Gene Kim
CTO, Tripwire, Inc.

tripwire™

Practical Steps to Mitigate Virtualization Security Risks

WHITE PAPER

Configuration Control for
Virtual and Physical Infrastructures

Contents

Executive Summary

The prospect of increased agility and the increasing cost and complexity of IT has contributed to the rapid adoption of virtualization technologies. Virtualization makes it possible to build and deploy IT releases and changes into production faster and more economically than ever. Some virtualization experts claim that virtualized environments are fundamentally no less secure than physical environments. However, others claim that virtualization can enable better security. Who is correct? Both claims can be correct, but only under certain conditions.

Every day, information security practitioners live with the reality that they are a single change away from a security breach that could result in front page news, brand damage, or regulatory fines. These issues are clearly not confined to security, but impact business at the highest level. Consequently, security practitioners strive to implement IT controls to mitigate issues such as the risk of fraud, loss of confidential customer information, disruption of critical business services and data integrity, and inaccurate financial reporting.

Security must be baked in from conception, not addressed later as an afterthought. But since virtualization is already here, what steps can we take to implement effective security controls? Where do we start, and in what order? And how do we do this in a way that creates value rather than the perception of information security creating bureaucratic barriers to getting real work done?

These are the types of questions that I've been trying to answer since 1999, when I started studying high performing IT operations and information security organizations. At this point, I can confidently say that I've seen the best and worst of information security. The high performing organizations I've studied consistently had the best security, the best compliance posture, the greatest ability to make changes quickly and successfully, and optimal efficiency.

In this paper, I describe seven practical steps that IT organizations can take to mitigate the unique security challenges of virtualization. While many of these steps are solid best practices that apply to both physical and virtualized environments, some are directed specifically at virtualized environments.

Achieving a known and trusted state is a challenging task for even the most technically adept and process-focused organizations. Tripwire, the recognized leader of configuration control with over 6,000 customers worldwide, enables organizations to fully realize the benefits of both their virtual and physical environments by ensuring that the entire data center achieves and maintains a known and trusted state. Tripwire specifically addresses the security of virtual environments with CIS- and VMware-issued policies aimed directly at securing VMware ESX Servers, the hypervisor most used to virtualize machines. In addition, Tripwire® Enterprise integrates with critical systems—such as change management and asset management solutions—allowing us to maintain full visibility and control into the data center and any changes made to it.

The Unique Information Security Challenges of Virtualization

Every day, information security practitioners live with the reality that they are a single change away from a security breach that could result in front page news, brand damage, or regulatory fines. These issues are clearly not confined to security, but impact business at the highest level. Consequently, security practitioners strive to implement IT controls to mitigate issues such as the risk of fraud, loss of confidential customer information, disruption of critical business services and data integrity, and inaccurate financial reporting.

Effectively balancing risk with controls is made even more difficult by the constant pressure on IT to respond quickly to urgent business needs. Most business functions now require IT in order to conduct operations. In fact, almost every business decision requires at least one change by IT—a trend that continues to grow.

The resulting need for increased agility and the increasing cost and complexity of IT has contributed to the rapid adoption of virtualization technologies. Virtualization makes it possible to build and deploy IT releases and changes into production faster and more economically than ever before. Some virtualization experts claim that virtualized environments are fundamentally no less secure than physical environments. Others claim that virtualization can enable better security. Both claims can be correct, but only under certain conditions. The reality is that when information security controls are improperly implemented or neglected in virtualized environments, real security risks and exposures are created faster than ever. This is the potential *dark side of virtualization*, and the information security controls that adequately controlled risks before virtualization may no longer suffice.

Virtualization is Already Here

Virtualization enables rapid deployment of computing resources, potentially allowing insecure IT infrastructure to be deployed throughout the organization faster than ever. The unfortunate truth is that the people who deploy this infrastructure often circumvent existing security and compliance controls when doing so. Worse still, the risk these deployments introduce is only discovered when a security breach occurs, an audit finding is made, or the organization loses confidential data or critical functionality.

For better or for worse, virtualization is here. Tripwire surveyed 219 IT organizations and found that 85 percent were already using virtualization, with half the remaining organizations planning to use virtualization in the near future. Furthermore, VMware found that 85 percent of their customers are using virtualization for mission-critical production services. In other words, inadequate information security controls may already be jeopardizing critical IT services with risk introduced by virtualization.

Most information security practitioners now attribute the majority of security failures to misconfiguration resulting from human error. According to Gartner, "the security issues related to vulnerability and configuration management get worse, not better, when virtualized."[1] Gartner also asserts that, "Like their physical counterparts, most security vulnerabilities [with virtual machines (VMs)] will be introduced through misconfiguration and mismanagement."[2] Why? Because, among other reasons, insecure virtual server images can be replicated far more easily than before, and once deployed, require great effort to discover and bring back to a known and trusted state.

Analysts have published some startling predictions on these information security implications: Gartner predicts that "Through 2009, 60 percent of production VMs will be less secure than their physical counterparts" and that "30 percent of deployments [will be associated] with a VM-related security incident."[3] The good news is that it doesn't have to be this way.

Gene Kim's Practical Steps to Mitigate the Security Risks of Virtualization

There is nearly universal agreement that information security and IT operations must properly manage virtualized servers the same way as physical servers. Security must be baked in from conception, not addressed later as an afterthought. But, if virtualization is already here, what steps can we take to implement effective security controls? Where do we start, and in what order? And how do we do this in a way that creates value rather than the perception of information security creating bureaucratic barriers to getting real work done

These are the types of questions that I've been trying to answer since 1999, when I started studying high-performing IT operations and information security organizations. At this point,

I can confidently say that I've seen the best and worst of information security. The high performing organizations I've studied consistently had the best security, the best compliance posture, the greatest ability to make changes quickly and successfully, and optimal efficiency.

What I learned was that high performing IT organizations have figured out how to build sustainable security controls that integrate into daily IT operational processes and deliver value to other business stakeholders. In these high performers, information security simultaneously enables the business to respond more quickly to urgent business needs and helps provide stable, secure, and predictable IT services.

How these information security organizations achieved their "good to great" transformation has been codified in the handbook *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps*. Although *Visible Ops Security* is not dedicated solely to the topic of virtualization, it describes and examines the core chronic issue that exists in every IT organization, and helps explain why virtualization is so compelling. **Vi***sible Ops Security* also describes why security has so much to gain or lose through virtualization, and how security can meaningfully integrate into and add value to an IT organization's virtualization strategy.

This paper describes typical information security risks that practitioners will face with virtualization, presents seven practical steps to secure the virtualized environment, and discusses the business value of implementing these steps.

When We Hear These Things, We Know We Have a Problem

Here are just a few of the real-life experiences that illustrate the issues and risks introduced by virtualization.

THE CHALLENGE	THE REALITY
Virtualization may bypass secure configuration standards	In an attempt to be proactive, information security spent two quarters building secure configuration standards for Windows, Linux and eight other OS platforms. But, one year later, we did a vulnerability scan and we found that no one is using those configuration standards, and we're more insecure than ever. We did some analysis, and we finally figured out why: the server engineering groups were using virtualization to clone insecure builds, making us more insecure than ever.
Security network scans may never detect insecure virtual servers	How did those insecure virtual servers get into production? It turns out that there are virtual machine administrators in virtually every IT group, and that they are adding and removing virtual servers on a daily basis without us even noticing, and we certainly didn't see them during our weekly network scans.
Information security must dig deeper to document virtualized IT environments for compliance requirements	Now that more and more of the production applications are being deployed and run in a virtualized environment, it's getting more and more difficult to keep track of all the IT infrastructure that is deployed. Worse, with all the increased regulatory and contractual requirements for IT controls, it's getting even harder to comply. Why? We're finding out at the last minute about applications that don't meet compliance requirements for IT controls, and we as the security team have to spend more and more time in a reactive mode trying to get things in a state where the auditors won't generate more findings.
Information security relied upon the slow rate of physical server deployment to "stay secure"	We used to be able to head off many of these releases and deployments at the pass when we spotted boxes of servers showing up at the loading dock, or when large cabling projects started. We'd do some digging, and usually find that there was an upcoming deployment we didn't know about. We'd then assign information security resources to do a security review to make sure the right IT controls were put in place before it went into production. Virtualization took away that safety net, and we've got to figure out how to overcome this issue.
High risks due to virtualization	Some of us are starting to lose sleep at night because of the potential risk of loss of confidential information. I said, "Look, you can't put private health information out on the public Internet on this infrastructure." There are real mission-critical services that contain confidential data that must be adequately secured. But, when we try to mitigate these risks, we're viewed as hysterical, paranoid, and an obstacle.

What We Can Do About It: Seven Practical Steps

The issues and indicators described above are typical when information security is not adequately plugged into IT operational and software and service development processes. These issues are all magnified by virtualization because it enables such rapid change.

Our goal is to start gaining control at the relevant parts of the virtualization lifecycle, and start generating value for the relevant parties. By doing this, we replicate the observed high performing attributes, which are codified in *Visible Ops Security*:

- **Business aligned** – High performing information security teams understand how security advances and protects business goals. Low performing teams focus on things the business doesn't care about, like the improbable or irrelevant and other technological minutia. Often other groups in the organization consider these low performing teams paranoid and fear-mongers.

- **Plugged in** – High performing information security teams integrate into the right functional groups even though they don't have direct operational responsibility. Low performers aren't present where the work is done and often expend effort helping the wrong people, reinforcing the perception that information security is irrelevant.

- **Adding value** – High performing information security teams provide value to business and IT process owners, and they know what they need from these process owners in return. Low performers don't help advance the operational objectives of their colleagues, nor do they clearly articulate what they want people to do differently to meet information security requirements. Consequently, these low performers are often viewed as incompetent.

The following steps are adapted from *Visible Ops Security*. More information on the handbook is available at the end of this paper.

Securing the Virtual Machine Managers (VMMs)

The first three steps focus on gaining situational awareness and controlling configurations and changes at the virtualization layer—the virtual machine managers (VMMs), hypervisors, and host OSes.

STEP 1: GAIN SITUATIONAL AWARENESS

Our first required step is to build *situational awareness*, defined in military parlance as "the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regard to the mission."4 In the virtualization context, we must learn where virtualization technologies are being used, what they are being used for, and who is responsible for their management. This information will help us answer these important questions:

- What IT services are being enabled by virtualization (e.g., e-commerce, point of sale, financial reporting, order entry, etc.)?

- Who are the business and IT units, and how are they organized (e.g., the centralized IT services group, an IT outsourcer, etc.)?

- What are the relevant regulatory and contractual requirements for the business process enabled by virtualization (e.g., SOX-404, PCI DSS, FISMA, etc.)?

- What are the technologies and IT processes being used (e.g., VMware Fusion, Citrix XenServer, Microsoft Virtual Server, etc.)?

- Are there any high-level risk indicators from the past (e.g., repeat audit findings, frequent outages, etc.)?

With answers to these questions, we can establish an opinion on the magnitude of the business and technology risks so that we can better prioritize our efforts.

STEP 2: REDUCE AND MONITOR PRIVILEGED ACCESS

Once we know where virtualization technologies are being used and who is responsible for managing them, we must integrate information security into the access management procedures. Our goal is to reduce access wherever possible and to ensure that some form of effective access control exists.

Excessive access and privileges make it possible for people to make uncontrolled changes to critical systems. Such changes expose IT systems to risk of disrupted service and create unnecessary vulnerabilities for malicious and criminal acts that could jeopardize the organization. The potential for introducing risks from excessive user access and privileges is especially evident in the VMM. Often the VMM resides on a host operating system, which has privileged user accounts that can modify security configuration settings, modify virtual machines, as well as activate and deactivate virtualized computing environments.

The necessary actions in this step include implementing the following preventive controls:

- Document all the virtualization administrators who have privileged access to the VMM and ensure we can reconcile them back to authorized staff. Any ghost accounts that cannot be reconciled to authorized staff should be disabled or deleted.

- Work with virtualization managers to reduce the number of administrators to the minimum needed. This number will vary, but we know that if we have 25 administrators, we have too many—in other words, everybody has root. On the other hand, one is too few because if something happens to that one person, nobody can get root.

- Ensure that when personnel changes occur from actions such as hiring, firing, and transferring, access is appropriately revoked or assigned.

To ensure that these preventive controls are working, we must have the following detective control requirements:

- Monitor privileged VMM user account adds, removes and changes, wherever they are stored (e.g., /etc/passwd, LDAP, Active Directory). Privileged accounts include service accounts that do system maintenance and tasks like back up accounts and manage the enterprise batch scheduler.

- Reconcile each privileged VMM user account add, remove and change with an authorized change order from the virtualization manager. This reconciliation process may be manual (a signed paper form) or automated (for example, a BMC Remedy work order).

- Reconcile each VMM privileged account with an authorized user. For example, reconcile the account with an HR record. Alternatively, reconcile the accounts with an authorized service; for example, an authorized Unicenter backup program.

- Routinely re-accredit accounts—quarterly or yearly, depending on turnover—to ensure that management can reconcile privileged accounts to reports from HR and payroll.

STEP 3: DEFINE AND ENFORCE VIRTUALIZATION CONFIGURATION STANDARDS

As with any complex application, VMMs have configuration and logical security settings that are designed to limit the risk of human error, fraud, and security incidents by ensuring that the technology only performs as designed. Examples include proper password settings for the system BIOS, hypervisor host operating system settings and permissions, network configuration settings,

and virtual machine policies. However, risk can be introduced if these settings are improperly configured.

Our goal in this step is to ensure that all these VMM configuration settings are properly defined, implemented and verified. We can use guidance from respected third parties and vendors, including:

- VMware ESX Server 3.x Benchmark Version 1.0, from the Center For Internet Security (CIS)

- VMware Infrastructure 3, Security Hardening, from VMware

In order to operationalize this, we need the following preventive controls:

- Work with IT management and virtualization managers on a policy that defines which virtualization security standard(s) should be used.

- Mandate that all virtualization technologies use these secure configuration settings, and create a plan for deploying virtualization technologies with the secure settings.

- Define a time limit for initial implementation and express expectations around how quickly corrective actions must be taken when configurations are non-compliant.

In order to ensure that these VMM controls function correctly, we must have the following detective control requirements:

- Assess and continuously monitor VMM configuration settings wherever they are stored (for example, Unix or Windows files, or Windows registry settings).

- Test configuration settings against your internal security policies, external compliance requirements, and industry best practices. Report on any variances.

- Verify that corrective actions for non-compliant configurations are properly implemented in the required timeframe.

SECURING THE VIRTUAL MACHINES

These remaining four steps address gaining control over configurations and changes at the virtual machine layer, which includes the guest OSes, the VMMs, and the applications they run.

STEP 4: INTEGRATE AND HELP ENFORCE CHANGE MANAGEMENT PROCESSES

Once VMMs are in a known and trusted state, all changes made to the VMM should be authorized, scheduled, and substantiated by change management. We will do this by:

- Helping assess the potential impact of changes on information security and operations.
- Improving procedures for change authorization, scheduling, implementation, and substantiation.
- Ensuring that change requests comply with information security requirements, corporate policy, and industry standards.

To accomplish these objectives, we must:

- **Get invited to the Change Advisory Board (CAB) meetings**. These meetings are the forums for assessing the risks of proposed changes, approving or denying change requests, reviewing the status of changes being planned, agreeing on implementation schedules, and reviewing the success of implemented changes. By being part of these meetings we ensure that we have a say in the review and approval process for VMM changes and that VMM changes are subject to the change approval process.

- **Build and electrify the fence**. We need a detective control that assesses configuration settings against internal and external standards, gives visibility to changes made in the VMM, helps determine whether the change was properly authorized and conforms to required standards, and provides relevant forensics data to support an investigation in the event of a security breach.

- **Ensure "tone from the top" and help define the consequences**. Auditors use the term "tone from the top" to express the fact that words and actions from the boardroom on down set the tone for the behavior of everyone in the enterprise. We must convince top management to set the appropriate tone from the top regarding information security as: "The only acceptable number of unauthorized changes is zero. Senior executives will not tolerate people circumventing the change management process." Your Chief Information Officer (CIO) or VP of Operations may be able to accomplish this by simply sending an e-mail message to all organizational units that expresses the zero tolerance policy, explains the potential damage unauthorized change can cause, and specifies the consequences for those who intentionally circumvent policy.

- **Substantiate that the electric fence is working**. To prove compliance with change management processes, we need to prepare for audits in advance. We'll need the following evidence: change requests and their approvals, changes detected on all relevant IT systems, reconciliations of detected changes to approved changed requests, and any corrective actions undertaken for unauthorized changes.

By taking these actions, we will have integrated information security into the necessary preventive change management processes. We also will have created detective controls to ensure that those preventive controls are working. And, we will have created evidence proactively to prove to auditors that effective change controls exist.

STEP 5: CREATE A LIBRARY OF TRUSTED VIRTUALIZED SERVER BUILDS

Virtualization makes it easier and faster than ever to deploy infrastructure on demand and without adequate controls. The results of these rapid, poorly controlled deployments include security breaches, compliance and audit findings, and other potential negative outcomes.

In this step, we create a library of known, trusted, and approved virtual images that can be used and re-used, making it easier to deploy an authorized, secure configuration rather than an unauthorized, insecure configuration. These secure builds combine mandatory and recommended configurations to reduce the likelihood of operational and information security failures that create vulnerabilities—vulnerabilities that an intruder can exploit.

To create this library of trusted builds, we must document the standards we will apply and maintain for these builds. This requires us to:

- Develop standards that specify how to secure and harden the builds we release into production or check into the definitive software library (DSL). Configuration standards for information security are published by trusted external organizations such as the Center for Internet Security (CIS), DISA, the SANS Institute, and virtualization vendors. As these external standards evolve, we will revise existing documents and/or create new ones so that they can be used across the enterprise.

- Work with the server provisioning and virtualization teams to build a library of standardized and secure virtualized server builds. We will want to integrate independent configuration standards and checklists, as well as take the standard steps of reducing security risks by:

  – Turning off unnecessary features and modules that are enabled by default

  – Disabling un-needed services (e.g., http, DNS, and SMB)

  – Disabling un-needed open network ports

- – Deleting or disabling unnecessary user accounts

- – Changing default passwords

- Ensure that necessary passwords are changed before systems move from development to production—for example, developers who know ODBC and application passwords for a new order entry system no longer need these passwords when the system enters production.

- Include standard monitoring agents in each trusted build.

Once we've defined the policies and standards that create the library of approved virtual image builds—our preventive controls—we need detective controls to ensure the preventive controls are working with the following detective controls:

- Verify virtual image configurations against known internal and external standards to ensure they are in a known, approved, and secure state.

- Monitor the approved virtual image library to ensure that all adds, removes, and changes conform to internal and external standards.

- Reconcile all adds, removes, and changes to an authorized change order. Reconciliation may be done manually or may be automated. For example, we could reconcile manually with a signed change order from a virtualization manager, or automatically by reconciling with a BMC Remedy work order.

STEP 6: INTEGRATE INTO RELEASE MANAGEMENT TESTING AND ACCEPTANCE PROCEDURES

To better safeguard the production environment, information security requires standardization and documentation, implementation controls like checklists, and continual control of production variance. Release management shares many of these key objectives. While development often focuses on specific components, release management focuses on collections of components and whether the components work together. In this step, we engage with release management to ensure that they take information security requirements into account when testing release packages.

Release management is often driven by checklists and templates, so we must ensure that security requirements are added to their lists. In order to do this, we must:

- Develop templates for release management and interface with them, QA, and project management to ensure that information security and regulatory compliance requirements are methodically collected at the start of each project.

- Establish an agreed-upon protocol for when and how release management should engage information security. This protocol should include criteria such as those defined in Step 2 with the Project Management Organization (PMO)—for example, when releases include code that involves authorization, encryption, financial transactions, and compliance requirements.

- Integrate automated security testing tools into the release testing process and run these tools against code, builds, and releases. Use vulnerability scanning and management testing tools, even if they could potentially crash applications during testing—it's better to find vulnerabilities in pre-production rather than in production. Use the same tools in the pre-production and production environments to prepare IT operations for potential problems when these tools are used in the production environment.

- Use detective controls to compare releases and virtual images being deployed against known and trusted states to mitigate the risks introduced by human error, missed steps, mis-configurations, and other sources.

In some situations, the security testing conducted by QA is sufficient for us to approve a release. In other cases, we need to conduct independent security testing. In either case, arming QA with the same tools we use reduces findings for security testing because corrections are made by QA—typically at a lower cost, with less stress, and with higher success rates for releases.

The preventive controls are the release testing protocols, including checklists and test procedures. To ensure that these preventive controls are working, we need the following detective controls:

- Verify that deployed image configurations match the approved and tested builds. In other words, make sure approved and tested builds are in a known, approved, and secure state by testing them against known internal and external standards.

- Detect all changes made to the test environments.

- Reconcile changes to an authorized change order either manually or automatically. For example, reconcile with a signed change order or with a BMC Remedy work order.

STEP 7: ENSURE VIRTUALIZATION ACTIVITIES GO THROUGH CHANGE MANAGEMENT

Information security must work with change management and the virtualization managers to ensure that activating and deactivating a virtual computing environment is defined as a change.

Consequently, these actions must be treated as any change would be—they must be authorized, scheduled, and audited by change management.

To underscore why virtualization actions should be viewed as a type of change, consider the following scenario: A business has an application critical for a revenue-generating business process. This business process is in scope for SOX-404, and the potential consequences of an unauthorized deactivation of the computing environment could include jeopardizing financial reporting, revenue, and information security objectives. Clearly, this type of change must be authorized and scheduled before being implemented.

In addition to stating this policy requirement about what change is in the context of virtualized environments, information security must work with IT management to set the "tone from the top" about a zero tolerance for unauthorized changes.

Information security, change management, and virtualization managers will likely need to answer the following questions and be in agreement on their answers:

- Under what conditions are virtual machine activations, deactivations, and restarts changes that require approval? Consider, for example, whether changes require approval if the change delivers a new IT service, enables a service that has security or regulatory requirements, or introduces outage risk to a mission-critical service.

- Who must approve standard and emergency changes for virtual machines?

The preventive controls are the policies that define how virtualization actions should interface with change management processes. In order to ensure that these controls are working, we will also need a corresponding detective control to substantiate that the policy is being followed. This detective control will monitor all virtualization activations and deactivations and ensure that they are reconciled with an authorized and scheduled change. Such monitoring lets information security ensure that virtualization activity that could introduce information security risk is adequately reviewed and mitigated. In addition, monitoring and vetting activations and deactivations helps control unauthorized virtualization sprawl—the uncontrolled and unauthorized activation of virtual servers released undocumented into the computing environment.

Business Value of Good Information Security Controls

The 2006 and 2007 ITPI *IT Controls Performance Study* was conducted to establish the link between controls and operational performance. The studies revealed that, in comparison with low-performing organizations, high-performing organizations were more effective and efficient. The studies found that the same high performers have superior information security effectiveness. The 2007 IT controls study found that when high performers had security breaches:

- The security breaches were far less likely to result in events such as financial, reputation, and customer loss. High performers were half as likely as medium performers and one-fifth as likely as low performers to experience security breaches that result in loss.

- The security breaches were far more likely to be detected using automated controls instead of finding breaches through external sources such as the newspaper headlines or a customer complaint. High performers automatically detected security breaches 15 percent more often than medium performers and twice as often as low performers.

- Security access breaches were detected far more quickly. High performers had a mean time to detect measured in minutes, compared with hours for medium performers and days for low performers.

However, the value of good information security is not just about better loss recovery capabilities. Instead, when information security controls are built into daily IT operations, the entire IT organization is more effective and efficient. These high performing IT organizations also had the following attributes:

- Production system changes fail half as often.
- Releases cause unintended failures half as often.
- Emergency change requests occur with one quarter the frequency.
- Repeat audit findings occur with one quarter the frequency.
- Unplanned work and firefighting is cut in half.
- Server-to-system-administrator ratios are two times higher.

In short, these studies confirmed that high performing IT organizations have figured out how to simultaneously advance the goals of information security and IT operations. These IT organizations take proactive and decisive steps to promote teamwork. The information security group in these organizations works

with IT operations to manage production systems efficiently and securely, integrates with development to streamline the introduction of new systems into production, and properly manages risks to systems without introducing unnecessary controls or significantly impeding development efforts.

Avoid the Dark Side of Virtualization with Configuration Control

So far we've discussed and presented the preventive and detective controls that information security can use to secure and control virtual environments. We've also discussed the characteristics of high-performing organizations. One of these characteristics is that these organizations take a pro-active approach that builds information security into IT operations; namely, by employing many of the preventive and detective controls described in the seven practical steps to secure virtualized environments.

The preventive controls described are more hands-on activities that we must undertake, such as attending CAB meetings, determining policy, establishing protocol, and helping set "tone from the top." The detective controls described in the seven steps equate to *configuration control*—the process of assessing the state of IT configurations against known standards and effectively combining that assessment with change auditing to maintain a known and trusted state throughout virtual and physical environments.

Applying these detective controls to the physical environment is a known best practice, but it is every bit as critical that we apply these controls to secure the virtual environment. Only by doing this can we avoid the dark side of virtualization and fully realize the cost-savings and flexibility virtual environments offer.

Establishing the Known and Trusted State

Mature organizations tend to have some set of policies against which they test the configuration of their data center to determine the "goodness" of the data center's state. Business needs, performance requirements, regulations, and any number of internal and external forces may drive these policies. With mandates to secure personal and confidential data coming from regulations such as PCI, HIPAA, Sarbanes-Oxley, and others, standards

developing organizations (CIS, NIST, DISA, and vendors) have defined industry standards. These standards define specific benchmarks against which configurations may be tested and constitute best practices for both securing the data center and optimizing operations.

Configuration assessment is the process in configuration control of assessing and validating the state of the data center's configurations by proactively testing against these industry standards, as well as against an organization's internal policies and best practices. Configuration assessment compares the settings and configurations of IT infrastructure elements—for example, minimum password length, directory permissions, and network security settings—against those settings and configurations defined by these policies. The result of the assessment should be a report that indicates how each element measures up, along with detailed, actionable information that points out what configuration setting(s) specifically cause an element to be out of compliance with internal or external policies. Armed with this information, the organization can either adjust individual policies to better reflect their goals and needs, or can correct the settings for any out of compliance elements. Once compliance issues have been addressed and corrected, another configuration assessment should be automatically run to verify that the data center configuration has achieved a known and trusted state.

Gaining Visibility Into and Control of Change

The moment IT puts a system or device into production is the moment potential change can occur, so just because the data center achieves a known and trusted state following the configuration assessment doesn't ensure it will maintain that state. In fact, it's almost a given that within weeks, configurations and settings for most data center elements will have departed from that state.

Security professionals widely recognize that IT configuration integrity—having the data center in a known and trusted state—is fundamental to a sound security strategy. Change auditing gives visibility and control to configuration changes of data center elements that cause them to depart from a known and trusted state. To provide that visibility and control, the configuration control solution must take a snapshot, or establish a baseline, of the data center configurations in a known and trusted state. Subsequently, when any change is made, the Configuration control software solution detects any differences

between the baseline setting state and the new, changed setting, confirming if the change was within policy and authorized. Depending on the severity and priority of the differences, the solution notifies appropriate individuals through a variety of alert types, and in some cases may even automatically roll back changes to the previously known, good state.

In addition, the configuration control solution generates reports that flag the detected differences resulting from changes in configuration files or system files. These reports provide relevant information in an appropriate format to each person along the management chain. For example, the CISO may receive a dashboard report that gives him or her an at-a-glance sense of the overall health of the data center. The further down the management chain, the more detailed the information, down to the point where details point out the specific configuration that changed, the current value, along with the expected value—details that allow technical staff to go in and immediately correct an issue caused by improper and unauthorized change.

The Value of Configuration Control

With the complex nature of today's data center that now increasingly includes virtualized environments, having a single point of control for gaining visibility into and ensuring consistency of IT system configurations is a must. A single point of control for configuration assessment and change audit ensures that in the face of dynamic environments that include application upgrades, automatically installed patches, user-made system setting changes, virtual machine managers, and virtual machines, we can still deliver high availability and performance and comply with operational and security standards. Configuration control helps organizations:

- Mitigate security risk from both internal and external sources;
- Lower costs by optimizing IT infrastructure resources;
- Reduce unplanned work for IT staff, freeing them for more strategic projects;
- Increase availability by identifying potential issues before they cause outages;
- Speed mean time to repair (MTTR) with details that let IT zero in on the exact cause of an issue; and
- Reduce time, effort and cost of regulatory compliance audit activities.

The Role of Tripwire Enterprise in The Seven Practical Steps

As I mentioned at the beginning of this section, the detective controls mentioned in the earlier seven practical steps for securing the virtual environment include configuration control. The role of configuration control is to:

- Allow organizations to enforce the organization's configuration policies, so that all configurations within the hypervisor and virtual machines comply with internal and external policies. External policies include configuration requirements as described by CIS, VMware, and DISA, and also include operational policy to ensure performance and availability of IT systems.
- Help develop a library of trusted virtualization builds and help monitor testing and production environments against these builds to ensure images match.
- Ensure that activating and deactivating a virtual machine and/or hypervisor is captured as a change and therefore is subject to the rigors of the change and configuration management processes.

Tripwire Enterprise is the recognized leader of configuration control, and in the next sections, we'll revisit each of the prescriptive steps to see how Tripwire helps us address those detective control requirements.

STEP 1: TRIPWIRE'S ROLE IN GAINING SITUATIONAL AWARENESS

Getting a complete picture of your data center elements is best accomplished through an asset management application. From there, configuration control steps in, harvesting data about these elements, including system files, configurations, and all their associated settings and metadata. This is the starting point for implementing configuration control.

If Tripwire Enterprise agents are included in standard VM templates and are configured to start automatically, they will notify the TE Console when a new standard build is deployed. Tripwire Enterprise can integrate with asset management systems, capturing any data about all elements in the data center—the servers, routers, switches, applications, hypervisors, databases, and more—and capturing the details about any settings applied to the configurations and system files associated with those

elements. These details are crucial for creating an image of the entire data center that is used by configuration assessment and change auditing solutions. Tripwire Enterprise captures data on virtual environment elements, including the virtual machine manager (VMM), sometimes called the hypervisor depending on the particular implementation. It also captures data on guest OSes and any applications and databases installed on top of them.

In order to manage your virtual environment, you first need to determine what virtual elements are out there. Tripwire helps capture that virtual information and it captures the same information about the physical elements from one point of control.

STEP 2: TRIPWIRE'S ROLE IN REDUCING AND MONITORING PRIVILEGED ACCESS

While organizations often have strictly enforced policies about who can create and modify physical elements of the data center, they often fail to take the same strict approach to managing the introduction and modification of virtual elements. These virtual elements probably warrant greater attention and enforcement of access policy because when someone makes an undesirable change to a single virtual element, that change can ripple through and impact the other virtual machines running on the same host machine. Undesirable change in virtual environments can cause problems that spread exponentially.

Tripwire Enterprise helps monitor user access to physical and virtual machines. With Tripwire, IT can manage user account adds, removes, and changes, and reconcile them with authorized change orders from virtualization managers. By monitoring the permissions, groups and access controls in the VMware ESX Server and within virtual machines, Tripwire enables organizations to gain better visibility and control over their virtual environments. In addition, if you use a tool such as Active Directory to manage your VMware administrator group, Tripwire Enterprise also monitors for changes such as adds, removes, and modifications within the Active Directory grouping to ensure visibility to and control of access and permissions change.

STEP 3: TRIPWIRE'S ROLE IN DEFINING AND ENFORCING VIRTUALIZATION CONFIGURATION STANDARDS

In this step, we use configuration assessment to proactively establish that the virtual elements of the data center—the VMM, hypervisor, host OS, guest OS, and applications—are initially configured according to industry standards. It is also impor-

tant, and sometimes more valuable, to ensure that the virtual elements comply with our own organizational policies.

First, Tripwire establishes a trusted state by performing a comprehensive configuration assessment of our virtual—and physical—elements against these defined policies and their associated benchmark tests. Once we've established the trusted state, we automatically take a snapshot of the configurations in this known, good state. We've now created a baseline against which to test the configurations in the future.

Next, Tripwire Enterprise automatically combines the result of configuration assessment with change auditing to monitor these virtual elements for change that departs from that known and trusted state. When Tripwire detects undesirable, out-of-compliance change, it alerts IT and provides reports they can drill down into for detailed information about specifically what changed, when it changed, and who made the change. Once corrective measures have been made, IT can follow up to see if these measures were taken in the required timeframe. Tripwire can even rollback or provide remediation prescriptive guidance to keep the virtual element in compliance.

Tripwire provides over 100 out-of-the-box assessments against policies issued by the Center for Internet Security (CIS) and other security standards-developing organizations such as NIST and DISA. These assessments contain thousands of tests against standards benchmarks designed to ensure the integrity and security of the data center, including its virtual elements. Tripwire even includes VMware ESX Server 3.x Benchmark Version 1.0 defined by CIS, and VMware Infrastructure 3, Security Handling defined by VMware—specific policies designed for VMware ESX Server, the most popular hypervisor on the market. These assessment tests serve as a jumpstart to organizations with incomplete or no security policies, but may also be modified by more mature organizations with greater experience defining sound security policy to meet specific business objectives and regulatory requirements.

STEP 4: TRIPWIRE'S ROLE IN INTEGRATING AND HELPING ENFORCE CHANGE MANAGEMENT PROCESSES

In this step, we assume that the VMMs are in a known and trusted state. Now configuration control enables us to determine what change was made to the VMM by continuously comparing the configuration in a previously known and trusted state against the current configuration. When change is detected that fails to comply with standards and policy, appropriate staff are notified and forensics data is collected to provide an audit trail

in the event a security breach or compliance audit occurs. This audit trail also provides IT critical information for remediating the issue and identifying the critical who, what, when, and where information of the change that circumvented policy and introduced risk.

Tripwire's configuration control solution continuously monitors the entire enterprise data center for changes that take IT systems out of a known and trusted state. When unauthorized or detrimental change occurs, including change to VMMs and other virtual elements in the data center, Tripwire immediately flags the change for further investigation and provides very specific information on what values changed within what files or configurations.

Tripwire also helps close the loop on the change management process by helping IT reconcile changes discovered through continuous monitoring with authorized change tickets. When changes are made that circumvent the change management process, Tripwire provides details about who made the change so senior executives can enforce the zero tolerance policy for unauthorized changes.

Tripwire further generates reports that serve as an audit trail for change to data center elements so that when the organization is audited, they can easily prove compliance with relevant standards.

STEP 5: TRIPWIRE'S ROLE IN CREATING A LIBRARY OF TRUSTED VIRTUALIZED SERVER BUILDS

Configuration assessment helps you create this library of trusted and approved virtual images. By testing these virtual images against security, industry, and internal policy, IT can verify that these images comply with corporate standards. When new virtual machines are deployed based on these trusted builds, the likelihood of introducing risk decreases.

Tripwire's out-of-the-box configuration assessments provide thousands of tests needed to verify that a specific build is trusted. These tests include benchmarks developed by CIS and VMware that specifically harden the builds for virtualized machines based on VMware ESX Server. Tripwire also includes a comprehensive library of tests for regulatory compliance with the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), and the Federal Information Security Management Act (FISMA). In addition, Tripwire enables organizations to modify or disable specific out-of-the-box assessments to meet their particular needs. Tripwire's Golden Policy feature even captures and preserves "golden" internal best practice IT

configuration settings as defined by the organization. By testing all configurations against these benchmarks, IT can easily create a library of trusted virtual images that may be used each time a new virtual machine is deployed. And, because Tripwire monitors all change, it can monitor the approved virtual image library to make sure that when images are added, removed, or modified, these changes are authorized.

STEP 6: TRIPWIRE'S ROLE IN INTEGRATING INTO RELEASE MANAGEMENT TESTING AND ACCEPTANCE PROCEDURES

Emulating the production environment is one of the greatest challenges faced by release management. To ensure that the production environment functions as expected after a release, release testing must be done on a configuration that exactly matches the production configuration. By testing the configuration of the testing environment against the production environment configuration, IT can detect and correct any small differences in the testing environment that invalidate testing and cause a release to fail.

Tripwire helps release management configure their testing environment so that it exactly matches the production environment they are trying to emulate. Release management can then assess their testing environment against that trusted state, eliminating the many small variables that can invalidate testing or cause their patch, system update, or other release activity to fail. When QA testers use Tripwire to verify that the testing environment matches the production environment, releases succeed and security issues are discovered before they impact production systems. In addition, Tripwire detects any releases as a change to the production environment, verifying that a release does not jeopardize the known and trusted state of the data center.

STEP 7: TRIPWIRE'S ROLE IN ENSURING VIRTUALIZATION ACTIVITIES GO THROUGH CHANGE MANAGEMENT

Change to virtual machines must follow established change management processes and workflow if organizations are to avoid virtual sprawl. The best way to ensure that they follow these processes is by viewing activation, de-activation, and configuration modifications as change that must be subject to change management processes. Configuration control ideally detects these changes in virtual environments and provides sufficient detail to reconcile changes made with authorized change requests.

Tripwire monitors the entire data center, and detects changes made to any elements, including the VMM, hypervisor, host OS, guest OS, and almost all applications or services running on virtual machines. By comparing detected change against scheduled, authorized changes, Tripwire is able to determine if a change is unauthorized, and if so, notifies appropriate IT staff. Because Tripwire defines activating and de-activating virtual machines and configuration modifications as changes, it detects these activities, reconciles them with a change ticket, and additionally determines if the change complies with security, compliance, and operational policy. When change is unauthorized, Tripwire provides information on who made the change, so senior executives can take appropriate action to discourage further circumventing of change processes and enforce the zero tolerance policy for unauthorized change. And when changes introduce risk into the environment, Tripwire alerts IT to the issue and provides detailed information so they can immediately correct the issue.

Conclusion

When organizations use the detective controls offered by Tripwire's leading configuration control solution in conjunction with the preventive controls described in the seven practical steps, they avoid the dark side of virtualization and experience the benefits of a secure data center. These benefits include increased availability, decreased time for recovery, reduced unplanned work, higher performance, decreased risk, lessened time and effort for audits, and overall lower costs to deliver IT services. And they can accomplish this all through a single point of configuration control—Tripwire Enterprise.

ABOUT GENE KIM

Gene Kim is CTO and founder of Tripwire, Inc. In 1992, he co-authored Tripwire® while at Purdue University with Dr. Gene Spafford. Since then, Tripwire solutions have been adopted by over 6,000 enterprises worldwide. Gene began studying high performing IT operations and security organizations in 1999, which led him to co-found the IT Process Institute (ITPI) in 2004. In conjunction with the ITPI, Gene co-authored "*The Visible Ops™ Handbook: Implementing ITIL in 4 Practical And Auditable Steps*" which has sold over 75,000 copies.

He was a principal investigator on the IT Controls Performance Study project, and in 2008 co-authored "*Visible Ops Security*", a handbook describing how to link IT security and operational objectives in four practical steps by integrating security controls into IT operational, software development and project management processes.

Gene currently serves on the Advanced Technology Committee for the Institute of Internal Auditors where he is part of the GAIT task force, which has created guidance on how to scope IT general controls for SOX-404. In 2007, Gene was presented the Outstanding Alumnus Award by the Department of Computer Sciences at Purdue University for achievement and leadership in the profession.

ABOUT VISIBLE OPS SECURITY

Visible Ops Security derives from years of operational experience, customer engagements, and rigorous research and benchmarking performed by the IT Process Institute. Working with top performing organizations to tease out what differentiates them from medium and low-performers, *Visible Ops Security* has found that high-performing security teams have unique cultural characteristics. Based on this research, *Visible Ops Security* identifies 4 phases for integrating information security into development and operations so that it becomes business as usual. The steps for each phase offer a prescriptive sequence of measurable actions, supported by true life examples that readers can easily identify with and use to help build momentum and support. By working together, development, security, and IT are in a better position to achieve common objectives and demonstrate business value. For more information on *Visible Ops Security* and the ITPI visit: http://www.itpi.org.

1   Gartner, Inc. "Security Considerations and Best Practices for Securing Virtual Machines" by Neil MacDonald, March 2007.

2   Gartner, Inc. "How To Securely Implement Virtualization" by Neil MacDonald, November 2007.

3   Ibid.

4   http://www.dirauxwest.org/TCTF/situational_awareness5.htm

ABOUT TRIPWIRE

Tripwire helps over 6,000 enterprises worldwide reduce security risk, attain compliance and increase operational efficiency throughout their virtual and physical environments. Using Tripwire's industry-leading configuration assessment and change auditing solutions, organizations successfully achieve and maintain IT configuration control. Tripwire is headquartered in Portland, Oregon, with offices worldwide.

tripwire™

www.tripwire.com