



Security Assessment for Virtualized Environments

Achieving an Enterprise-class, Secure Virtual Infrastructure

At a Glance

- Improve security of virtualized environments without compromising virtualization benefits
- Identify security risks and priorities for remediation
- Understand the levels of security needed
- Establish virtualization security policies, management, and technology plans

The benefits associated with virtualization technologies are creating real value across enterprise IT and network environments – increasing flexibility, improving responsiveness to business opportunities, and offering greater operational efficiencies. And, improvements in systems management are addressing several of the challenges presented which, heretofore, limited visibility and control over virtualized infrastructure and the VMs themselves, configuration compliance, and the challenges of VM mobility.

The greater challenge today is to maximize the benefits of virtualization without compromising security and compliance. While these improvements in systems management are addressing numerous challenges in managing virtualized infrastructure, organizations must also consider the potential for security implications and risks within virtualized environments.

The EMC Security Assessment for Virtualized Environments helps customers understand the security posture of their virtualized infrastructure, and establish optimum plans which achieve policy or compliance objectives, without compromising the value of virtualization technology. By leveraging the security experts of RSA, The Security Division of EMC, and by leveraging best practices and industry standards, the security assessment focuses on the application of virtualization technology in your environment to identify security risk and remediation plans without compromising the business value of virtualization.

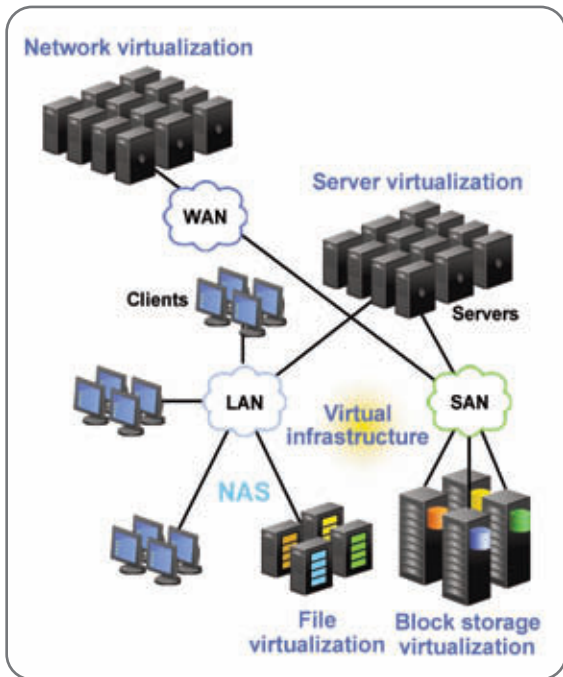
The service provides the knowledge needed to protect information – identities, data and systems – across the entire virtualization infrastructure, including VMWare, Hyper-V, XenServer systems, and corresponding management structures. This service provides an understanding of the level of protection that is appropriate for a given set of operational requirements, and recommends the best combination of policy, management and technology improvements to assure a comprehensive virtualization security strategy.

Scope and Deliverables

The Security Assessment for Virtualized Environments provides a comprehensive approach to assessing the posture of your virtualized infrastructure in the context of security. It provides a comprehensive review of VM lifecycle management policies or standards, VM operation management processes, and InfoSec policies and controls with regard to VM infrastructure hardening.



The Security Division of EMC



Virtualization poses new security challenges

RSA is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

An analysis is performed to identify current VM state and VM operational gaps, with the outcome comprising specific recommendations and roadmap, a list of prioritized next steps, and an overall presentation for discussion and socialization.

EMC Security Consultants will assess the security of server platforms, virtual host types, virtual and real network configurations, management systems, access controls and relevant operational and security controls to determine the state of an existing virtualized environment. The assessment process includes the evaluation of policy and technical characteristics of the infrastructure to determine security posture and risk. Once the assessment is completed, a high-level Gap Analysis is presented outlining the current infrastructure vulnerabilities and recommended risk mitigation efforts. The recommendations may include some, or all of the following areas:

- User and resource security
- Access controls
- Network configuration
- Platform security
- Data security
- Physical security
- Security monitoring
- Security policy management
- Operational controls (change management, asset management, etc)

An important benefit of the assessment is evaluating the effectiveness of the security mechanisms currently in place against reference criteria, including:

- Deviations from industry best-practices (ISO 27002)
- Any known vulnerabilities (e.g., as reported by the CERT or other security related sites)
- Any security baseline criteria proposed by EMC

©2009 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, and the RSA logo are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.