boldonjames
A QinetiQ Company

30 YEARS 1985 - 2015

SOLUTION BRIEF

# ENSURING PERSISTENT DATA PROTECTION

## STREAMLINING MICROSOFT RIGHTS MANAGEMENT WITH USER-DRIVEN DATA CLASSIFICATION

Data boundaries of organisation's are more permeable than ever before, and there is an increasing need for collaboration with partners, customers and other external stakeholders. Relying on encrypting and controlling access to static data appears increasingly inadequate as sensitive data needs to be shared and accessible to a mobile workforce.

Providing users with encryption tools can alleviate some concerns but may force your business partners to change their practices in order to work with you. A further challenge is for the users to understand which data needs protection and what protective controls to apply. Leaving the user to make these decisions gives rise to inconsistency as each user needs to understand the precise nature of the protective controls in order to correctly choose between them.

Traditional encryption solutions are good at protecting content as it passes between originator and recipient, but do nothing to control what the recipient may then do with that content once decrypted. Where businesses collaborate and share sensitive data, it is unlikely that staff from differing organisations can be relied upon to respect the safeguarding wishes of the data originator, leaving information vulnerable to mishandling.

Furthermore, the sharing of encrypted data can prevent IT solutions such as Antivirus, Search, Indexing and Data Loss Prevention (DLP) from delivering their full value.

# ENSURING PERSISTENT DATA PROTECTION

SOLUTION BRIEF

## THE CHALLENGE WITH RIGHTS MANAGEMENT

In today's mobile and collaborative world, protection needs to travel with data and that protection must be capable of including the usage rights for such data – that is persistent protection. It has been the responsibility of Digital Rights Management (DRM) solutions to deliver such protection, with Microsoft Rights Management, in the form of AD RMS, at the forefront. However, solutions such as AD RMS have remained difficult to manage and deploy, especially beyond the corporate boundary, and have proved difficult for users to grasp.

In response to these shortcomings Microsoft has introduced Azure Rights Management (Azure RMS). Microsoft Azure RMS is a powerful persistent content protection solution that encompasses collaborative scenarios and the breadth of today's mobile device platforms. It offers fine-grained control over who can see content, what they are allowed to do with it and how long they are permitted access. Azure RMS uses encryption, identity and usage policies to secure files and email, and it works across multiple devices—including phones, tablets and PCs. The protection remains with the data throughout its journey, for example, when a document is emailed to a partner company, or saved to a cloud drive. If you need to prevent a document from being printed or to block users from copying text from one document to another, Azure RMS will meet your needs.

At the heart of RMS is the concept of 'Rights Policy Templates'. A template is a set of permissions that are assigned to users via a Group Policy.

Users normally access the Azure RMS functionality by navigating to the 'Protect Document' menu within Microsoft Office. The menu item entitled 'Restrict Permission' shows a list of all the RMS templates. The user then selects the template that best matches the content they are generating.

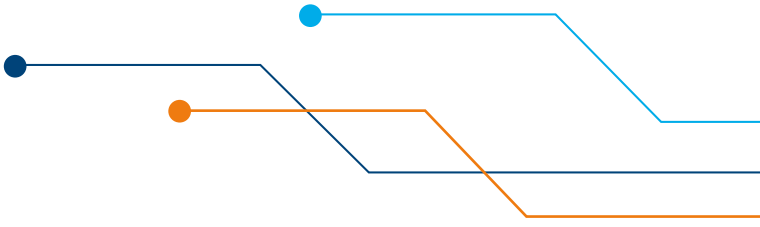
However, the user is given no assistance in identifying which information needs protection, has to remember where to find the permissions menu and to understand the differences between each of the templates before they can apply the necessary protection. In practice this process is disruptive to the workflow of the user and can lead to errors in selection resulting in a lack of confidence in the solution and, ultimately, low user adoption.

## THE SOLUTION: DIRECTING RIGHTS MANAGEMENT WITH USER-DRIVEN CLASSIFICATION

User-driven data classification captures the user's knowledge of the context and business value of the data they create and handle, so that informed decisions can be taken about how it is managed, protected and shared. Boldon James Classifier enables users to capture their understanding of the value and sensitivity of the data they handle in the form of visual and metadata classification labels. Based on the choice of label Classifier can then directly apply the appropriate persistent protection profile using Azure RMS without the user having to make further decisions.

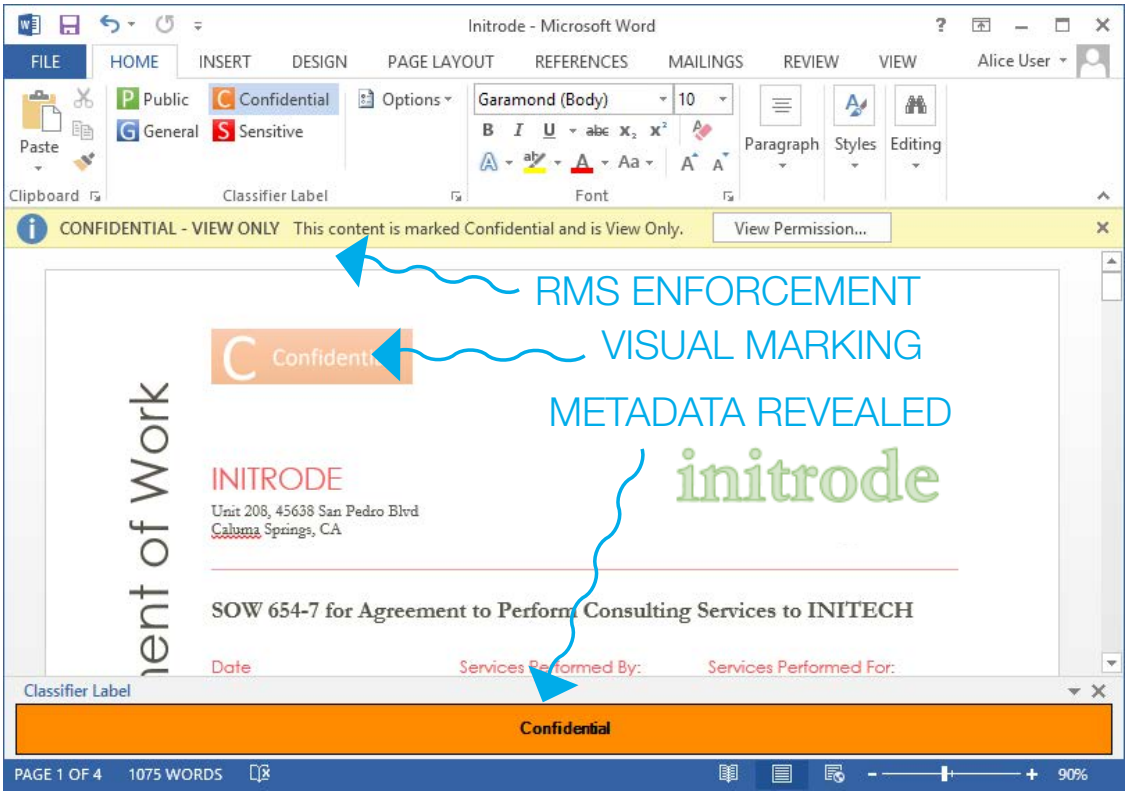
Boldon James Classifier simplifies and streamlines the whole user experience by automatically applying the appropriate Azure RMS Template based upon the classification that the user has selected for the document or email. In this way the user only has one simple choice to make around classification which is a selection that relates closely to their normal business activities and level of understanding. User-driven classification becomes part of a normal workflow and the choice of classification label effectively automates the entire Rights Management process.

To enable this automation the Classifier Administration Console allows the creation of an 'Apply RMS policy' rule. The Classifier Rules Wizard acquires and presents the full set of RMS templates that can be referenced by the rule. The administrator simply needs to select the RMS Policy that they wish to associate with the relevant classification label.



# ENSURING PERSISTENT DATA PROTECTION

SOLUTION BRIEF




## CONCLUSION

In today's digital world protection needs to travel with the data and that protection must be capable of including the usage rights for such data – that is persistent protection.
Microsoft Azure RMS makes persistent protection an effective proposition both in collaborative scenarios and across a wide variety of mobile device platforms.

Boldon James Classifier streamlines the process of applying the persistent protection afforded by Microsoft Rights Management, seamlessly integrating it into a familiar, business-centric workflow, whilst at the same time delivering more effective data protection and control. The ability to secure sensitive corporate data in a consistent and accurate manner both within and beyond the organisation, whilst at the same time addressing legal and regulatory compliance, creates a compelling solution for any organisation.

### ABOUT BOLDON JAMES

For 30 years, Boldon James has been a leader in data classification and secure messaging solutions, helping organisations of all sizes manage sensitive information securely and in compliance with legislation and standards, in some of the most demanding messaging environments in the world.

Our Classifier product range extends the capabilities of Microsoft core infrastructure products to allow users to apply relevant visual & metadata labels (protective markings) to messages and documents in order to enforce information assurance policies, raise user awareness of information security and orchestrate multiple security technologies.

Our customers range from commercial businesses to Government, Defence & Intelligence organisations and we are a Microsoft Global Go-To-Market Partner and a Gold Application Development Partner. Boldon James is a wholly-owned subsidiary of QinetiQ, a FTSE 250 company, with offices in the UK, US, Australia and Europe and channel partners worldwide.

## More Information

CLASSIFIER

**FOR MORE INFORMATION ABOUT HOW YOU CAN TRANSFORM YOUR DATA SECURITY WITH A USER-DRIVEN APPROACH USING BOLDON JAMES CLASSIFIER, PLEASE CONTACT US OR CALL +44 (0)1270 507800.**