# Secure Collaboration with RightsWATCH and Azure RMS

Email has evolved to become more than a way of exchanging brief messages, it's now the de facto method for collaboration of all types, regardless of the volume and sensitivity of data being exchanged. This creates a nightmare scenario for IT security officers: How do we protect and control access to sensitive corporate information across not only our own user base but also a myriad of third parties with whom they want to collaborate?

## Sensitive information and users you don't know

Organizations have long struggled with how to protect and control sensitive information that users demand to share with external parties, i.e. users that are not "known" to IT authentication systems. The users want simple and easy information exchange, while IT struggles with their mandate as guardian of the corporate information asset. This has been a show stopper for many organizations implementing Information Rights Management (IRM) as the default Information Protection & Control (IPC) technology for sensitive data. The key question has been, "if I can't validate the identity of a receiving party, how can I ensure our information is protected?"

## Letting advanced technology handle the complexity for you

RightsWATCH now provides a simple way to overcome the "External User" dilemma, enabling companies to flexibly collaborate between various business partners in a secure and transparent fashion that requires little effort from internal users.

Using RightsWATCH's seamless integration with Microsoft's Azure Rights Management (Azure RMS), users can share encrypted, rights-managed files as well as send protected, rights-managed email messages to external parties, without the overhead and complexity of IT staff "onboarding" and managing "outside" users in your system.

Leveraging RightsWATCH's powerful and unique integration with Azure RMS, users don't have to change their workflow, yet the information sent remains protected. Best of all, you have a level of assurance that the receiving party is in fact the intended recipient… and you control what they can do with it.

- Protect and control sensitive information being exchanged via email or files, regardless of whether the recipients are 'known entities' in your Active Directory

- Deliver seamless support for Microsoft's Office 365 and Azure RMS offering, regardless of how far along you are in your cloud adoption

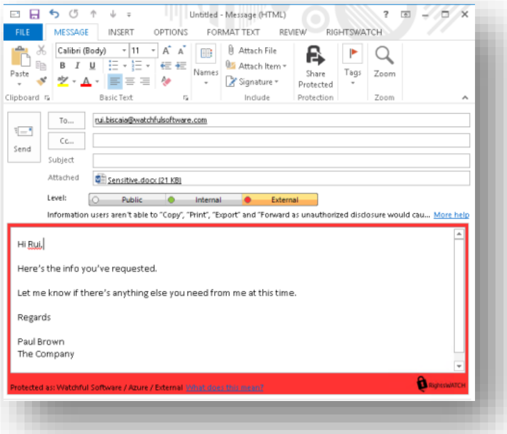
- Provide a simple way for users to exchange Rights Management protected emails and documents without changing their workflow

## Essentials of RightsWATCH to address the "External User"

RightsWATCH fully supports Microsoft's Azure RMS offerings to provide comprehensive data-centric security that works across classic network and domain boundaries.

## Encrypted email made easy

Your users can send emails to trusted third parties as normal, without any additional work or intrusion. Through the RightsWATCH content-aware policy engine, emails with sensitive information being sent to external users (a user "not known" to the organization) can be either manually or dynamically classified, marked, meta-tagged, and encrypted with an Azure RMS "Do Not Forward" (DNF) template.



To... rui.biscaia@watchfulsoftware.com

Attached: Sensitive.docx (21 KB)

Level: ○ Public ● Internal ● External

Information users aren't able to "Copy", "Print", "Export" and "Forward as unauthorized disclosure would cau...

Hi Rui,

Here's the info you've requested.

Let me know if there's anything else you need from me at this time.

Regards

Paul Brown
The Company

Protected as: Watchful Software / Azure / External What does this mean?

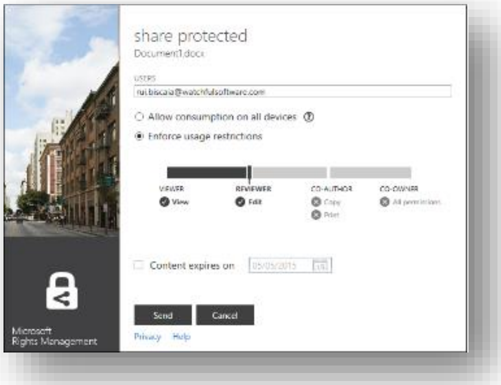
The receiving party simply opens the message as normal, as Azure RMS authenticates them as a valid recipient using either their corporate or 'RMS for Individuals' credentials. Usage rights are enforced on the email message, controlling their ability to perform actions such as copy, print, export or forward of any sensitive information.

## Enabling BYOD with full security

RightsWATCH also extends this ability to mobile devices, allowing users to exchange Azure RMS protected emails with external parties even when using their respective iOS and Android smartphones and tablets.

## In-depth collaboration with secure file exchange

In the case of an MS Office documents and other files, users can leverage the Share Protected capability provided by the Microsoft RMS Sharing App to exchange RMS protected files with "external parties".



share protected
Document1.docx

USERS: rui.biscaia@watchfulsoftware.com

○ Allow consumption on all devices
● Enforce usage restrictions

VIEWER: View
REVIEWER: Edit
CO-AUTHOR: Copy, Print
CO-OWNER: All permissions

□ Content expires on 05/05/2015

## Seamless User Experience

RightsWATCH leverages the Azure RMS 'trust fabric' to allow Azure to handle the credentialing and authentication – so that you don't have to. Your users see very little change in their workflow, and the external users can leverage either their company's Azure RMS credentials, or they sign up for a free 'Azure RMS for Individuals' account. The sign up process is simple and easy; anyone can sign up for Azure RMS HERE where they can select a Username and Password to have their free account provisioned.

Contact us today for more information on how RightsWATCH enhances Azure RMS.
More info at: www.watchfulsoftware.com and info@watchfulsoftware.com.