Tripwire and HITRUST

Partnering for Automated Compliance

Three Benefits of Using Tripwire Enterprise for HITRUST Compliance

1. Quickly achieve and maintain compliance, including audit-ready proof of compliance
2. Accurately align with the HITRUST CSF with Tripwire's HITRUST-certified mapping
3. Keep up with new HITRUST CSF versions while strength-ening your cybersecurity posture

The HITRUST CSF rationalizes relevant regulations and standards (such as NIST, CIS, and HIPAA) into a single overarching security and privacy framework. Now, with Tripwire® Enterprise, organizations can automate HITRUST CSF assessment and reduce the burden of compliance.

Any organization that collects or stores personally identifiable information (PII) faces a relentless stream of cyberattacks. The development of a variety of security standards and regulations is the result of this threat environment, but this patchwork of compliance requirements creates complexity and cost for affected organizations. Additionally, demonstrating security compliance to suppliers and customers is becoming a more routine requirement for all industries.

These frameworks and standards all share the common goal of helping organizations protect confidentiality, integrity and availability of critical assets, infrastructure and information. Tripwire has a long history of helping organizations achieve and maintain compliance with these standards. The HITRUST CSF was created to help organizations quickly achieve automated compliance with several standards, and to provide a process by which any organization can provide independent certification of their security program. The HITRUST CSF started in healthcare, but is now used across industries globally.

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The Cost of Manual HITRUST Compliance

Without automated HITRUST compliance assessment, organizations are left to manually collect evidence of compliance. This manual effort not only increases the cost of compliance, it greatly increases the chances of human error. If your organization has 100 settings to verify on 100 servers, for example, the work piles up faster than most organizations are resourced to keep up with.

And in addition to all the extra time and effort it takes to track compliance manually, information that is manually collated into a report can be hard for an auditor to verify. Also, with manual compliance efforts audits are more time consuming, giving administrators an excessive backlog of work to manage.

Tripwire and HITRUST

Tripwire has a proven track record of helping organizations achieve and maintain compliance with HIPAA, PCI, and SOX, and adhere to security frameworks like NIST and CIS——with over 755,000 tests across 55 platforms and 3200 policies.

Now, Tripwire can help organizations automatically achieve and maintain compliance with HITRUST CSF:

» **Broader platform support:** Another common issue faced by most organizations is a lack of broad platform support. If you have a solution for one platform in your environment, it may not work on others. Tripwire solutions work on a wide range of network devices, web servers, Linux servers, Windows servers, and more.

» **The best of both agentless and agent-based discovery—**Tripwire Enterprise can leverage trusted, low-impact agents for greater depth of coverage than agentless solutions, but Tripwire also supports agentless assessment for assets that can't support an agent.

» **Advanced reporting—**Tripwire solutions can run reports at any point in time to give you a clear view of where you stand in regard to compliance across the organization.

» **Step-by-step remediation guidance—** Tripwire Enterprise offers clear instructions to help you quickly remediate controls that are not HITRUST compliant.

Tripwire has a variety of solutions that can enforce HITRUST compliance. Tripwire Enterprise can verify various controls, and Tripwire LogCenter® helps organizations meet their HITRUST auditing requirements. Tripwire Enterprise can verify just about any OS prescriptive control specified in the HITRUST CSF— from password length to encryption requirements and more.

To get started, head to the Tripwire Customer Center to download the available content appropriate for the platforms you use in your IT environment.

Available content includes the following platforms:

» Cisco
» Debian Linux
» Microsoft IIS
» Microsoft SQL Server
» Red Hat Linux
» SUSE Linux
» Ubuntu Linux
» Microsoft Windows
» Solaris

Summary

Organizations are faced with the question of how to effectively and efficiently achieve and maintain compliance with the HITRUST CSF—even more so how to automate their compliance. Now, through the partnership of HITRUST and Tripwire, automated HITRUST compliance is within reach.

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions and answer any of your questions. Visit **tripwire.me/demo**