

RSA Security Brief

Security Compliance in a Virtual World

Best Practices to Build a Solid Foundation

Authors

Bret Hartman, Chief Technology Officer, RSA, the Security Division of EMC

Dr. Stephen Herrod, Chief Technology Officer and Sr. VP of R&D, VMware

Dave Shackelford, Chief Security Strategist, EMC Ionix

Charu Chaubal, Sr. Architect, Technical Marketing, VMware

Nirav Mehta, Sr. Manager, Product Management, RSA, the Security Division of EMC



The Security Division of EMC

RSA Security Briefs provide security leaders and other executives with essential guidance on today’s most pressing information security risks and opportunities. Each Brief is created by a select response team of security and technology experts who mobilize across companies to share specialized knowledge on a critical emerging topic. Offering both big-picture insight and practical technology advice, RSA Security Briefs are vital reading for today’s forward-thinking security practitioners.

Contents

The Intersection of Virtualization and Security Compliance	1
A Growing Compliance Landscape	1
Key Dimensions of Security Compliance in a Virtualized Environment	2
Best Practices for Security Compliance in a Virtualized Environment	2
1. Platform hardening	2
2. Configuration and change management	3
3. Administrative Access Control	4
4. Network Security and Segmentation	5
5. Audit Logging	6
The Security Bonus of Virtualization	6
Practitioner Guidance: Solutions for Security Compliance in a Virtualized Environment	7
1. Platform hardening	7
2. Configuration and change management	7
3. Administrative Access Control	8
4. Network Security and Segmentation	8
5. Audit Logging	9
Conclusion	9
Appendix: Biographies	10

The Intersection of Virtualization and Security Compliance

Virtualization enables organizations to consolidate hardware and run multiple “virtual” machines on one physical machine. Several virtual machines, each with a different operating system and multiple applications, can be run on the same physical machine, thereby optimizing hardware resources.

Virtualization is being adopted widely and swiftly by IT organizations worldwide. While virtualization at first focused on the data center, organizations are now looking at the broader opportunity to virtualize additional IT environments, such as desktops.

The drive to virtualize is due to a wide range of benefits including gaining greater leverage of existing IT resources by pooling common infrastructure, reducing data center costs by scaling back physical infrastructure and increasing availability of hardware and applications to improve business continuity. In addition, by inserting security controls at the virtualization layer organizations can achieve better security than was otherwise possible. Given the many benefits virtualization has to offer, it is not surprising that it is being adopted so aggressively. However organizations adopting virtualization technology need to understand how it will impact their compliance programs.

Regardless of the regulation, rule or standard, the process of compliance requires analyzing and managing IT risks on a continuous basis. This includes situations where new technology or software applications are introduced into an IT environment. Virtualization is no different. The introduction of virtualization requires an organization to evaluate how changes to IT will affect their risk posture and to mitigate these risks by ensuring that virtualization technologies are deployed and used securely.

Introducing virtualization into an IT environment that is subject to compliance requirements typically involves discussions between executives in IT, security, audit and legal, as well as technical and operational professionals. This paper is offered as an educational tool to help executives understand several key aspects of virtualization security in the context of compliance and for use by technical personnel in their dialogues with stakeholders.

Because virtualization represents a paradigm shift in computing, organizations need to invest time and effort in learning how to get it right. This means ensuring that the implementation aligns with internal compliance programs and enables organizations to meet government, industry and contractual obligations. As IT and security teams develop competencies in virtualization, organizations will be able to reap the rewards of an advanced IT infrastructure that is cost-effective, competitive, compliant and secure.

A Growing Compliance Landscape

Over the past several years, the compliance landscape in IT security has become quite complex. Many governments and industry associations worldwide have put in place regulations and standards that mandate the protection of various types of information. For example, in the US, there are industry-specific privacy regulations such as HIPAAⁱ in healthcare and GLBAⁱⁱ in financial services; as well as a patchwork of state regulations dictating requirements for handling personal information. Companies operating in Europe also have to abide by the European Union’s Data Protection Directive and its specific implementations by individual countries. Privacy regulations are also now emerging in other geographies such as India and China. Corporate governance regulations such as Sarbanes Oxley require controls on financial data. Federal government agencies in the US have to safeguard government information systems under FISMAⁱⁱⁱ. Globally, credit card data must be protected as per the PCI DSS^{iv}. With a continuous stream of new or updated regulations and standards on the horizon, the compliance landscape will continue to be complex.

Most large organizations are generally subject to a wide range of requirements and therefore recognize that the best approach is to implement a holistic risk-based program. A risk-based approach ensures that as new or updated requirements arise, organizations have a process in place to address them. Many are using a well-recognized standard such as ISO 27001/2, the NIST SP^v 800 series, and/or COBIT^{vi} to help guide the development of their process and the implementation of specific controls. Regulators and auditors as well as customers and business partners (through contracts) increasingly expect organizations to have a robust information risk management program in place and to use

security best practices. Although the compliance landscape is complex, with a risk-based approach guided by standards, organizations are able to implement innovative technology to meet business objectives, such as reduced costs, while also achieving compliance.

Key Dimensions of Security Compliance in a Virtualized Environment

When implementing virtualization technology, organizations must ensure that they can continue to maintain a secure environment and meet their compliance obligations. This requires analyzing and managing the risks that might affect protected information (e.g., credit card data, healthcare records). Virtualization does not change the approach to compliance. It still requires demonstrating adherence to security standards, robust processes and best practices. What changes is that organizations must learn how to apply these to secure virtualized environments. In general, all areas of virtualization security are important for compliance, but there are several common areas of concern:

- How do we prevent unauthorized access to protected information¹ in a virtualized environment?
- How can we ensure that, despite the consolidation enabled by virtualization, separation of administrative duties is maintained?
- How do we isolate systems that are processing protected information? Can we trust the logical separation between virtual machines provided by virtualization software?
- How do we monitor access to protected information in a virtualized environment?
- How do we control where the protected data is being physically processed?

Virtualization is a relatively new entrant in the IT and compliance world so it is no wonder that questions such as these arise. This document provides guidance on key best practices that not only help address these common compliance concerns but also represent a solid foundation for virtualization security.

Best Practices for Security Compliance in a Virtualized Environment

The following best practices are widely accepted in the field of information security. It is important to recognize that they apply not only in securing virtual systems, but also physical systems. However, there are some unique aspects that must be managed when virtualization is introduced.

1. Platform hardening

Summary: Harden both the hypervisor and the administrative layer according to guidelines from the virtualization vendor as well as the Center for Internet Security (CIS)^{viii} and the Defense Information Systems Agency (DISA)^{ix}.

Virtualization adds new layers to the computing infrastructure including the hypervisor layer (also known as the virtual machine manager) which allocates the hardware resources of the “host” to each of the virtual machines or “guest” operating systems. Virtualization infrastructure also includes virtual networks with virtual switches connecting the virtual machines. All of these components which, in previous systems, used to be physical devices are now implemented via software. Virtualization also introduces a new administrative layer for managing the virtualization infrastructure. To reduce the risk of unauthorized access, just as with physical systems, the hypervisor layer and the administrative layer must be properly “hardened.”^x

¹ Depending on the regulation or standard, protected information could be personally identifiable information (PII), financial data, payment card data, etc.

System hardening helps minimize security vulnerabilities by taking a series of actions such as configuring the virtualization platform with secure settings, removing unused components and applying the latest patches. Hardening checklists for virtualization platforms are available from several sources. Organizations should work with internal and external auditors in selecting the right hardening guide for their organization. The hardening guides from vendors, Center for Internet Security and the Defense Information Systems Agency are well-established and accepted as industry best practices.

2. Configuration and change management

Summary: Ensure that existing configuration and change management processes and systems are extended to encompass the virtual infrastructure. Take advantage of benefits of virtualization such as the ability to easily re-provision a secure machine profile when a machine's profile changes from an expected standard. Pay attention to the ease and speed with which changes can be made in a virtual environment and institute the proper work flows to avoid mis-configuration.

In virtualized environments, configuration and change management is governed by the same principles as in the physical environment. First, it is important to ensure that the system has been setup properly ("hardened" as discussed above). Then on an on-going basis, it must maintain a "gold standard" of configuration – it must have all the right settings and patches and meet any required security policies. As changes occur, such as new software is added or system settings are changed, a good change management process ensures that a virtual system continues to meet the "gold standard," and that any changes made are limited to authorized changes. As in the physical environment, the goal of configuration and change management is to reduce the risk of someone exploiting a vulnerability caused by an error or omission in the way the machines have been setup; and then gaining unauthorized access. In a virtualized environment, such configuration and change management must be applied to the virtualization software in addition to the virtual machines it hosts.

In virtualized environments, there is no longer a one-to-one relationship between a physical host and a server. System administrators can no longer rely on knowing that a particular physical host is running a particular server, with a particular configuration. Now, a virtual machine can run on one of many physical hosts, while a host can run a wide variety of virtual machines. This association changes dynamically making it difficult to keep up with changes. The result is that configuration and change management practices become even more critical in virtualized environments. While this may require extra diligence, it is worth the time to ensure that well-documented configuration and change management processes exist which include approvals by appropriate personnel.

To meet compliance requirements, organizations will have to prove to internal and/or external auditors that good configuration and change management procedures are in place. The underlying virtualization host must be properly configured; as well as the association between the host and guests, the network configuration and the storage infrastructure. There are configuration management tools that can help maintain conformance to the "gold standard" by generating alerts on any deviations. Organizations should take advantage of the tools that already exist in their physical environment in order to lessen the burden of managing conformance within a virtual infrastructure.

One characteristic of a virtual environment that drives extra diligence in change management is that, in a virtual world, things can be done or changes can be made extremely quickly. For example, server deployment cycles can go down from days to minutes – or even seconds. The ability to make fast changes is a great benefit. Resources can be allocated quickly when and where they are needed, but there is also a need to mitigate the risk of malicious activity and errors just as quickly. If organizations lack good change management, the speed factor can exacerbate existing weakness in any existing processes. Organizations should consider instituting proper work flow for changes in order to obtain all necessary approvals and ensure servers are properly configured before they are deployed. Good change management processes will enable organizations to reduce time and reduce risks.

A related challenge is VM mobility. Virtual machines are a lot more mobile than physical machines; servers and applications can be moved to hardware within the same data center or even to a data center located across the planet. Again, this is an enormous benefit, enabling optimization of resources. However, there is still the need to mitigate the risk that a server will be moved to an unauthorized location. For example, the EU privacy regulations expect organizations to restrict where protected data is processed because it can only be processed in certain countries which have similar

protections. To meet the EU or other similar requirements regarding the physical location of data, organizational security policies should dictate any restrictions regarding where certain VMs can be located. These policies must then have corresponding controls in place. Virtualization systems that allow VM mobility to be controlled should be used so that servers that process protected data cannot be deployed to or moved to unauthorized locations.

Another area which may require special attention is bringing offline VMs online again, which is very easy to do. But if a VM has been offline for too long, it may be out of date with respect to patches, anti-virus signatures, etc. Organizations should be aware of any test or development environments which may be turning on and off VMs. A possible scenario is a developer takes some VMs, uses them for a week or two, and turns them off; then two months later he/she goes back to that particular project and brings them on-line again without proper patches. Also watch for redundant servers that will only be used when servers go down. Processes should be developed to ensure that before any servers are brought on-line, they meet the gold standard, have all required patches and meet the expected secure configuration profile.

Finally, another crucial aspect is patch management. Guest virtual machines and the virtualization infrastructure itself must be regularly evaluated and the latest security patches applied using the standard processes that most organizations follow for patching systems within their physical infrastructure.

3. Administrative Access Control

Summary: Maintain separation of administrative duties even when server, network and security infrastructure is consolidated within the virtualization infrastructure. Define specific roles and granular privileges for each administrator in the central virtualization management software and limit direct administrative access to the hypervisor to the extent possible.

With a physical infrastructure, servers and networks are managed through separate and numerous applications. Within a virtual infrastructure, servers and networks may all be managed using software provided by the virtualization vendor. Control over the virtual servers and virtual networks should be assigned to server and networking administrators respectively, and they should update their skills to operate the virtualization software proficiently and avoid mis-configuration. The specific privileges of each administrator need to be mapped to the particular organizational structure.

Careful separation of duties and management of privileges is an important part of mitigating the risk of administrators gaining unauthorized access either maliciously or inadvertently. Depending on the sophistication of the virtualization software, it is possible to define specific roles and granular privileges and assign those to individual administrators.

A virtual switch is a software representation of a layer-2 network switch commonly implemented in hardware. It allows virtual machines on the same host to communicate with each other using the same protocols that would be used over physical switches, without the need for additional networking hardware. For assigning control of the virtual switches to network administrators, one challenge has been that the networking administrators are familiar with controlling switches through the network management application they use for their physical network. Network equipment vendors have introduced virtual network switches which are software implementations of their hardware switches. By deploying such a switch in a virtualized environment, the network administrator is now able to manage and monitor the virtual switch using the exact same interface they use for managing the other physical switches.

Another important practice is ensuring that only authorized administrators are able to access the hypervisor for administrative functions. An administrator can perform several critical functions locally if they gain administrative access to a single physical server. This access should be managed carefully because it is difficult to monitor access to many thousands of physical servers in several data centers. It is preferred that organizations disable all local administration of the hypervisor and require the use of a central management application.

4. Network Security and Segmentation

Summary: Use virtual switches and virtual firewalls to segment virtual networks. Extend and replicate your physical network controls within virtual networks. Use change management tools and work flow to limit the risk of mis-configuration. Work with internal and external auditors to determine the acceptable mix of physical and virtual network segmentation.

As with a physical infrastructure, organizations need to securely set up the virtual network. One of the important aspects for compliance is making sure machines that process protected information are isolated so that the data is not co-mingled or accessible through other machines. A virtual network is similar to a physical network except that it is embodied in software within the virtualization platform and not in hardware.

Virtualization platforms provide the capabilities to implement effective network segmentation. It is possible to logically group virtual machines and virtual switches into virtual LANs and provide further segmentation using virtual firewalls. The segmentation policy can be enforced regardless of the physical server on which the virtual machines are running. In addition, just as a physical network administrator can mis-configure network equipment, it is possible for virtual networks to be mis-configured. But if network administrators understand and follow proper configuration procedures, segmentation on a virtual network can be just as effective as on a physical system. Virtualization software and network management vendors provide a rich combination of supporting capabilities. Network security and segmentation is a matter of understanding the capabilities available and avoiding configuration errors.

Another aspect is making sure there is visibility into the traffic on the virtual network to reduce the risk of unauthorized access to this traffic. Organizations need to use virtual security devices such as virtual firewalls and virtual IDS/IPS. Security companies are starting to port their existing physical hardware-based network security appliances to run in virtual machines or as virtual appliances. For example, some commercially available firewalls can now be run as virtual appliances and can secure both physical and virtual networks.

As with physical systems, an auditor will require proof that the network has been well-designed by showing him/her the entire view of the network and the controls that are in place. Organizations should demonstrate that they can audit the system on a regular basis and can effectively manage change. For example, if a virtual switch has been set up on a sensitive network, demonstrate how virtualization software can be configured to send an alert if a new virtual machine is added to that network.

In most organizations, there will be a hybrid of networks end-to-end from the desktop all the way to the server. Given this situation, how can it be proven to auditors that the network is indeed the one that carries protected information and is isolated? Organizations will need to produce configurations and logs from both the physical and virtual firewalls and switches to show how the network segmentation has been setup and whether it is effective. For virtual networks and firewalls, the configuration information may be in a different place than the physical network. Network management software and security information and event management (SIEM) solutions that manage and monitor physical and virtual networks from a single console can help with such tasks.

One of the most discussed issues regarding network segmentation for virtualization is regarding PCI DSS requirements and whether in-scope (e.g., virtual machines that process cardholder data) and out-scope systems can be consolidated on the same physical server. The PCI DSS does not directly address this question, leaving it open to interpretation. Organizations should work with their auditors to demonstrate how they plan to securely segment their network, including their specific use of the virtual network segmentation technologies. Depending on the applications and current

How do we know that the hypervisor is secure?

There has been a lot of media attention focused on potential vulnerabilities in the hypervisor. It is important to consider this, just as one would consider the security of any third-party software that is being introduced into the environment. Ask the vendor to provide assurance regarding the security of their product. Keep in mind that hypervisor vulnerabilities need to be addressed by the virtualization vendor, and they are not actionable by your organization. It is a misperception that the biggest risks in virtualization are the hypervisor software. The biggest risks are actually operational and stem from mis-configuration and mismanagement, not the core platform. There is no “silver bullet answer” to the question of whether hypervisor technology is secure; it depends on the specific technology and how well it is deployed.

security posture, organizations and auditors can work together to determine the acceptable mix of virtual and physical network segmentation to isolate in-scope systems.

5. Audit Logging

Summary: Monitor logs from the virtual infrastructure along with the rest of the IT infrastructure. Correlate server and network logs across physical and virtual infrastructures to reveal security vulnerabilities and risk.

Audit logging is critical to managing the security of any IT environment and a specific requirement of many regulations and standards. It provides the ability to track and monitor activities within IT systems. Depending on the product, virtualization software records all system events and administrator actions for alerting and reporting.

Logs from virtualized systems can also be imported to a security information and event management (SIEM) solution so that the virtual infrastructure can be monitored and events analyzed in the central security operations console for the entire IT infrastructure.

In order to really understand what is going on in the entire IT environment, logs must be reviewed from all devices in the environment, such as VPN, IDS, and firewalls. They should not be viewed in isolation. With a SIEM solution, events in the virtualization infrastructure can be correlated to events within other parts of the IT infrastructure. For example, consider that an administrator moved a virtual machine from one server to another. This event can be correlated to other events and show that the administrator logged in over the VPN at four o'clock in the morning, incorrectly logged into four servers, and then logged into the virtual system to make this change. Through correlation of events, organizations are provided with a complete picture of what occurred.

Historic reports from virtualization software and from a SIEM solution are also effective tools in unambiguously demonstrating compliance to internal and external auditors.

The Security Bonus of Virtualization

Most organizations today are not deploying virtualization just to improve security. As discussed earlier, the main drivers are decreased capital and operating costs. Because the cost savings are so compelling, this has been the main focus for moving to virtualization. However, there are significant security benefits that virtualization brings and as the technology evolves, virtualization will enable 'better than physical' security.

Virtualization offers a unique vantage point in the IT infrastructure. In a fully virtualized environment, the virtualization layer can provide secure visibility into everything from disk I/O to packets to every instruction and memory access. Such visibility means more data to collect for auditing. Virtualization is also a unique security policy insertion point that enables security policy to be applied to all virtual machines in the infrastructure without requiring insertion of agents on guest virtual machines or 'bump in the wire' devices.

Also, consolidating hardware dramatically improves physical security because the fewer physical hosts and data centers that are required, the easier it is to secure them physically versus having them overflow into unsecured areas. Resource-constrained organizations that could previously not afford to have so many hardware servers for various security functions, such as a logging server, can now set up such servers as VMs on existing hardware.

Remote management of VMs, for example, at a retail point of sale, helps to ensure security. If something goes wrong with an application at a retail store, an administrator sitting at headquarters can actually restart that VM or even delete it and deploy a new VM within minutes – all from a central location. This speed is much harder to achieve with physical systems.

Another important benefit of virtualization is the ability of the hypervisor to place restrictions on what anything running inside the guest virtual machine can do. This can provide better security controls than what is possible in a physical server. Some examples include:

- Prevent spoofing by disallowing MAC address changes
- Avoid unauthorized code execution through hypervisor-enforced white listing of guest memory pages
- Enforce arbitrary layer-2 segmentation at the virtual switch

When deploying data loss prevention solutions as virtual appliances on the same host as the virtual machines, organizations can prevent data loss closer to the source of the data rather than at the physical network boundary. Further, virtual security appliances can be widely deployed without the hassle of managing several physical security appliances.

The speed of deploying new virtual servers can also help in disaster recovery efforts and help to ensure high availability. And if a problem does occur, virtual machines can be isolated quickly for incident response.

Practitioner Guidance: Solutions for Security Compliance in a Virtualized Environment

There are a set of core best practices to adhere to in order to achieve security compliance in a virtualized environment. In order to meet this goal, organizations need access to technology solutions that can support best practices. This section of the paper will outline potential solutions that align with each best practice. This is not intended to provide a comprehensive view of possible solutions from RSA, EMC Ionix and VMware, but rather serve as introductory guidance for technology practitioners.

1. Platform hardening

VMware provides a comprehensive hardening guide for its virtual infrastructure. Automated tools are available that may ease the administrative burden on the IT organization. For example, EMC Ionix[®] Server Configuration Manager (SCM) may help to ensure that each system has been configured in compliance with an industry standard or customized configuration profile and that changes are monitored and managed.

2. Configuration and change management

Configuration and change management is an integral part of ensuring security compliance in a virtualized environment. Examples of supporting capabilities from EMC and VMware:

- EMC Ionix Server Configuration Manager provides a view into the system to show auditors how it has been configured and how the process works to manage any changes. And, as most organizations will have hybrid environments, Ionix SCM enables configuration and change management for the complete hybrid physical and virtual environment. It includes a work flow engine for sending requests for change approvals and email alerts to the right administrators.
- VMware vCenter[®] provides granular privilege management that could be used to limit who can deploy virtual machines to specific networks and storage devices. Combined with well-defined operational processes and work flows, this capability can be used to take advantage of VM mobility while managing the risk.
- VMware's vCenter Orchestrator enables custom work flows to be built for any of the hundreds of tasks that can be performed through the vCenter management console (e.g., create VM, start VM, clone VM). In addition, patch management is clearly a key component of any security compliance process. For customers operating VMware virtualization, it is possible to wake up and patch virtual machines that are suspended to minimize the impact of patching on production environments.
- VMware vSphere[®] Host Profiles provides the capability to streamline configuration for ESX hosts and can be configured to alert administrators in case of any drift from a desired profile.
- VMware Update Manager may be used for patching ESX hosts and select Windows[®] and Linux virtual machines from a single place. Most organizations have deployed a patch management system in their physical infrastructure which can be extended to patch virtual machines as well.

3. Administrative Access Control

Failure to effectively manage privileges and ensure separation of duties may compromise a security compliance program. Such fine-grained administrative access control is enabled by VMware's vCenter management platform. Specifically, a system administrator can be restricted to manage Unix systems only or be able to deploy virtual machines in the internal network but not the DMZ. Or, an administrator may be assigned full control over the entire network or only be allowed to control part of the network, with no access to sensitive areas. In addition, the configuration of VMware virtual switches (vSwitches) can be controlled centrally from the VMware vCenter management platform, including security policies.

In addition, RSA SecurID® authentication can be used to enforce strong, multi-factor authentication of administrators before they can use the VMware ESX Service Console for hypervisor administration.

4. Network Security and Segmentation

When identifying a virtualization platform, it is critical to have the ability to effectively segment the virtual network. VMware provides virtual switches that emulate physical network switches. Further, it is possible to logically group virtual machines into virtual LANs to provide separation. VMware vShield Zones enable organizations to go further and firewall or isolate virtual machines into multiple 'zones' defined by their logical organizational and trust boundaries. This segmentation policy is then enforced regardless of the physical server on which the virtual machines are running. Granular rules can also be set up to control the type of traffic that is allowed between zones. RSA and VMware have demonstrated a proof-of-concept integration between VMware vShield Zones and RSA Data Loss Prevention (DLP) technology to demonstrate how organizations can reliably detect protected data traversing virtual networks and block it.

Applying security best practices to virtual infrastructure

Most of the security considerations in the virtual world are the same as those in the physical world. For example, all the best practices mentioned in this document are important for both physical and virtual infrastructure. The following table summarizes the additional considerations when virtualization is introduced.

Best Practices	Virtualization-specific Considerations
Platform Hardening	<ul style="list-style-type: none">Learn how to harden the virtualization software using available hardening guides from CIS, DISA and your virtualization vendor
Configuration and Change Management	<ul style="list-style-type: none">Pay special attention to the speed of changes enabled by virtualization, VM mobility, and offline VMs coming onlineEnsure that patch management practices extend to the virtualization software in addition to the virtual machines
Administrative Access Control	<ul style="list-style-type: none">As servers and networks are consolidated within the virtualization infrastructure, use fine-grained access control to ensure separation of duties between the administrator roles within the virtualization software
Network Security and Segmentation	<ul style="list-style-type: none">Use the capabilities provided by virtualization software (virtual switches, virtual firewalls) to properly segment virtual machines and virtual networks.Requires extra diligence to avoid errors, especially at first, because of the increased reliance on logical separation provided by software as opposed to plugging wires into hardware
Audit Logging	<ul style="list-style-type: none">Automated tools and SIEM systems should be adapted to integrate logs from physical and virtual infrastructure for a complete picture of the hybrid environment

Virtualization software security assessment checklist – questions to ask your vendor

- How long has the product been around and how mature is it?
- What is the security record?
- Do you have certifications from independent labs such as Common Criteria certification?
- Are there endorsements from trusted organizations that are using the product in their IT environments subject to compliance oversight?
- Do you have a secure software development lifecycle process in place for the development of virtualization software?
- How do you train your developers in secure coding practices?
- Has your code been tested using automated code analysis or manual code analysis?
- Have you done architectural analysis, risk analysis and threat modeling on your software?
- Have you built in security functions such as authentication, authorization and logging?
- Do you provide guidance regarding how to deploy it in a secure manner?
- How do you respond to security vulnerabilities that are discovered?
- Do you have a team dedicated to deal with vulnerabilities?
- Are there open lines of communication with security researchers?
- What is your track record on providing patches in a reasonable amount of time?

5. Audit Logging

Effective audit logging is dependent upon the capabilities within the virtualization platform and technologies that have been implemented in order to better manage security events across the enterprise. VMware provides native audit logging functionality and enables alerts to be set on specific events. Further, the RSA enVision® platform is being integrated with VMware vSphere and vCenter, enabling organizations to get comprehensive information on events and actions from throughout their hybrid environments. The RSA enVision platform can be configured to alert on certain anomalous or suspicious events, such as a new machine coming up in a certain part of the network or on correlated events such as changes in administrative privileges that occur just before major configuration changes.

Conclusion

Over time, IT and security teams and external auditors will increase their knowledge and competencies in virtualization. IT and security teams should work closely with each other and their internal and external auditors in the design and implementation of virtual systems and educate them about the specific risk management methods and security procedures being used. As skills are mastered, organizations will be able to virtualize systems, and auditors will assess those systems with increased confidence. The benefits of virtualization are transforming how IT enables business. Capabilities provided by virtualization software providers and the security industry in general are enabling organizations to accelerate the adoption of virtualization without compromising security objectives or compliance.

Appendix

Biographies

Bret Hartman

Chief Technology Officer, RSA, the Security Division of EMC

Bret is responsible for defining the corporate security technology strategy for EMC, as implemented by the RSA division. Mr. Hartman has over twenty-five years of experience building information security solutions for major enterprises. His expertise includes Service Oriented Architecture (SOA) and Web Services security, policy development and management, and security modeling and analysis.

Dr. Stephen Herrod

Chief Technology Officer and Sr. VP of R&D, VMware

Steve is responsible for VMware's new technologies and collaborations with customers, partners and standards groups. Stephen joined VMware in 2001 and has led the VMware ESX group through numerous successful releases. Prior to joining VMware, he was Senior Director of Software at Transmeta Corporation co-leading development of their "Code Morphing" technology.

Dave Shackelford

Chief Security Strategist, EMC Ionix

Dave is the Chief Security Strategist for EMC Ionix, where he develops security architecture and controls for data centers and also heads the Center for Policy and Compliance, a group focused on developing controls for industry and regulatory compliance initiatives. Dave is currently a SANS Certified Instructor and course ware author. Dave has managed information security for several Fortune 500 companies and has consulted with hundreds of organizations in the areas of regulatory compliance, security and network architecture and engineering.

Charu Chaubal

Senior Architect, Technical Marketing, VMware

Charu is chartered with enabling customer adoption and driving key partnerships for data center virtualization. His areas of expertise include virtualization security, compliance and infrastructure management, and he has been responsible for defining and delivering VMware's prescriptive guidance on security hardening and operations.

Nirav Mehta, CISSP, ISSAP

Senior Manager, Product Management, RSA, the Security Division of EMC

Nirav is responsible for defining infrastructure security solutions including secure virtualization and cloud computing. He has also led the development of a secure software design methodology for EMC products. Nirav has 15 years of global experience in assessing and designing infrastructure security.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

ⁱ HIPAA: Health Insurance Portability and Accountability Act

ⁱⁱ GLBA: Gramm Leach Bliley Act

ⁱⁱⁱ FISMA: Federal Information Security Management Act

^{iv} Payment Card Industry Data Security Standard

^v ISO: International Standards Organization

^{vi} NIST SP: National Institute of Standards and Technology Special Publications

^{vii} COBIT: Control Objectives for IT framework from ISACA

^{viii} CIS guidelines are available at http://www.cisecurity.org/bench_vm.html

^{ix} DISA STIG is available at http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf

^x VMware Virtual Infrastructure Hardening Guide is available at <http://www.vmware.com/vmtn/resources/726>