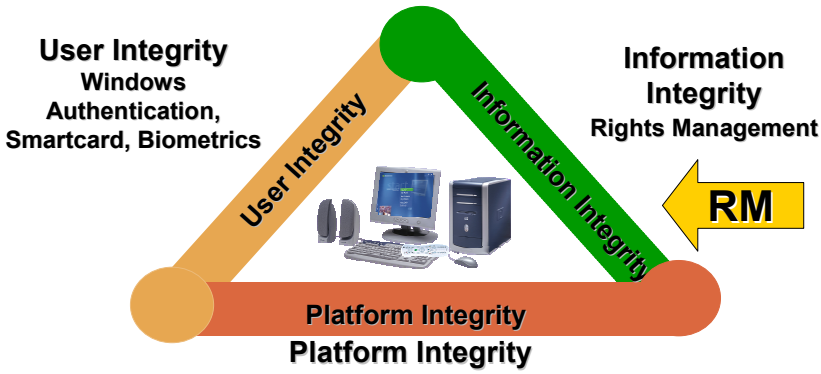
Case Study: Windows Rights Management

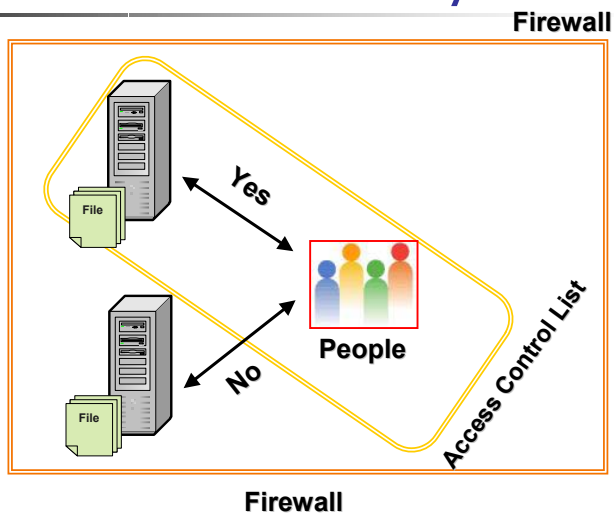
Microsoft Long-Term Investments



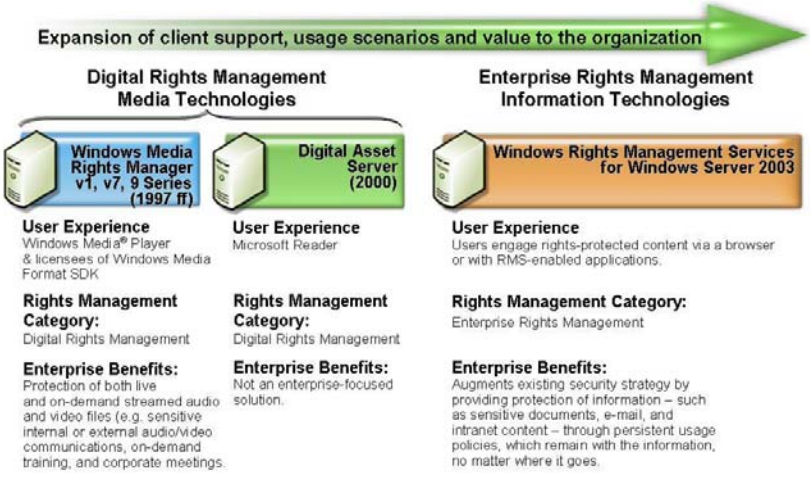
NGSCB

Together, these capabilities create a more secure working environment

Access Control Today



RM for Enterprise Information



Rights Management

- Technology that…
  - Allows individuals and businesses to project usage policy onto the information that they own
    - Any application
    - Any format
  - Policy persists with information
    - Sample rights include view, read-only, copy, print, save, forward, modify, and time-based
    - Rights live within the file wherever the file goes

Why Rights Management?

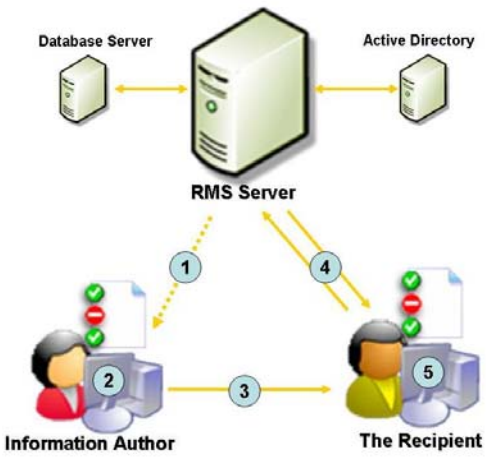
- "Thirty-two percent of the worst security incidents were caused by insiders; 48% in large companies!"
  - Information Security Breaches Survey 2002, PWC
- "Proprietary information theft caused the greatest financial damage of all security failures."
  - FBI Computer Crime and Security Survey, 2001
- Costs
  - Consultant fees, down time, brand damage, legal liability, customer confidence, etc.

Components Of RM

- Windows Rights Management Services (RMS)
  - Windows Server 2003 premium service
  - XrML-based certification of trusted entities
  - licensing of rights-protected information
  - enrollment of servers and users
  - administration functions
- Updates to Windows client
  - Rights Management APIs for Windows 98SE+
  - Rights Management Add-on for Internet Explorer
- Software Development Kits
  - One each for client and server
- RM-enabled applications
  - create and/or view rights-protected information
  - Office 2003 is the first major Enterprise app to implement RM

Workflow

- Get a license certificate from RMS
- Create rights-protected object with RMS-enabled app: Office03, Email, etc.
- Define usage rules of the object
- RMS-enabled app encrypts the object, and creates **publishing license**
- Receipt open the obj, RMS-enabled app contacts the RMS for validation of receipt and rights, and issue a **use license** sent back.
- RMS-enabled app enforce rights in use license



Enterprise RM Scenarios

- Enforce policies for Web content
  - E.g., database-backed content
    - Sales and financial reporting, HR records, etc.)
- Enforce policies for confidential email and documents so they can't be forwarded, printed, saved, etc.
  - Marketing plans, merger proposals, and contracts
- Set email and documents to expire…
  - …At a specific point in time
  - …X days after publishing
  - …Every X days, requiring acquisition of a new license
- Corporations centrally manage RM policies
  - RMS Policy Templates for policies such as "Company Confidential"
  - Exclusion of rogue/broken applications

RMS Security Model

- User attributes:
  - Identity, role, group, clearance, etc.
- Object attributes:
  - Type, classification, etc.
  - Application specific attributes
- Conditions:
  - Time, location (?), etc.
- Obligations:
  - Send receipt to object owner
  - Refresh license information periodically.

RMS Services

- RMS is an ASP.NET Web service
  - Protocol is SOAP over HTTP/HTTPS
  - Internet Information Server (IIS) 6
  - Single request/response transaction model
  - Stateless – all processing handled on front end
  - XrML-based input/output
- Deployment Scenarios
  - Business Intranet
  - Business-to-Business Collaboration
  - Hosted Services

RM Inside Microsoft

- Windows Rights Management infrastructure is 100% deployed inside Microsoft
  - Office 2003 used to protect information between employees, vendors, and partners
  - Rights Management Add-on for Internet Explorer being tested as well
- RMS front-end licensing servers deployed centrally
  - Servers in Redmond
  - Supporting 75,000+ Active Directory users
  - Deployed across three Active Directory forests