



The Security Division of EMC

RSA Solution Brief

## The RSA Solution for VMware View: Securing the Virtual Desktop Environment



According to the Open Security Foundation, 28 percent of all information security breaches ever reported have been the result of a stolen desktop or laptop<sup>1</sup>. In an effort to reduce risk, many organizations have started to migrate to a hosted virtual desktop environment. By moving data from hundreds or thousands of individual desktop devices into the data center, organizations can reduce risks to the sensitive data and intellectual property they create, collect and store.

---

## An Overview of the VMware View Virtual Desktop Infrastructure

---

The VMware View solution lets IT run virtual desktops in the data center while giving end users a single view to their applications and data in a familiar, personalized environment – on several devices and from any location. VMware View uses virtualization to break the bonds between the desktop hardware, associated operating system and applications. With VMware View, organizations can realize the benefits of:

- **Improved security.** Since all data is maintained within the corporate firewall, VMware View minimizes security risk that results from a lost or stolen device.
- **Lower costs.** Organizations are able to reduce the costs associated with the management and maintenance of individual desktops and applications, in some cases up to 50 percent<sup>2</sup>.
- **Greater management and control.** IT can manage all desktops centrally in the data center and provision desktops instantly to new users, departments or offices.
- **Business continuity and disaster recovery.** Desktop backup and recovery can be automated and quickly transferred to another server or data center in the event of a business disruption to minimize the impact on operations.

---

## Challenges to Securing a Virtual Desktop Environment

---

The VMware View hosted virtual desktop environment is a strategic and valuable investment that provides organizations with numerous benefits, including the ability to enhance security. Yet, it is still an investment that needs to be managed and secured. For example, as users gain access and work with sensitive information on a virtual desktop, that information can still be put at risk. Without appropriate access and data controls in place, organizations could still expose sensitive information to users who should not have access to it.

Managing risk associated with information in a virtual desktop environment is just as important as managing risk associated with data anywhere within the IT infrastructure. Organizations that deploy VMware View are still confronted with security challenges and need to implement the proper controls to address the following security objectives:

- **User authentication.** How do I authenticate users trying to gain access to virtual desktops?
- **Data controls.** How do I ensure that users handle sensitive information appropriately during a virtual desktop session?
- **Monitoring and reporting.** How do I identify anomalies and vulnerabilities such as inbound and outbound traffic summaries associated with sensitive assets within the hosted virtual desktop environment?
- **Security configuration and vulnerability management.** How do I maintain secure configuration of the virtual end point and detect and remediate vulnerabilities promptly across hundreds or thousands of desktops?

---

<sup>1</sup> Open Security Foundation, Data Loss DB

<sup>2</sup> IDC white paper (sponsored by VMware)  
*Quantifying the Business Benefits of VMware View*, September 2009



## RSA Solution for VMware View

RSA and EMC have developed a security solution to help organizations reap the security advantages of hosted virtual desktops while addressing the traditional challenges associated with securing user access and data in a desktop environment.

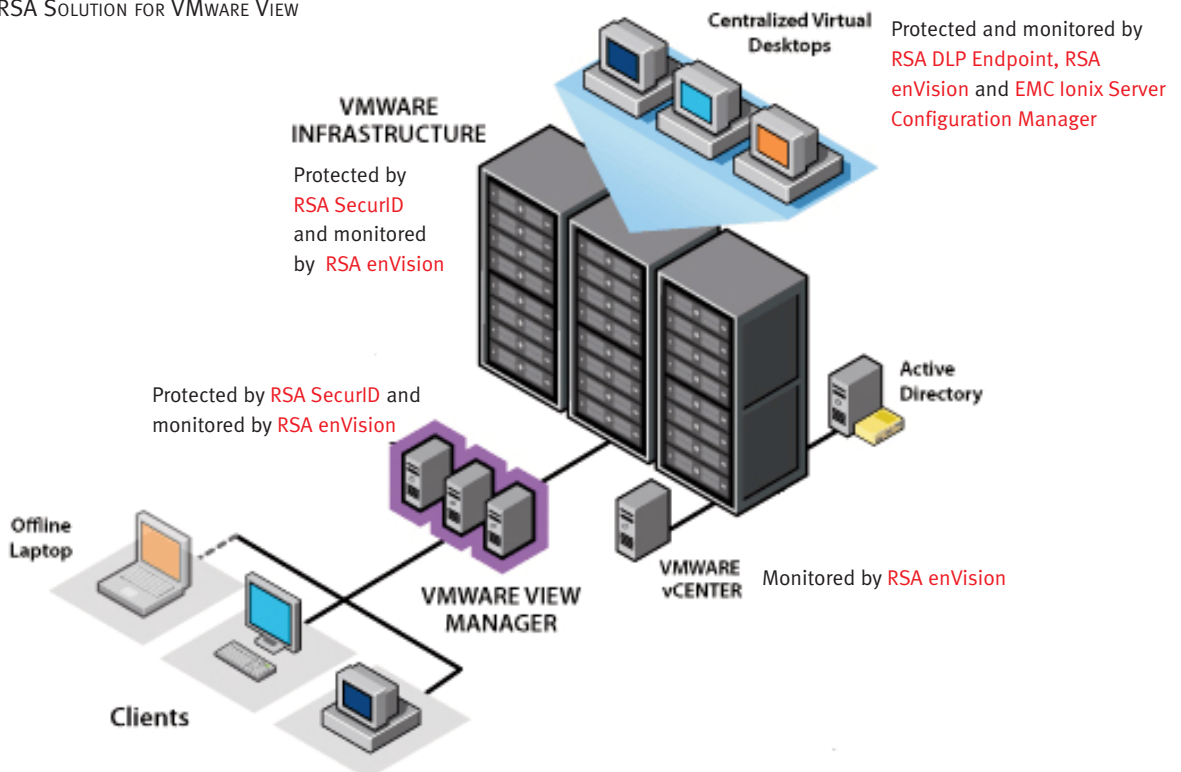
### User Authentication


Validating the identity of users before allowing them to access information and applications is critical. This is especially true in a hosted virtual desktop environment where users require access anytime, anywhere, often requested through devices over which the enterprise has little control. Positively establishing the identities of users prior to granting access to a virtual desktop, particularly to those users with administrative access and privileges, is an essential security objective.

Two-factor authentication provides an additional layer of security to ensure that only the right users can access the right virtual session and the most sensitive content within the virtual desktop environment. By requiring employees and third parties to use stronger authentication technology, organizations can reduce the risk of exposure in the virtual session by assuring only authorized users gain access to sensitive information through their desktop image.

RSA SecurID® two-factor authentication generates a new one-time password (OTP) code every 60 seconds making it difficult for anyone other than the genuine user to input the correct token code at any given time. To access their virtual desktop, users simply combine their secret personal identification number (PIN) with the token code that appears on their SecurID authenticator display at that given time. The result is a unique, one-time password that is used to positively assure a user's identity.

### RSA SOLUTION FOR VMWARE VIEW





RSA SecurID authentication currently integrates with VMware View in two ways:

- Ensuring that only trusted identities access virtual desktop sessions
- Enforcing user authentication for administrative access to the backend VMware ESX platform. With RSA SecurID authentication, it is possible to configure strong, two-factor authentication to the ESX Service Console.

RSA SecurID authenticators are available in a number of form factors including hardware, software and on-demand (SMS) authenticators to meet the needs of different user populations.

#### Data Controls

RSA® Data Loss Prevention (DLP) Endpoint monitors and controls the usage of sensitive data on end points such as laptops, desktops or mobile devices. RSA DLP Endpoint comes in two modules – Discover and Enforce. The Discover module discovers sensitive information by analyzing the content of files stored on the virtual hard disk. The Enforce module monitors what the user is doing with classified sensitive data; this includes actions such as printing, saving, copying or emailing sensitive information via their web mail. Organizations can apply policies on the usage and handling of sensitive data during a virtual session. RSA DLP Endpoint enforces and controls end user actions that violate those policies through actions such as alerting, blocking or other file control mechanisms.

RSA DLP Endpoint, with a single agent and unified policy management architecture, can be easily deployed and managed, regardless of the geographic location where the workstation resides. From a

centralized location, administrators can configure policies and enforce controls across all workstations in the virtual environment. With VMware View, the deployment of RSA DLP Endpoint agents is substantially simplified because the agent can be built into the master image and then quickly rolled out to all virtual desktops.

With RSA DLP Endpoint, completely configurable agents are deployed in a permanent mode where the agent resides on the end point for future scans. Distributed agent technology allows the Enforce module to actively monitor end points and enforce policies, even when the device is disconnected from the network.

The Enforce module also allows fine-grained controls to be inserted at the point of use (the virtual session and the physical hardware itself) to ensure that if a policy is violated, only that specific activity is blocked instead of blocking access altogether. In addition to blocking, policy actions can be created to either inform users that the action they are performing violates a corporate policy or ask users to justify the action. User justification messages are logged for further review.

Once sensitive data is discovered or a user action is blocked, RSA DLP Endpoint initiates an incident tracking workflow process to log and monitor the data at risk. It maintains an audit trail of incidents and offers a built-in notifications and alerts workflow, using the Microsoft® Active Directory hierarchy, to inform data owners as individuals or groups about potential violations. It also offers a self-remediation option that allows incidents to be directly handled by the user.

Careful separation of duties and management of privileges is an important part of mitigating the risk of administrators gaining authorized access either maliciously or inadvertently.



## Monitoring and Reporting

The rapid adoption of virtualized infrastructure has led to an urgent need for organizations to monitor new sets of activities; for example, user access to the virtual desktops from a variety of devices, administrative operations such as central creation, modification and deletion of desktop images, and access to sensitive data via a virtual desktop. In addition, organizations need to measure systems for compliance, operational needs and overall security as virtualization becomes a bigger part of the IT infrastructure.

The RSA enVision® platform is a security information and event management solution that offers a scalable, distributed architecture to collect, store, manage, and correlate event logs generated from VMware View Manager, the backend VMware infrastructure and the RSA SecurID and RSA DLP Endpoint solutions. RSA enVision reports on major operational and administrative events related to VMware View and inbound and outbound traffic summaries associated with sensitive assets and offers an effective tool for prioritizing security incidents occurring within the VMware hosted virtual desktop environment.

The RSA enVision platform enables organizations to perform analysis of event logs in a uniform and centralized fashion across all the physical and virtual systems that comprise the IT infrastructure. By using RSA enVision technology within the virtual environment, organizations can:

- Monitor information security policies across virtual machine operations, cluster and resource management, virtual network infrastructure, storage, users, groups and permissions to assure corporate compliance; user activities on virtual desktop (e.g., user authentication attempts to access virtual sessions), as well as administrator activities within the virtual desktop environment (e.g., creation of entitlements for virtual desktops, change of profile setting)
- Collect, protect and store data in a secure, non-filtered and non-normalized fashion
- Establish baseline levels of activity for the entire virtual environment to define “normal activity” and detect “abnormal” or unusual activity

RSA enVision technology helps organizations to perform analysis of event logs in a uniform and centralized fashion across all the physical and virtual systems that comprise the IT infrastructure.

- Send alerts when deviations from baseline levels or patterns of malicious activity across multiple, disparate devices are detected
- Perform forensic analysis to correct policies and settings on systems and provide a debug-level view of all changes and the effect they have on the environment
- Establish a closed-loop, incident management workflow to ensure that incidents are recorded, escalated and remediated in a timely manner
- Gain insight into the traffic and events occurring within the virtual environment from any perspective
  - including by geography, by users, by system, by line of business, by division, etc.
- Streamline the auditing and reporting process with over 1,400 “out-of-the-box” reports that can be easily customized to meet internal and external compliance requirements

Furthermore, the RSA enVision platform can be leveraged beyond the boundaries of the virtual desktop environment to monitor system both locally and remotely and measure the associated systems for compliance, security and operational needs.



## Security Configuration and Vulnerability Management

Unplanned change is the leading cause of many IT security and compliance incidents. While centralizing end points as virtual machines in the data center simplifies the process of hardening, anti-virus updates and patching, ensuring that these processes are properly functioning and that configurations are not a source of security risk is critical. For many organizations, endpoint change management is a major challenge and having a tool that can automate the process of identifying configuration changes that violate policy can help reduce security risk.

EMC Ionix Server Configuration Manager (SCM) inspects, analyzes and allows remediation of detailed configuration items from servers and workstations, across physical and virtual environments. EMC Ionix SCM monitors virtual desktops, generates automatic alerts when systems need to be fine-tuned to resolve problems or ensure compliance, and can automate common tasks to increase operational efficiency, decrease costs, and ensure secure, compliant and up-to-date configurations.

EMC Ionix Server Configuration Manager also offers powerful visibility into the IT infrastructure. High-level dashboards provide the right level of information needed to make change, configuration and patch management processes more effective – for example, verifying the deployment of patches and detecting and fixing security threats that arise from incorrect configurations. In addition, organizations can view details about the changes happening within the virtual environment and track the impact those changes have on service levels and compliance.

The EMC Ionix Center for Policy and Compliance provides detailed security and compliance analysis content based on industry recommended best practices and regulatory mandates. The Center's content works alongside Ionix SCM to ensure that all systems, both physical and virtual, meet corporate security standards.

# Unplanned change is the leading cause of many IT security and compliance incidents.

### RSA Solution for Securing the VMware View Environment

The RSA Solution for VMware View offers organizations the ability to:

- Discover and analyze sensitive data on the end points such as desktops and laptops
- Attain high levels of accuracy and speed in identifying sensitive data
- Manage how sensitive data is used at the end point by monitoring and controlling actions such as printing, saving, copying, or emailing sensitive information via a user's webmail
- Provide end users with secure anytime, anywhere access to sensitive data
- Simplify and automate the process of collecting, fixing and managing configuration changes to ensure compliance
- Apply a unified, consistent security policy that can be extended to other virtual and physical infrastructure resources
- Understand the security posture of their virtualized infrastructure and establish plans to achieve policy or compliance objectives



## Risk Management in a Virtualized Environment

VMware View addresses many of the risk management concerns of the organization while introducing other sources of risk inherent with the technology. RSA, in conjunction with EMC Consulting, is uniquely equipped to look for and identify risk to the organization across the entire virtualized infrastructure - from desktops and networks to servers and storage.

The EMC Security Assessment for Virtualized Environments service helps organizations understand the security posture of their virtualized infrastructure and establish plans to achieve policy or compliance objectives, without compromising the value of virtualization technology. Combining RSA's security expertise with industry best practices and standards, the security assessment focuses on the application of virtualization technology in the IT environment to identify security risk and remediation plans without compromising the business value of virtualization.

The service also provides organizations with insight into 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.

---

## RSA SecurBook™ for VMware View

Today, RSA has many of the capabilities that organizations need to reduce risk and leverage the unique dynamics of virtualization to increase security. 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 can help organizations that have deployed VMware View to understand and manage their information risks. By leveraging RSA security controls within virtual sessions, end points (e.g. desktops, laptops) and other data repositories, organizations will be better prepared to manage both emerging security threats and new compliance mandates.


RSA SecurBook for VMware View is an easy to follow solution guide that gets to the root of security issues within the hosted virtual desktop environment and offers tips on how to establish flexible controls that will enable dynamic and persistent hosted virtual desktop security as deployment grows. Further, the RSA SecurBook guide is designed to help organizations reduce implementation time and total cost of ownership. The SecurBook offers guidance in the following areas:

- Solution architecture for securing VMware View
- Solution deployment and configuration guides
- Operational guidance for effectively using the solution
- Troubleshooting guidance

---

## Conclusion

Security should never be a hindrance, but rather help organizations accelerate their business initiatives. By deploying the right access and data controls, organizations can unlock the value of their investment in VMware View, leverage the full capabilities of operating a virtual environment and effectively manage their compliance requirements.



## 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](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

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

HVD SB 1009



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC