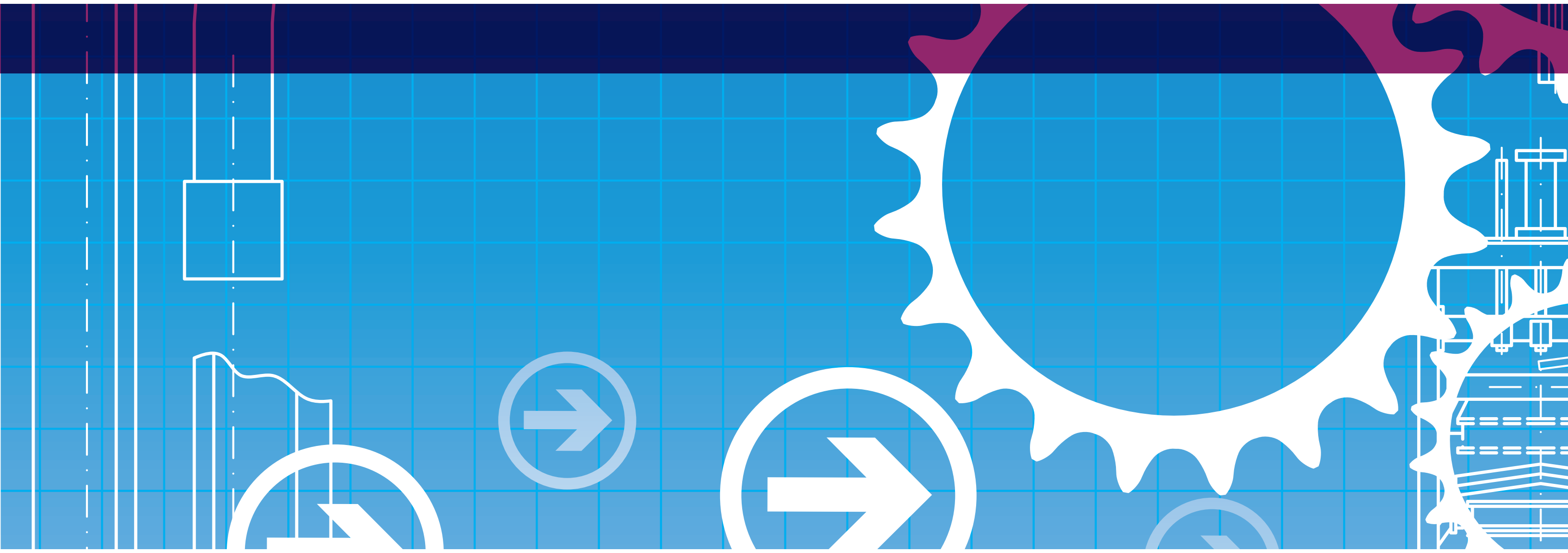
tripwire™

WHITE PAPER



Automation Makes Perfect:

Taking the Time Crunch Out of IT Compliance with Automation

Executive Summary

CIOs are ready to reclaim the precious time currently wasted on compliance. Automation makes compliance part of day-to-day operations, so enterprises are in a position to pass audits and fix vulnerabilities both now and in the future. But significantly, automation will enable CIOs to reallocate wasted time to more important initiatives—like a security strategy that protects the business, rather than simply pleases an auditor.

Regulatory mandates have been a mainstay for years, so shouldn't compliance be second nature by now? As time-consuming as flipping a light switch?

CSO
Custom Solutions Group

Sadly, nothing could be further from the truth. Whether preparing for an audit or manually running reports against internal policy, compliance activities are straining valuable IT resources at ever-increasing rates. In fact, according to IDG Research Services, 91 percent of IT leaders claim that the amount of time their organizations spend on compliance has increased or remained the same in the past 12 months.

In a bold stand to reclaim that time, some CIOs are taking the crunch out of compliance by automating the mundane tasks. "By making compliance repeatable, you can go beyond minimum baseline, which for most is just north of negligent," says Joshua Corman, research director, enterprise security, at The 451 Group, an independent technology analyst firm. That will reduce the time and energy IT commits to compliance, "so you can focus more on the dynamic aspects of security," he says.

In fact, the case can be made that automation is the only way to reliably get ahead of the compliance curve.

Protect, Detect, Correct … with Tripwire

Continuous compliance can help you narrow the gap between identifying compliance vulnerabilities and repairing systems to an audit-passing state. Tripwire's Enterprise is designed to do exactly that:

- ✔ **PROTECT**—systems by continually assessing the security posture against security policy;
- ✔ **DETECT**—in real time—changes that may threaten that security; and
- ✔ **CORRECT** vulnerabilities automatically before a breach occurs.

This end-to-end security solution helps reduce the risk window from improper configurations and returns systems to their compliant state. In the end, compliance becomes part of everyday operations while saving you time and money.

Compliance Sprawl

Forget virtual sprawl; compliance sprawl is the number one crippler of IT departments today. In addition to holding to internal gold standards, CIOs are increasingly slammed by ever-evolving regulatory requirements—from federal mandates like the Federal Information Security Management Act (FISMA) to state and local government statutes such as California's SB-1386. Even industry-specific requirements govern some sectors; for example, the Payment Card Industry Data Security Standards (PCI DSS) in the retail and financial sectors, and the North American Electric Reliability Corporation (NERC) guidelines in the energy space.

Complying with these regulations can be onerous. PCI DSS, for instance, is a landmark regulation dictating the protection of credit card data and a template for many state data privacy laws. The standard has 12 requirements and more than 200 controls—ranging from how to store data to how to transmit it. "This regulation alone results in a lot of stress and complexity," says Cindy Valladares, solutions marketing at Tripwire Inc., a global provider of IT security and compliance automation solutions based in Portland, Ore.

Of course, enterprises have to comply and keep current with such policies or face the consequences. The fines that come with noncompliance are stiff and swift. Just consider the NERC Critical Infrastructure Protection (CIP) standards, which define requirements for protecting the North American bulk electric system. With the compliance deadline of June 2010, violators can face fines of up to $1 million per day per violation.

Worse though, are the repercussions of potential security breaches. No enterprise wants to be the face of scandal, as with Heartland Payment Systems. The infamous breach compromised 130 million credit/debit cards, and the retailer is reportedly settling with the major card companies—Visa ($60 million), MasterCard ($41.4 million) and American Express ($3.6 million). Beyond the hard dollars, fallout in terms of customer confidence and shareholder loyalty can prove even more devastating.

Still, compliance is no easy task. IT managers must dissect each mandate, translate the intricacies of relevant policies, ready their systems, and then keep them ready. Equally arduous is the task of preparing for audits, fixing vulnerabilities, and cleaning up the damage. And some regulations are not long on prescriptive guidance. They reference sound objectives for risk mitigation, but provide little direction on exactly how to get there. "Regulations are subject to interpretation," says Michael Thelander, product marketing manager at Tripwire. "When one asks you to 'ensure that passwords adhere to best standards for authentication,' it adds tremendous amounts of time to the process just to create a testable, repeatable standard."

And even when prescriptive measures are defined, compliance can be a moving target. Enterprises are constantly introducing change—new systems, new people and new outcomes—that muddy compliance waters. CIOs all too often find their overworked staff on a never-ending treadmill toward short-term goals with little long-term reward.

A Strategic Calling

Even given all this complexity—or more likely because it—many enterprises take a tactical approach to compliance. Often they tackle it in a siloed manner, either department by department, or by addressing one mandate at a time without considering the redundancies or interdependencies among individual efforts.

A reactive rather than proactive stance tends to be the norm. Instead of arming systems and processes for "continuous compliance," initiatives are summarily designed to pass an audit or perhaps deal with a specific vulnerability. "Some organizations just want to get auditors out the door," laments Valladares. But one-off efforts are time-consuming, very costly, and often are not always the best route to securing the infrastructure. CIOs simply "end up in the same boat year after year," she warns.

But CIOs should "fear the attacker more than the auditor," says The 451 Group's Corman. Compliance as the end goal is too narrow. Instead, he says, it should be a natural by-product of a broader security strategy. "You can devote 100 percent of security spend to compliance, but that doesn't cover 100 percent of your risk," he contends, urging CIOs to stop aiming for compliance and start aiming for sustainable security practices with on-demand compliance.

Forget virtual sprawl; **compliance sprawl is the number one crippler of IT departments today.**

A more strategic approach is in order, according to a May 2010 report by the IT Policy Compliance Group, called "Automation, Practice and Policy in Information Security for Better Outcomes." The study suggests that without the right strategy, enterprises on average experience 16 or more losses or thefts of sensitive information and 16 or more deficiencies to correct in order to pass audits annually. Equally concerning, CIOs are looking at 60-plus hours of lost productivity due to IT disruptions or failures.

With the right strategy, however, the research indicates that enterprises experience fewer losses and less than four hours of lost productivity—time that can certainly be put to better use.

Automation Makes Perfect

When it comes to getting it "right," security-minded CIOs are working toward a more efficient and effective strategy by proactively promoting a better overall security posture rather than acting reactively to audits or specific security events. They're putting systems, processes and technology in place to make compliance an integral part of their day-to-day reality.

Continuous compliance affords CIOs the "unconscious confidence" they need today. "Streamlining and connecting disparate controls could eliminate inefficiencies and liberate limited staff," says Corman. So compliance doesn't occupy 100 percent of IT's bandwidth, and staff can move beyond compliance to focus on security, he says.

Automation is the key to that strategy, as compliance typically comprises many mundane tasks that prove time-consuming and ill-fated when left to manual processes. According to Thelander, it's not rocket science; these tasks can be as simple as closing a port or shutting down an application.

Indeed, according to the IT Policy Compliance Group, best compliance outcomes were achieved by one out of 10 organizations, and a primary characteristic of those organizations is that they've automated at least 74 percent of their processes and policies. Automation levels for organizations reporting the worst outcomes are said to average only 26 percent.

The proper foundation for automation can be accomplished in several layers. First, a protection layer automates assessment against policy and security sources. That includes predefined templates for key regulations like PCI and NERC as well as security benchmarks like The Center for Internet Security (CIS). This real-time or periodic assessment ensures that all systems are in their ideal, compliant state.

Second, a detection layer automatically checks for changes in that ideal state. File integrity monitoring (FIM) is proactively performed against file servers, devices, databases and directories. Real-time monitoring reports any deviations with critical details into not just what changed, but who, where and when that change occurred.

With these two foundational pieces in place, IT managers can easily put systems into a protected and compliant

The process is simple, fast and effective. And what could have taken weeks or months to identify, let alone fix, is accomplished in minutes—locking out mal-intents from wrecking havoc in the IT infrastructure.

state and be alerted to any change in that state. But that still leaves remediation in the hands of already harried staff. Fortunately, today's technology goes a step further, providing a third layer of automation to complete the circle of compliance automation: automated corrective action.

The Remediate Path

Capabilities to protect and detect may alert CIOs to vulnerabilities and provide a list of open issues for an audit, but what does it take to fix what's broken?

The ability to automatically correct non-compliant configurations is critical to compliance—and to reining in the costs and time associated with compliance. With these capabilities, systems automatically offer up remediation recommendations regarding how to fix identified vulnerabilities and get back to that ideal state. Even better, some systems build this advice into automated scripts that allow the fixes to be executed at the click of a button.

Built-in, role-based workflows allow, in these otherwise automated systems, for approval, deferral, denial or execution of remediation processes across security and operations groups. This "automation with oversight" helps IT organizations adhere to process, ensuring that glitches get fixed. It also expedites fixes, reducing the time between breach and full remediation. What could take a week to fix is accomplished in only minutes. "The auto-fix capability closes doors for a better overall security posture," says Valladares.

Here's how all this might play out in the real world:

Before introducing a new box to the IT infrastructure it must be configured to its ideal, compliant state. Manually, that seemingly minute task can take an average technician eight hours to complete. With automation, the whole process requires as little as five minutes. And if there are 10 new boxes coming into the environment, those minutes can be multiplied times 10 for greater productivity gains.

Once the boxes are deployed, unplanned software upgrades, application integrations or misguided administrative changes can easily bring them out of compliance. Instead of assigning administrators to monitor all systems by hand—indeed, a tedious job—they can be automatically assessed for deviations from the desired state. And because the automated process isn't a slave to competing projects and workloads, the breach-to-detection gap can often be closed before it gets a chance to be exploited.

The breach can be identified in real time, with remediation coming quickly on its heels. A manual analysis of the situation would take hours, during which time an unknown assailant could have access to the "keys to the kingdom." But with automated remediation, the best correction option is literally spelled out in real time. The system prompts a security administrator to approve the course of action; and with a simple click of the mouse, remediation is activated.

The process is simple, fast and effective. And what could have taken weeks or months to identify, let alone fix, is accomplished in minutes—locking out mal-intents from wrecking havoc in the IT infrastructure.

Rewards Aplenty

"The evidence shows it [automation] is worth the effort," reports the IT Policy Compliance Group. Factoring in the cost of audits, downtime and exposure to data loss against customer retention and revenue, the researcher demonstrates that those organizations that more fully embrace automation enjoy profits of 6.4 percent; while organizations with low automation levels experience losses of 6.9 percent.

Right or wrong, though, for most CIOs and CISOs it all comes down to audit burden. They can drown in that burden, defer it, or conquer it, Thelander concludes. "Automation is the silver bullet that allows them to control that burden rather than succumb to it." And all the while, they'll be saving a boatload of time—and money—that can be reallocated for more strategic initiatives.

www.tripwire.com

tripwire™

CSO
Custom Solutions Group