



The Security Division of EMC

White paper

Information-centric Security for the Virtual Data Center



How can you speed virtualization without adversely affecting security?

“Nearly every organization has concerns about ensuring security, compliance and trust in physical and virtual environments. Addressing these issues will speed up the pace of virtualization and accelerate the associated cost savings and operational efficiencies. With the right approach, organizations can extend virtualization into

environments containing sensitive data and also leverage virtual technologies to increase security beyond what is common in purely physical IT environments.”

Charles King
Principal Analyst
Pund-IT, Inc.

Growth in the volume of infrastructure, applications and data being managed has turned the enterprise data center into a major cost center. It's been estimated that seven out of every ten dollars directed at the data center are spent on energy and maintenance costs, rather than strategic IT initiatives.¹ Such an imbalance is clearly unsustainable in the current age where cost savings and efficiencies can be the difference between success and failure.

The need to reduce data center expenditures was a key driver in the push to virtualization, which has proven to be a powerful tool for enabling organizations to optimize the costs, efficiency and availability of information resources. It's because of these benefits that 95% of the Fortune 1000 have implemented virtualization to some degree, or have an initiative in place to do so.²

Many of these initial efforts have focused on deploying virtualization in non-production, tier-three and other low-risk environments. As organizations work to expand these deployments into production environments and move towards a completely virtual environment – employing a service-based infrastructure model with business-critical operations containing sensitive and regulated data – security concerns are brought to the forefront.

The Challenges of Securing the Virtual Environment

Security strategies within conventional, non-virtualized data centers typically rely heavily on physical isolation and segmentation of information and systems. In virtual environments, however, information and infrastructure are more dynamic and fluid. For example, entire virtual machines can be moved from one physical server to another. While this provides significant benefits in terms of efficiency and optimization, it can also reduce the segmentation afforded by physical separation.

Essentially, the virtual data center has eliminated conventional perimeters and boundaries. The resulting conundrum – how to balance the appeal of virtualization with the need for security – often results in two unsatisfactory options:

- Forge ahead on virtualization projects while ignoring the incremental risk created by these new technologies
- Limit the extension of virtualization technologies into environments containing sensitive information

¹ VMWare Fortune 100 Customers

² The InfoPro: Real-time Update (RTU)#1/Information Security Wave II

In the first case, organizations are potentially exposing themselves to a risk level that cancels out their cost savings. In the second case, organizations are likely to fall behind both competitively and in their own cost-control programs. Obviously, neither scenario is ideal. The solution in both cases is an information-centric, contextual, risk-based security solution that can maintain its integrity and effectiveness in the virtual world and, eventually, live in the enterprise cloud.

Extending enterprise security controls to virtualized applications – enabling persistent, pervasive and scalable deployment of security solutions across the virtual infrastructure – requires a four-pronged approach:

1. Assess and Understand Risks

In order to understand the security implications of implementing virtual technologies, organizations must systematically analyze the virtual environment to discover and classify all information assets, document existing security controls, determine vulnerabilities within the system and identify viable threats. How are the risks in the virtual environment the same or different from those in the physical environment?

2. Secure Virtual Infrastructure

The goals of securing the virtual infrastructure include ensuring the inherent security of the virtualization platform. To that end, it's important to validate that vendors are good security citizens and develop secure virtual platforms and deliver timely patches. It's also critical that organizations validate that their current controls continue to function when deployed on virtualized resources, and then expand those controls to secure the virtual infrastructure, including the management interfaces.

3. Leverage Virtual Infrastructure

Leveraging the virtual infrastructure enables organizations to take advantage of the unique characteristics of the virtual layer to both optimize security and improve productivity. In fact, the unprecedented visibility offered by the virtualization layer makes it an ideal insertion point for

security controls.

For example, security solutions such as data loss prevention can be deployed as a virtual application within a virtual server that can monitor data as it traverses boundaries between virtual machines. Unlike a non-virtualized solution that would be incapable of monitoring this data because it never travels on a physical network, deploying data loss prevention technology in a virtualized manner helps protect sensitive data as close to the virtual machine processing the data as possible.

Virtual machines are often pooled together on physical resources. While it's important that virtual applications are properly segmented, the benefit of centralization is that it allows the efficient deployment of patches and updates to thousands of virtual machines. If leveraged correctly, the virtual infrastructure allows organizations to deploy security controls in a persistent, pervasive and scalable manner that is impossible or impractical in the physical world.

4. Secure Cloud Computing

Virtualization is the key enabler of enterprise cloud computing. And a secure cloud is impossible unless the virtual environment is secure. The ultimate goal is to implement a secure service-based IT infrastructure that enables organizations to improve their security posture above and beyond what's possible in today's physical IT infrastructure. In essence, organizations will be able to embed virtualized security applications into their virtualized infrastructure, as well as deploy security controls as cloud services to enable secure and highly scalable cloud architectures.

Growth in the volume of infrastructure, applications and data being managed has turned the enterprise data center into a major cost center.

RSA and Securing Virtual Infrastructures

Marrying the flexibility and agility of virtualization with the needs of the contemporary enterprise for information security, privacy and compliance demands that more intelligence and decision-making around security be embedded in the infrastructure itself. RSA's risk-based approach helps customers ensure security and compliance without sacrificing the operational flexibility and mobility of information that is a hallmark of virtual infrastructure and cloud computing.

With this information-centric, risk-based approach, RSA helps customers apply security best practices to make virtualization safer in the short term, and apply virtualization best practices to improve their security posture in the long term.

Securing Virtual Environments: A Starting Point

RSA, The Security Division of EMC, offers industry-leading solutions in identity assurance and access control, data loss prevention, encryption and key management, compliance and security information management, and fraud protection. Many of these solutions are part of a comprehensive strategy for securing the virtual data center. In addition, RSA offers the RSA Virtual Security Assessment Service to systematically assess the security posture within an organization's virtual environment. Focus areas include policy management, infrastructure hardening, operational processes and lifecycle management. After this systematic review, formal recommendations for risk remediation are prioritized and presented.

RSA's risk-based approach helps customers ensure security and compliance without sacrificing the operational flexibility and mobility of information that is a hallmark of virtual infrastructure and cloud computing

RSA and RSA Security 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 or services mentioned are trademarks of their respective owners. ©2009 RSA Security Inc. All rights reserved.

VIRTU WP 0509



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

The Security Division of EMC