Align with Cyber Essentials Using Tripwire Solutions

UK Government Entities Rely On Tripwire

As global events have led to many of us working from home, it has become more important more than ever to ensure your organisation's network is protected and secure. Cyber Essentials is an important information assurance scheme that you can use to ensure this is the case. If you are looking to meet the standards of Cyber Essentials, Tripwire® Enterprise, Tripwire IP360™, Tripwire Log Center™, and Tripwire ExpertOps℠ are fantastic tools to help you accomplish this.

TechValidate Research Findings

85% of surveyed customers rated Tripwire's effectiveness of product capabilities as better when compared to the competition.

Source: TechValidate survey of 53 users of Tripwire. TVID: EF5-102-13D

Tripwire Enterprise

Tripwire Enterprise is an industry-leading file integrity monitoring (FIM) solution that enables you to achieve, maintain, and report on your known and trusted state. With many changes happening in your environment all the time, it is crucial to have a solution that will detect, monitor, and report these changes so you are aware of everything happening on your network. Tripwire Enterprise will help you sort through the desired changes to find any potential vulnerabilities or threats that you will need to bring attention to. Tripwire Enterprise is one of the many solutions Tripwire offers that will help you achieve the Cyber Essentials.

Tripwire IP360

Tripwire IP360 is an enterprise-class vulnerability management (VM) solution that helps you find, prioritize, and remediate vulnerabilities in your environment. Tripwire IP360 is a scalable solution that gives you complete visibility into your network, scanning for cyber threats on all of your network devices and associated operating systems, applications, and vulnerabilities. With the industry's most comprehensive vulnerability scoring, it is easy to pinpoint and prioritize the highest risks and most advanced threats facing your environment. From there, Tripwire IP360 will provide insight as to how to address these risks and threats. Thanks to its continuous analysis of your organization's attack surface, you can feel confident that your environment is secure.

Tripwire Log Center

Tripwire Log Center provides you with a full picture of your environment and its potential cyberthreats by collecting and storing tens of thousands of events per second from any readable audit, accounting, or operational log. The solution automatically indexes files, allowing you to easily search and report on all collected log data. It uses security analytics and forensics to immediately detect incidents to prompt response. Tripwire Log Center even processes customized log files out-of-the-box, so it is easy to address every collected log in your network.

Tripwire ExpertOps

Tripwire ExpertOps is a managed service solution wherein a Tripwire expert will run your solutions for you. Tripwire

ExpertOps can handle your security configuration management (SCM), FIM, and VM processes for you, so you have more time in your day to focus on more important projects. If you have a small team, this is an excellent option—you will still have a top of the line, enterprise-class solution, but with much less of the work.

Ready for the Next Step?

If you would like to learn more about how you can use Tripwire to align with Cyber Essentials, please reach out to Emanuel Ghebreyesus at eghebreyesus@tripwire.com

How Tripwire Addresses the Five Main Technical Controls of Cyber Essentials

Control	How Tripwire Helps
Firewalls	Firewalls are essential assets, a first line of defense for protecting valuable and sensitive data. Both Tripwire Enterprise and Tripwire IP360 help keep them secure. The FIM solution Tripwire Enterprise detects change by capturing new versions of all files and configurations, comparing them against a highly detailed and trusted state. It also applies change intelligence, helping you figure out if a change is merely business as usual or is a sign of a potential attack. Tripwire IP360 is a vulnerability management solution that prioritizes the most important vulnerabilities facing your environment—such as ones that may jeopardize its firewalls. Instead of a never-ending list of "high risk" vulnerabilities, the tool ranks vulnerabilities on a scale of 1–50,000, making it easier for you to identify and tackle the greatest risks first. Additionally, Tripwire IP360 has a built-in integration with Tripwire Enterprise, allowing you to enable Adaptive Threat Protection—which helps you track changes on tagged critical assets, such as firewalls. When there is an actionable configuration or file system change detected, a vulnerability scan will automatically run, ensuring you quickly attain the information you need to mitigate a potential breach.
Secure settings	Tripwire Enterprise helps keep your network secure by establishing a known and trusted baseline of every file and asset. This baseline is compared against your current state to track changes. Real-time monitoring notifies you of every change that breaks away from this baseline—including details such as what changed, who changed it, and more.
User access control	Although Tripwire does not provide direct user access control functionality, it can monitor your organisation's Active Directory. Because Tripwire Enterprise keeps a baseline version of Active Directory attributes, it will detect any changes to user attributes and roles, and helps you delineate acceptable and unacceptable changes.
Malware protection	While Tripwire solutions don't stop malware from being deployed, they can immediately alert you of changes happening in your environment so you can respond to threats quickly. Integrating with a SIEM solution such as Tripwire Log Center will show you if a large number of files are changed in a short period of time. Tripwire Enterprise will show you how files have been altered due to malware, helping you decide a best course of action for responding to the attack.
Patch management	Tripwire does not provide a solution designed specifically for patch management, however many organisations rely on Tripwire to confirm their patch management solutions are working correctly and ensure that nothing is being missed due to human error or system restrictions. Most patches released by vendors only cater for the latest vulnerabilities disclosed, so organisations need to check for previous vulnerabilities even if the latest patch has been run on a system. This is where Tripwire solutions can assist, as Tripwire reports on actual vulnerabilities that exist on a system rather than relying on what "should be" patched based on information provided by hotfixes, etc.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

TNCE1a 2010