# THE 5 STEPS
## TO EFFECTIVE
## DATA PROTECTION ▶▶

**INCLUDING**

- **IDENTIFY YOUR CROWN JEWELS**
- **DISCOVER BEFORE YOU DEFEND**
- **CLASSIFY YOUR DATA**
- **SECURE YOUR DATA**
- **MEASURE AND EVOLVE**

## INTRODUCTION ▶▶

Every day your businesses are creating more and more data. Data gets saved, employees move on, data is forgotten and lost. Valuable information sits on your file servers and document stores, not protected and unrecoverable because no one knows where to find it.

Using data classification helps you regain control over your unstructured data. By involving your users in data classification, they will automatically become more data-aware, with a greater understanding of your policies and the value of your organisation's data.

This whitepaper will take you through the 5 steps to implementing effective data classification within your organisation, and detail how data classification can also enhance previously implemented tools, such as data loss prevention tools (DLP), data discovery tools, data overnance tools and more.

## STEP 1:
## IDENTIFY YOUR
## CROWN JEWELS ▶▶

Using data classification as part of a strategy to secure corporate data assets is sometimes referred to as 'locking up the crown jewels'. But data security neither starts nor ends with the act of controlling access to information. Nor

should a security policy be limited to protecting only the most valuable data; even less critical information can damage the business if it's lost or leaked at the wrong time.

First, you need to build a strong foundation of knowledge around your data, to understand exactly what you hold and the potential risks to its security. Picture your organisation as the Tower of London. If you don't know where your crown jewels (and less sparkly assets) are you'll end up locking every door – or leaving the wrong doors open, exposing them to risk.

This process begins with identifying the types of data that are of greatest importance to the business, so you can pinpoint where you need to focus protection and controls.

Your most valuable and confidential data (your crown jewels) might include:

- **Data assets -** such as the information on a CRM database
- **Business-critical documents -** including strategic plans and agreements
- **Documents or information that are subject to regulations**
- **Intellectual property (IP) -** such as product designs and technical specs
- **Personal information -** for instance employees' details

More often than not, however, a company's most vulnerable point will not be its crown jewels; it's likely they'll already have been recognised and heavily protected. It's the more everyday sensitive data that people don't think about, like customer lists, contracts, or time sensitive documents such as company results and press releases that are most likely to be leaked or lost. This data must also be identified and protected.

▶▶ **IBM estimates that between 0.5% and 2% of an organisation's data is 'critical' - in other words, it has a significant financial value to the company. This can account for up to 70% of brand or market value." ▶▶**

A helpful way of determining the value of a piece of information – and the risks to be managed – is to think about the impact if it was leaked or lost. Would it harm the business, for example by damaging the brand, incurring a fine from the regulators (for breaching the EU GDPR, for example) or eroding competitive advantage? If it got into the public domain, would it expose your customers, partners or suppliers? Would it put an employee's security or privacy at risk? Would you be breaching a contract?

Once you've defined the data that is most at risk, you can start to find out where your sensitive data is located.

## STEP 2: DISCOVER BEFORE YOU DEFEND ▶▶

By classifying data according to its value or sensitivity, organisations can reduce the risk of security breaches by ensuring that appropriate protections are implemented and consistently enforced. Having identified your 'crown jewels', and other data that needs safeguarding, it's time to carry out a discovery exercise to find out exactly what you've got, where it is and who might have access to it.

Unknown data makes you vulnerable to attack. The best thought-out security policy is ineffective if you're not certain what you hold and, therefore, what controls you need to put on it. Data governance, compliance with regulations such as the EU GDPR and ITAR and – just as importantly – demonstrating said

compliance are also impossible when you don't know where key documents reside and who has access to them.

A discovery exercise will give you visibility of your data and how it's being accessed and used. This enables the protection strategy and solutions to be built around the types of data you have. It provides an opportunity to cut retention costs, too, by disposing of redundant data; mid-sized organisations spend £435k per year on storing and managing obsolete data, according to the Vertitas Databerg report. Discovery also makes it easier to use data as a resource, deriving insights that will inform strategies and improve operations.

### ▶▶ YOU WILL NEED TO ESTABLISH: ▶▶

- **What data you hold**
- **What data is being collected**
- **What is being created**
- **Where it's stored or located**
- **Why you have it**
- **How sensitive it is, and**
- **Who is accessing, using or sharing it.**

Getting a grip on this is a challenge. Alongside structured data held in on-site databases, companies typically have huge volumes of unstructured data such as emails, PowerPoint decks, Excel files and PDF documents.

Information is also stored and shared across an expanding variety of systems, devices and platforms, including the cloud, collaboration tools like Microsoft SharePoint, file share sites

like Dropbox and OneDrive, and 'shadow IT' (unsanctioned tools and apps not designed for enterprise use).
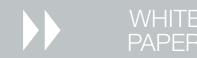
Data discovery tools and software provide an efficient and accurate way to find assets you can then classify. They examine file stores and databases, scanning for certain types of information, key words, criteria and classification metadata. This enables you to see what your data is, its location, and who has access. According to Forrester 44% of North American and European technology decision-makers use data discovery tools.

Once you've defined the data within your business you'll be able to home in on the most valuable and confidential information and make accurate decisions about how it should be handled, and who is allowed to access which files. You'll then be ready to classify it according to its importance or sensitivity to ensure data is appropriately controlled.

## STEP 3: CLASSIFY YOUR DATA ▶▶

A corporate data security policy that sets out how valuable information should be handled will be ineffective unless it's consistently and accurately enforced. Organisations often have a written policy that's available on their company intranet and handed to new starters. In practice, however, employees are rarely sure how to apply it to their daily activities.

The security policy needs to be made actionable – and the best way of doing this is with the classification of data. This is the first of the two steps that involve actively securing data, with the second being the implementation of technology solutions that will protect it downstream. Classification makes those solutions more effective.

# THE 5 STEPS TO EFFECTIVE DATA PROTECTION ▶▶

Data classification is the categorisation of data according to its level of sensitivity or value, using labels. These are attached as visual markings, and also embedded into the metadata of the file. When classification is applied in association with downstream security solutions, the metadata ensures that the data can only be accessed or used in accordance with the rules that correspond with its label.

It's possible to completely automate the process, but our clients get the best results when they combine human input with the use of software toolsets to support successful implementation. This is known as user-driven data classification.

With this approach the employee is responsible for deciding which label is appropriate, and attaching it at the point of creating, editing, sending or saving. The user's insight into the context around the data leads to more accurate classification decisions than a computer could ever make.

## DEFINING THE CLASSIFICATION POLICY
First, be clear on who should have access to each type of data. The work you did in steps 1 and 2 will prepare the ground for this. Next, decide how many categories you'll have. Aim for three or four – the fewer the options the simpler it is for users. Labels that indicate **Confidential**, **Internal only** and **Public** are a good start, with perhaps a fourth category relating to information that's subject to regulatory controls – such as EU GDPR, ITAR controlled or HIPAA/HITECH restricted.

## SELECTING YOUR CLASSIFICATION TOOL
The right technology will help your users to consistently apply the classification scheme, and will also add the all-important metadata. The most effective tools make classification a seamless part of business-as-usual; integrating the labelling process into the standard applications employees already use. Ensuring breadth of coverage across operating systems and application types is vital to future-proof your investment.

## ROLLING IT OUT
Start by classifying your 'live' data – the emails, files and documents that are being created and handled right now. If you've followed steps 1 and 2 you'll know exactly what and where it is. By doing this, you're ensuring that all your 'crown jewels' will be safely locked up from this point forward. When that is established decide how to label the existing and legacy data that is stored and held around the organisation. This process usually works well in combination with a discovery agent or tool.

Once you've labelled your data, it's time to turn your attention to the enterprise security solutions and information management technologies that will control and protect it throughout the remainder of its journey.

# STEP 4: SECURE YOUR DATA ▶▶

Data that is classified according to its sensitivity instantly has a layer of protection surrounding it. The next task (having identified, discovered and classified your data) is to put in place the higher grade controls – in the form of enterprise security and information management solutions – that will safeguard it when it's accessed or used later. By classifying first you'll already have added the 'magic ingredient' that makes

these solutions more effective: the metadata sitting in the properties of each document, message or file.

The embedding of the label as metadata supports the consistent enforcement of data security policies by directing the actions of downstream solutions – triggering automatic rules that correspond to the label the data has been given. This means the technology makes more accurate 'decisions', reducing the false positives that slow business down and minimising the risk of data being exposed because it isn't recognised as sensitive. It also supports governance, compliance and data management efficiencies.

Solutions that become more effective when combined with data classification include:

### DATA LOSS PREVENTION (DLP) SOLUTIONS
These will shield the business against intentional and accidental data loss by, for example, blocking employees from uploading a file marked 'Confidential' to Dropbox, or stopping a file containing credit card numbers from being emailed to a third party.

### EMAIL GATEWAYS
These will automatically encrypt any file marked 'Confidential'.

### DISCOVERY TOOLS
Enabling employees to rapidly locate information and understand instantly how it can be used.

### SECURITY INCIDENT AND EVENT MONITORING (SIEM) TOOLS
These pick up on potentially risky user behaviour before a breach occurs – flagging up, for example, if someone keeps copying sensitive documents to a storage device. Concerns can then be addressed through training or strengthening of policy.

### SEARCH AND RETRIEVAL TOOLS
Making it easier to keep an audit trail and quickly find documents needed to prove compliance with industry standards, or to meet information requests from regulators.

### ACCESS CONTROL TOOLS
These use classification labels to dictate who can access a file in a shared area.

### DATA GOVERNANCE TOOLS
The label enables these to audit who is accessing sensitive information, and who might be violating policy, keeping a detailed audit trail of any risky behaviour or activities. This also supports the demonstration of compliance.

### DATA RETENTION
When you've marked what's valuable, you can more clearly see what isn't important or needed, and therefore what can be archived or deleted. Retention rules can also be set for different classifications – for instance, 'keep this type of file for 10 years' or 'expire after 6 months' – perhaps for files which should not be held for legal reasons.

The effect of integrating data classification with other security technologies and toolsets is that of adding layers of security around your 'crown jewels' and other sensitive data; strengthening the walls and creating an 'inner sanctum'. But data protection doesn't stop there. Like any walls, you have to keep checking and maintaining them to keep them intact.

## STEP 5: MEASURE AND EVOLVE ▶▶

If you have followed the first four steps in this series (Identify, Discover, Classify and Secure), you'll have successfully secured the organisation's valuable and confidential

information by using data classification and downstream toolsets to enforce the security policy. It's not 'job done' yet, however.

Legislation, threats (external and internal) and the business itself will constantly evolve, while demands from regulators and the board for better governance will intensify. Ongoing measurement of the effectiveness of your security policy is the only way to check that the controls you've put in place remain fit for purpose.

The monitoring of classification activities is a powerful way of doing this. Monitoring and reporting tools track how data is being accessed, used and classified, and provide visibility to the business via structured audit data and analytics.

This improves the chances that a breach will be quickly detected – helping the business to comply with notification periods required by regulators, as well as to minimise damage. If there is a breach, the detailed audit information will allow you to demonstrate that the appropriate steps to protect data were taken.

More importantly, real-time monitoring of how people use classification tools will allow any behaviour that deviates from 'normal activity' to be identified and addressed before a breach occurs. This could include flagging up a user who repeatedly labels documents incorrectly, and therefore might represent an insider threat. The clear audit trail of activity also enables compliance with legislation to be measured and demonstrated to government and industry regulators, many of which have strict auditing and reporting requirements.

Ongoing monitoring builds an organisation-wide picture of how effective the security policy is – a picture which can be shared with the board – along with an understanding of how to improve it.

> ▸▸ **Using data classification software removes the need for manual workarounds, helps organisations enforce a classification policy and ensures their employees are following the same guidelines in a consistent manner** ▸▸

Using a classification reporting tool in conjunction with a security incident and event monitoring (SIEM) solution and a behavioural analysis toolset is the 'gold standard' in situational awareness. The combined data makes it possible to forensically analyse an individual's behaviour to establish the cause, as well as to highlight broad behavioural patterns and trends. If a large number of people regularly under-classify documents, for instance, this may indicate a weakness in the policy or simply show that it's not properly understood.

This insight will equip you to make informed decisions about how to address the issue: through tightening the security policy, providing further training, or carrying out disciplinary procedures.

Integrating monitoring and reporting capabilities into the data security strategy is the only way an organisation can fully realise the value of its data classification and other security solutions. Measuring effectiveness will provide the intelligence needed to evolve the strategy in line with threats and business changes. It will also give you the information you need to demonstrate value – proving that the solutions purchased are delivering expected benefits and ROI. This assurance will communicate the value of the security organisation, and secure the future investment that will keep the 'crown jewels' safely locked up for good.

# THE 5 STEPS
# TO EFFECTIVE
## DATA PROTECTION

## ABOUT
## BOLDON JAMES ▶▶

For over 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.

Global brands trust us to protect their sensitive data:

**BARCLAYS**  Ministry of Defence  **Honeywell**

**PRUDENTIAL**  DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA ·  **AMGEN**

**SOCIETE GENERALE**  **Allianz** ⑩  **Raytheon**

## More Information

Ⓒ**LASSIFIER**

FOR MORE INFORMATION ABOUT HOW YOU CAN IMPLEMENT A DATA CLASSIFICATION SOLUTION AS PART OF YOUR DATA PROTECTION STRATEGY, PLEASE CONTACT US OR CALL +44 (0)1270 507800.

ALTERNATIVELY REGISTER FOR A LIVE DEMONSTRATION OF CLASSIFIER. ▶▶

**boldonjames.com**

REQUEST A DEMO OR CONTACT US