

Tripwire Enterprise for VMware ESX Server

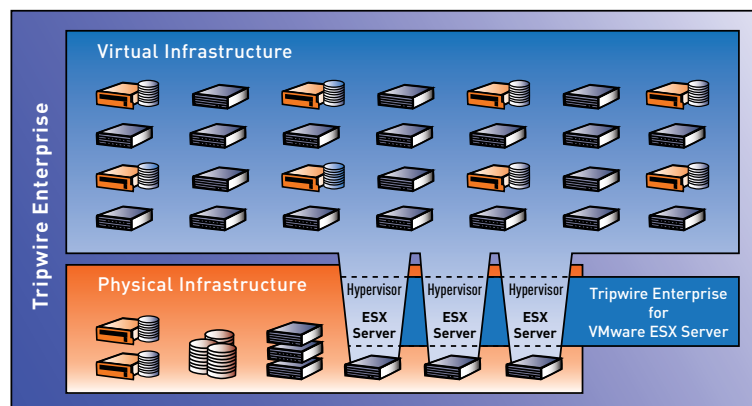
Configuration Integrity for Your Hypervisor

VMware ESX Server, the market-leading hypervisor, partitions a single physical machine into multiple virtual machines, each using a share of the physical machine's computing resources to run its own operating system and applications. Virtualization provides organizations with an attractive, low cost means of meeting the demands of the most agile of businesses. In the rush to virtualize, organizations often forget to hold these virtual environments accountable to the same operational, regulatory and security standards as their physical counterparts. Controlling the IT infrastructure requires powerful configuration audit and control across both your virtualized and physical environments—all from a single point of control.

GAIN CONTROL OF YOUR VMWARE ESX SERVER WITH TRIPWIRE ENTERPRISE

With powerful configuration assessment and change auditing, Tripwire Enterprise ensures configuration integrity across the VMware ESX Server hypervisor. Tripwire Enterprise for VMware ESX Server provides out-of-the-box assessment tests based upon the Center for Internet Security (CIS) VMware ESX Server security policies, proactively identifying potential security risks within the ESX Server. Once the hypervisor is in a known and trusted state, Tripwire keeps it there through continuous change auditing that detects any changes within the hypervisor.

Tripwire Enterprise for VMware ESX Server addresses the following key challenges of virtualized environments:



Tripwire Enterprise for VMware ESX Server provides out-of-the-box configuration assessments and change auditing capabilities to enable organizations to effectively achieve and maintain a known and trusted state for the ESX Server environment. Tripwire also monitors the state of all virtual machines managed by the hypervisor.

- **Protects against circumvention of systems** and from inadvertent configuration errors. Tripwire Enterprise assesses ESX Server configurations against industry regulations and standards and continuously monitors for change. Tripwire detects configuration issues due to improper change quickly, so system administrators can promptly remediate them.
- **Operates in concert with Tripwire's VM configuration assessment tools** that work in both physical and virtual environments. Tripwire Enterprise offers a single point of control for configuration assessment and change monitoring. Tripwire also creates a complete audit trail of change to prove compliance with critical industry regulations and standards.
- **Delivers visibility into virtual environments;** virtualization amplifies security risk with the portability, increased connection points, and quick addition and removal of virtual machines. By comparing virtual machine settings against internal and external policies, Tripwire helps increase reliability and performance of business critical systems.



TRIPWIRE ENTERPRISE FOR VMWARE ESX SERVER TECHNICAL SPECIFICATIONS

Recognizing the implications of security issues endemic to virtual environments, CIS recently added policies targeted at the security of VMware ESX servers. Tripwire's out-of-the-box CIS policy addresses these security concerns, including:

Network Security Settings	Tripwire tests verify that the ESX Server configuration prevents changes to the MAC address by the virtual machine guest OS to secure the environment for the ESX Server Host and the virtual machines that it supports. This could otherwise create the potential for spoofing the source MAC address.
Installation Considerations	Ensure ESX servers are deployed with secure settings using Installation Considerations. For example, when ESX server is installed, the option to create a default network for virtual machines is enabled by default. CIS considers this an insecure configuration because it allows all virtual machines to share the same network interface as the service console. Tripwire policies verify that this setting is disabled.
Minimizing Boot Services	Tripwire tests verify that the ESX server is running only the minimum services CIS recommends for VMware, including SSH for console access and the firewall, thereby reducing the threat vectors for the ESX server.
Kernel Tuning	Tripwire tests help ensure compliance with specific CIS recommendations for the kernel. For example, enabling reverse path source validation to identify spoofed source addresses and enabling the kernel to ignore all ICMP ECHO and TIMESTAMP requests sent via broadcast/multicast, which improves network security robustness.
File/Directory Permissions	Tripwire tests ensure critical permission settings are configured properly and stay that way. For example, Tripwire tests verify root logins to the System Console are restricted and that only authorized users run scheduled tasks. Tripwire also verifies that default permissions have not been modified, ensuring that proper user access to the ESX Server is maintained.

TRIPWIRE BRINGS VIRTUAL ENVIRONMENTS INTO COMPLIANCE —AND KEEPS THEM THERE

A single attack on a hypervisor can impact the operation of each associated virtual machine, potentially disrupting application availability and compromising data center integrity. With minimal visibility into virtual infrastructure change, attacks could remain undetected for some time, further intensifying their impact. Tripwire Enterprise gives VMware customers visibility into changes to ESX Server configuration files and individual virtual machines to ensure these changes—whether intentional or accidental—comply with internal policies and external standards. Tripwire also creates an audit trail and generates reports on configuration changes so organizations can quickly prove compliance in an audit.



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