FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Security Configuration Management

Foundational Security with Tripwire Enterprise

In a very real sense, IT security configurations are the proverbial “keys to the kingdom” when it comes to data protection and information security. They define system safeguards while balancing acceptable risk against the need for productivity. Hackers and attackers understand this balance all too well: the 2011 Verizon Data Breach Investigations Report noted that 83 percent of successful attacks were targets of opportunity and 92 percent were not difficult to carry out. It also found that 67 percent of breaches exploited easy-to-guess login credentials, a weakness IT security policies routinely address.

Organizations could prevent the bulk of these attacks from succeeding simply by hardening configurations. The SANS Institute backs up this claim. It lists secure configurations for hardware and software in the top five of its list of the top 18 critical security controls an effective security program must have.

> *“Eighty percent of what we need to do is stuff we already know how to do—getting the basics of Information Assurance right will of itself raise the bar for malicious activity.”*
>
> —**Iain Lobban**,
> Director, UK Government Communications Headquarters (GCHQ)

A World-wide Emphasis on Secure Configurations

The US Government’s IA Newsletter raises security configuration management’s importance in Department of Defense (DoD) networks by stating plainly, “Every system in this environment needs to be protected.” It goes on to say that the required level of system hardening may vary (based on the system’s value, the importance of its data, or its operational environment), but that every system needs to be hardened and its configuration settings continuously monitored.

Other international organizations also emphasize the need to continuously assess IT security configurations. Germany’s IT-Grundschutz, or “IT Baseline Protection Method,” asks users to catalogue configuration items and routinely compare them to established guidelines. Similarly, the UK’s GPG 13 touts the need for continuous monitoring of configuration states. One GPG 13 protective monitoring control (PMC4) even calls for “a set of alerts and reports that identify configuration and status changes on internal workstations, servers and network devices.”

Challenges to Managing Security Configurations

So why isn’t IT managing configurations more rigorously and monitoring them continuously to avoid these issues? Do system administrators simply not care about security? Nothing could be farther from the truth.

In most cases, IT doesn't know about these vulnerabilities. That's understandable given the large number of IT assets they must manage, the many unique configuration items each asset has, and the frequent changes that are made to them. Yet one small configuration change can dramatically increase a system's vulnerability. A very basic, yet important, example is a change to the number of milliseconds that a TCP "keep alive" should be retained.

Configuration changes occur inadvertently through what many call "configuration drift." But configuration items also change as attackers constantly seek to widen cracks in IT defenses. They add user accounts, elevate privileges, and change port or service settings—all in order to more deeply penetrate their targets.

Even organizations that routinely assess their configurations or pass audits are only secure for a moment in time. Without tight integration between assessment capabilities and real-time change monitoring, these organizations have a false sense of security. In reality, risk increases every second that passes after an audit or assessment. And after each second, the "known and trusted" configuration state becomes less of a reality and more of a belief.

To address these issues, organizations need security configuration management (SCM), a set of integrated IT controls that delivers a foundational level of security. SCM does this by hardening configurations against known vulnerabilities, and then continuously monitoring them to ensure they remain in that hardened, secure state. Specifically, SCM automatically assesses configurations for vulnerabilities—for example, login settings for all access points that use weak or default credentials. After it remediates these vulnerabilities, a true SCM solution continuously monitors configuration items for changes that indicate an attack may be underway. Examples include port compromises with RDP, or SSH tunneling that circumvents firewall policy. Fortra's Tripwire® Enterprise, a security configuration management (SCM) suite, offers this level of foundational protection to servers, databases, endpoints, directory services and network devices across the enterprise.

Establishing Foundational Security with Tripwire SCM

Compared to almost any other security control, SCM provides the most security "bang for the buck" against today's threats. That's why the SANS Institute places so much importance on using it. That's also why the U.S. Department of Defense includes it in all of its IT security requirements. And with Tripwire Enterprise as your SCM solution, that foundational control extends across the enterprise infrastructure. Immediately, without developing custom rules. It then helps maintain that secure state in spite of ongoing, countless daily changes.

How SCM with Tripwire Enterprise Works

Tripwire Enterprise provides end-to-end SCM with a complete spectrum of preventive, detective and corrective controls. It prevents breaches by hardening configurations, detects the changes that cause configurations to move out of their hardened state, and then corrects those changes—whether accidental or malicious—using automated remediation.

Prevent

Policy Manager hardens configurations against industry security benchmarks

Tripwire Enterprise immediately reduces the attack surface of your IT infrastructure. By hardening configurations with security benchmarks established by trusted industry sources, attacks are prevented from becoming breaches. For example, Policy Manager in Tripwire Enterprise lets you align configurations with benchmarks established by the Payment Card Industry Data Security Standard (PCI), the Center for Internet Security (CIS) and NIST. You can also easily customize built-in policies to reflect your own security needs.

Detect

File Integrity Manager detects changes that introduce risk

A rock-solid SCM solution needs to do more than simply assess configurations against a security policy. It must also continuously monitor configurations for changes that compromise security. Tripwire Enterprise includes File Integrity Manager, the industry-leading file integrity monitoring (FIM) solution that detects all changes in near real-time. It then uses ChangeIQ™ to determine if changes takes a configuration out of compliance and if they were accidental—or are evidence of an attack.

Correct

Remediation Manager returns configurations to a secure state

Inevitably, a configuration will drift out of a secure state. Obviously, the more time it's in that non-secure state, the more time hackers have to intrude. With Remediation Manager in Tripwire Enterprise, you can automate the process of returning configurations to their secure state. That reduces the time your systems are exposed and vulnerable. And in the small chance a breach does occur, potential damage is minimized by reducing the time before it's detected.

Turn to Tripwire SCM to Return to the Basics of Data Security

Iain Lobban of GCHQ was absolutely right when he noted that the vast majority of what's needed to deter malicious activity is "stuff" that's already known. Tripwire Enterprise provides this foundational level of protection from misconfigurations that open systems to breaches and compromised data. It does this by ensuring that configuration settings align with trusted security best practices, immediately detecting the changes that take configurations out of a secure state, and then automatically remediating these changes. With Tripwire Enterprise, you can quickly and effectively take control of your configurations with a single, tightly-integrated SCM solution.

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.com/demo.

TRIPWIRE INTEGRATES FOUNDATIONAL SECURITY CONTROLS FOR END-TO-END DATA PROTECTION

Tripwire Enterprise integrates preventive, detective and corrective controls in a single end-to-end SCM solution. This means it offers far greater security than an SCM solution that relies on individual, non-integrated controls. Then take advantage of the out-of-the-box integration with Tripwire LogCenter®—and the data it provides—in a single, easy-to-manage solution. This is how Tripwire shifts your data protection strategy into overdrive. Correlate SIEM and FIM data to identify events that need immediate investigation. Easily use controls data in the reporting and analysis tools you use most to identify security trends and status. View your Tripwire-monitored IT assets within business context such as business unit, geographical region or risk level. Learn more at tripwire.com.

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.