Enterprise Rights Management: Protection beyond the perimeter
Introductions

Guardian Technologies Limited
• Barrie Kenyon
• Rupert Beeby
AGENDA

• Guardian Technologies
• Security Background
• What is the problem
• How does ERM address
• Adoption of Rights Management
• What if......
• Overview of Rights Management
GUARDIAN TECHNOLOGIES - FOCUS

• Young, value-added Provider of products and services in the Information and Asset Security market
• Focussed on addressing fundamental areas of risk with innovative and ‘breaking’ technologies
• One of the first companies to provide DLP solutions to international market with VerSec
• Innovative solutions for access controls, information protection and attack intelligence
• Clients across finance, credit control, public sector
Common Scenarios

• Information security during collaboration – within and outside the enterprise
  – Information security technologies give ‘perimeter’ protection. Perimeter is no longer effective and cannot protect once information is outside
  – Once information is outside the organisation there is no way to control access to it - E.g.. M&A, bid work, RFPs, etc.

• Information Leakage during outsourcing
  – Organisations find it difficult to ensure security policies within outsourcing partner’ operations
  – Results in increased costs associated with physical and process audits and control of the outsourcing partner. In some cases it prevents outsourcing

• Tracking and auditing the flow of information with the value chain
  – Compliance to digital asset management policies of regulatory frameworks like ISO, SOX, GLBA & PCI means not only internal compliance but also compliance of the value chain of partners, vendors and customers

• Security for the Cloud
  – Cloud security is still evolving and is a detractor for adoption as information protection is difficult
  – Microsoft cloud offerings use RMS which is ‘all or nothing’
THE PROBLEM .....
Traditional Security Approach: Protect the Perimeter

- Anti-virus
- Disk Encryption
- Application Firewall
- DLP
- SSL
- UTM
- PIM
- Anti-spyware
- Email
- Networks
- Applications
- Devices
- People
The Challenge of the Perimeter Definition
The Solution…
Borderless Security: Is it Possible?

Rights Management protects your information…

…any digital information that resides in files

…wherever it goes
Make Information the New Perimeter
Information-Centric Security

**WHO** can use info
People & groups within and outside of the organization can be defined as rightful users of the information.

**WHAT** can (s)he do with info
Individual actions like reading, editing, printing, distributing, copy-pasting, screen grabbing, etc. can be controlled.

**WHEN** can (s)he use info
Information usage can be time based e.g. can only be used by Mr. A till 28th Sept OR only for the 2 days.

**WHERE** can (s)he access/use info
Information can be linked to locations e.g. *only 3rd floor office* by private/public IP addresses.

**Easily Define, Attach, Enforce & Audit**
Granular Usage Policies

www.guardiantechnologies.co.uk
Usage Policy Attributes

Permanence
Protection will always persist with the file

Remote-Control
Change your usage policies for information sitting anywhere in the world

Audit Trail
All activities on information tracked: Users, activity type, date/time, location
WHO accessed the file, WHAT did the user do, WHEN & WHERE, is captured from distributed usage environments & consolidated centrally for simplified reporting.
Data Expiration

• Expire your data....
  – After a consultation with a potential customer, do not leave your methods and costs behind – expire it!
  – After a third party is no longer required then do not leave your plans behind – expire it!
  – If you have sub-contractors working on services such as utilities with updated plans then don’t let them access out-of-date information – expire the old versions
  – Bid processes leave information behind and can get into competitors hands – Expire it!
Essential Device Support

Desktop / Laptop
Client, Lite, and Browser

iOS
iPhone, iPad, iPad mini
Client, Lite, and Browser

Android
SmartPhone & Tablet
Client, Lite, and Browser
Enterprise Rights Management

Summary

• Technologies that protect sensitive information from unauthorized access inside and outside the organisation
• ERM is a technology which allows for information (mostly in the form of documents) to be ‘remote controlled’
• Information and its control can now be separately created, viewed, edited & distributed

What is it for?

• Information security during collaboration
  – Often seen as “mutually conflicting” goals
  – Security systems perimeter centric – rendered useless when information leaves the perimeter
• Information breaches during outsourcing
  – Security, privacy and compliance expectations while outsourcing
  – Present day solutions archaic and centered around “building walls”
• Information audits
  – Present systems help IT systems audits and not information audits
  – Compliance to ISO, HIPAA, PCI, SOX, ...
ERM Architectures: Different Landscapes

Key differentiator is the architectures (and therefore cost)!

1. Some vendors build rights management directly into their applications which is the platform approach
   - Microsoft RMS
   - Adobe

2. Others build upon platform providers to extend capability
   - GigaTrust
   - Foxit

3. Some vendors use a plug-in approach
   - Seclore
   - WatchDox
Platform-based ERM

- The main player is Microsoft with AD RMS and Azure RMS
- Platform approach can provide tighter integration and easier to deploy if a Microsoft AD user
- Platform approach builds upon existing infrastructure to include rights management.
- Scaling can be an issue
- Platform approach particularly Microsoft will only use their product base to provide authentication
- Particularly suited if all parties are with your AD environment
- Extension outside the organisation can be problematic
- To integrate with other applications requires use of MS SDKs
- Best suited to organisations with heavy investment in Microsoft products and services
Platform Extension Approach

• Extension approach requires significant investment in the platform if no deployed
• Purchase of extension product may be overtaken by increase in functionality of platform vendor
Plug-in Approach

- Plug-in approach can support more file types and give users more versatility in setting controls, policies, etc
- Plug-in solutions can start small and grow as required
- The time for a new recipient to be able to access is usually significantly less than platform approach (less than one minute)
- Cost of solution and cost of deployment is less than a platform approach and more configurable
Considerations

- Consider the risk of misappropriation and try to put a value to it
- In general, costs are proportional to the amount of information that needs to be protected
- What formats is the critical information maintained such as CATIA, CAD, etc
- Most vendors support the common document such as Office, PDF. However, check what you need to be protected and then check the vendor coverage
- Plug-in approach may be more secure than say, Microsoft as smaller vendors are less of a target for hackers
- Key adoption of ERM in an organisation is the user experience. It has to be easy for the users to protect documents or access protected documents. Most vendors focus on the protection and forget the users.
- Be aware of the costs – try to start small and protect the critical information first.
- Consider the amount of sharing required by your organisation:
  - If a lot then a platform approach may require more administration and configuration
Who are the players?

• Seclore – leading vendor with over 100 types of files protected and versatility of protection
• Adobe® LiveCycle® Rights Management ES2
  – Good for PDFs and Office
• EMC – integrated with Documentum
• GigaTrust – expansion of RMS
• Liquid Machines (now part of Checkpoint) – uncertainty in product direction
• Microsoft RMS – only protects office documents and PDFs – complexity is the issue and cost.
• Oracle – withdrawn.
The Document Recipient is key!

• Support for all methods of access
  – Windows desktop client
  – Web Viewer View documents inside web browser
  – Tablet / Phone Free App for iPad and Android
• Permitted first time users need access quickly and efficiently
• Policy on information security needs to be promoted to users
• All though information that is passed on cannot be accessed, people can be tracked and they need to know it.
• Consider repercussions of sending unauthorised information to third parties
View of the Analysts

Because ERM allows data to protect itself via encryption, it is theoretically the perfect security technology for a world where the “dissolving perimeter” is an established fact. But historically, most enterprises don’t use ERM on an enterprise-wide basis and do not use it to protect documents shared outside company boundaries. High cost, application rigidity, and integration shortcomings have limited market adoption. Forrester expects that ERM’s appeal will widen in the future. Integration with data leak prevention technology, content management infrastructure, and other risk mitigation solutions will drive adoption growth, particularly as enterprises roll out the latest versions of Microsoft Exchange and SharePoint.

Forrester Research Market Overview: Enterprise Rights Management
Questions?
MODES OF PROTECTING INFORMATION
1. Manual Protection

A document on users’ desktops/laptops can be manually protected by:

- Using mouse right click option or
- As soon as the document is created on a user driven prompt or predefined settings
2. Folder-Based Protection

A document gets protected as soon as the document is placed in a certain location: e.g. Folder/File Server
3. Email Protection

A document gets protected along with the email content by using FileSecure’s email protection functionality.
A document gets protected using pre-built connectors for ECM systems such as:

- MS SharePoint
- IBM FileNet
- EMC Documentum
- Omnidocs
5. Extending Reach of DLP Systems

A document gets protected as soon as it is “discovered” or “tagged” by a DLP system.

All DLP processes monitoring Endpoint, Network and Storage can invoke API to protect file-based content.
Seclore FileSecure
ARCHITECTURE
Overview - How Does ERM Work?

- Recipient opens the document
- Usage policies are applied by FileSecure while opening the document
- Protects the document and Assigns Usage Policies to the document
- User creates a normal document on his machine
FileSecure Architecture

**Document Protector**

**Document Consumers**

**Internal Users**

**External Users**

**External Users With Web View**

**Use rs**

**WEB CONNECT**

**https://INTERNET**

**FileSecure Protection**

**FileSecure Web**

**Policy Server**

**FileSecure Web Services**

**JDBC**

**LDAP**

**Components**

**Files**

**Use rs**

**Applications**

**FileSecure Hot Folder Servers**

**DMS like Sharepoint**

**DLP like Symantec**

**Other Custom Applications**

**www.guardian technologies.co.uk**