

# Protecting Sensitive Data with the Integrated Microsoft AD RMS and RSA Data Loss Prevention Solution

## Business Need

The business challenges that customers are facing related to the security of their data are becoming more pronounced. With information residing in more places and users working in a more mobile fashion, companies are facing growing risks of data leaks. Data breaches are becoming more common – since 2005, 245 million records of U.S. residents have been exposed due to security breaches.\* Additionally, the cost of a data breach is growing – according to the Ponemon Institute, in the U.K., the cost of a lost customer record in 2008 increased 28% from the prior year to £60 per record. Companies must also continue to comply with a wide range of corporate and industry regulations to protect sensitive data such as Personally Identifiable Information (PII), Payment Card Industry (PCI) and Intellectual Property (IP), even as the cost of remaining compliant grows.

With that context, business information must still be accessible to authorized users when they need it, wherever they are. The need for information to be used across company boundaries is also growing. Increasingly, information needs to be shared with trusted business partners, suppliers, vendors and customers. Information protection solutions must therefore strike the right balance between security and providing appropriate access to the right people.

Microsoft and RSA have brought together industry leading solutions in enterprise rights management (ERM) and data loss prevention (DLP) to help organizations more effectively protect their sensitive and confidential information wherever it resides based on content and identity awareness.

## Microsoft Active Directory Rights Management Services

Microsoft Active Directory® Rights Management Services (AD RMS) in Windows® Server 2008 helps safeguard digital information from unauthorized use – both online and offline, inside and outside of the firewall. AD RMS augments an organization's security strategy by protecting information through encryption and persistent usage policies that define how the recipient may use the information, e.g., open, modify, print, forward or take other action. These policies remain with the information – whether documents, spreadsheets, presentations or e-mail messages – no matter where it goes or how it is stored. With AD RMS, organizations can help eliminate unauthorized viewing and distribution of sensitive corporate data.

Centralized AD RMS usage policy templates such as “Company Confidential – Read Only” can be defined and applied directly to sensitive information such as financial reports, product specifications and employee or customer data to control access and usage restrictions.

### Persistent information protection with AD RMS



## RSA Data Loss Prevention Suite

The RSA Data Loss Prevention Suite is an integrated suite of products that provides a proactive approach to managing the business risk associated with enterprise data loss. The DLP Suite is made up of three products – Datacenter, Network and Endpoint – which discover and protect sensitive data throughout the infrastructure based on a centrally managed set of policies.

Customers typically start by creating and developing information-centric security policies and use RSA DLP to identify sensitive data at the source through precise discovery and classification techniques. Once the sensitive data is identified, RSA DLP helps establish control by mapping the appropriate enforcement mechanisms to the data. Sophisticated workflow, notification, audit and reporting mechanisms work together to uncover and define broken business processes – often at the root cause of breaches.

\*Source: Privacy Rights Clearinghouse



## RSA DLP and AD RMS Integrated Solution Overview

RSA and Microsoft have integrated DLP with AD RMS to automate the application of RMS protection and policies to sensitive data at rest. With this solution, customers can discover sensitive legacy documents at rest and automatically apply RMS protection using a centrally managed set of policies. This reduces risk of leakage and helps meet compliance requirements by protecting the most important data based on content and identity awareness.

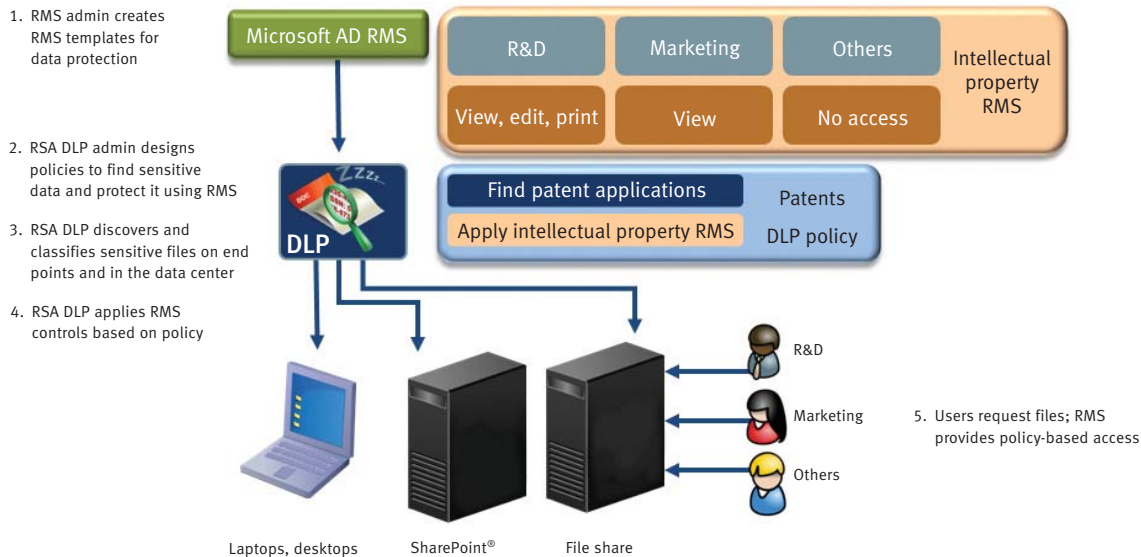
With the integrated solution provided by Microsoft and RSA, customers can:

- Find and protect their most important information today with best in class DLP and ERM solutions
- Leverage data security processes and workflows already in place
- Reduce the cost and complexity of securing information across the enterprise

### Product requirements

- RSA DLP 6.5 – DLP Datacenter and/or DLP Endpoint Discover
- AD RMS in Microsoft Windows Server 2008

### Use case example of Integrated RMS and DLP Solution



### Microsoft and RSA Partnership Futures

The companies are working together to establish a built-in “systems” approach that helps protect information throughout the infrastructure based on content, context and identity. The partnership will take advantage of resources and technology from Microsoft and RSA. Microsoft will build the RSA DLP content classification technology into the Microsoft platform and future information protection products. The resulting collaboration is designed to enable organizations to centrally define information security policy, automatically identify and classify sensitive data virtually anywhere in the infrastructure, and use a range of controls to protect data at the endpoints, network and data center. RMS and the DLP Suite are future ready, and investments made today in these solutions will carry forward to future offerings.

### Additional Resources

<http://www.microsoft.com/rms>

<http://www.rsa.com>

