RSA CONFERENCE
CHINA 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

权限管理服务和信息保护生态系统

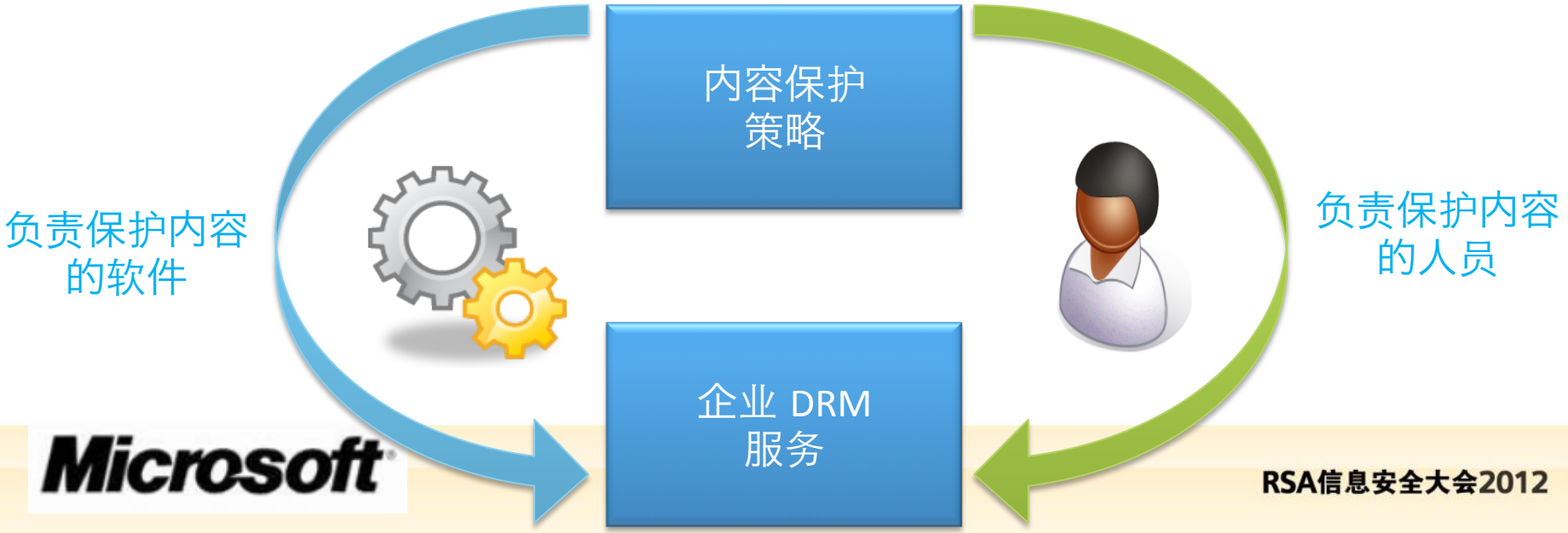
Gagan Gulati
Microsoft 公司

RSA CONFERENCE CHINA 2012

前言：定义和方法

- **保护**：加密 + 策略 + 策略实施
  - **加密**：为传输中的数据或静态数据提供用前保护
  - **策略**：用于确定谁（身份）可对受保护的项执行哪些操作（条件）的定义
  - **策略实施**：用于强制执行常见标准行为的特定应用代码

- **企业权限管理 (ERM)**：
  依赖于“用户”或“SPO 库”对文档应用保护
- **可识别内容的数据泄漏保护 (DLP)**：
  依赖于“代理”对内容应用保护（加密 + 策略）



不断变化的格局

行业趋势促使客户和 Microsoft 做出调整

RSA CONFERENCE CHINA 2012

IT 外部化

应用程序虽部署在本地却处于云中

IT 消费化

用户需要从任何设备进行访问

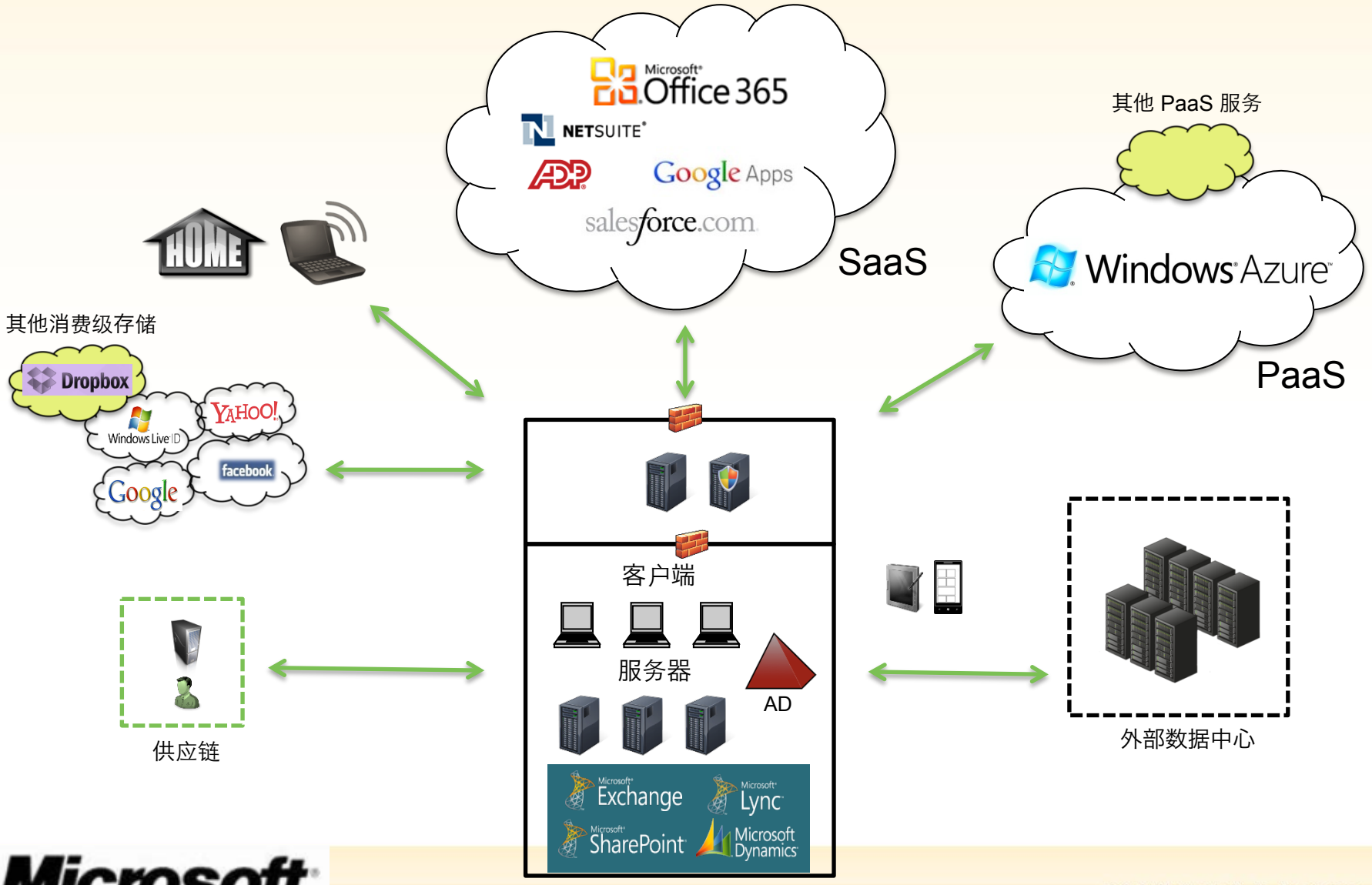
信息激增

分散的企业数据需要保护

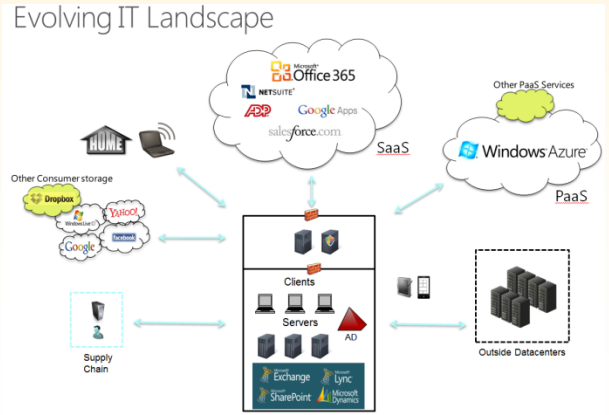
传统的边界正遭受飞速侵蚀
迫切需要一种没有典型“边界”的保护。

Microsoft

不断演变的 IT 格局


Microsoft Office 365
NETSUITE
ADP
Google Apps
salesforce.com
SaaS
其他 PaaS 服务
Windows Azure
PaaS
HOME
其他消费级存储
Dropbox
Windows Live ID
YAHOO!
facebook
Google
客户端
服务器
AD
供应链
外部数据中心
Microsoft Exchange
Microsoft Lync
Microsoft SharePoint
Microsoft Dynamics

信息保护要求



- **在源处保护数据**
  - 现代应用程序会直接将数据保存到“外部存储”， 因此数据在离开应用程序之前必须加密。
- **在“可用区块”处保护数据**
  - 使用模式处于文档级别；而非全驱动器级别（例如：BitLocker）
  - 在资源有限的移动设备上尤为如此；还有就是在基于共享云的存储上

信息保护要求

- **静态加密强而有力；应用程序保护相当出色**
  - 假设静态数据暴漏给对手（授权前）
  - 假设用户“值得信赖，但可能有些疏忽”（授权后）
  - 灵活的激活模型支持最重要的审核或脱机使用；　　决定采用这类模型
  - 自动化 RM (CA-DLP)；每应用程序优化（Outlook 与 Word）；应用程序上下文内容

每应用程序策略以及定制可提高合用性（减少摩擦）

满足客户需求：方法

- **借 EFS 保护文件**
  - 日常比喻：锁住自行车架 – 只在特殊位置有用，别处根本没用。
- **使用 BitLocker BitLocker**
  - 日常比喻：认证的邮件在保留期结束后需经过重新认证才能重新使用。
    对使用条款灵活且传输不限的“混乱”环境数据提供保护

满足客户需求：方法

- **SharePoint “安全库”**
  - 日常比喻：在运作良好的公共图书馆里，图书管理员会实际要求核实您的身份
  - 托管可集中的数据的有效方法需对离开的数据提供保护
- **SharePoint “安全库”**
  - 日常比喻　在运作良好的公共图书馆里　图书管理员会实际要求核实您的身份
  - 托管可集中的数据的有效方法需对离开的数据提供保护

满足客户需求：投资

- **应用程序目标：“让我的工作流对文档提供强劲保护”**
  - Office 和 Office 365 目前可支持 RMS… 而且在不断改进。
  -
  -
    使用“受权限保护的文件夹”格式提供的普通保护
    -

使用“受权限保护的文件夹”格式提供的普通保护

- **设备目标：“让我可随处使用受 RM 保护的文档”**
- 正在向 、Android 和 Metro 努力中
  iOS

满足客户需求：投资

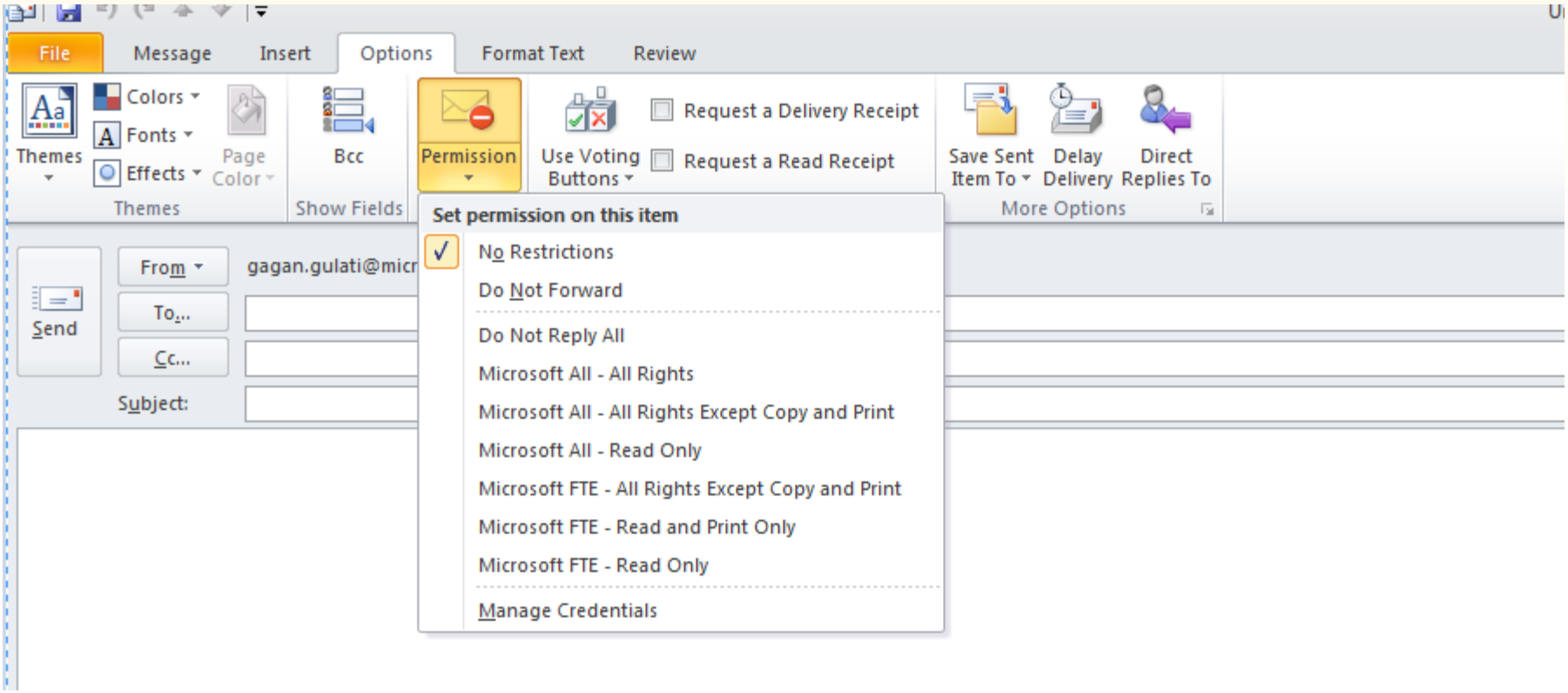
- **操作准备：“我能在自己的组织中使用 RMS”**
  - Microsoft 的 AD RMS 大幅改进了 ERM 作为基本功能（基础）
    - 提供基本功能、目标和使用。

    保护。

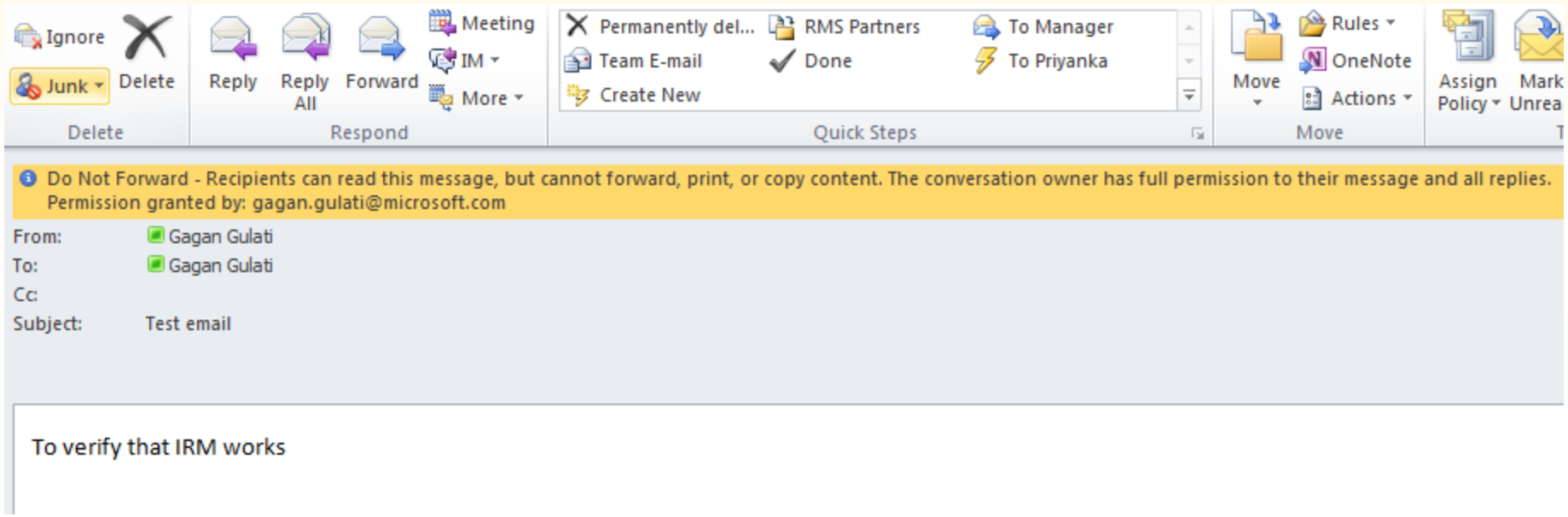
    Microsoft FOPE 和众多其他合作产品共同支持这一需求（过去和未来）。
    -
- **高人气的解决方案 ISV 社区**
  - 许多很有用的服务均基于核心 MSFT IRM 平台：Gigatrust、Secure Island 等。

面向开发商的 AD RMS 服务

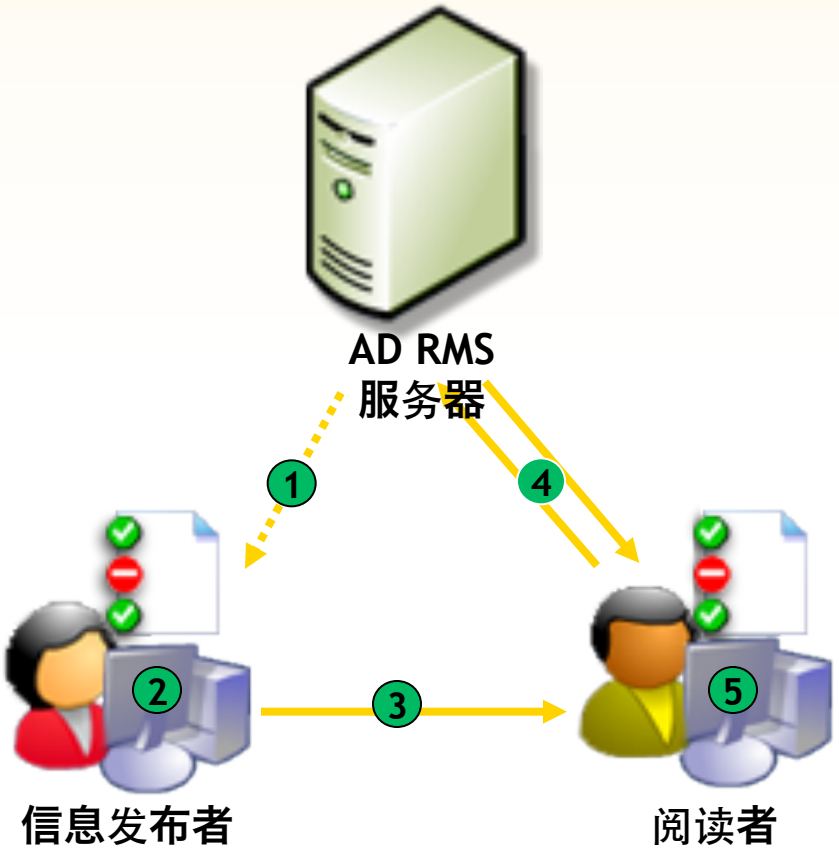
Outlook：发布者


File
Message
Insert
Options
Format Text
Review
Themes
Colors
Fonts
Effects
Page Color
Themes
Bcc
Show Fields
Permission
Use Voting Buttons
Request a Delivery Receipt
Request a Read Receipt
Save Sent Item To
Delay Delivery
Direct Replies To
More Options
Set permission on this item
No Restrictions
Do Not Forward
Do Not Reply All
Microsoft All - All Rights
Microsoft All - All Rights Except Copy and Print
Microsoft All - Read Only
Microsoft FTE - All Rights Except Copy and Print
Microsoft FTE - Read and Print Only
Microsoft FTE - Read Only
Manage Credentials
Send
From
gagan.gulati@micr
To...
Cc...
Subject:

Outlook：收件人


Ignore
Junk
Delete
Delete
Reply
Reply All
Forward
Meeting
IM
More
Respond
Permanently del...
Team E-mail
Create New
RMS Partners
Done
To Manager
To Priyanka
Quick Steps
Move
Rules
OneNote
Actions
Move
Assign Policy
Mark Unrea
Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.
Permission granted by: gagan.gulati@microsoft.com
From: Gagan Gulati
To: Gagan Gulati
Cc:
Subject: Test email
To verify that IRM works

AD RMS 工作流



1. 发布者获得必需的证书和模板以允许使用权限管理
2. 发布者针对文件定义一组使用权限和规则；应用程序将加密该文件
3. 发布者分发文件
4. 阅读者单击要打开的文件，应用程序将调用 RMS 服务器以验证用户
5. 应用程序呈现文件并强制实施权限要求

什么是支持权限的应用程序

- AD RMS 依赖于支持权限的应用程序来执行如下操作：
  - 创建策略（不打印、不转发、全部回复）
  - 加密文档
  - 强制实施限制
- 支持 AD RMS 的应用程序指的是为配合使用 AD RMS 而增强的常规应用程序
  - 使用 AD RMS SDK 来增强应用程序

回顾历史：MSDRM

RSA CONFERENCE CHINA 2012

- MSDRM 是第一种为支持权限管理服务而提供的客户端/SDK/API

- MSDRM 是一种低级别的 API
  - 需要深入了解 AD RMS 功能
  - SDK/API
    - MSDRM 是一种低级别的 API

AD RMS SDK 2.0 (MSIPC)

- 针对 Windows 发布于 2012 年 5 月
- 针对 Windows 发布于 2012 年 5 月
    - 极低的集成成本
- Microsoft 内部的权限管理实施移至全新 SDK（Office 15、SharePoint 和更新版本的 Exchange）
    - 来自 Office 开发商的评论
    - “通过在 *Office* 中运用 *MSIPC* 让我们获益良多… 这样使得我们学习 *RAC*、*CERT*、*CLC* 及其工作方式的计划时间数周数周地减少”
    - “我意外地发送一封含有大附件 *(9MB)* 的 *IRM’d* 电子邮件，却看到了难以

MSIPC：AD RMS SDK 2.0

开发商成本	MSDRM（旧）	MSIPC（新）
API Surface 函数	84 个函数	20 个函数（仅需要其中几个函数）
集成成本	约 4000 行代码	约 200-400 行代码
起步时间	需详细了解证书、格式和拓扑，而且限于多线程	仅需基本了解权限实施
需要更新以支持新功能	是（可能需要进行大量更改）	否
新的 RMS 功能可确保正常工作	否（适用于加密不明情况、证书格式、撤消方案）	是
多拓扑支持	大量开发和测试成本	免费（只要使用所有拓扑）
维修	MSDRM 功能在每个操作系统版本中都存在些许差异	MSIPC 可带来一致的功能行为。您可以捆绑更新。

AD RMS SDK 的下一步行动

下一步行动：AD RMS iOS SDK

- 使用 iOS 设备上受保护的内容
-

SDK 测试版将于 2012 年秋季发布

下一步行动：File API

File API

- 访问和创建受 AD RMS 保护的文件，不必担忧文件格式问题
- 集成更紧密，性能更高
- File API
  访问和创建受 AD RMS 保护的文件，不必担忧文件格式问题
- 集成更紧密，性能更高
- 使用程序模型和文件格式所有者提供保护程序，客户购买保护程序

File API 测试版将于 2012 年秋季发布。

其他资源

- AD RMS SDK 2.0 可在 Microsoft 下载中心获得
- 下面是一些宝贵的资源：
  - 下载链接：https://connect.microsoft.com/site1170/
    - 一盒型测试环境
    - 《快速入门》指南用于构建简单的富客户端应用程序

谢谢大家！

RSA CONFERENCE
CHINA 2012