



The Security Division of EMC

RSA Solution Brief

The RSA Solution for Cloud Security and Compliance



The RSA Solution for Cloud Security and Compliance enables end-user organizations and service providers to orchestrate and visualize the security of their VMware virtualization infrastructure and physical infrastructure from a single console. The solution offers a solid foundation that enables security of VMware environments to be addressed systematically so organizations can confidently continue their journey to virtualization and cloud computing models.

According to a recent Forbes Insights report on setting cloud strategies, “Among current technologies coming into the mainstream, virtualization is clearly seen as the antecedent to private cloud computing.” In fact, of the 235 CIOs and IT executives surveyed for the report, nearly half (48%) have virtualized at least a quarter of their organization’s servers in order to reduce infrastructure costs and deliver applications more rapidly. However, adoption of virtualization as the foundation for cloud computing is not without its barriers. Chief among them is security, which 43% of the survey respondents identified as their top concern.¹ Taking control of security and compliance in the virtual infrastructure is a critical step to accelerating cloud strategies.

Overview of Virtualization as the Bedrock of Cloud Computing

As IT continues to face pressure to reduce complexity and costs while also delivering more value to the business, virtualization and cloud computing are increasingly seen as imperative, not optional. Virtualization accelerates an organization’s internal transition to agile and business-responsive cloud computing models by abstracting complexity and creating an elastic pool of computing, storage and networking resources.

Taking control of security and compliance in the virtual infrastructure is a critical step to accelerating cloud strategies.

Specific benefits of virtualization include:

- Increased efficiency, flexibility and reliability of IT services
- Reduced capital and operational costs
- Higher availability and better preparation for disaster recovery

Adoption of virtualization for test and development IT environments is growing rapidly, but as companies look to extend the benefits of virtualization to mission-critical applications, new security and compliance concerns emerge. Virtual computing environments are more fluid, agile and portable, creating greater flexibility and convenience. However, this increased flexibility raises anxiety about data security and the ability to ensure compliance as the traditional physical boundaries that define and protect information transform or disappear.

Compliance Challenges in the Virtual Infrastructure

For the most part, regulations do not differentiate between physical and virtual IT infrastructure, although some, such as the Payment Card Industry (PCI) Data Security Standard, are being revised to include guidelines for virtualized systems. However, whether the infrastructure is physical, virtual or hybrid, organizations and cloud service providers must harden their environment, evaluate the

¹ Forbes Insights report (sponsored by EMC), “Seeding the Cloud: Enterprises Set Their Strategies for Cloud Computing.” 2010.

performance of their control framework, resolve deficiencies and report compliance both internally and externally.

The process of managing security and proving compliance is quite similar for both physical and virtualized IT, but it is important to note that virtualization presents some unique challenges. Among them is the rapid rate of change in the virtual infrastructure, with virtual machines brought up and down or moved from one server to another on a frequent basis. Also, security and compliance teams may not be included in the planning stages of virtualization projects, and they may find themselves lacking the same visibility and control in the virtualized IT environment that they have in the physical infrastructure. As a result, virtualized servers may be less secure than physical servers. In fact, Gartner predicts that through 2012, 60 percent of virtualized servers will be less secure than the physical servers they replace, with that number dropping to 30% by 2015.²

Security and compliance issues associated with virtualization and cloud computing can be costly to the business if they are not addressed proactively. These costs include:

- Unrealized capital and operational savings when virtualization projects are delayed over security and compliance concerns
- Regulatory audit failures and fines resulting from insecure virtualized infrastructure
- Impacts to brand and shareholder confidence stemming from security breaches

As enterprises and cloud service providers continue to pursue virtualization as the foundation for private and public cloud strategies, a clear framework for managing security and compliance is needed—one that enables businesses to realize the benefits of virtualization for mission-critical applications without compromises on the security front. Such a framework must consistently address security and compliance for physical, virtualized and hybrid environments rather than create new models for virtualization security.

RSA Solution for Cloud Security and Compliance

RSA has developed a solution that enables organizations to meet their security and compliance requirements as they accelerate their journey to virtualization and the cloud. This solution comprises policy management and implementation, security and compliance measurement, issue remediation, and reporting—all within a single management system for both physical and virtual infrastructure, as shown in Figure 1.

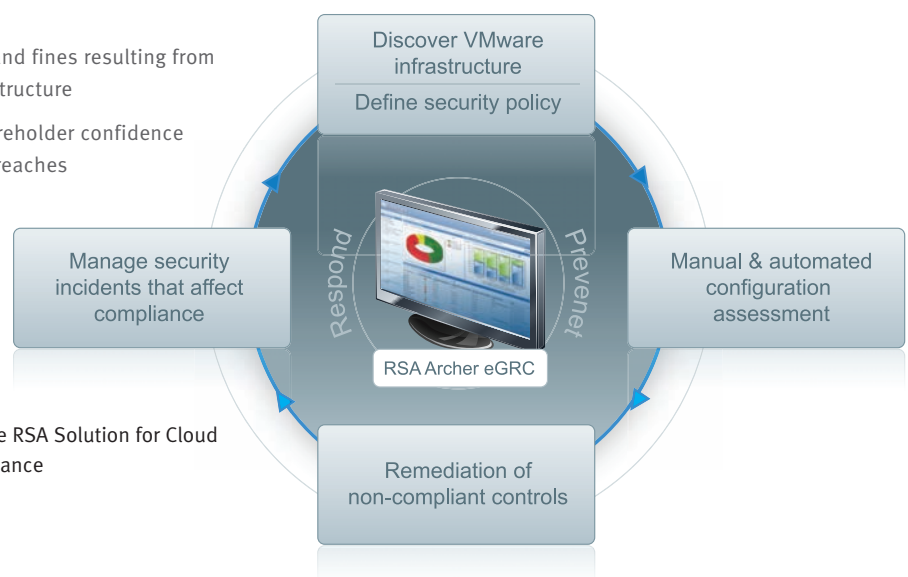


Figure 1.
Cycle enabled by the RSA Solution for Cloud Security and Compliance

² Gartner, "Addressing the Most Common Security Risks in Data Center Virtualization Projects," by Neil MacDonald. 25 January 2010.

Policy Management and Implementation

Security and compliance teams are challenged with rationalizing the complexity of compliance requirements across both physical and virtual environments – especially in today’s evolving regulatory landscape. The RSA Archer eGRC Suite for enterprise governance, risk and compliance answers this challenge with the industry’s most comprehensive library of policies, control standards, procedures and assessments mapped to current, global regulations and industry guidelines. More than 130 control procedures in the library are written specifically against the VMware vSphere 4.0 Security Hardening Guide³ and mapped to security policies and authoritative sources such as PCI, COBIT, NIST, HIPAA and NERC. In addition, the library includes thousands of other control procedures for operating systems, databases, network devices and other infrastructure assets, which are mapped to the same laws, regulations and industry standards, forming the basis of a complete technology controls approach.

The VMware control procedures provide specific instructions for configuring and hardening VMware infrastructure in the following areas:

- Access control
- Platform security
- Information security
- Operational security

Using automated workflow within the RSA Archer eGRC Platform, a project manager can distribute security policies and control procedures to appropriate administrators for both physical and virtual infrastructure. For example, VMware ESX configuration steps are sent to the VMware administrator, storage configuration steps are sent to the storage administrator, network security configuration steps are sent to the security administrator, and so forth.

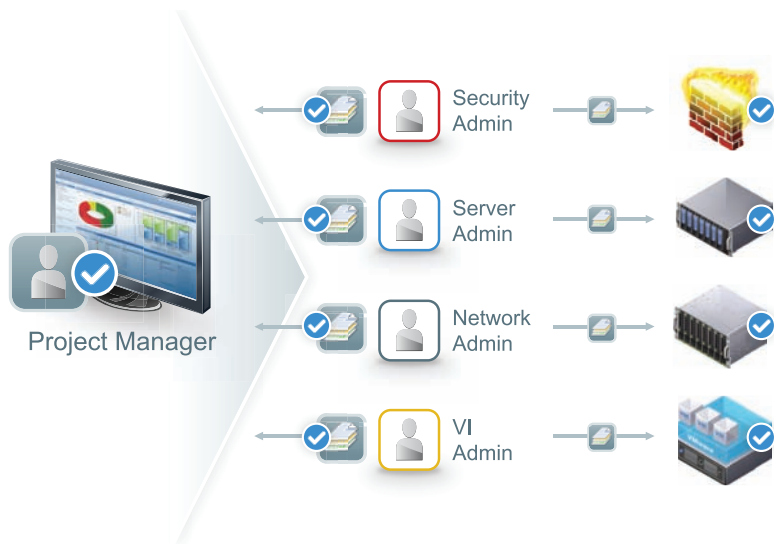
Within the RSA Archer eGRC Platform, the project manager can then track the implementation of those control procedures from a single dashboard interface, as illustrated in Figure 2.

By automating and centralizing the policy management process across physical and virtual environments and between IT and security operations teams, organizations can improve efficiency and accuracy.

Security and Compliance Measurement

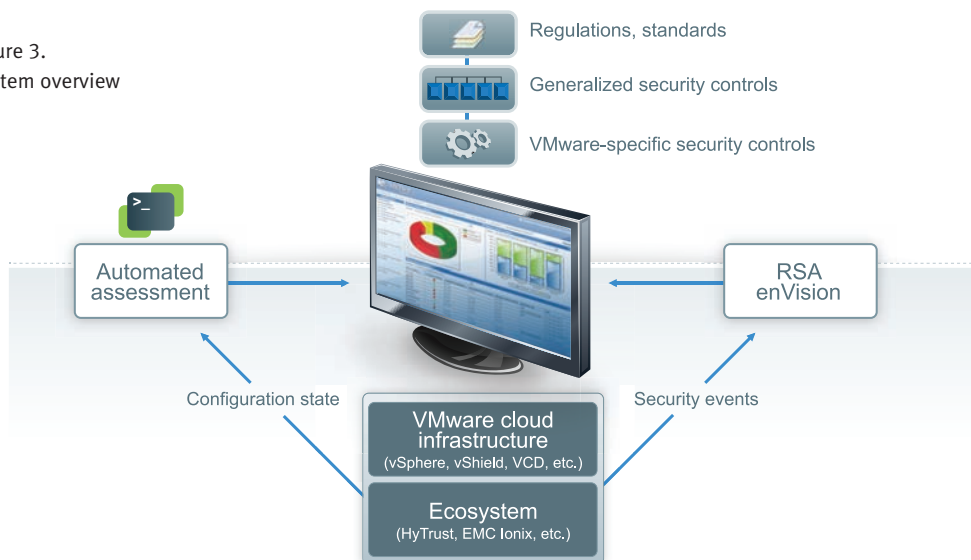
RSA’s solution includes new software that substantially automates the assessment of whether VMware security controls have been implemented correctly. The results of these automated configuration checks are fed directly into the RSA Archer eGRC Platform, which also captures the results of configuration checks for physical assets via pre-built integration with commercially available scan

Figure 2.
Distributing and Tracking
Control Procedures



³ VMware, “VMware vSphere 4.0 Security Hardening Guide.” May 2010.

Figure 3.
System overview



technologies. As a result, the Platform serves as a point of consolidation for continuous controls monitoring across the physical and virtual infrastructure.

While a significant number of the VMware control procedures are tested automatically, the remainder must be tested manually because their status cannot be directly inferred from the environment. For these control procedures, project managers can issue manual assessments from the RSA Archer eGRC Platform, using a pre-loaded bank of questions mapped to control procedures and regulatory requirements. Project managers can create new questionnaires within minutes and issue them to appropriate users based on asset ownership. Those users are automatically notified of their assessments via rules-driven workflow and “My Tasks” lists, and they can complete their assessments online.

Results for both automated and manual assessments are consolidated in the RSA Archer eGRC Platform and mapped to applicable control procedures, regulations and standards. IT and security operations teams can then monitor compliance with regulations and internal policies across the physical and virtual infrastructure by device, policy, procedure, regulation and other criteria. This information is presented through a graphical dashboard view, making the information easy to digest and understand.

Issue Remediation

Configuring the physical and virtual infrastructure according to best-practice security guidelines and regulatory requirements is critical. However, the security and compliance process does not stop there. Organizations also require the ability to monitor misconfigurations, policy violations and control failures across their infrastructure and to respond swiftly with appropriate remediation steps.

Deficiencies identified through automated and manual configuration checks are captured within the RSA Archer eGRC Platform for management. Control failures are then assigned to appropriate personnel, who can respond by completing remediation tasks or logging exception requests that identify effective compensating controls.

RSA’s solution also enables security operations teams to manage policy violations and control failures. The RSA®Archer eGRC Platform integrates with RSA enVision® log management to collect and correlate security and compliance events from a variety of sources, including the RSA Data Loss Prevention suite, VMware vShield and VMware Cloud Director. Integrations with other tools, including EMC Ionix® and HyTrust, will be added to the solution over time.

RSA enVision log management prepares reports of relevant security events within the physical and virtual infrastructure and passes these reports into RSA Archer, as shown in Figure 3.

RSA has developed a solution that enables organizations to meet their security and compliance requirements as they accelerate their journey to virtualization and the cloud.

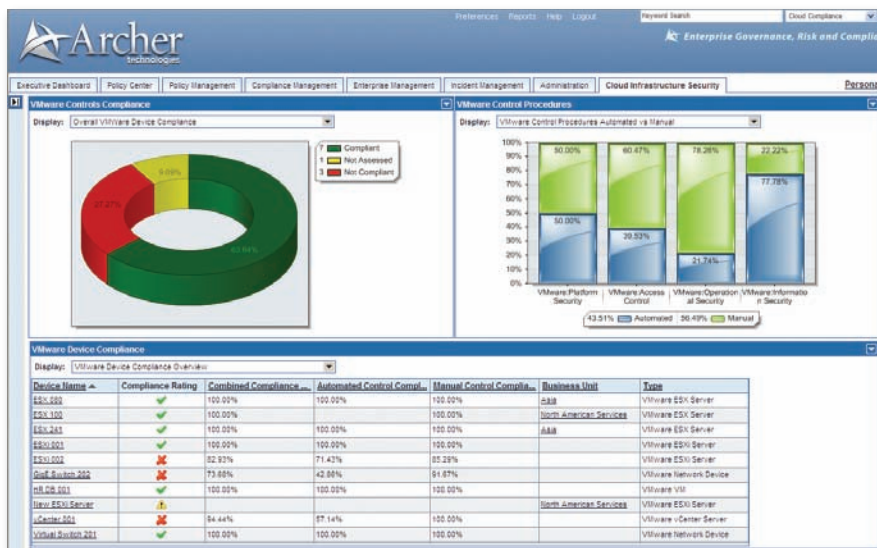


Figure 4. VMware Security Dashboard in the RSA Archer eGRC Platform

Security and Compliance Reporting

In order to extend the benefits of virtualization beyond the test and development stages to mission-critical application environments, organizations and cloud service providers need a repeatable and comprehensive methodology for deploying and operating virtualization infrastructure securely. Answering this call, RSA provides a centralized, customizable view of security intelligence, business and regulatory impact, and issue remediation across both virtual and physical infrastructure. The RSA Archer eGRC Platform offers a holistic dashboard of compliance and remediation efforts, and with a simple click of the mouse, users can expose the details of any area or activity.

RSA's solution also includes a dedicated VMware security dashboard, shown in Figure 4. This centralized, real-time view enables IT and security operations teams to monitor:

- Compliance by VMware security domain (access control, platform security, information security and operational security)
- Compliance by device (VMware ESX, vSwitch, etc.)
- Compliance by authoritative source
- Non-compliant control procedures for VMware
- Remediation status
- Accountability work queues

RSA SecurBook for Cloud Security and Compliance

The RSA SecurBook for Cloud Security and Compliance is an easy-to-follow solution guide that provides detailed instructions for deploying and administering RSA's solution in a virtualized environment. Designed to help organizations reduce implementation time and total cost of ownership, the RSA SecurBook offers guidance in the following areas:

- Solution architecture for managing VMware security and compliance
- Solution deployment and configuration guides
- Operational guidance for effectively using the solution
- Troubleshooting guidance

Conclusion

Today, RSA offers many of the capabilities that organizations require to manage security and compliance in the virtual infrastructure as they accelerate their journey to private and public cloud computing. RSA is committed to furthering the proliferation of virtualization technology and is continually enhancing its products and services in an effort to ensure the integrity of the virtual environment.

RSA helps organizations to rationalize a multitude of compliance requirements, control frameworks, standards and best practices into a set of centralized security policies that can be administered consistently across both virtual and physical infrastructure. Additionally, IT and security operations teams can work cooperatively to manage compliance to those security policies, streamlining processes and ultimately reducing administrative costs.

Security and compliance concerns are top of mind for IT executives and can hinder adoption of virtualization for mission-critical applications. However, with the right tools, processes and coordination among IT and security operations teams, organizations can take control of security and compliance across the physical and virtual infrastructure—building the foundation today for tomorrow's cloud strategies.

RSA Solution for Cloud Security and Compliance

With RSA, organizations that are deploying virtualization as the foundation for cloud computing can:

- Take advantage of best-practice security policies and control procedures aligned with VMware guidelines and regulatory requirements
- Distribute security policies and control procedures to appropriate users
- Continuously monitor, measure and enforce IT controls in both physical and virtual environments
- Collect and correlate security and compliance events across the hybrid IT infrastructure
- Employ automated workflow for issue prioritization and remediation
- Centrally report on their security and compliance posture
- Implement a sustainable, coordinated process that can keep pace with the evolving IT landscape and regulatory climate

RSA is continually enhancing its products and services in an effort to ensure the integrity of the virtual environment.



RSA is your trusted partner

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.

©2010 EMC Corporation. All Rights Reserved.
EMC, RSA, enVision, Ionix® and the RSA logo are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products and services mentioned are trademarks of their respective companies.

CLDINF SB 0810



The Security Division of EMC

www.rsa.com