



Beyond Tripwire ConfigCheck

DATASHEET

USING TRIPWIRE ENTERPRISE TO SECURE YOUR VIRTUAL—AND PHYSICAL—IT INFRASTRUCTURE

Tripwire® ConfigCheck™, a free, simple-to-use utility developed by Tripwire in cooperation with VMware, rapidly assesses the configuration settings of individual VMware ESX hypervisors

“Most security problems in the virtual world will be introduced through misadministration, mismanagement or just plain old mistakes. The fact that we have to use different tools in the physical world than in the virtual world compounds that problem.”
— Neil MacDonald, Gartner Analyst¹

compared to the VMware Infrastructure 3 Security Hardening guidelines. Through the evaluation of ESX settings, users gain visibility into possible misconfigurations. But in order to gain continuous configuration control, an organization may choose to implement Tripwire Enterprise, which addresses misconfiguration risks

throughout the entire virtual and physical infrastructure.

COMPLETE CONFIGURATION CONTROL

Tripwire’s industry-leading configuration assessment and change auditing solutions enable IT organizations to achieve and then maintain configuration control. Tripwire Enterprise is the first solution to effectively combine those capabilities, enabling automatic and sustainable policy-based control of all IT configurations.

Configuration assessment ensures the integrity of IT configurations by proactively comparing them against internal policies, compliance standards and security best practices. Tripwire Enterprise provides nearly 100 out-of-the-box policies to assess and validate configurations against well-known standards (e.g. CIS, PCI, NIST) as well as custom-developed Operational policies for optimized IT performance and reliability. Tripwire Enterprise proactively identifies misconfigurations and provides prescriptive

remediation guidance to enable a rapid return to a known and trusted state.

Change auditing makes change visible and ensures control by continuously detecting and reconciling all changes. Tripwire Enterprise scans systems to create a configuration baseline, compares subsequent scan results to that baseline and reports deviations. This provides a verifiable audit trail and version history of each system’s state, enabling rapid troubleshooting and proof of compliance in all IT infrastructures, both virtual and physical.

TRIPWIRE’S VIRTUAL ENVIRONMENT CAPABILITIES

	Tripwire Enterprise	Tripwire ConfigCheck
Configuration Assessment (policies)		
VMware	✓	✓
Security (CIS, DISA, NIST, ISO)	✓	
Compliance (PCI, NERC, SOX, FISMA, FDCC)	✓	
Operational	✓	
User-defined	✓	
Change Auditing/Baselines	✓	
ESX 3.0 & 3.5	✓	✓
ESX 3i	✓	
vSwitches	✓	
Guest OS	✓	
Remediation Guidance	✓	✓
Reporting and Notification	✓	
Reconciliation	✓	

DATASHEET

THE BENEFITS OF AN ENTERPRISE-CLASS SOLUTION

Listed below are just some of the differences between Tripwire Enterprise and Tripwire ConfigCheck.

Enterprise-Class vs. Focused Utility	Tripwire ConfigCheck is a specialized utility used to determine if VMware ESX hypervisors are configured according to VMware's hardening guidelines. Tripwire Enterprise is an enterprise-class solution used by over 6,000 customers worldwide to ensure organizations achieve and maintain configuration control across their virtual and physical infrastructures.
Configuration Assessment and Change Auditing	Tripwire ConfigCheck contains just a small subset of the rich configuration assessment capabilities found in Tripwire Enterprise. In addition, Tripwire Enterprise includes robust change auditing capabilities that enable an organization to detect and reconcile all changes occurring on all their IT systems, no matter the source. The two solutions work together seamlessly to provide configuration control for your virtual & physical infrastructures.
Deeper Policy Capabilities	Tripwire ConfigCheck uses a single policy (VMware's hardening guidelines) for evaluating VMware ESX and tests on an individual basis. Tripwire Enterprise includes nearly 100 out-of-the-box policies based upon compliance standards such as PCI and SOX, security best practices from CIS, NIST, DISA and performance tuning, and centrally tests, reports and monitors the infrastructure for risks. Tripwire Enterprise also enables organizations to create custom internal policies for continuously evaluating their systems.
Wide Platform Support	Tripwire ConfigCheck works on a single platform: VMware ESX. Tripwire Enterprise not only provides configuration assessment and change auditing for ESX hypervisors, but monitors the configuration states of VMs themselves. Beyond supporting virtual environments, Tripwire Enterprise supports a wide variety of nodes such as databases, directory services, server and desktop file systems, and network devices. This enables organizations to monitor and control their entire IT infrastructure—not just VMware ESX.
Automated Solution	Tripwire Enterprise is a completely automated system. Rather than performing configuration assessment manually, as with Tripwire ConfigCheck, Tripwire Enterprise enables systems to be monitored constantly. Configuration assessment can be performed anytime a change occurs to a system or according to a pre-set schedule or when an administrator desires.
Rich Reporting Capabilities	Due to its focused design, Tripwire ConfigCheck generates a simple list displaying which VMware ESX configuration settings are passing and failing. Tripwire Enterprise provides rich reporting and dashboards that capture the security and policy states of all systems. This not only shows how a single system is performing, but how all systems are changing over time, as well as an informative audit trail for auditors, compliance personnel and IT personnel performing system forensics for systems having issues.
Reconciliation	It is valuable to know what configuration settings are not in line with VMware's hardening guidelines, such as Tripwire ConfigCheck enables. Even more valuable is knowing when your trusted state changes. But not all change is created equal and Tripwire Enterprise not only detects when changes occur, but automatically reconciles those changes against planned change requests to ensure that unauthorized change does not introduce unnecessary risk into the environment.

SUMMARY

Tripwire ConfigCheck is an excellent utility for rapidly assessing the security of individual VMware ESX configurations. Tripwire Enterprise's policy-driven configuration assessment, seamlessly integrated with a change auditing function, provides a single point of configuration control across entire virtual and physical infrastructures to help reduce security risks, attain compliance

and increase operational efficiencies. If you wish to leverage the power of Tripwire across your heterogeneous environments, please contact Tripwire for further information.

¹ "Five Tips to Audit and Improve Virtual Server Security," CIO, May 11, 2008



ABOUT TRIPWIRE

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