

VMware Virtual Desktop Infrastructure

Securely Deliver Virtual Desktops from the Data Center



Partner Brief

Business Challenge

Managing PCs has always been a time-consuming and challenging task. Whether IT is dealing with more remote users, rolling out patches and upgrades, protecting and backing up data or ensuring users do not install unlicensed and personal software - it is easy to understand how managing desktops can sap IT resources.

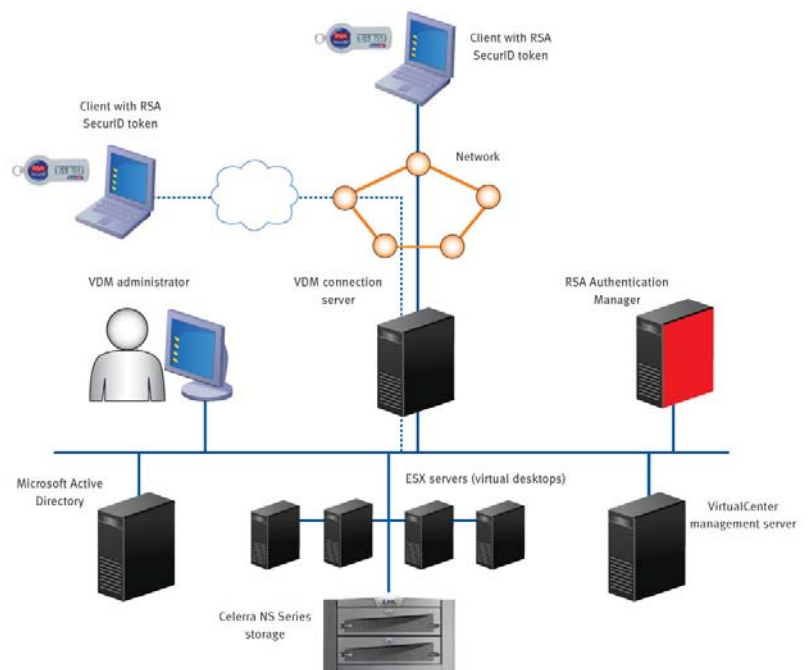
To reduce these management costs, many organizations are adopting virtualization technology for their desktops using a virtual desktop interface (VDI). Organizations use VMware VDI to replace traditional PCs with virtual desktops that run on servers in the data center. Administrators can provision new desktops in seconds, giving users their own personalized desktop environments while eliminating the need to manage many individual systems. This approach centralizes desktop management in one location, simplifies administration and enables a common user experience.

A user's desktop image is a critical set of data. If the desktop is accessed by the wrong person this could have significant damage to the individual and company. Integrating the VMware VDI solution with two-factor authentication from RSA ensures that the user is who they claim to be, reducing risk of improper access and distribution of sensitive information.

Solution Description

VMware Virtual Desktop Infrastructure (VDI) is an end-to-end solution for server-based virtual desktop computing that improves control and manageability while providing end users with a familiar desktop experience. Users access the virtual desktops and applications from a desktop PC client or thin client using a remote display protocol. They get the same features as if the applications were loaded on their local systems, with the difference being that the applications are centrally managed. IT benefits include a significant reduction in desktop administrative and management tasks; applications can quickly be added, deleted, upgraded, and patched; security is centralized; and data is easier to safeguard and back up.

Controlling access to confidential data is easier because all virtual desktops reside in a central location. VMware's VDI management platform (VDM) offers native support for RSA SecurID two-factor authentication. This integration allows customers to require that an employee use two-factor authentication to request their desktop image, ensuring that the user is the appropriate person to access the image. Additionally, strong network encryption protects data in transit. These features





help reduce the risk of data leakage and malicious code intrusion while also helping to ease regulatory compliance burdens.

Key Features & Solution Benefits

- Control and manageability in a single product: Administrators can more easily provision, manage and maintain desktops because the servers and storage are centrally located in the data center.
- Familiar end-user experience: End users get flexible access to a personalized virtual desktop that behaves just like their normal PC.
- VMware Infrastructure 3 integration: VMware VDI lets you extend enterprise class infrastructure capabilities to the desktop to leverage backup, failover and disaster recovery capabilities.
- Lower TCO: VMware VDI can help you lower the cost of operating corporate desktops by streamlining administration, reducing energy costs and extending the useful life of PCs.
- Support for strong authentication: Strengthen access control to individuals Virtual Desktops through two-factor authentication using RSA SecurID®.
- Strong network security: Protect sensitive corporate information using SSL tunneling to ensure that all connections are completely encrypted.

About VMware

VMware is the global leader in virtualization solutions from the desktop to the datacenter. Customers of all sizes rely on VMware to reduce capital and operating expenses, ensure business continuity, strengthen security and go green. With 2007 revenues of \$1.3 billion, more than 120,000 customers and nearly 18,000 partners, VMware is one of the fastest growing public software companies. Headquartered in Palo Alto, California, VMware is majority-owned by EMC Corporation and on the web at www.vmware.com.

About RSA

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle - no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, 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.



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

The Security Division of EMC

RSA, SecurID, RSA Secured are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a trademark of EMC Corporation All other trademarks mentioned herein are the property of their respective owners. ©2008 RSA Security Inc. All rights reserved.