

A close-up, high-contrast photograph of an owl's face. The owl's feathers are dark and textured, with a prominent red eye and a dark pupil. The background is blurred, showing a bright, hazy light source.

# RightsWATCH. Data-centric Security

[www.watchfulsoftware.com](http://www.watchfulsoftware.com)  
[Info@watchfulsoftware.com](mailto:Info@watchfulsoftware.com)

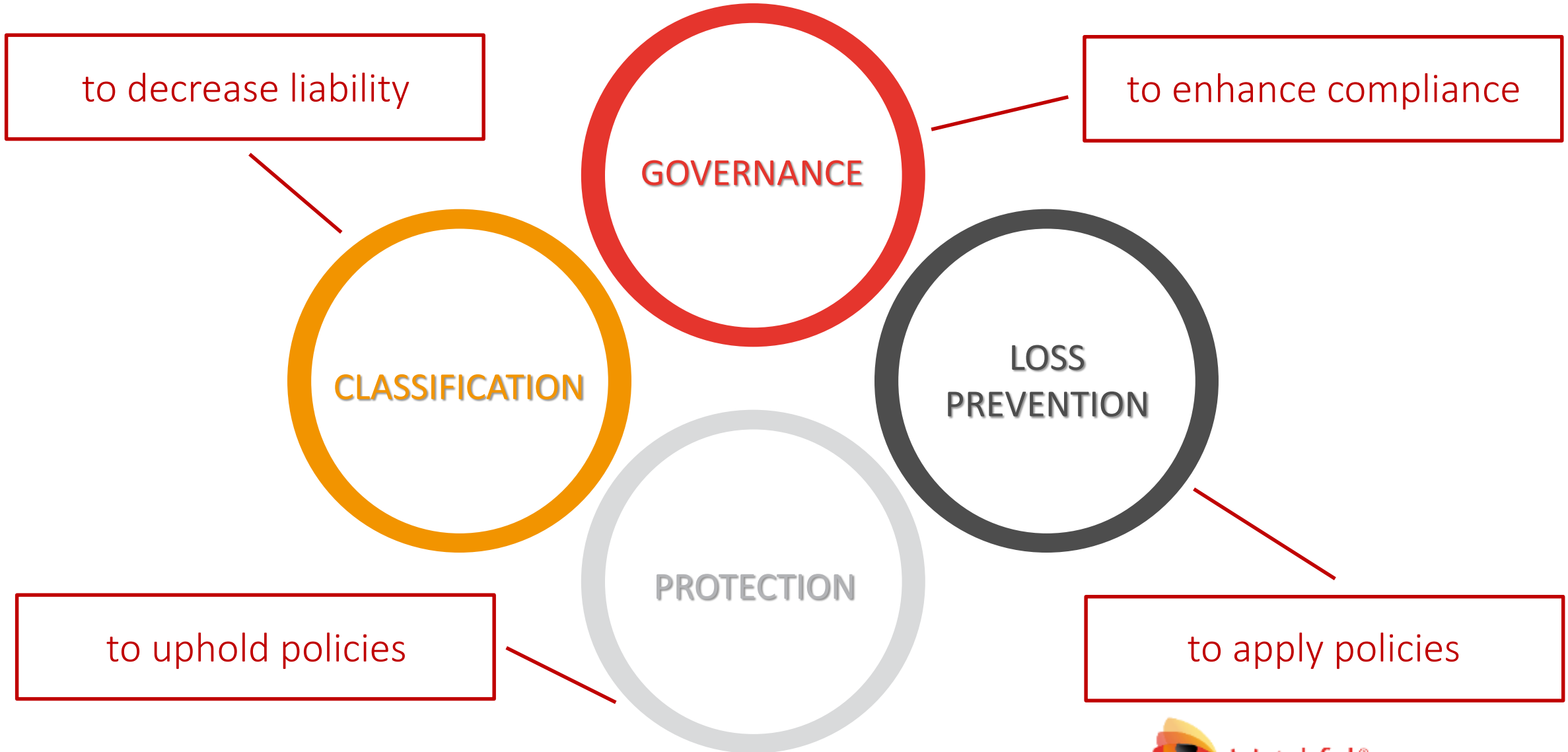
Watchful Software  
Keep IT Secret



# A New Paradigm in Data-centric Security



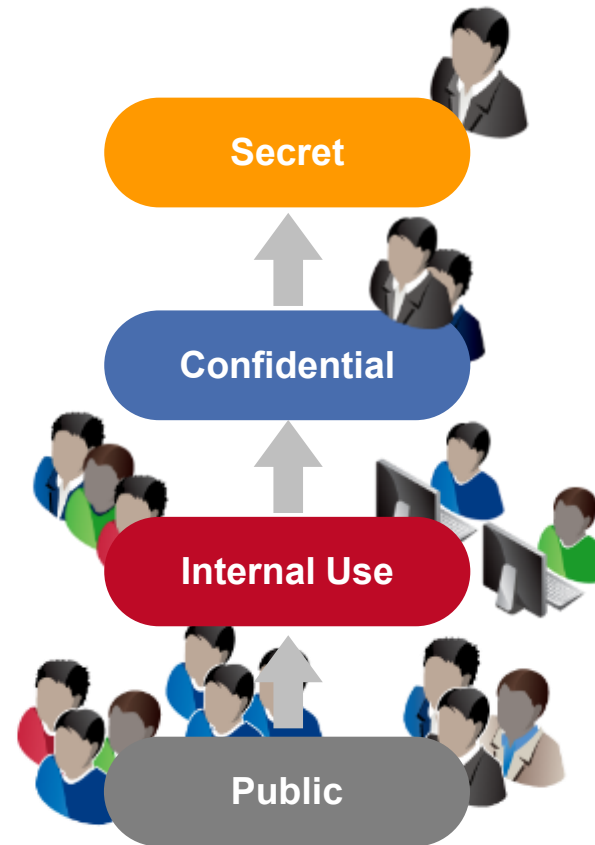
# A New Paradigm in Data-centric Security



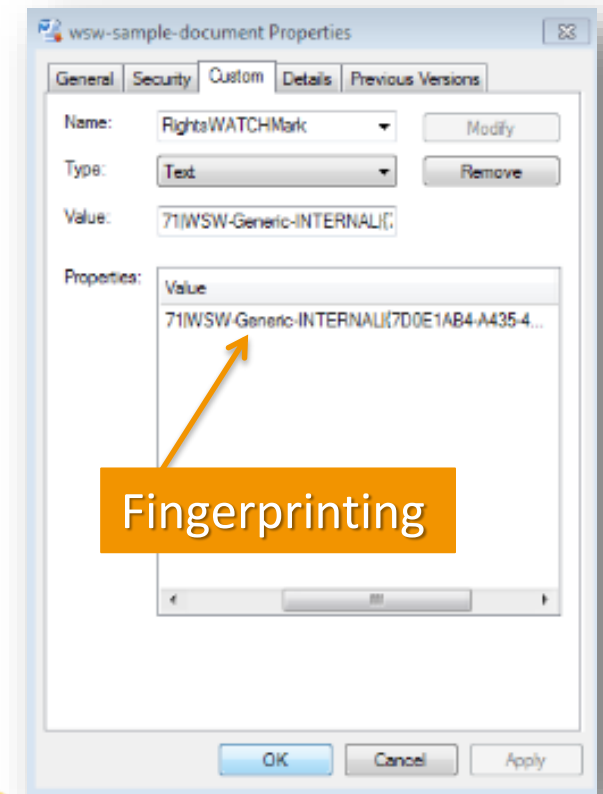
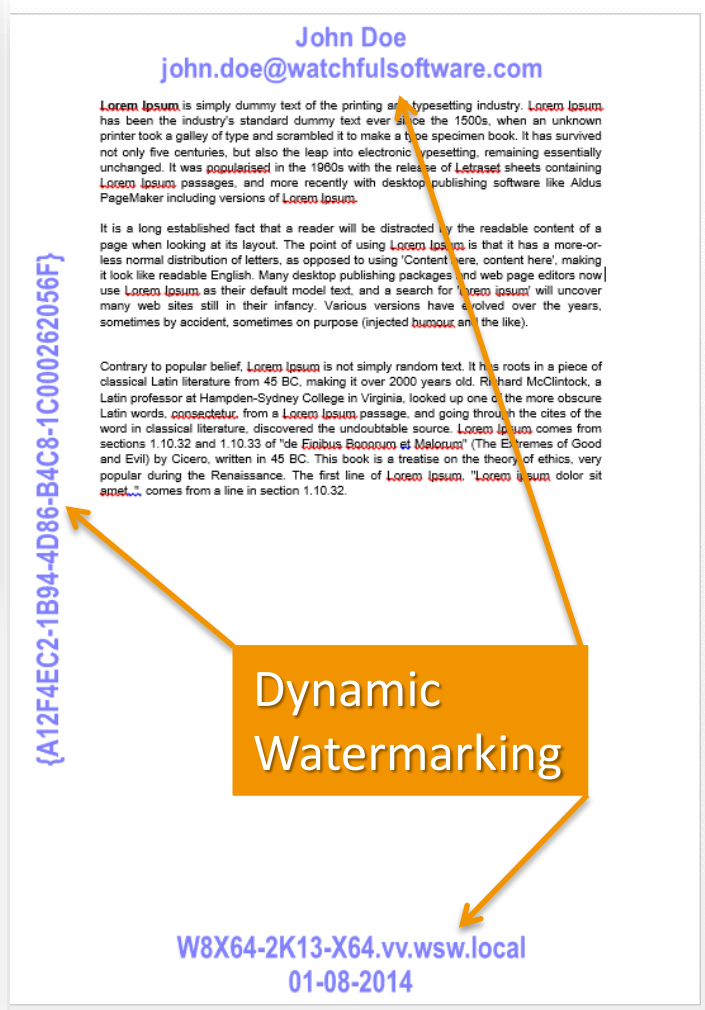
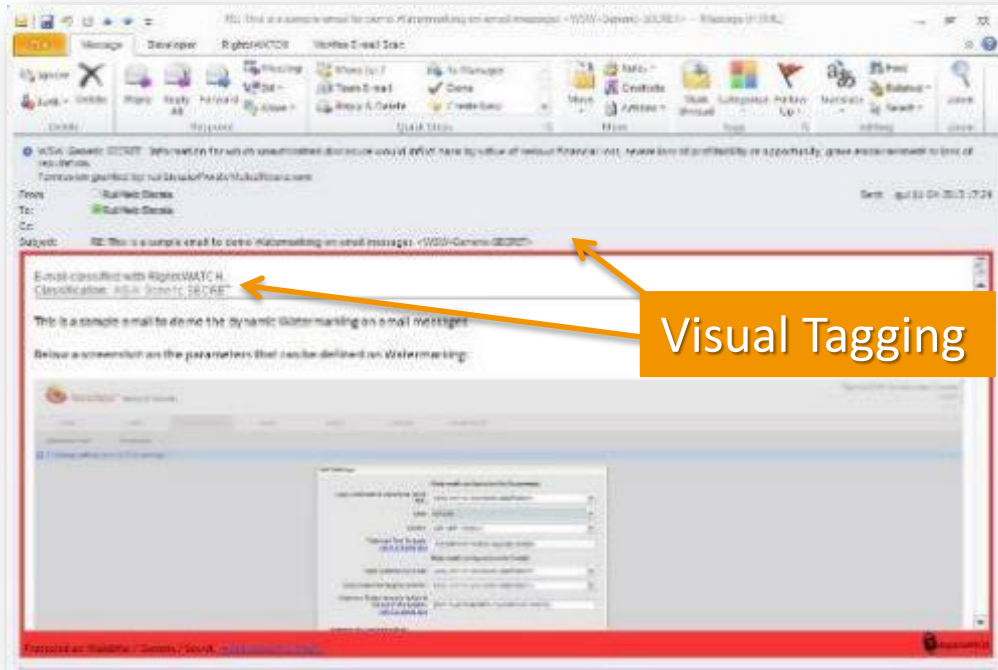
# RightsWATCH & DATA Governance



- Deploy a Multi-level Security Model
- Extend the Multi-level Security Model and apply Role Based Access Control over Data
- Grant/revoke/deny each user/group of users with multiple security clearances
- Log and have a comprehensive audit trail on who, had done what, when and how.



# RightsWATCH & DATA Classification



- Data Tagging
- Dynamic Watermarking
- Data Fingerprinting

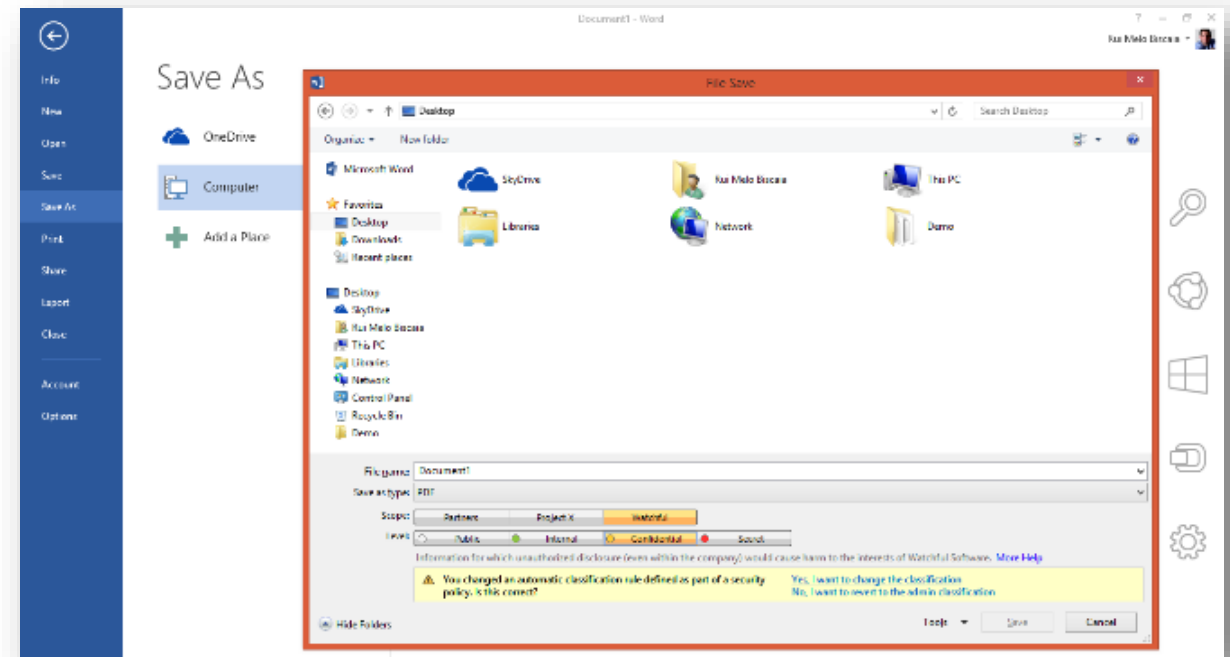
# RightsWATCH & DATA Protection



- Enhances Rights Management Services:
  - Better user experience
  - Support for more platforms and file types
  - Role Based Access to RMS templates
  - Automatic application of RMS rights
  - RMS encryption on iOS, Android & BB



**=** Better User Experience  
Broader Support  
Faster Implementation  
Rapid ROI



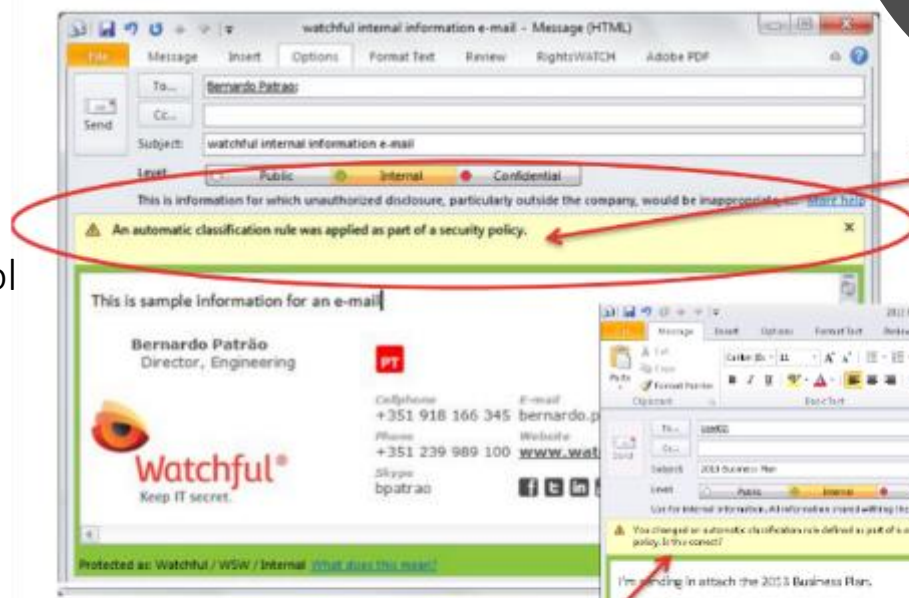
# RightsWATCH & DATA Loss Prevention



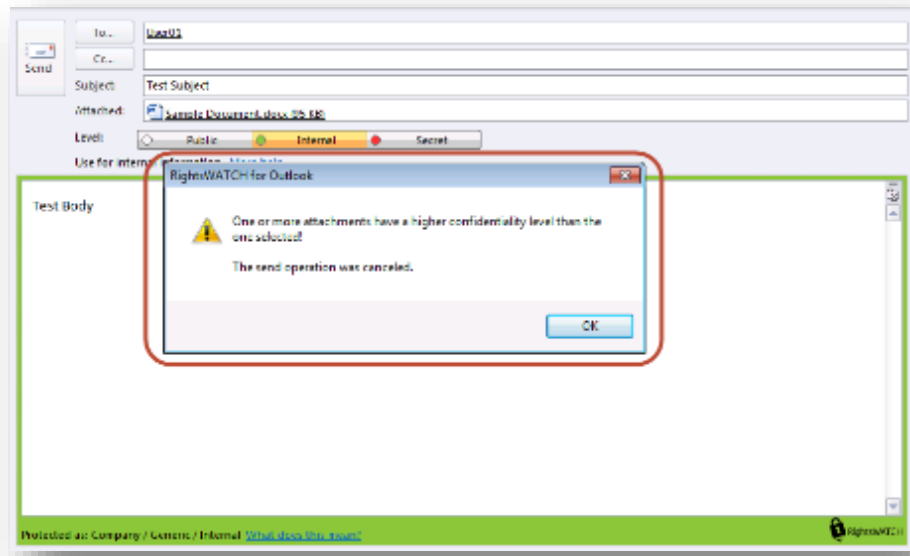
- Email & MS Office Content & Context Aware

Policy Rules to:

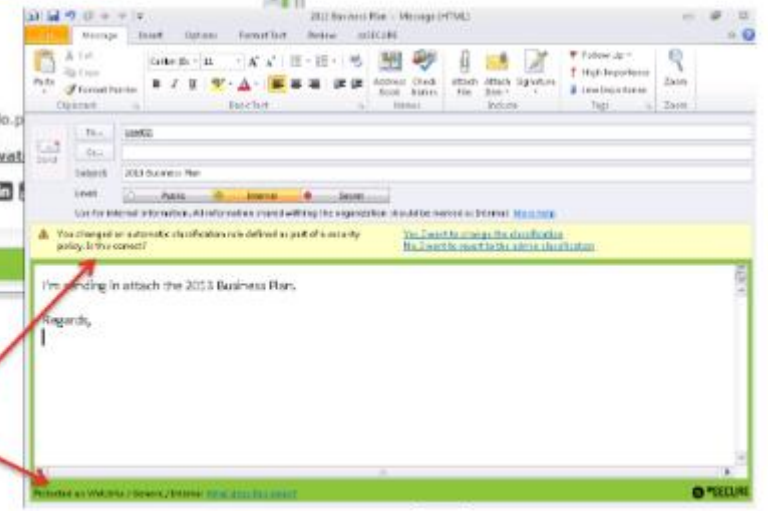
- Automatically Classify & Protect data
- Enforce corporate Information Security Policies
- Enhance ANY existing DLP/Firewall/Gateway tool



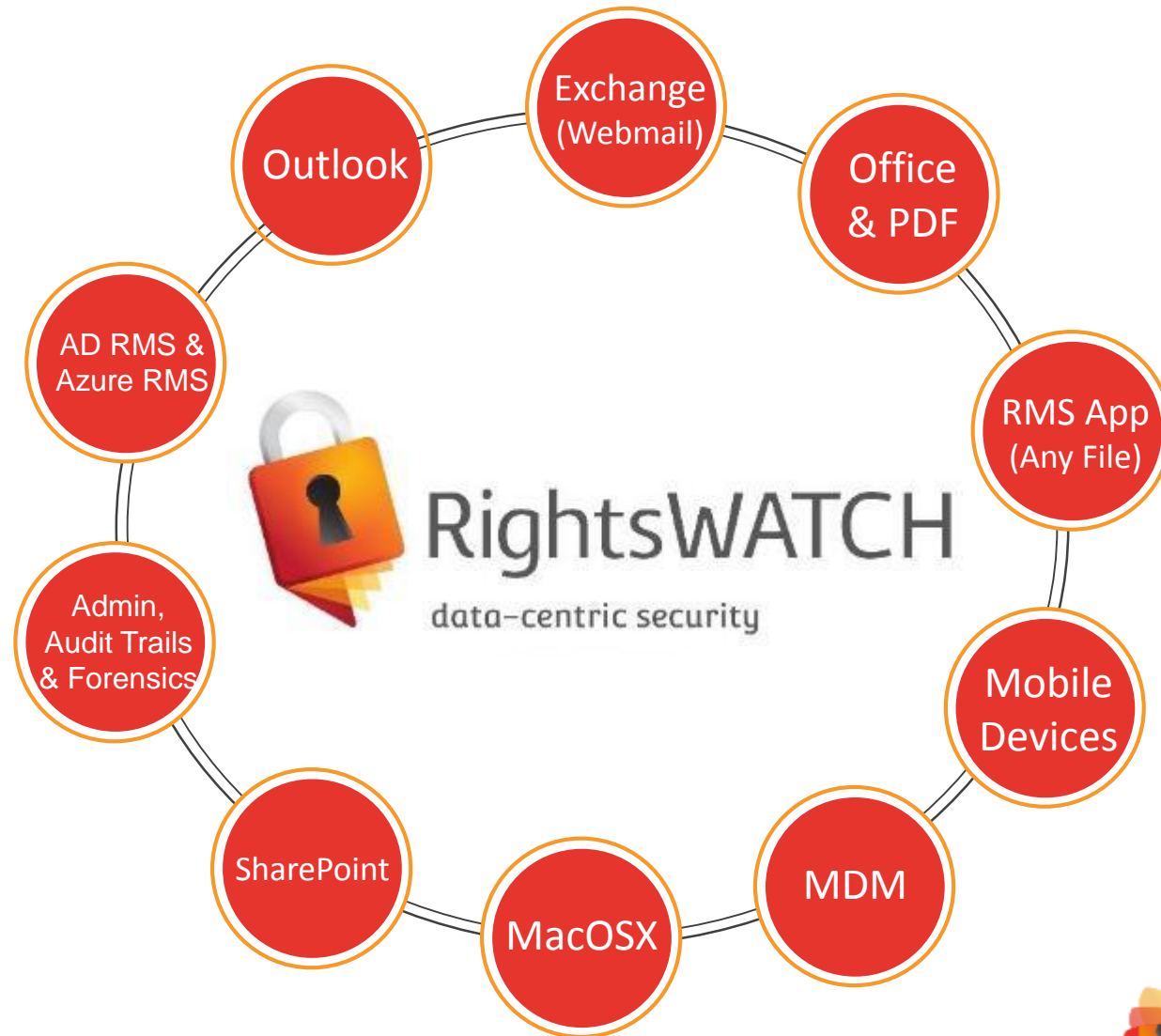
Enforces corporate policies



Educates users with visual clues and prompts



# RightsWATCH integration & Support capabilities

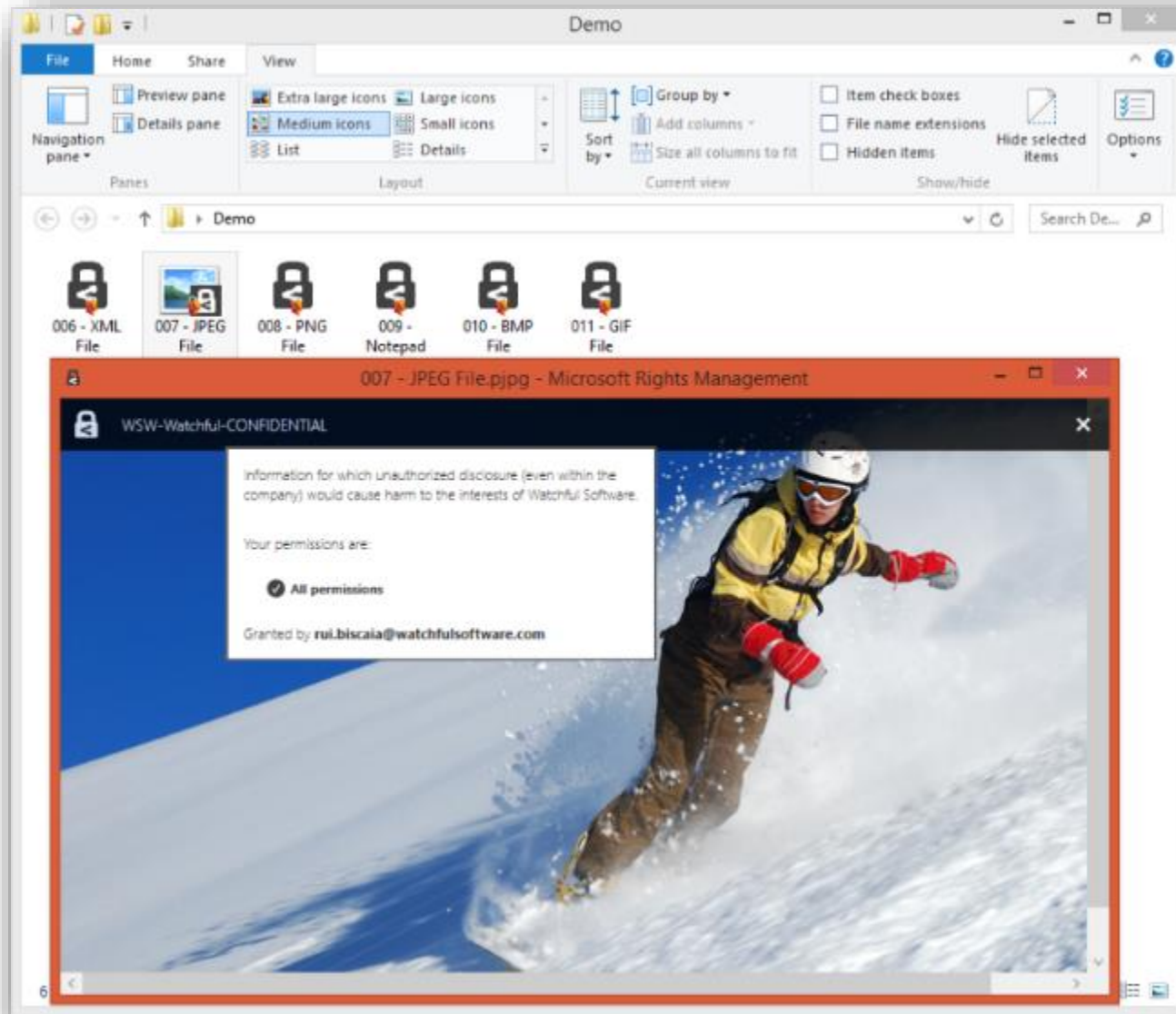




# Classification & Protection of Email, Webmail & Office files

The screenshot shows the Microsoft Word 'Save As' dialog box. The file name is 'Document1' and the save type is 'PDF'. The 'Scope' is set to 'Watchful' and the 'Level' is set to 'Confidential'. A warning message is displayed: 'You changed an automatic classification rule defined as part of a security policy. Is this correct?'. Below the message are two links: 'Yes, I want to change the classification' and 'No, I want to revert to the admin classification'. The background shows the 'Save As' ribbon with options like OneDrive, Computer, and Add a Place.

# Rights Management Sharing App & Global (File) Protector



- ❑ Ability to Classify & Protect “ANY” file type
- ❑ Leveraging Microsoft’s “.PFILE” technology and the RMS App (to view the encrypted files)
- ❑ Ability to BULK Classify and Re-classify files (eg: Legacy data)

# Classification & Protection of PDF files

The screenshot displays the Foxit Reader interface. The title bar shows the document name: "Watchful\_Software\_Confidential.pdf (SECURED) - Foxit Reader". The ribbon menu includes FILE, HOME, COMMENT, VIEW, FORM, PROTECT, SHARE, and HELP. A yellow security overlay is present at the top of the document content, displaying the text: "WSW-Watchful-CONFIDENTIAL - Information for which unauthorized disclosure (even within the company) would cause harm to the interests of Watchful Software." The document content consists of several paragraphs of placeholder text. A "Properties" dialog box is open in the bottom right corner, showing the "Security" tab. The "Security Method" is "PDF Encryption". The "Protection Policy Information" section contains the following text: "WSW-Watchful-CONFIDENTIAL - Information for which unauthorized disclosure (even within the company) would cause harm to the interests of Watchful Software. You are currently allowed to view this document." Below this, a table lists various permissions and their status:

Permissions	Status
Print	Not Allowed
Print Content	Allowed
Print Content Restrictions	Not Allowed
Print Content Restrictions	Not Allowed
Print Content	Allowed
Comments in the document	Allowed
Manage pages and bookmarks	Allowed
Use Document Assembly	Allowed
Content Copying for Accessibility	Allowed
Content Copying for Accessibility	Allowed
Content Copying for Accessibility	Allowed

- ❑ Foxit is the default reader for RMS encrypted PDF files;
- ❑ Same look & feel, Watermarks and Fingerprints as with MS Office files;
- ❑ RMS policy usage rights are enforced.

Properties

Security

Security Method: PDF Encryption

Protection Policy Information: WSW-Watchful-CONFIDENTIAL - Information for which unauthorized disclosure (even within the company) would cause harm to the interests of Watchful Software. You are currently allowed to view this document.

Permissions	Status
Print	Not Allowed
Print Content	Allowed
Print Content Restrictions	Not Allowed
Print Content Restrictions	Not Allowed
Print Content	Allowed
Comments in the document	Allowed
Manage pages and bookmarks	Allowed
Use Document Assembly	Allowed
Content Copying for Accessibility	Allowed
Content Copying for Accessibility	Allowed
Content Copying for Accessibility	Allowed

# Support for Mobile Devices - Supporting a BYOD world



	App	App	Plug-in	
Is RightsWATCH installed on the device?	App	App	Plug-in	
Can I read protected emails?	✓	✓	✓	✓
Can I read protected emails offline?	✓	✓		
Is data encrypted and protected during transport and storage?	✓	✓	✓	
Can I read protected PDF files?	✓	✓		
Can I read protected PDF files offline?	✓	✓		
Can I read protected Office files?	✓	✓		✓
Can I read protected Office files Offline?	✓	✓		✓
Are the RMS Policies enforced on the device?	✓	✓	✓	✓
What is the oldest OS version supported?	6.0 / 7.0	2.3.3 / 4.4.2	6 / 7	7 / 8.1
Can I compose, classify and encrypt e-mail?	✓	✓	✓	
Can I reply and forward protected e-mails?	✓	✓	✓	✓

# RightsWATCH integration with MDM solutions



Single Sign-on and PIN Authentication – One password to access all enabled apps

Automatic App Configuration – Distribute required App configuration settings

AppTunnel Integration – App specific VPN connectivity (when made available)

Secure Data Removal - Wipe an app and data on a phone that was lost or stolen

Device Pinning - Only allow corporate users to log to an App on the device

Classify & Protect Emails online & offline

Read Protected .DOCX, .PPTX, .XLSX & .PDF files online & offline

Apply & Enforce RMS templates usage rights on the device (Copy, Print, ...)

Apply & Uphold an Information Security Policy to classified Information

Role Based Access to sensitive Information



+  
MDM

	✓
	✓
	✓
	✓
	✓
✓	✓
✓	✓
✓	✓
✓	✓
✓	✓

Support for:  



# RightsWATCH integration in MacOSX



Define a Multi-level Security Model

Role-Based Access Control

Watermarking, Tagging & Fingerprinting

Easy User Experience

Automatic & Intelligent Content & Context Aware Policy Rules

Apply RMS Templates Access and Usage Rights

Support for Emails (MS Office for MAC 11)

Support for MS Office

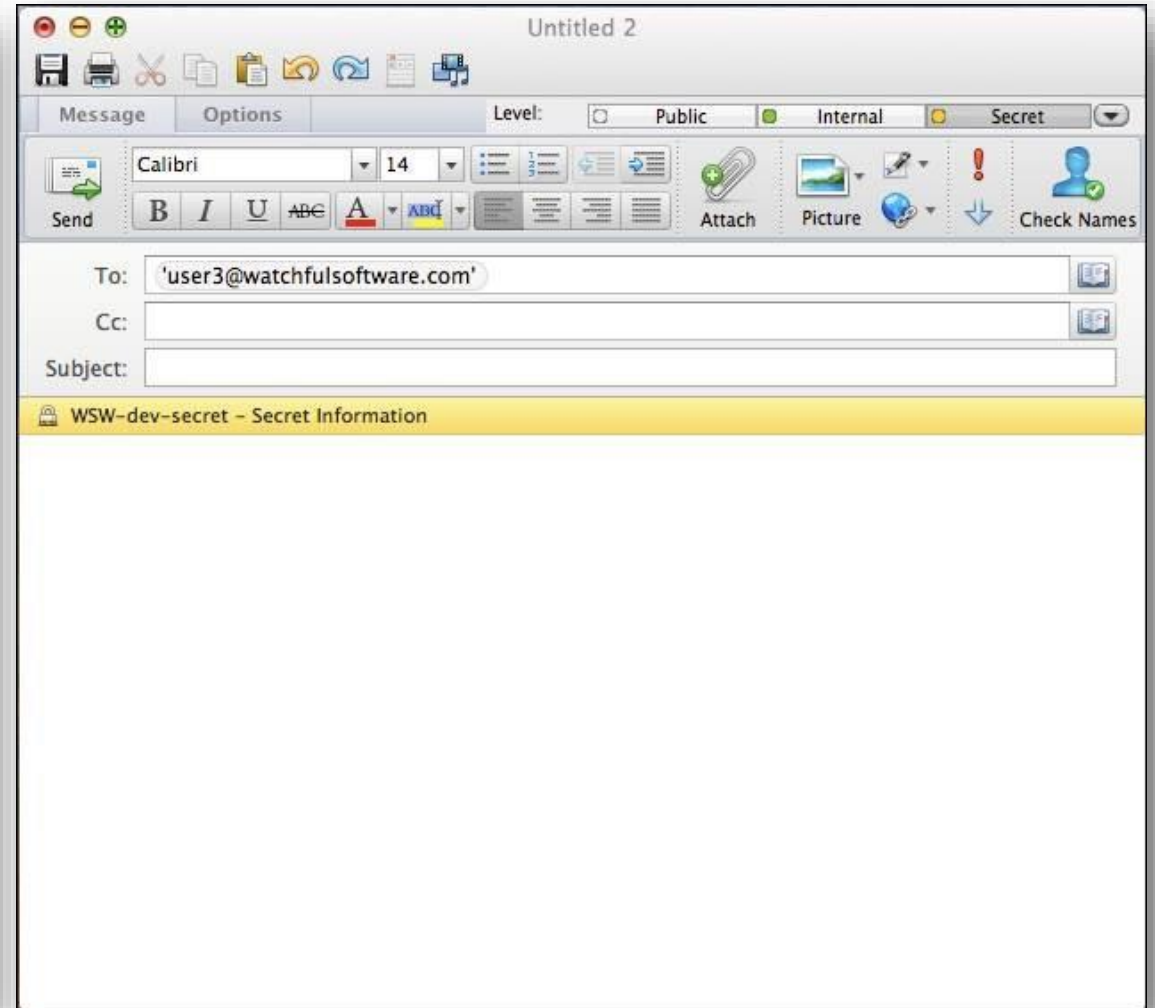
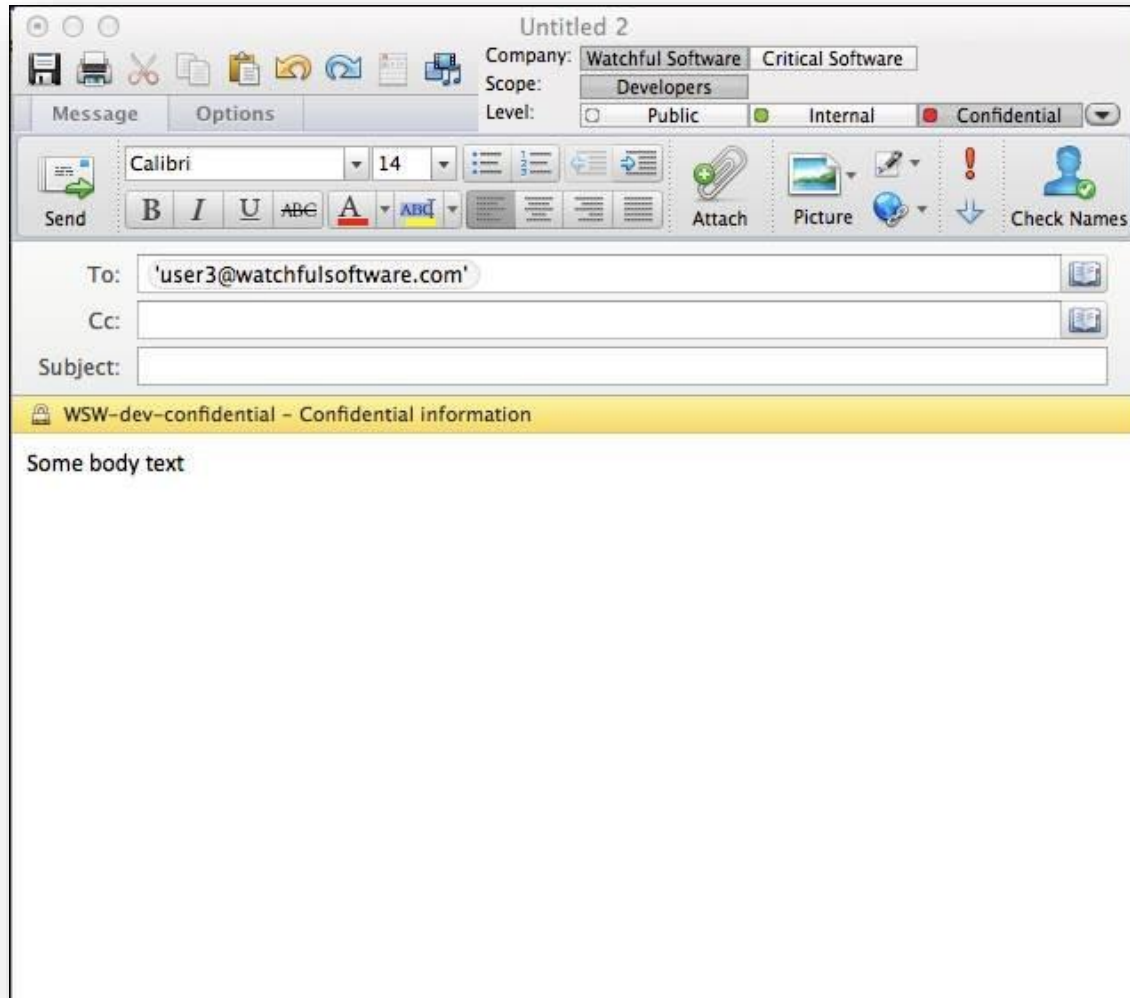
Support for PDF files

Support for "other" file types

Audit Trail & Forensics



# RightsWATCH integration in MacOSX (screenshots)



# Enhancing the SharePoint security experience

Site Actions: Home > RightsWATCH SharePoint Add-in Administration

Home

Libraries

Public Folder

Confidential Folder

Secret Folder

Read Folder

Restricted Folder

Lists

Calendar

Discussions

Team Discussion

Recycle Bin

All Site Content

General Settings

RightsWATCH SharePoint Service location - Fetched updated Classifications List

http://rms.w.wsw.local/RightsWATCH/sharepoint-webservice/RightsWATCHSharePoint.asmx

RightsWATCH Default Behavior - Current available options are: Upload Check Classification; Do Nothing

Upload Check Classification

RightsWATCH Default Classification - Default minimum classification accepted for uploads/check-ins

Not Classified or Public

Not Classified or Public

WSW-Partners-Non-Restricted

WSW-Other-project A

WSW-Other-project B

WSW-Partners-Restricted

WSW-Other-Offline

WSW-Azure-Confidential

WSW-WSW-Confidential

WSW-WSW-Secret

WSW-WSW-Top Secret

Confidential Folder - (f64bc716-ab52-4f5d-8528-89c5d788180a):

WSW-WSW-Confidential

Customized Reports - (6b816623-8b9f-41b8-bd2f-94a8f6f7eed4):

Use Default Setting

☐ If user tries to upload a file with a classification below the minimum threshold specified for that SharePoint library, RightsWATCH asks the user to upgrade the classification of the file



# “All-in-One” Simple, powerful, centralized Admin Web Interface

- ❑ Segregated access to the Admin interface;
- ❑ Centralized ability to define and implement policies, rules, roles and classification models;
- ❑ Streamlined process to propagate amongst various domains & multi-AD Forest environments;
- ❑ Offloads AD (and RMS) workload

Watchful® Keep IT secret.

HOME USERS CLASSIFICATIONS ROLES RULES LICENSES SYSTEM SETUP

Changes were successfully synced with the RMS server and clients.

Show only:

Rights	Anyone	Board	Staff
Watchful (Company)			
Generic (Scope)			
Watchful-Generic-Public	Custom	Full	Full
Classify	X	✓	✓
Watchful-Generic-Internal	Custom	Full	Full
Classify	X	✓	✓
Read	✓	✓	✓
View Rights	X	✓	✓
Export	X	✓	✓
Save	X	✓	✓
Print	X	✓	✓
Extract	X	✓	✓
Edit	X	✓	✓
Allow Macros	X	✓	✓
Forward	X	✓	✓
Reply	X	✓	✓
Reclassify	X	✓	✓
Watchful-Generic-Secret	None	Full	Custom
Classify	X	✓	✓
Read	X	✓	✓
View Rights	X	✓	✓
Export	X	✓	X

Edit (Create Draft)

# Logging, Audit Trails, Forensics and Damage Control actions

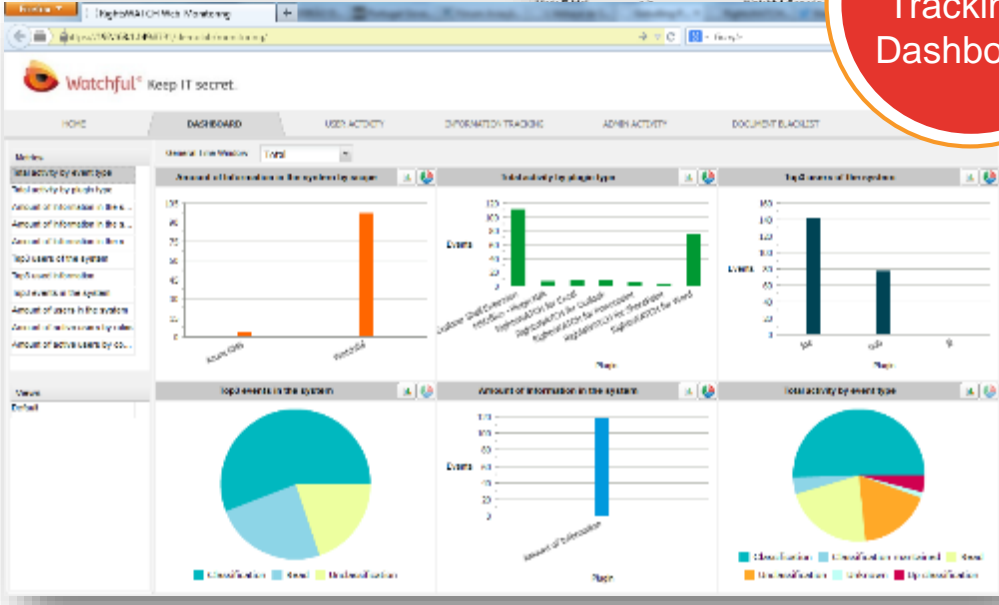
- ❑ Content Rich Database
- ❑ All-in-one Centralized Management
- ❑ Scalable Architecture
- ❑ Secure Implementation
- ❑ Comprehensive Audit Trails
- ❑ Information Tracking for Forensic Analysis



Event Listing & Blacklisting

Event	Original Classification	Changed to	Origin	File Type	File Name	User	Station	Event Date	...
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:58	X
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:54	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:47	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:42	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:38	X
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:35	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:32	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:28	X
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:25	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:22	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:19	X
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:17	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:14	X
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:11	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:08	X
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:05	✓
Read	na	Watchful-General-S...	MS-Files	na	na	JUPITERUser1	R055	20110212 10:55:02	✓

Information Tracking & Dashboards



# RightsWATCH product versions



Supported

	Individuals	Standard	Enterprise
Define a Multi-level Security Model			
Role-Based Access Control			
Dynamic Watermarking, Tagging & Fingerprinting			
In Workflow Interface. Easy User Experience			
Automatic & Intelligent Content & Context Aware Policy Rules			
Apply RMS Templates Access and Usage Rights			
Support for Emails, MS Office files, PDF & "other" file types			
Support for Smartphones & Tablets			
Exchange & SharePoint			
Centralized Admin Interface			
Audit Trail & Forensics			



A close-up photograph of an owl's face, focusing on its large, striking red eye. The owl's feathers are dark and intricately patterned. The background is a soft, out-of-focus landscape with a bright light source, possibly the sun or moon, creating a bokeh effect.

# RightsWATCH. Data-centric Security

[www.watchfulsoftware.com](http://www.watchfulsoftware.com)  
[Info@watchfulsoftware.com](mailto:Info@watchfulsoftware.com)

Watchful Software  
Keep IT Secret

