



# Hassle-free compliance

Make compliance just another part of your processes by taking an operational approach to security ▶ BY SANDRA GITTLEN

## Inside:

- ▶ Compliance is a fact of business life challenging organizations of all sizes
- ▶ Simply ticking off boxes on audits is not enough to keep you secure
- ▶ Integrating standards processes with security guarantees continuous compliance
- ▶ You must account for compliance in your physical and virtualized environments
- ▶ Tripwire's approach to operational security delivers compliance as an ongoing feature

If your company is like most, you likely approach compliance as a set of check boxes designed to meet auditor requirements. Shortly before auditors arrive, you pull in IT and business team members to manually cull through months of logs and configuration files to ensure there are no major vulnerabilities. Often you are left awkwardly trying to answer the inevitable request for more information. If you're lucky, this ad-hoc process results in certification and everything returns to normal—until the next audit. ▶

**tripwire**

It's a huge waste of time and precious IT resources. What's worse, while the auditors may have checked the boxes for their requirements, they did not prove that your enterprise is secure. The checklist approach treats compliance as a project rather than a process. It is a fire drill to meet on-the-spot audit requirements versus an opportunity to intelligently integrate compliance into your overall enterprise security strategy.

"The intent of compliance is to make sure that companies implement best practices surrounding security. Yet focusing on satisfying annual or quarterly audits results in gaping holes in your network protection," says Scott Crawford, research director at Enterprise Management Associates in Boulder, Colo.

The irony of this is magnified as companies try to deal with multiple mandates from multiple organizations. For instance, hospitals must not only meet HIPAA regulations surrounding patient privacy, but also the Payment Card Industry Data Security Standard (PCI DSS) for protecting financial transactions. Individual states chime in with their own privacy laws, too. Imagine trying to carry out one-off audits for each of these standards with limited budgets and staff. It would quickly become overwhelming and would drain resources from something more important—the overall protection of customer data.

Yet the threat of fines and other penalties has IT teams scrambling to meet these requirements in what some believe has to be a trade-off to true security. Crawford says the critical mistake lies not in trying to deal with compliance, but in thinking that it's an either/or situation. "Compliance should be the natural outcome of a sound security strategy," he says.

Gene Kim, co-founder and CTO of Portland, Ore.-based Tripwire, agrees. "There shouldn't have to be a heroic effort to comply with standards. Security, by definition, involves safeguarding confidential information, protecting against fraud, ensuring systems are available so you can generate revenue,

and making sure there are no errors in the stack. When you do all these things, you inherently wind up fulfilling the intent of all major regulatory and industry compliance requirements," he says.

### ► The checklist conundrum

In most cases, compliance mandates outline requirements for securing access, transmittal and storage of data. To verify that you have met these standards, they either send auditors on-site or require you to perform a self-audit. Either way, you must be able to report on the soundness of your user authorization, change and configuration management controls. For instance, you must be able to prove that only authorized users are able to access, configure and update servers holding sensitive customer information.

While this seems simple enough, some IT departments encounter serious difficulties performing these audits because there is separation between their security and operations teams: security lacks visibility into operations' processes and vice versa. The result is an inability to develop a known good state for network infrastructure that can be used as a benchmark to ensure compliance. Without this, when it comes time to prepare for the audit, security teams must pore over event logs and configuration files to try to spot policy infractions.

More importantly, in between audits, changes in configurations or unauthorized access to critical files go undetected, which can lead to data breaches—the exact events that compliance was intended to prevent. "Compliance alone is merely a snapshot in time. It's not a way to keep up with the threat landscape," Crawford says. He adds that this type of point-in-time view increases the chances for threats to enter your network.

Virtualization further complicates the situation. As IT teams ramp up their knowledge in this area, it's easy for mistakes to be made. For example, a virtual switch can be misconfigured,

making data on a protected part of the network suddenly available to the public.

The dynamic, mobile nature of virtualization poses challenges to security teams trying to manually enforce policies. Some laws, such as the Sarbanes-Oxley Act of 2002, require companies to know where their data lies at all times—yet VMware’s popular VMotion tool automatically moves virtual servers among physical hosts for load balancing and fault tolerance. Internal standards bodies, such as those at law firms and service providers, demand that competing clients cannot have their data commingle and, therefore, should not be allowed on the same physical host. Trying to manually track this with the rate that virtual machines can be spun up is nearly impossible.

“We’ve had customers hold off on virtualization, even though it promised to save them money and improve availability, because they didn’t think they could guarantee compliance,” says Steve Hall, director, marketing strategy at Tripwire.

### ► More than security risks

Handling compliance manually on a standard-by-standard basis makes your organization reactive instead of proactive. This is not just a security risk. It’s also a waste of staffing and budget resources.

“A compliance manager at a large retailer told me he mobilizes over 600 of his workforce, spending tens of millions of dollars in labor, to get his stores ready for the auditors,” Kim says. “That’s a horrible amount of time and money to spend on compliance. The worst part is as soon as he passes one audit, he has to turn around and do it again six months later. That’s not sustainable.”

As soon as the auditor leaves, the organization tears down its makeshift processes because that’s not how they typically do things. “Compliance is supposed to be a report of how controls work in daily operations, but that is not reflected in most audits,” Kim says.

## Operational Security Checklist

Before you move from a manual approach to compliance to an automated one, we recommend you walk through these five easy steps:

- 1. Know the standards** you are required to meet. Most organizations fall under several mandates, including those from federal government, state government and industry. You may also have to comply with vendor guidelines. And if you conduct business overseas or have data centers located there, you’ll need to familiarize yourself with each country’s restrictions. For instance, the European Union has strict laws regarding privacy.
- 2. Understand the business** and IT risks you face in meeting compliance demands. You may have a network architecture that poses significant challenges to mandates. For instance, if you are a retailer with unattended servers at each location, you should highlight the risk this presents.
- 3. Determine where in the network the controls for those risks live.** Is that unattended server controlled by your data center? You’ll need to know this so that you can lock down ports or block on-site logins.
- 4. Test the controls.** You should be able to dispatch policies to network devices from anywhere. You don’t want to find out that your off-site servers can’t be controlled from the data center.
- 5. Monitor and report on the controls.** You need to be able to monitor the controls on your network equipment and generate reports on what happened. You have to be able to prove the effectiveness of your compliance efforts.

Merely following compliance mandates also adds a burden to your security team when threats are suspected because there is no reference point for the root cause. The audit may tell them something has changed, but it doesn't say what, when or by whom. Tracking down that information takes time and money.

And each new regulation forces your team to rush to update policies and processes and then try to enforce them. Given the number of new laws, industry standards and internal governance boards, that's a tall order.

Lastly, by trying to tackle compliance as a checklist, organizations miss the chance to create efficient, enterprise-wide business processes that could boost revenue. Integrating your security strategy into operational processes not only ensures compliance, it also streamlines the server provisioning process, thereby decreasing the time it takes to stand up servers and bring new applications online.

### ► Continuous compliance

To properly address standards, employ continuous compliance. Continuous compliance is built on the principle that compliance is not just a point-in-time audit, but also an ongoing set of processes.

The key to succeeding at continuous compliance is to develop an accurate known state for your infrastructure that takes into account all your compliance requirements. That way, when you provision a new server or virtual machine, it can be checked against this golden image before it goes online. With continuous compliance, you also do frequent system scans to make sure no critical files have been maliciously or accidentally changed. If they have, you can immediately return the server to its approved configuration. In other words, you seal up all your vulnerability windows.

It also makes the auditing process much faster and simpler because executives, IT staff and auditors are all on the same page. "You can use continuous compliance to figure out how

to intelligently and securely make changes, do releases and create reports. It moves compliance from a multi-month, 600-employee project to an ongoing effort where you can quickly and easily pull the right reports for auditors," Kim says.

Your risk is reduced because you now have the visibility across security and operations to set policies and monitor privileged accounts for adds, moves and changes. This visibility is also beneficial for virtualization. IT can set specific policies to be carried out through the hypervisor that stipulate whether a virtual machine can be moved and if certain virtualized applications can co-exist on a physical host. When it comes time for auditing, IT can generate reports showing that the compliance rules that exist for physical infrastructure were also applied to the virtual environment.

When done right, continuous compliance essentially offers three levels of value: basic compliance; the ability to integrate compliance into your security strategy; and the opportunity to enforce your operation goals.

### ► Getting to a good, known state

It cannot be overstated: approaching compliance manually and separate from security is dangerous and inefficient. Crawford says it's imperative that enterprises employ a sophisticated compliance tool, one that automatically allows them to define and then implement compliance objectives, and monitor the environment to ensure those objectives are being met.

If it detects any problems, the tool should be able to respond as your policy warrants. It should also be able to validate that the objectives were indeed deployed as expected.

The best tools feature a combination of configuration assessment and change auditing. "You don't just want to know the configuration—you want to be aware of changes that you did not authorize or accept and be able to determine if they are

legitimate or a true threat,” Crawford says. These capabilities must extend to the virtual enterprise and be seamless with the physical infrastructure because so many companies are mixing their physical and virtual enterprises these days, he adds.

Tripwire's flagship software, Tripwire Enterprise, can help. It features configuration assessment, change auditing and virtualization tools to automate your compliance efforts and align them with your security goals. Tripwire has over 6500 customers worldwide and operates in more than 15 countries. Their tight focus on ensuring the integrity of configurations makes them a best-of-breed solution for your compliance needs.

Tripwire Enterprise automatically assesses your entire infrastructure—applications, databases, servers, virtual environments and network devices—against your internal and external compliance regulations. Then, the software uses file integrity monitoring to detect in real-time if changes are made to files and configurations, what those changes are, when they were made, and who made them. Armed with this information, an IT manager can reconcile any changes with leading enterprise management systems and CMDBs, including those from BMC, CA and HP, to make sure they are authorized and compliant. If not, he can return an altered file or configuration to its most recent known good state.

The software manages compliance using

industry-based IT security policies such as PCI DSS and HIPAA. It also compares against security standards, including CIS, NIST, and vendor configuration best practices.

Meanwhile Tripwire Log Center provides real-time threat monitoring, event correlation and log management, without the need for a separate SIEM tool. It integrates seamlessly with Tripwire Enterprise so organizations get complete visibility into threats, configuration changes and policies impacted by suspicious activities.

Tripwire Enterprise and Log Center handle compliance from a unified interface. That means IT teams don't have to toggle between applications and can apply policies universally and be assured they are being enforced.

## ► Conclusion

If the fast pace of government and industry standards is any indication, IT teams will not get a break from compliance any time soon. To stay ahead of the game, you have to automate change auditing and configuration assessment in your physical and virtual environments and weave them into your organization's day-to-day security plan.

Not only does this improve your security posture and ensure that gaps in protection are filled, but it also helps your organization become more efficient by saving staffing and budget resources for more strategic projects. ◀

## Advantage Tripwire

Whether you're a large service provider or an upstart gaming company, complying with today's standards can prove daunting. Apply the wrong strategy and you'll wind up failing your audit or wasting time and money searching for the changes that brought down your network. Tripwire Enterprise has saved

more than 6,500 customers worldwide the grief that can be caused by compliance, configuration and change management.

Take, for instance, Vesta, a company that manages risk and process payments for international companies such as AT&T, ►

Ericsson and Verizon. Vesta has data centers in North America and Ireland so it is subject to numerous national and international standards, including PCI DSS and SAS 70. The company also conducts internal audits.

Vesta CISO James Summers says trying to approach each audit as an independent event with its own set of unique controls would be overwhelming. Instead, he's adopted a holistic security policy that includes automated continuous compliance.

He uses Tripwire Enterprise's configuration assessment to evaluate each system's compliance with Center for Internet Security benchmarks and Vesta's own security policies. He says having the same system compare configurations and audit for change spares him the time and expense of buying and managing multiple software packages.

Summers credits Tripwire with enabling him to quickly respond to outages or service degradation by checking and mitigating recent changes. He says that capability alone has decreased the company's mean time to repair by hours and increased uptime to 99.95 percent. And because everything can be viewed in one place, the audit process takes less than a third the time it used to. Vesta gives Summers and his team the confidence they need to know that security policy is being followed across the enterprise.

The goal at Sitel, a global business process outsourcing leader, was to achieve "audit-ready" operations. The company, which has 2,000 customers worldwide, has to ensure that its 10,000 servers are in line with PCI DSS. Sitel estimates that handling compliance manually would have required an additional headcount of 50 staff. With Tripwire Enterprise, they were able to avoid that expense and cut the audit time down from five days to just one.

Sitel credits this success to being able to do

continuous configuration assessments and uncover problems that needed to be resolved to stay compliant. The company says the ongoing monitoring of thousands of servers to catch any infrastructure changes has also been beneficial.

"Robust security and PCI compliance demands the creation of a multi-tier strategy that combines good operational and change management processes with real-time monitoring to highlight any incidents of unexpected or unexplained changes to the system infrastructure," says Robert Foster, Sitel's director of EMEA data systems. He adds that Tripwire has allowed Sitel "to increase both uptime and stability, which is delivering quantifiable bottom-line benefits."

Another company that has seen cost savings is MarketLive, a provider of enterprise-class e-commerce retail technology and services for mid-sized businesses. While MarketLive initially purchased Tripwire to deal with PCI DSS compliance, its side benefits have proven just as valuable.

MarketLive deals with an enormous amount of changes to its server builds—the operations team might deploy as many as 400,000 changes a week. Of those 400,000, perhaps two dozen could potentially interrupt service or pose a compromise to security. Before Tripwire, instead of trying to find the culprit among hundreds of thousands of changes, the IT team would opt to rebuild entire systems. That process alone involved unnecessary work and could subject the environment to new problems.

With Tripwire Enterprise, the MarketLive team has complete visibility so suspect changes can be quickly identified and surgically repaired. This saves time and resources, and ensures greater data integrity and less risk.

On the PCI DSS front, MarketLive used ▶

Tripwire to ensure it was certified compliant by Visa and MasterCard early on. Now, when its clients undergo an audit, MarketLive is able to make the whole process a simple, straightforward and cost-effective task.

Bwin Interactive Entertainment had a similar outcome thanks to Tripwire. The company's overall revenue grew by an astonishing 19 percent in a single year. Combined with a 2 million-strong customer base, such rapid growth left bwin struggling to keep up with various regulations and in a constant state of vigilance against fraud and malicious intrusion. "We needed to be safe, secure and trustworthy, and instill customer confidence with controls you would expect of any financial institution or entertainment enterprise," says Oliver Eckel, head of corporate security at bwin.

In addition, the company had to quickly become PCI DSS compliant or face stiff fines. So bwin deployed Tripwire Enterprise on its 50 servers hosting credit and financial data. Thanks to the monitoring tools, bwin was able to produce a report that allowed them to pass their audit in record time.

The company has since added Tripwire to more than 1,600 servers to automate compliance processes (including configuration assessment) for Europe's ISO 270001 and other regulations. Bwin says this has resulted in security and IT operations being in sync so they experience fewer failed change and service incidents overall. If incidents do arise, there is a detailed change history to help determine if change is the cause and then pinpoint where the changes are located. This improvement in efficiency has reduced repair times and increased availability.

As these customers clearly demonstrate, Tripwire Enterprise not only tackles the tough chore of easing compliance audits, but also works to improve security and operational efficiencies overall.

The above customer comments from Vesta, Sitel, MarketLive and bwin Interactive Entertainment were drawn from Tripwire case studies. You can read more at <http://www.tripwire.com/resources/case-studies/>