tripwire Enterprise can compare configurations of systems to "golden systems" and report variance from them.

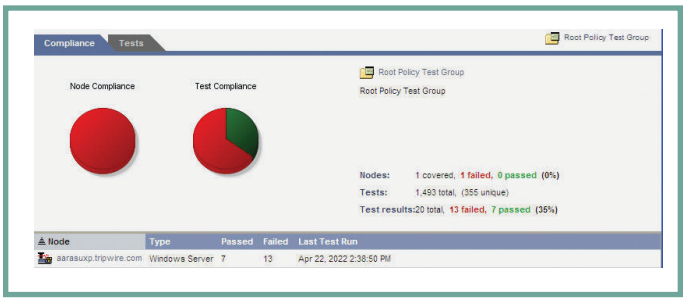
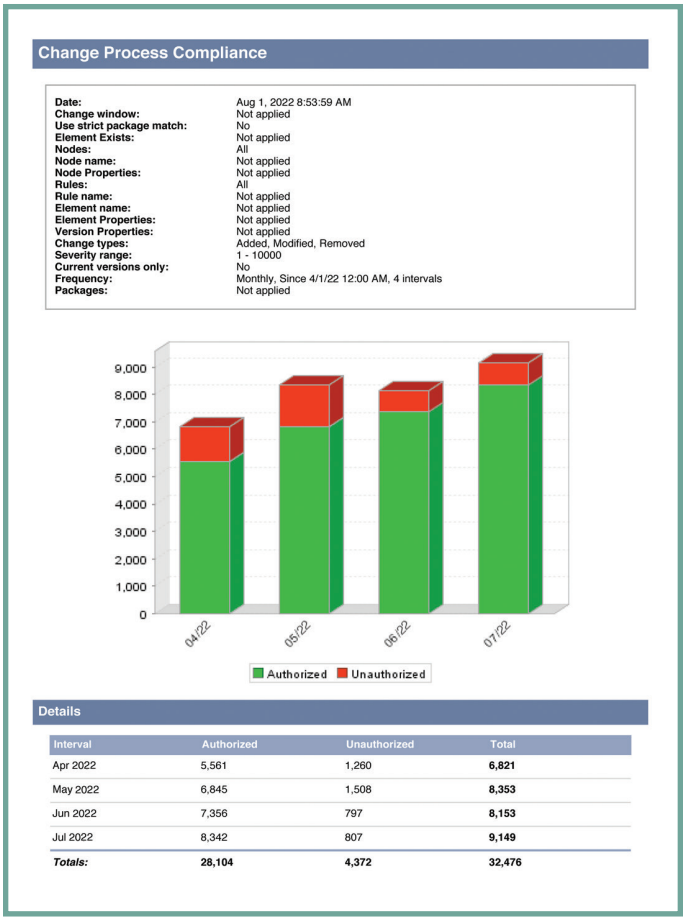


Fig. 2 Tripwire reports the number percent of systems that are not in line with defined IT standards.



Change Process Compliance

Date:	Aug 1, 2022 8:53:59 AM
Change window:	Not applied
Use strict package match:	No
Element Exists:	Not applied
Nodes:	All
Node name:	Not applied
Node Properties:	Not applied
Rules:	All
Rule name:	Not applied
Element name:	Not applied
Element Properties:	Not applied
Version Properties:	Not applied
Change types:	Added, Modified, Removed
Severity range:	1 - 10000
Current versions only:	No
Frequency:	Monthly, Since 4/1/22 12:00 AM, 4 intervals
Packages:	Not applied

Details

Interval	Authorized	Unauthorized	Total
Apr 2022	5,561	1,260	**6,821**
May 2022	6,845	1,508	**8,353**
Jun 2022	7,356	797	**8,153**
Jul 2022	8,342	807	**9,149**
Totals:	**28,104**	**4,372**	**32,476**

Fig. 3 Tripwire reports can document the percent of changes that are unauthorized.

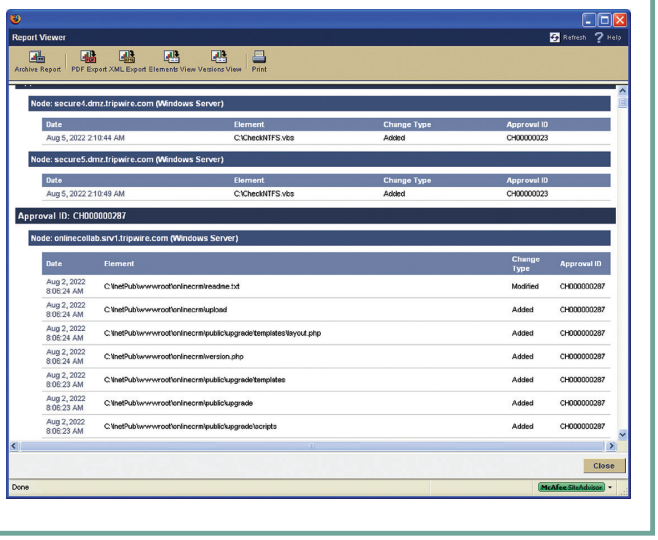


Fig. 4 This Tripwire report shows Approval IDs for each change. If the change was unauthorized the Approval ID would be blank.

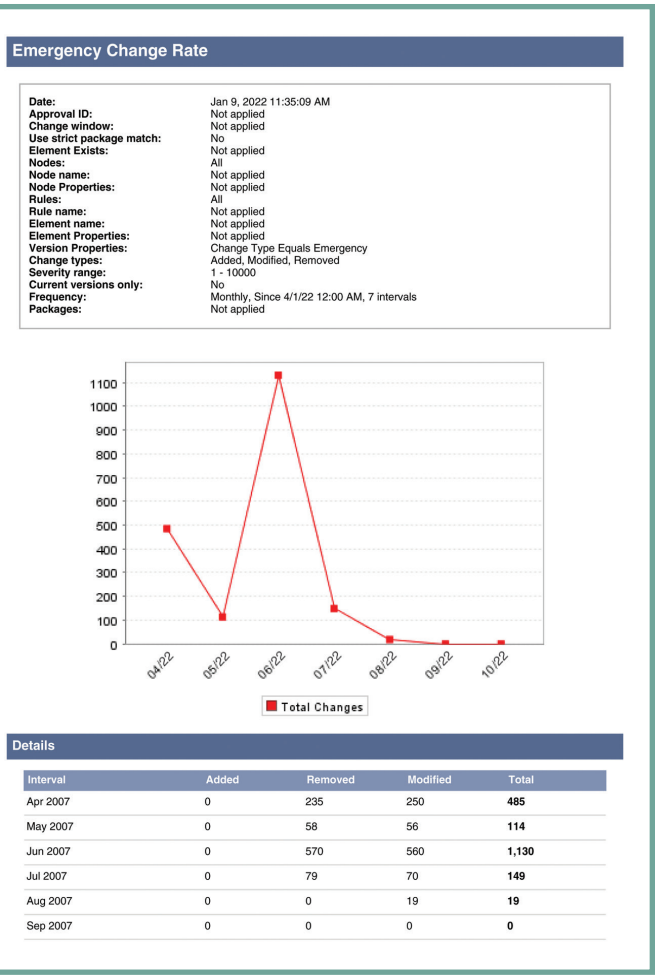


Fig. 5 This Tripwire report shows the emergency change rate.

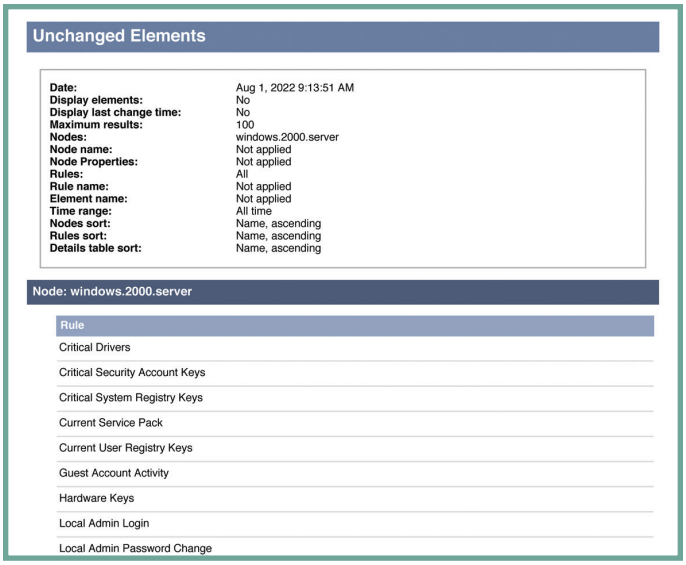


Fig. 6 This Tripwire report identifies all elements for which Tripwire Enterprise did not detect a change in the specified time range.

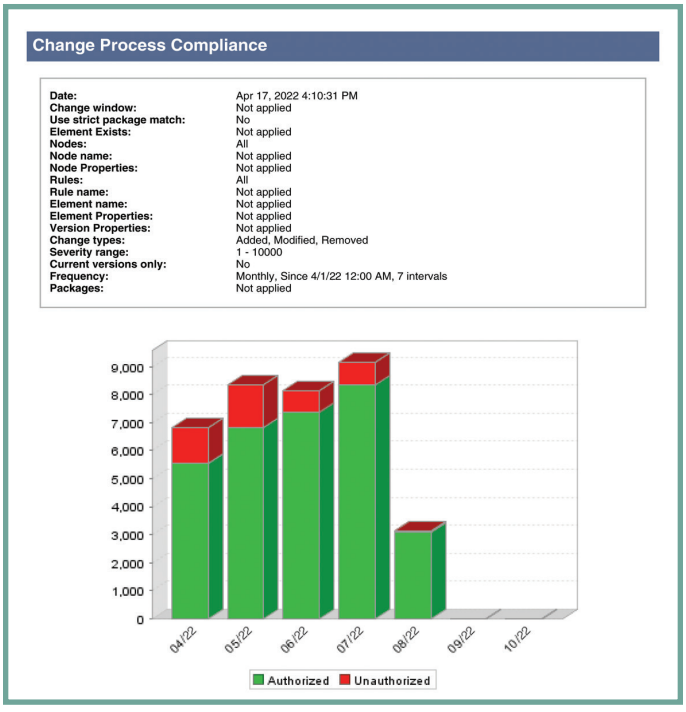
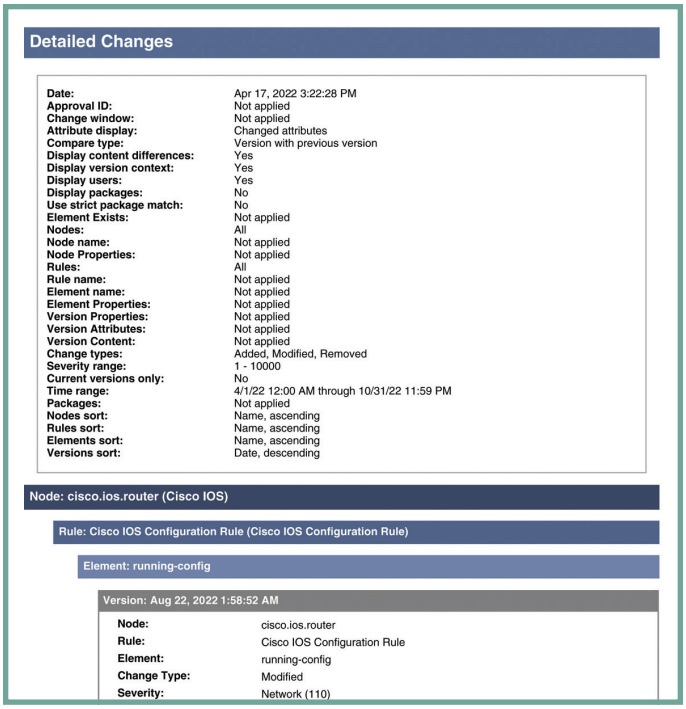


Fig. 7 This Tripwire report identifies authorized and unauthorized changes over a period of time, displaying trends in the effectiveness of and adherence to change process controls.



Detailed Changes

Date:	Apr 17, 2022 3:22:28 PM
Approval ID:	Not applied
Change window:	Not applied
Attribute display:	Changed attributes
Compare type:	Version with previous version
Display content differences:	Yes
Display version context:	Yes
Display users:	Yes
Display packages:	No
Use strict package match:	No
Element Exists:	Not applied
Nodes:	All
Node name:	Not applied
Node Properties:	Not applied
Rules:	All
Rule name:	Not applied
Element name:	Not applied
Element Properties:	Not applied
Version Properties:	Not applied
Version Attributes:	Not applied
Version Content:	Not applied
Change types:	Added, Modified, Removed
Severity range:	1 - 10000
Current versions only:	No
Time range:	4/1/22 12:00 AM through 10/31/22 11:59 PM
Packages:	Not applied
Nodes sort:	Name, ascending
Rules sort:	Name, ascending
Elements sort:	Name, ascending
Versions sort:	Date, descending

Node: cisco.ios.router (Cisco IOS)

Rule: Cisco IOS Configuration Rule (Cisco IOS Configuration Rule)

Element: running-config

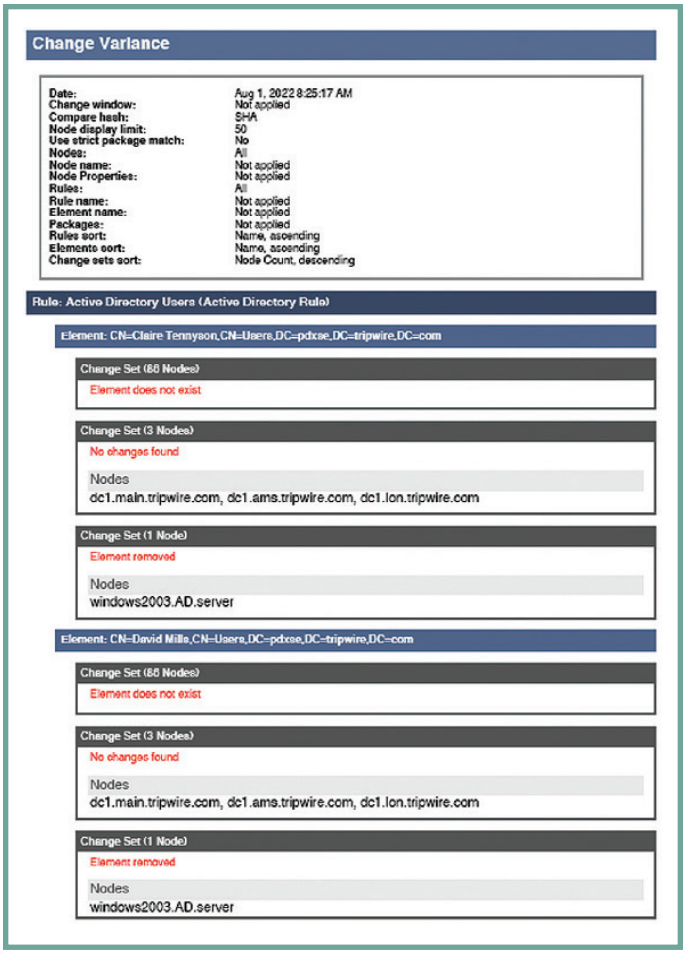
Version: Aug 22, 2022 1:58:52 AM

Node:	cisco.ios.router
Rule:	Cisco IOS Configuration Rule
Element:	running-config
Change Type:	Modified
Severity:	Network (110)

Fig. 8 If variances occur between test and production they are documented in a Detailed Changes report.

"We were looking for a suite of detective controls tools that would support our IT security and control objectives for meeting Sarbanes-Oxley. We recognized that Tripwire Enterprise would support both objectives."

— John Lambeth, Vice President, Information Technology, Blackboard, Inc.



Change Variance

Date:	Aug 1, 2022 8:25:17 AM
Change window:	Not applied
Compare hash:	SHA
Node display limit:	50
Use strict package match:	No
Nodes:	All
Node name:	Not applied
Node Properties:	Not applied
Rules:	All
Rule name:	Not applied
Element name:	Not applied
Packages:	Not applied
Rules sort:	Name, ascending
Elements sort:	Name, ascending
Change sets sort:	Node Count, descending

Rule: Active Directory Users (Active Directory Rule)

Element: CN=Claire Tennyson,CN=Users,DC=pdxse,DC=tripwire,DC=com

Change Set (88 Nodes)

Element does not exist

Change Set (3 Nodes)

No changes found

Nodes

dc1.main.tripwire.com, dc1.ams.tripwire.com, dc1.lon.tripwire.com

Change Set (1 Node)

Element removed

Nodes

windows2003.AD.server

Element: CN=David Mills,CN=Users,DC=pdxse,DC=tripwire,DC=com

Change Set (88 Nodes)

Element does not exist

Change Set (3 Nodes)

No changes found

Nodes

dc1.main.tripwire.com, dc1.ams.tripwire.com, dc1.lon.tripwire.com

Change Set (1 Node)

Element removed

Nodes

windows2003.AD.server

Fig. 9 This Tripwire Enterprise report shows the elements that differ between specified monitored systems. It is frequently used to compare changes on nodes after a patch/install has been implemented, and changes that are inconsistent across the nodes are flagged and reported.

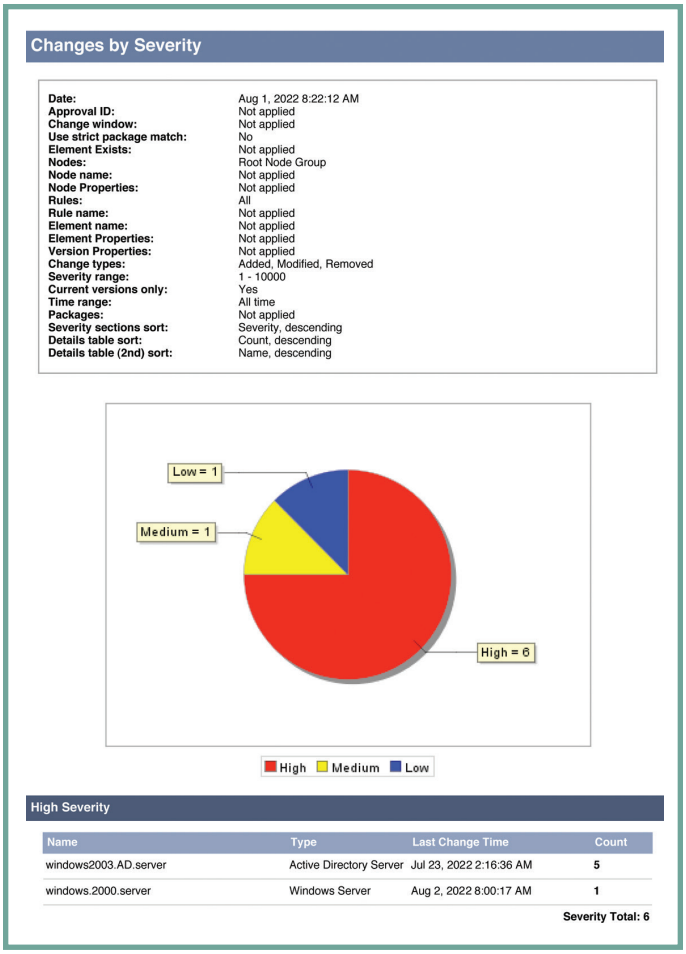


Fig. 10 This Tripwire Enterprise report shows the total number of changes detected on selected monitored systems that fall within a specified range of severity levels, helping IT staff identify changes that have the potential to adversely impact service quality.

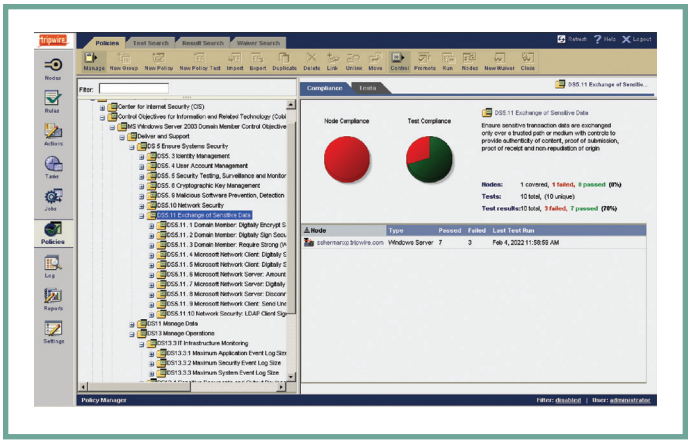


Fig. 12 Tripwire Enterprise configuration assessments test Encrypt Secure Data Channel is enabled to ensure the exchange of sensitive data is protected.

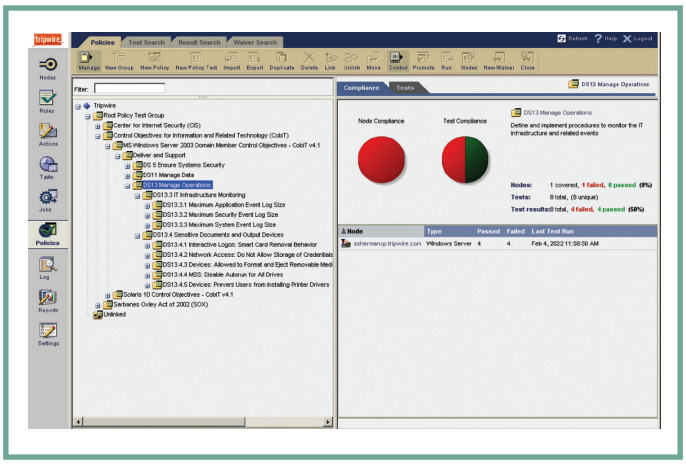


Fig. 13 With Configuration Assessment, Tripwire has policies to test systems to ensure maximum application event log size as well as ensure printer daemons are disabled if a particular server isn't a print server

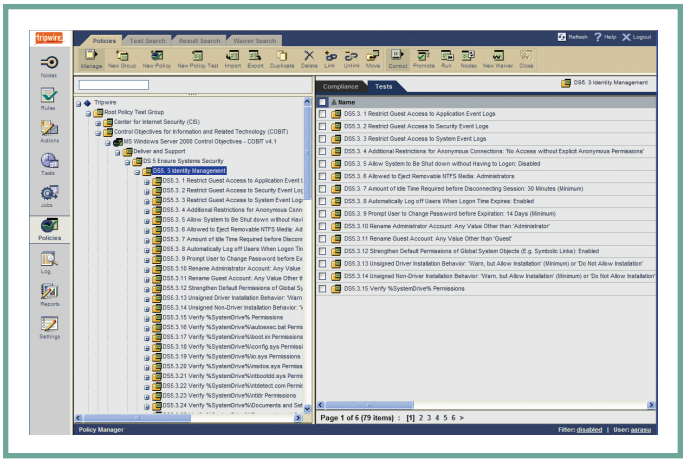


Fig. 11 Tripwire Enterprise configuration assessments help enforce the default owners and access permissions for critical files and prevents users from subverting the system's normal access control mechanisms.

Ready to Talk to Someone?

Contact Tripwire today to learn how you can sustain and automate SOX compliance and create a more secure IT infrastructure for your enterprise.
Visit tripwire.com/contact-us

References

1 Jahmani & Dowling, "The Impact of Sarbanes—Oxley Act," 6 Journal of Economics and Business No. 10, p. 57 (October 2008) and sources cited therein (hereafter "Impact of Sarbanes—Oxley Act').
2 "Impact of Sarbanes—Oxley Act" at 61—63.
3 United States Securities and Exchange Commission, Guidance Regarding Management's Report on Internal Control Over Financial Reporting, June 2007, at pp. 18—19.
4 Ibid.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.