FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Balancing Compliance with Security

Use Tripwire Solutions to Collect the Data You Need and Then Act on It

There is a misunderstanding that if you are compliant, you are secure. This isn't the case. For example, adhering to PCI DSS v4.0 will only allow you to tick the box to say you are PCI compliant in that moment. It gives you a snapshot in time of where you are in your compliance journey. But it won't prevent your company from suffering a breach—along with incurring fines and reputational damages afterward.

As such, many teams today are not putting in place the people, processes, and technology they need to strengthen their cybersecurity. They are collecting the data (compliance), but they are not acting on it (security). This makes it impossible for organizations to fulfill their security requirements and to keep up with the ever-evolving threat landscape.

With the pressure of limited time and resources, organizations sometimes overlook security to just focus on ticking the box of compliance. Some reduce the number of assets they monitor to reduce their costs, for example. In making this decision, organizations lose visibility into potential sources of risk that malicious actors could exploit when targeting them in the future. This leaves them wide open to attack along with all the expense and disruption that brings. They also may not notice a tightening of compliance requirements, leaving themselves open to non-compliance fines if they fail an audit. Surely, there is a better way.

Fortunately, there is: Fortra's Tripwire solutions combine security and compliance, enabling teams to achieve both while maximizing their existing resources.

HIGHLIGHTS

- Fortra's Tripwire® Enterprise supports over 4,000 policies, covers all platforms, and works with most frameworks right out of the box.
- Tripwire Enterprise has historical chains of audit trails to help customers to see who made changes and how their baselines have evolved over time.
- Tripwire solutions support templates for Windows XP and other older systems so that all organizations, even critical national infrastructure owners with legacy systems, can meet their compliance and security needs.

Product Overview

Tripwire Enterprise

Tripwire® Enterprise is a security configuration management (SCM) suite that provides fully integrated solutions for policy, file integrity, and remediation management. Organizations can use these capabilities together for a complete end-to-end SCM solution. In this capacity, Tripwire Enterprise helps organizations develop an accurate inventory of their assets using passive discovery tools. It then walks organizations through the task of defining

acceptable secure configurations for each type of managed asset. It will then assess those assets at a predefined frequency, notify of configuration drift, and help admins restore their assets to their known and trusted baselines[1].

Alternatively, organizations can use Tripwire Enterprise's file integrity monitoring (FIM) or policy management solutions on their own to address today's pressing security and compliance challenges—all while building a foundation that positions them to address the hurdles of tomorrow. Tripwire's FIM capabilities are designed to help security teams cut through the noise. They automatically provide security professionals with the insight and actionable intelligence they need to determine whether changes in their environments are good or bad, information that they can use to quickly remediate potential security issues[2].

With over 4000 policy/platform combinations, Tripwire Enterprise offers out-of-the-box compliance testing for well-known standards and frameworks including PCI, GDPR, SWIFT, and IEC 62443. Organizations can use that testing to proactively implement measures that will help block digital attacks. Simultaneously, they can leverage regular evaluations as a way of monitoring their compliance status and assessing how changes in their environments affect that status[3].

Tripwire ExpertOps

Tripwire ExpertOps℠ is a Security-as-a-Service (SECaaS) offering of Tripwire Enterprise that bolsters the expertise of organizations' internal teams with a group of external experts. Not to be mistaken with a Professional Services offering, Tripwire ExpertOps provides continuous staffing to operate and manage Tripwire solutions at peak efficiency. Security teams can perform at a much higher capacity thanks to ongoing support, guidance, and customized reporting that adapts to meet organizational objectives[4]. This means that organizations can just deal with the elements they really care about while Tripwire ExpertOps looks after the details in the background.

Key Benefits

Proven

Tripwire solutions take some of the pressure off security teams. This is particularly true for Tripwire ExpertOps. Security teams are already busy managing changes and investigating potential incidents, so why should they need to worry about updating their security tools? Or about managing the security communication between the agents and the platform? Or about generating reports?

EXPERT ADVICE

Compliance is a minimum requirement. Just because someone thinks they're secured doesn't mean they are. So, they want to make sure they're addressing security as their primary concern and using that foundation to build compliance. Tripwire can help with that.

With Tripwire ExpertOps, they don't have to. Tripwire does all this for them. As such, it frees up security teams to dedicate their time and effort elsewhere.

This could include achieving compliance with any compliance standard—or multiple standards at once, for that matter. If they are shooting for PCI compliance, they can cover ISO 27001 while they're at it, as the policies have some overlap. They can ultimately solve both compliance requirements at the same time using Tripwire Enterprise and its included policies.

Value

On the compliance side of things, Tripwire helps provide customers with results very quickly. This is important, as the initial phase of becoming compliant ordinarily takes a significant amount of time. Tripwire collects the data that organizations need to submit to audits, and it shows them a visual representation of where they stand in short order Not only that, but Tripwire also offers remediation advice to users that they can use to fix identified issues.

That latter point is useful when it comes to the time and effort needed for compliance and security. Tripwire monitors customers in real time, so when a change happens, it rapidly alerts personnel of the change. This allows team members to prioritize changes as they're seen, fix them on a timely basis, and get back to their day jobs. These actions might only take up a few minutes a day, but this spares organizations from having to annually to set aside a month—or more—to address those issues all at once.

Given the rate at which security and compliance are changing, organizations just don't have that time. Take how compliance standards change as an example. Many

changes tend to be simply tightening up on best practice. A standard may have initially required collecting logs only. In its next iteration, it could ask in-scope entities to also collect baselines and file status. The following year, it requires organizations to check those logs each month. This moves to a weekly basis in the release that comes after. This can happen continuously and on multiple compliance standards.

Security and compliance teams can't keep up with this level of change on their own. Tripwire designed its solutions with this dynamism in mind to make sure that teams can keep pace with these changes. Subsequently, organizations won't need to reinvest in a new solution every time a standard or security requirement changes.

Recognized

In terms of compliance, Tripwire is well-known for helping organizations achieve compliance very quickly. Some entities might have an order coming up where they need to conform to some framework or a set of standards in a short time frame. With Tripwire solutions, organizations can quickly get results into their compliance posture and obtain advice on how to fix them so that they can start budgeting and managing their resources.

Tripwire is also recognized in terms of the security services it provides. Its solutions cover the broadest number and types of platforms to help entities regardless of the specifics of their environments. Tripwire covers all aftermarket operating systems, and it officially supports 90% of all platforms—things like AIX databases, network devices, and other assets therefore fall under the purview of Tripwire's solutions. This level of support leaves far fewer security blind spots. It also saves organizations time and money in that they don't need to purchase and train their teams on different solutions for different types of systems/devices.

Reliable

Let's say something changes and an environment goes down. In a normal environment, IT and security teams will turn to a Security Information and Event Management (SIEM) tool to look around at suspicious activities. They'll also go to operating system owners and stakeholders to discuss and research potential changes. While all this is happening, the system is still down. It could be days (if not weeks) before the affected environment gets back up and running again. That can mean a huge loss of revenue for companies.

It's a different story with Tripwire. IT and security teams can use Tripwire's snapshot of the affected environment to realize, for instance, that someone changed an IP address route. They can gain all the context they need to understand what happened using Tripwire's real-time monitoring, and they can then take the necessary action to get back to system uptime within a matter of minutes, not days.

Summary

Compliance literally means that organizations are collecting the required data to be compliant. If they wish to be secure, organizations must not only collect that data but also act on the information to protect themselves. This is resource intensive.

Tripwire can help them to sift through the data, evaluate potential issues, and prioritize them. Such functionality can help internal teams balance their everyday workloads and drive organizations' security programs going forward.

Sources

1. https://www.tripwire.com/state-of-security/security-data-protection/security-controls/security-configuration-management/
2. https://www.tripwire.com/solutions/file-integrity-and-change-monitoring
3. https://www.tripwire.com/products/tripwire-enterprise/tripwire-enterprise-policy-manager-harden-your-systems-register
4. https://www.tripwire.com/products/tripwire-expertops

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

 (tw-ds-1123-r1-hm)