SOLUTION BRIEF

Elevate EPP/EDR with Tripwire Solutions

Endpoint Protection for Cyber Risk Reduction

Key Capabilities

- Detect threats, control change and prove compliance in real time
- Discover assets, identify vulnerabilities and prioritize risks
- Reduce the amount of time your cybersecurity resources spend dealing with unauthorized change and compliance drift
- Ensure the security, safety, and availability of enterprise and industrial environments
- Maintain control in the cloud with Tripwire's public, private, and hybrid cloud solutions

Endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions play a critical role in reducing the risk of successful attacks that exploit weakly configured endpoints and systems. These solutions alert security teams on potential cyberattacks, help with remediating misconfigurations, and can be delivered via an agent or through a service in the cloud.

Where EPP/EDR Can Improve

Endpoint protection solutions significantly reduce the risk of successful attacks on critical endpoints, but their means of doing so is more reactive than proactive. Most endpoint protection vendors start checking devices for malware based on a list of known threats. This is a great solution for knocking down simple attacks, but often not good enough for advanced persistent threats (APT). The leading EPP/EDR vendors also utilize behavioral analytics to watch how a system behaves and to alert when it starts acting "out of the norm."

This helps an organization identify a previously unknown threat. But since the malware is already causing the device to behave differently, teams end up responding later than ideal in the kill chain—the malware has already changed the system(s) and is active, weaponized, and likely spreading. Detection is later than it needs to be, and the response could be slowed without knowledge of what changes were made. What if you could be made aware of changes to a system as they occur so that you could react and remediate before the malware weaponized? You can do that with Tripwire.

Move Left on the Kill Chain with Tripwire

Tripwire is the perfect complement to any EPP solution. Tripwire's configuration monitoring solutions elevate the security and alerting capabilities of your EPP solutions by automating the verification process, checking configurations in real time, and reporting on the when, who, and why context of the change.

Tripwire monitors system configurations and will alert on any alterations from a known good state. This is the perfect early warning system that malware is present and trying to alter the device. A faster time to identification results in quicker response and less potential damage and risk.

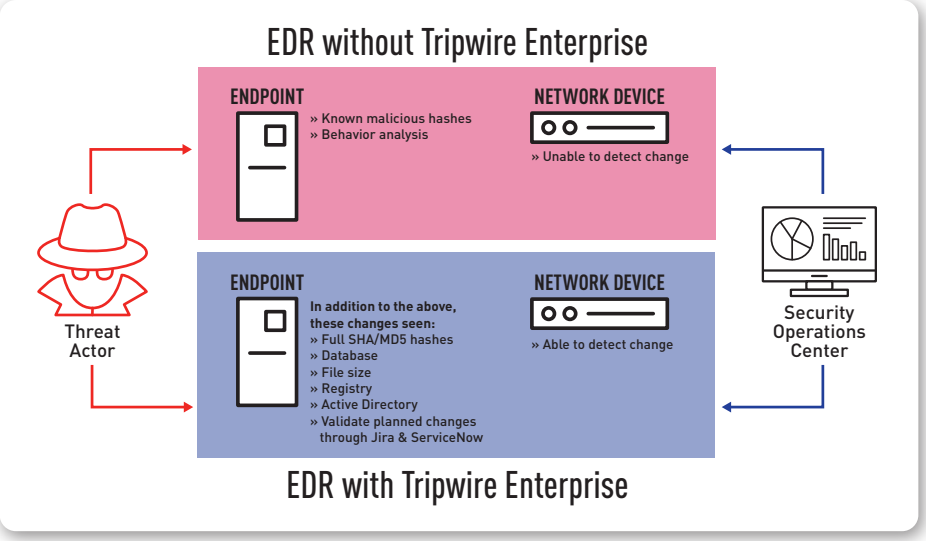

Fig. 1 Tripwire monitors system configurations and will alert on any alteration from a known good state. A faster time to identification results in quicker response and less potential damage and risk.

Damage Can Only Occur When There is Change

If your systems are starting from a known good state, the only way you increase your risk posture is through change.

Change can happen in three ways:

- Internal planned change (IT-approved and planned change to systems and processes),
- Internal unplanned change (unauthorized change completed by accident or deliberate internal user changes), and
- External change (attack and malicious activity from outside actors).

Let's look at each of these individually.

Internal Planned Change: All IT systems need authorized and traceable updates to improve performance, utilize the latest drivers and software, and fix faults in existing software. This happens every day—multiple times a day for some organizations—and is a never-ending process. Tripwire can monitor the changes that were made to the systems and validate those changes through API integrations with a ticketing system like ServiceNow, Remedy and Jira, among others, to see if they were planned changes and who initiated them. But most importantly, Tripwire delivers a risk score of the change (based on the current vulnerability of the system) via API to ServiceDesk, a SIEM, or a threat intelligence platform and/or based on the trusted "gold build" of the system.

Internal Unplanned Change: There are times when an administrator makes a mistake on an upgrade or patch that has not been properly tested, an IT user makes a change to their system inadvertently, or a user makes unapproved changes in order to complete a task. When these things happen, you need to be able to identify the change, audit who made it, and pinpoint when the change happened. Tripwire delivers all these capabilities, as well as helping return systems back to their known good state. This reduces risk, saves IT teams time by not having to support rogue configurations, and improves process management through audit capabilities.

External Change: Malware and other forms of external intrusion are the most feared form of change. Being able to monitor configuration changes allows an organization to quickly identify unplanned, external changes to their systems and address them as soon as change is identified—they no longer have to wait for a change in behavior of a device or a new Threat Intelligence Platform update to identify a threat.

Summary

Tripwire brings a deep level of understanding, auditing, and reporting to the changes taking place in the enterprise. Utilizing integrations with SIEM/SOAR/ticketing platforms to quickly identify harmful change, score its risk, and allow prompt response and recovery reduces overall risk and helps ensure optimum performance of systems.

Tripwire should be an integrated component of all EPP/EDR/XDR deployments to prevent damaging changes and provide an added layer of cyber security to mitigate persistent challenges. Organizations can strengthen their cyber defenses by adding Tripwire to their environment.

Watch Tripwire in Action

Let us take you through a demo of Tripwire solutions—Tripwire® Enterprise, Tripwire IP360™, Tripwire LogCenter® and more—to see how they reduce cyber risk and improve compliance.
Visit **tripwire.me/demo**

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

SBEEPPEDR1b 2203