



Dynamic Data Center
Compliance with
Tripwire and Microsoft

WHITE PAPER ○

Configuration Control for
Virtual and Physical Infrastructures

For IT, gaining and maintaining compliance with one or more regulations or security standards is challenging, but necessary. In fact, most regulations and security standards just ensure that businesses and other types of organizations are doing what they should be doing anyway—protecting cardholder data from exposure or theft, ensuring the confidentiality of personal health information, providing proof of sound financial practices in publicly held companies, and securing sensitive or confidential data of any nature—generally good practices to follow.

Although most IT organizations want to meet the requirements laid out by regulations and security standards, compliance efforts often leave them feeling as though they're walking in a minefield. One misstep, and the business finds itself on the wrong side of the law (or standard), facing fines, penalties, stolen sensitive or confidential data, loss of ability to process cardholder data, lessened credibility with customers, and perhaps ultimately, lost business.

Why Compliance Is So Difficult

Compliance has increased in complexity for a number of reasons. Here are some of the major issues that make it so challenging to meet the demands of compliance.

HETEROGENEOUS IT ENVIRONMENTS

Today's IT infrastructure does not run on a single platform, with portions of server infrastructure running Windows, UNIX or Linux. And IT assets vary widely, including applications, servers, routers, firewalls, databases and numerous other devices. To ensure compliance, IT first has to gain visibility to their IT assets across the entire IT infrastructure before they can effectively manage that infrastructure.

VIRTUALIZATION

If it wasn't hard enough to maintain compliance when you could see the IT infrastructure—physical server boxes, network cables leading from box to box, and a large room filled with physical servers all humming along—it got really complicated when virtualization gained widespread use.

With virtualization, it becomes even more challenging to know what is in scope for compliance and what isn't. In fact, it's often difficult to get a complete picture of your virtual infrastructure, much less determine what's in scope for compliance. Even the standards-developing organizations and other

groups that define regulations and standards are playing catch up on how to address virtual infrastructure (VI).

OVERLAPPING RESPONSIBILITY

On top of all of this, the lines for who is responsible for compliance are blurred. Now IT operations, traditionally responsible for monitoring the health and performance of systems, has the added responsibility of ensuring and demonstrating that systems are compliant and secure. And of course, security and compliance still must work together to ensure they are on the same page.

"FUZZY" STANDARDS AND REQUIREMENTS

Though not intentionally difficult to interpret, many of the standards and regulations are complicated, lengthy or open to interpretation. For example, the security hardening guidelines issued by vendors simply don't provide explicit details and in general, regulations and laws offer very little prescriptive guidance, and both require extensive examination and interpretation to be of use.

In this paper, we'll discuss how Tripwire solutions help organizations subject to an ever-increasing number of complex regulations and security standards address compliance requirements—even with a far more complex IT environment. We'll also demonstrate how Tripwire helps manage and operationalize compliance with Microsoft System Center

Data Center Compliance with Tripwire

For over a decade, Tripwire has been the trusted source for datacenter compliance. Tripwire recognized the critical impact compliance would have on public businesses, federal civilian and defense agencies and other organizations with regards to their IT infrastructure. Many of the well-known laws, regulations and standards being released were either solely focused on IT controls or had a central aspect that addressed IT controls.

LEVELS OF DETAIL IN COMPLIANCE

Compliance requirements range from very general to highly prescriptive. For example, security benchmarks like those issued by the Center for Internet Security (CIS) prescribe an exact setting or range of settings a configuration must fall within to be compliant. On the other hand, frameworks such as COBIT and

ISO provide a general outline for a security program, leaving the details open to interpretation. Regulations and laws tend to be the most open to interpretation, requiring great effort and research to determine how to objectively implement the requirements.

DEEP EXPERTISE AND EXPERIENCE WITH COMPLIANCE

As a result of their early entrance into the compliance arena, Tripwire has developed deep expertise and knowledge around compliance requirements for a broad array of regulations and standards including the:

- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accounting Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- North American Electronic Reliability Corporation (NERC)

Tripwire has also developed expertise around security standard benchmarks and security frameworks such as those issued by the:

- Center for Information Security (CIS)
- National Institute of Standards and Technology (NIST)
- Defense Information Systems Agency (DISA)
- International Standards Organization (ISO)

In some cases, security recommendations for IT controls are issued as general guidelines or within a framework like the Information Technology Infrastructure Library (ITIL). Tripwire has reviewed guidelines and worked extensively with vendors like Microsoft to flesh out details so they can be more objectively applied.

TRIPWIRE POLICIES PROVIDE COMPLIANCE EXPERTISE

Tripwire packages its years of expertise and accumulated knowledge around a given regulation, standard or guideline into a Tripwire Enterprise configuration assessment policy library, so you don't have to build one from scratch. Each policy contains numerous tests that IT runs against IT configurations in scope for a given standard, regulation or guideline. For example, the CIS policy includes a test for password strength to ensure the password length is greater than or equal to 8. By assessing an IT configuration against a policy, IT learns what settings are compliant and what are not. Then Tripwire Enterprise provides step-by-step remediation guidance to get out-of-compliance configurations into a compliant state.

Currently, Tripwire Enterprise has over 147 out-of-the-box configuration assessment policies based on 45 compliance sources and that include more than 20,000 published tests. Thirty-seven of these policies are based on CIS-certified benchmarks, industry-trusted benchmarks developed by the Center for Internet Security. Out-of-the-box Tripwire policies include PCI, SOX, NERC, HIPAA, FISMA and ISO to help you achieve compliance with these critical regulations and standards and enable you to establish a central set of IT controls.

These policies Tripwire Enterprise tests configurations against IT assets across 27 platforms, which include versions of Windows, Cisco, Oracle, HP, AIX, SUSE, Solaris, VMware, i5/OS, DB2, SQL Server, Microsoft IIS and Exchange, and Red Hat. And Tripwire Enterprise policies apply to both physical and virtual environments.

By continuing to stay abreast of policy updates, and offering configuration assessments as quickly as possible, Tripwire Enterprise customers harden their IT systems and achieve and

SELECTED AVAILABLE POLICIES (Additional and new policies are available for download from the Tripwire web site)

Source	Policies	Platforms
CIS	28	AIX, Cisco, HP-UX, Linux (Red Hat and SUSE), Oracle, Solaris, Windows: Server, Desktop, SQL Server, Active Directory, Exchange and IIS, VMware,
PCI	27	AIX, Cisco, HP-UX, Linux (Red Hat and SUSE), Oracle, Solaris, Windows: SQL Server, Exchange and IIS, VMware
DISA	17	AIX, HP-UX, Linux (Red Hat), Solaris, Windows: Server and Active Directory, VMware
FISMA/NIST	12	Linux (Red Hat), Solaris, Windows: Server, Desktop and Active Directory
SOX	9	HP-UX, Linux (Red Hat and SUSE), Solaris, Windows, VMware
NERC	8	AIX, Linux (Red Hat), Windows: Server and Active Directory
Microsoft Security Guide	1	Windows Server 2008

maintain continuous compliance, thereby furthering their process maturity and improving service delivery.

Tripwire Enterprise Delivers Continuous Compliance

Tripwire Enterprise offers organizations continuous compliance through the combination of configuration assessment and file integrity monitoring. We've already discussed how configuration assessment works, but let's look at how it fits into the whole process for achieving and maintaining compliance.

ACHIEVE COMPLIANCE

Tripwire Enterprise assesses all in-scope configurations against the appropriate configuration assessment policy. Tripwire Enterprise produces a report that tells you exactly what IT assets failed a test, and from the report, lets you drill down into the details of a failed test and receive remediation guidance to get the configuration into a compliant state. Once all IT configurations are in a compliant state, you have achieved compliance, but for that point in time. Your mission then becomes *maintaining* a compliant state.

MAINTAIN COMPLIANCE

Prior to offering configuration assessment, Tripwire was well known for its change detection solutions. Tripwire Enterprise allows IT to perform file integrity monitoring to detect any change that is unauthorized by reconciling changes to authorized changes via a change ticket or other change management system. But Tripwire also compares any detected change against the configuration assessment policy to determine if it took the IT asset out of compliance or not. When a setting is out of compliance, Tripwire Enterprise again provides prescriptive guidance to return the setting to a compliant state.

PROVE COMPLIANCE

Tripwire Enterprise makes proving compliance just as easy as achieving and maintaining compliance, producing audit-ready compliance reports that provide proof of compliance, along with historical evidence of changes to in-scope configurations and remediation efforts for out-of-compliance settings. Tripwire Enterprise even includes waivers, so you can temporarily exclude an IT asset from an audit when there's a valid reason for doing so.

Continuous Data Center Compliance with Tripwire and Microsoft

With Microsoft System Center Operations Manager, IT operations can easily and effectively monitor the performance and health of physical IT environments. When you add Microsoft System Center Virtual Machine Manager, you get that same capability for your virtual machines, whether based on Microsoft Hyper-V or VMware. And because System Center solutions are designed to work seamlessly with each other, you can monitor your virtual machines alongside your physical machines within Operations Manager.

But now IT operations is being asked by security and compliance to ensure or provide proof that systems, devices and other IT assets in the IT infrastructure are in compliance with a variety of regulations and standards—a tough request given that operations has no time to learn new tools and is typically unfamiliar with the compliance world.

TRIPWIRE COMPLIANCE MANAGEMENT PACK FOR SYSTEM CENTER OPERATIONS MANAGER

With the Tripwire Compliance Management Pack for System Center Operations Manager, Tripwire and Microsoft provide Operations Manager and System Center Virtual Machine Manager (VMM) users with a central, end-to-end solution for monitoring the health and performance of the virtual and physical IT environment and for ensuring its compliance with critical regulations, standards and vendor security guidelines. Specifically, the Tripwire Compliance Management Pack offers users compliance expertise for the regulatory standards organizations face most, like PCI, SOX, HIPAA, NERC and FISMA; security standards like those issued by CIS, DISA, and NIST; and vendor-developed security hardening guidelines.

Complete Coverage of the Physical and Virtual IT Infrastructure

Tripwire Enterprise further complements System Center Operations Manager by providing visibility into a wide range of Windows and non-Windows IT assets, including servers, routers, applications, hypervisors and databases. When information from VMM is added to Operations Manager, you see performance, health and compliance information for virtual machines based on both Microsoft Hyper-V and VMware. And with Tripwire's support for heterogeneous environments, including Windows,

Linux and UNIX, the Tripwire Compliance Management Pack provides complete coverage of the IT environment.

Correlating Event Information with Configuration Change

With the Tripwire management pack, when a critical event occurs (e.g. a server experiences performance issues) Operations Manager sees the server as “unhealthy” and issues an alert. The user simply clicks that alert from within the console and can note and investigate any configuration changes that may have caused the issue. Tripwire also issues an alert when a change takes an IT asset out of compliance. In both cases, Tripwire provides step-by-step remediation advice from within the Operations Manager to help users repair undesirable and non-compliant changes. And the Tripwire Compliance Management Pack supports automated remediation of some settings, eliminating human error and increasing ROI.

If you only need to manage your Hyper-V or VMware virtual machines, you can use the PRO-enabled Tripwire Compliance Management Pack, which allows you to receive Tripwire’s remediation guidance within VMM using PRO-Tips.

Proof of Continuous Compliance

The Tripwire Compliance Management Pack offers IT operations a simple path to demonstrating compliance. With forensic proof, audit-ready reports and historical evidence of compliance that help you easily and quickly substantiate compliance, it can reduce audit preparation time up to 50 percent.¹

Operationalizing Compliance

Tripwire operationalizes compliance, giving Operation Manager users the ability to monitor health and performance while ensuring compliance with regulations, standards and guidelines with Tripwire’s out-of-the-box configuration assessment policies—all within the familiar context of the System Center user interface. With the Tripwire management pack, Operations Manager users now have a single pane of glass through which to monitor system health, compliance and security.

IMPLEMENTING THE TRIPWIRE MANAGEMENT PACK

Adding Tripwire’s compliance expertise to Operations Manager with the Tripwire Compliance Management Pack is straightforward, and requires little effort. The only requirement is that the Tripwire Enterprise console be within the domain that the Operations Manager administrator is watching.

For the Tripwire Enterprise Administrator

If you are the Tripwire Enterprise administrator, you install the Tripwire Compliance Management Pack plug-in on the Tripwire Enterprise server. Next, you define the policies you want to share with the Operations Manager administrator and the node scope—the machines the administrator needs to monitor for compliance. You’ll want to carefully consider and prioritize what machines and devices need to be monitored as well as the tests that should be run to avoid overwhelming the administrator with non-critical alerts. Then you edit a batch file that contains a command line that lets you deploy the Operations Manager agent on the Tripwire Enterprise server.

For the System Center Operation Manager Administrator

As a Operation Manager administrator, you can easily add the Tripwire management pack to a machine already in your network. Most likely your Tripwire Administrator will have already installed the Operation Manager agent on the Tripwire Enterprise server. If this is the case, System Center’s autodiscovery capability automatically adds the Tripwire Enterprise server to the its console and runs a script file that adds Tripwire data to the its user interface. However, if the agent has not been installed on the Tripwire Enterprise server, it’s easy enough to configure one command-line item to point to the server.

Views Added to System Center Operation Manager

Once the Tripwire Enterprise server is added to the Operation Manager console, you can see which IT assets are passing or failing a policy along with their health and performance information. The Tripwire Compliance Management Pack presents this information through three main views that it adds to the System Center user interface:

- Health Explorer that presents the health of an IT asset in an expandable/collapsible tree view;
- Alert View that presents active alerts, details about a selected alert, and remediation text for a selected alert; and

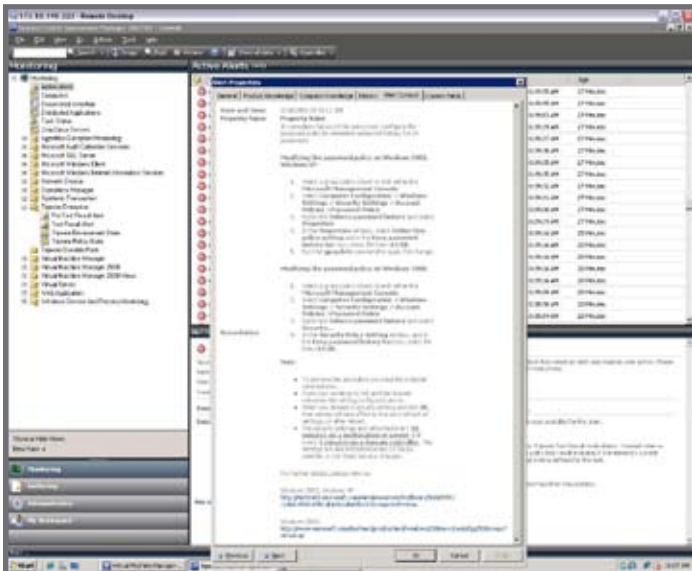
- Test Result and Revision History, which is a part of the Health Explorer view that provides forensic proof of compliance.

Operationalizing Compliance with Tripwire and Microsoft

Achieving and maintaining compliance with the wide array of regulations, security standards and other industry best practices has become increasingly complex, costly and demanding. Regulatory compliance is not just the responsibility of the IT department, it is the responsibility of the entire organization. Security has the daunting task of defining IT controls and policies to ensure a known and trusted state is achieved, and IT operations in turn has the responsibility of ensuring it is maintained. Organizations continually struggle with compliance

because documents and guidance for meeting compliance range from highly prescriptive to subjective and require interpretation, resulting in a point-in-time exercise that does not have the intended or desired results. Therefore, organizations across the globe require a solution that operationalizes compliance. They need a solution that provides critical compliance data, evidence, and monitoring from within a single pane of glass.

Tripwire and Microsoft offer that means of operationalizing compliance, delivering Tripwire Enterprise's policy-based compliance expertise and capabilities within the familiar Operations Manager and Virtual Machine Manager consoles. With the Tripwire Compliance Management Pack for Operations Manager, users of Microsoft System Center solutions can control and manage compliance, security and operations for their virtual and physical infrastructures, decreasing human error, increasing ROI, and significantly reducing compliance costs.



With the Tripwire Compliance Management Pack, you can see and then remediate all out-of-compliance systems and IT assets.

1 Tripwire Helps Put this Student Loan Financing Company at the Head of Its Class. Tripwire EdFinancial Case Study. 2008.

ABOUT TRIPWIRE

Tripwire is the leader in data center compliance and infrastructure management solutions, building confidence for IT across both virtual and physical infrastructures. Tripwire Enterprise and vWire software help over 6,500 enterprises worldwide meet their configuration auditing, file integrity monitoring, virtual infrastructure management and change auditing needs for IT operations, security and compliance. Tripwire is headquartered in Portland, Oregon, with offices worldwide. Tripwire can be found at www.tripwire.com, www.vwire.com, and [@vwire](https://twitter.com/vwire) on Twitter.



www.tripwire.com