FORTRA

Integrating Information Labeling and Microsoft Active Directory Rights Management Services (AD RMS)

Overview

Today's workplace is ever-diversifying, and information is being accessed from both inside and outside the enterprise from a wide variety of locations and on a wide variety of devices- corporate laptops, corporate home office desktops, home computer, mobile devices, from the coffee shop or the airport departure lounge, etc. Along with this proliferation of devices and access means that organizations are under more pressure than ever to meet the seemingly contradictory goals of providing simple access to necessary information and protecting confidential information, intellectual property and customer or employee privacy information. In addition, regulatory compliance in many cases is the "800 pound gorilla in the room"- always present and impossible to ignore. Information such as documents, briefs, budgets, letters, memos, and email are managed by internal security and privacy policies, but the means of enforcing these policies and monitoring compliance is not always prevalent.

In the majority of cases, enforcement of these policies is best addressed with the appropriate protection for the sensitivity of the data- internal budget forecasts or R&D material should be consistently highly protected, while casual email communication may have little or no protection (and should be clearly identified as such). While some technologies offer automatic "classification" or "categorization" of content based on context or key words, most organizations expect and may require that the producers of the content be aware of the sensitivity and classification of that content, and that they designate a label for the material as such.

This white paper will examine the challenges of content protection and user acceptance of this technology. It provides an overview of Microsoft's Active Directory Rights Management Services (AD RMS) and its integration with Titus' Document Classification and Message Classification product suites. This combination provides a powerful and intuitive solution for policy compliance and information protection.

General Information Protection Overview

Information protection has traditionally focused on controlling access to information, with little or no control on what is done with the content once it has been accessed. `cannot be done with information, but the means to enforce these policies is limited in many cases.

AD RMS Overview

The traditional technology components of policy enforcement have focused around controlling access to the content- for example, controlling who can access file shares, protecting assets behind a firewall, etc. The limitations of these approaches is that there is no control over the content once it has been accessed, and the protection is dependent on the location of the content- that is, if the user copies the document to a thumb drive or emails it as an attachment, the protection no longer applies. In addition, these approaches provide no means of controlling when the content can be accessed (a "best before" date) - for example, pricing lists that are only valid until 30 September, or a recall roster with out-dated contact information.

Problems AD RMS Solves

AD RMS is a file-based, persistent content protection solution that provides the means for publishers of confidential email messages and documents to control who can view their content, and what they can do with that content. File-based is defined as protection that remains with the file- whether it resides on a file server, is copied to a thumb drive, or is sent via email. What AD RMS' persistent content protection also provides is that the rights the recipient has over the content have been explicitly defined and are in-effect when the document or message is opened. For example, someone may be granted the right to read a document, but not modify, (i.e. cut, copy, paste) or print it, and only be allowed to access the document for a defined time-period (i.e. 30 days).

The capabilities of AD RMS provide persistent protection against inadvertent disclosure of intellectual property or personal information, and can be an integral component of an organization's overall information protection strategy. On its own, AD RMS does not protect against "rudimentary" attacks, such as taking a photograph of a computer screen or "shoulder surfing". It also does not guard against poor security practices such as shared/weak passwords, unlocked desktops or poor user provisioning- - user accounts with too many privileges.

In addition, AD RMS on its own does not provide any means of driving adoption; users must make a conscious decision to apply protection (i.e. encryption), and decide which AD RMS rights to grant (and to whom). End-user training is also a significant issue, to educate users why, when and how to apply AD RMS, and whether the recipient can consume the protected information internally or externally.

Titus Message and Document Classification Overview

It all starts with classification. Information that has been labeled can then be managed and protected. Labeling information helps enterprises protect sensitive information, allows records managers to determine what information should be retained/disposed, and makes it easier to find and retrieve information.

Titus Message Classification (TMC) and Document Classification (TDC) are easy-to-use labeling solutions that forces every Microsoft Outlook® email and Microsoft Office® (Word, Excel, and PowerPoint) document to be tagged before it can be sent, saved or printed. TMC and TDC's powerful policy enforcement options allow administrators to define security policy based on these labels, for example, forcing users to apply a business value to an email or document with a label, which then automatically triggers the application of encryption.
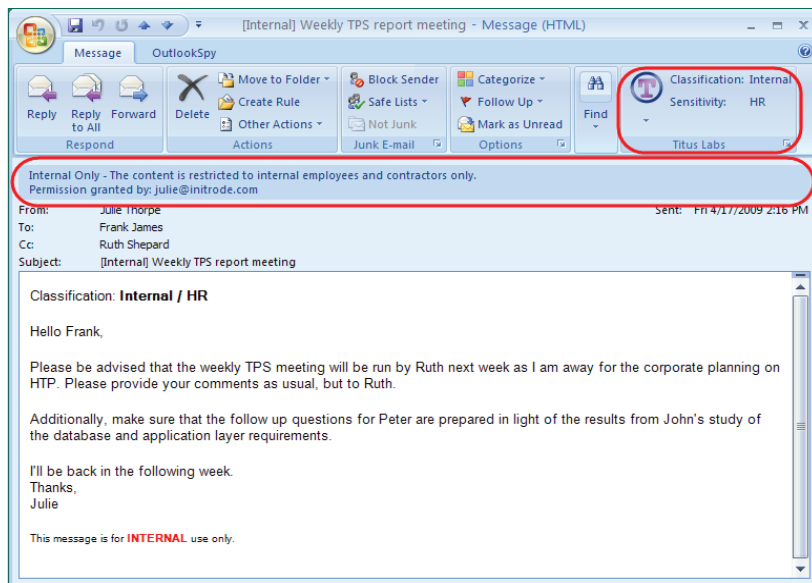
The TMC Label "Internal" automatically invokes the AD RMS template "Internal Only" restricting the distribution of the email.

AD RMS and Data Classification with Titus

The combination of Titus and Microsoft AD RMS provides a more comprehensive information protection solution by combining data classification and AD RMS protection. Every user is prompted to label the document or email based on the user's knowledge of its content, and if appropriate, the corresponding AD RMS is automatically applied, based on the label, as configured by an administrator. Titus also adds visual markings and metadata indicating the sensitivity of the document or email. These labels include metadata that can trigger existing technological investments in your organization, such as archiving solutions, data loss prevention, endpoint protection software, records management systems and email gateways.

Using Titus as the interface to AD RMS abstracts the encryption decision from the end user; they don't have to figure out what protection to apply or how. They simply label the content and AD RMS protection is automatic, transparent and consistent for every email and document. Labels are defined and applied based on the organization's information security and compliance policies, and AD RMS helps ensure those policies are enforced. The user doesn't have to answer the "what protection should I apply to this content?" question- they just designate the label or sensitivity of the document or email. For example, "Public" data should not be encrypted, while "Company Sensitive" data should only be accessible by full-time employees, but not by contractors.

Controlling the AD RMS Rollout

In addition, Titus can provide the means of controlling your AD RMS deployment by only allowing AD RMS-protected emails to be sent to other AD RMS-enabled users. Ordinarily, AD RMS can go "viral" in the early stages of deployment; members of the pilot group send AD RMS-protected messages to other users outside the group, who start using the technology to send to others and so on. Controlling the rollout of AD RMS ensures that your IT administration and

support structure is able to adjust to the new technology and ensure that it is implemented in a predictable progression, rather than all users becoming active, even distracted, at once.

Zero End-User Training

When using Titus as the interface for AD RMS, end user training becomes a non-issue as well. An example of this is a deployment of AD RMS and Titus Message Classification to the staff officers of an infantry battalion for a technical demonstration; training for all end users consisted of approximately 5 minutes. Users simply labeled messages before they sent them, which in a secure environment they are expected to do anyway, and AD RMS protection was applied automatically.

Conclusion

Microsoft AD RMS provides a simple, powerful and flexible information protection solution for your organization that can guard against inadvertent disclosure and form a key part of your information security policy enforcement strategy. However, information rights management on its own is not always enough. You also need to ensure that the technology is being adopted by users, and ensure that it can be leveraged with minimal end user training. The combined solution of AD RMS and Titus Message and Document Classification guarantees the use of encryption on certain classes of documents and email and ultimately guarantees greater content protection.

And aside from encrypting your documents and email, visual markings and metadata indicating the content's label is necessary to ensure adherence to policy and regulatory compliance. Titus Message Classification and Document Classification solutions provide the means to automatically and explicitly label content, add visual markings and (non-visual) metadata, and apply AD RMS policies when appropriate in a manner that is easy and intuitive to your end users.

FORTRA

Fortra.com