ENTERPRISE DATA **CLASSIFICATION:**

Enhancing Microsoft MIP In An Era Of Enhanced Regulatory Obligation

Why you need best-of-breed data classification

titus
by HelpSystems

Table of contents

Introduction

The data protection landscape and its associated compliance environment changed fundamentally with the implementation of the European-wide GDPR in May 2018, with many other privacy regulations following suit around the globe. It is no longer about what organizations think they need to be doing in order to control their data, but that they are being told what they need to do by regulators such as the ICO. Since the implementation of such data protection regulations, record fines have been issued, and these serve as a clear statement across the board that organizations simply cannot afford to ignore or fail in their data protection compliance obligations.

The main (but not the only) reason that organizations look at classifying the data they create and handle is to ensure that sensitive information can be controlled. A big part of designing a classification policy is understanding what data is sensitive, what is less so, and what is not. Who should have access to this information, and whether you should be holding that information, archiving or deleting it.

Organizations have myriads of relationships with external suppliers, partners, and vendors. When designing a classification policy, other aspects need to be taken into account, such as the way we communicate with external organizations. Just as organizations thrive from inter-dependent relationships, so should their data security tools. Classification has the ability to make so many other tools much more effective, whether that is DLP, discovery, RMS and many other applications that are considered important in the fight to keep data secure. Just as there is no "one-size-fits-all", there is also no "one-stop-shop" – no single solution or magic bullet. Instead, what is important is how the best-of-breed tools can work together to create a seamless and highly effective solution.

There are vendors today offering "one-size-fits-all" security solutions, which as a result, only support very basic classification (or labeling) functionality. This is a weak foundation for such a fundamental security component, and this approach causes more pain downstream as your business grows and evolves, and more granular classification requirements emerge.

The challenge for organizations today is to successfully negotiate complexity with a classification policy that works, and a tool that is incredibly flexible and configurable, but still easy to use. A best-of-breed classification tool should not be complex to work with, it should in fact, hide complexity. It should fit seamlessly into how end users work on a day-to-day basis. The bottom line is that complexity will not go away, and if you are having to design a classification policy around the limitations of a classification tool, then frankly, you are using the wrong tool.

Whether it is roadmap flexibility, technology integration and interoperability or support for applications and file types, your classification vendor choice must support the needs of your organization not just now, but well into the future.

> *"As much as Microsoft would like for everyone in enterprise IT to simply apply Microsoft RMS to every file type and buy EMS E3 or E5 licenses, this is simply not an organizational or operational reality at present. Not every device operating system or file type in use is from Microsoft."*
>
> Source: Gartner Enterprise DLP Magic Quadrant 2017 (Deborah Kish, Brian Reed)

Why data classification is critical for business success

Quite simply it is foundational; business can't function successfully without it. It's the unifying factor for all your information security and data management solutions – hence data classification must be robust, flexible, and all-encompassing.

Gartner states, *"Focus on controls that broadly address the problem, such as implementing people-centric security and data classification. These controls are the foundation upon which additional controls can be built."*

This is enforced up by Forrester:

Forrester Research say *"If you don't know what you have, where it is, and why you have it, you can't expect to apply the appropriate policies and controls to protect it."*

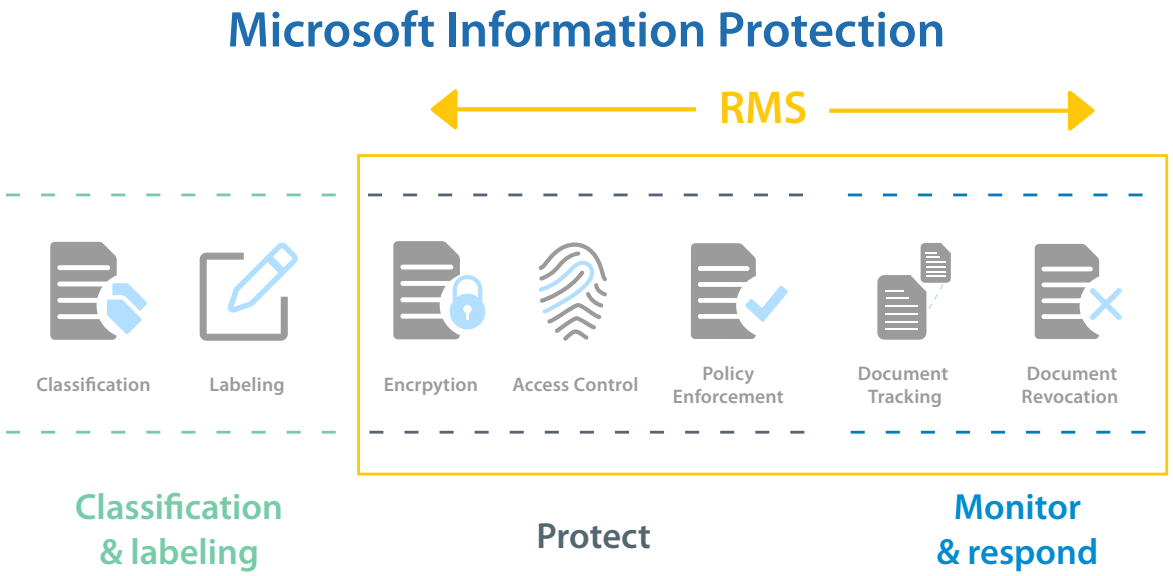
In the world of enterprise data protection and data classification, the requirement for a flexible solution combining best-of-breed functionality with sophisticated policy support is considered critical.

What is MIP?

The Microsoft Information Protection (MIP) suite is a "one-size-fits-all" security solution aimed principally at applying Rights Management rules to individual pieces of data; in particular, it provides a heavyweight application of Encryption techniques to frustrate hackers and would-be data thieves. Other Microsoft extensions, (for example, CASB), are available but the medium to large corporation is going to need something more sophisticated that meets its needs. The MIP labeling and classification interface is limited, falling short of the key compliance and governance metrics that larger organizations must meet and, by design, provides limited metadata relying on broad-based encryption and blunt post-delivery controls.

MIP encompasses Classification, Labeling and Protection (CLP):

- **Classification:** Data can be classified automatically or by users. Classification and labeling information are embedded in the document metadata and defined actions are enforced.
- **Labeling:** Visual and metadata labels record the classification and are embedded within a document.
- **Protection (Rights Management):** Azure Rights Management (RMS) encrypts the document and includes the authentication requirements and a definition of the use rights to the data (i.e. rights management). This ensures only authorized users have access to protected data and they can perform only allowed actions on the data.



Where did MIP come from?

Historically organizations have struggled with the complexity of implementing a Rights Management solution, principally because the User Interface was virtually impossible to implement successfully. As a result, Microsoft decided to add a simple data classification solution to try and increase uptake of its flagship Azure RMS product. Both facilitate movement of large organizations to Microsoft's Azure Cloud and to tie customers more closely to the Microsoft ecosystem.

Labeling within MIP has its limitations

There are a few points (below) to consider when looking at the capabilities of MIP labeling in the context of the new landscape of increasingly tight legislation, and regulatory authorities prepared to levy hefty fines to organizations which fail to comply. It makes sense, therefore, to integrate a best-of-breed classification solution, working with MIP, to hit the higher expectations of the regulators:

- **Limited metadata, 2 user-defined fields, 1 for sensitivity with two levels.** Cannot do CUI, ITAR and many other regulations.
- **Limited policy, as the conditions to control labeling are very limited.** For example, with Titus you can check to see if someone resigned in Active Directory or PeopleSoft and prevent downgrades which prevents people who are leaving from taking information.
- **If you create a PDF from Office using MIP, the labeling is lost.** Not with Titus.
- **Titus can classify any file on Windows.** MIP cannot.
- **MIP does not check meeting invites** which can have sensitive information included.
- **MIP is limited to a fixed framework.** Titus can run anything that can be run on a Windows machine.
- **Limited flexibility around the classification schema.** Only one value can be selected, only from a drop down list.
- **Limited flexibility in the visual markings applied.** Crude markings, limited formatting and content, no user control over whether they are applied.
- **Limited flexibility around metadata applied to an item.** Only able to read other metadata as part of a migration and then only from certain locations.
- **Limited flexibility for the user experience.** No ability to tailor the UI and messaging. Little user assistance.
- **Limited flexibility around the policy engine that is the foundation for the product.** Relies on other tools and products which results in a less favorable user experience.

This is further underlined by Gartner –

> *"MIP is best suited for organizations with a long-term Microsoft roadmap, but the cloud services requirements for its enablement may limit its appeal among highly regulated or conservative organizations with a strong preference for on-premises products."*

'Quantify the Value of Microsoft Enterprise Mobility + Security Suite E3 and E5 in Microsoft 365,' Various Analysts, December 2020

How can you enhance MIP?

In the world of enterprise data protection and data classification, the requirement for flexible solutions combining best-of-breed functionality with sophisticated policy support is viewed as critical. Most organizations initially adopt a heavily simplified classification policy, but shortly after implementation of a generalized solution they find it necessary to expand and adapt that policy as their maturity and experience in the use of data classification increases, and they encounter new business and regulatory challenges. This evolution continues as the business grows, to accommodate new business processes, organizational structures and the adoption of new IT and data governance solutions. This is why it is critical for any data classification solution to support not just the initial project requirements, but also the ongoing and future requirements of the business. Often organizations will not fully understand what their future needs will be, hence why it is important for the selected data classification solution to be able to evolve and grow with the business.

The MIP Ecosystem

Ecosystem Type	Titus Compatibility
RMS ecosystem A well-established ecosystem delivering the Protect part of MIP's Classify-Label-Protect	Titus data classification is a long-standing participant in the RMS ecosystem of Azure IP – facilitating and simplifying the use of RMS and linking classification to the assignment of rights. However, Titus opens up choice in terms of protective technology, enabling organisations to choose the most appropriate solution, including support for a mix of protective technologies
Labeling ecosystem A new and embryonic ecosystem based on a metadata framework for classification labeling – the Label portion of MIP's Classify-Label-Protect	Titus data classification is already a participant in the new MIP labeling ecosystem – giving customers new options and flexibility when constructing a classification solution

The partnership of Titus and MIP offers the benefit of MIP's integration with Azure protection applications combined with a huge range of enhanced functionality to allow your data protection landscape to evolve and grow. Augmenting Microsoft MIP with Titus data classification is a simple addition that will not disrupt your current MIP classification structure, but adds functionality and benefits, together with the ability to customise the user experience and classification schema with a powerful, best-of-breed solution.

Why you need more than just MIP

1. Protecting data costs you money so it is vital to create a solution which delivers the right approach

We know that all organizations create a significant amount of data.

- Some data is essential business information
- Some data belongs to your partners
- Some data is personal and private to your staff or your customers
- Some data is Intellectual Property
- Some of it is public
- Lots of it is for the trash bin

All data costs you money just by its existence, but not all data is equal. Meeting your compliance needs by universally restricting access, rigorously protecting it all to ensure it is not lost, stolen, or impaired will cost you more. Treating all of your data as if it is your "Crown Jewels" and using RMS to encrypt and apply post-delivery controls because you simply don't have a reliable method of assessing individual data files value, is expensive and inefficient.

Your organization needs to know the value of each piece of data as it is created:

- Your SAP or cloud-based CRM as data is downloaded,
- Your finance team as they discuss salaries,
- Your HR team as they manage pension and health data and,
- Most of all your customers and partners as they share their data with you.

So why don't you let your users tell you what the value is by combining tools which give them the power to differentiate and give the data utility, rather than arranging it into big, generic buckets.

Why you need more than just MIP

2. Compliance is a growing challenge

We have seen already how in today's highly regulated environments, achieving compliance across numerous data privacy laws and regulations is a growing challenge for businesses worldwide. Recent Forrester research showed that of the global security decision makers surveyed, a significant proportion have not yet invested in data discovery and classification (45%) in their efforts to fulfil compliance obligations. One thing that is certain is the growing complexity within the compliance landscape will increasingly impact organizations, not just in terms of regulatory fines and financial costs, but also in reputational damage should they be breached.

With the emergence of regulations such as GDPR, CCPA, CMMC, CUI, and ITAR as well as many more regional based regulations globally, there has never been a greater need to ensure the data your organization is creating and handling is appropriately protected. Combining MIP and Titus data classification gives the ability to offer the level of granularity required for compliance with many of these regulations. Seek out a best-of-breed, specialist solution provider who can provide the foundational expertise and regulatory knowledge necessary to accurately deliver the level of data security you require against all your different data categories.

Why you need more than just MIP

3. Your solution needs to be powerful, flexible and futureproofed

Standard classification might be where you start, but it is highly likely it won't be where you end up.

There are a number of reasons why organizations increasingly need to accommodate more complex changes to their classification policy, for example:

- New global data protection regulations
- Retention and reporting requirements vary when businesses operate in multiple jurisdictions
- Merger and acquisition activity demands changes in business structure
- Diversity in business operations drives a need for policy change (e.g., new product, service, division etc.)
- The ability to support changes in supply chain and business processes, for example, interoperability with partner classification schemes
- Ensuring adaptability for different end-user communities, for example, based on skill set
- Support interoperability with new systems and toolsets

As explained earlier, Microsoft views MIP labeling as a mechanism to drive RMS, therefore, only supports a moderate level of classification (or labeling) functionality. You may also find the single use case that you start off with (Titus would describe this as the 'Walk' stage) does not evolve with the growing needs of the business. This is a weak foundation for such a fundamental security component, and can cause more pain downstream as your business develops, and as more granular classification requirements emerge. Microsoft acknowledge these requirements, and appreciate that for some organizations, the need for a more sophisticated data classification functionality is a business necessity: one-size doesn't necessarily fit all situations.

The challenge comes when you look at evolving your business, and security and regulatory requirements inevitably change. Basic solutions will limit future flexibility, which will be required as the business expands, new partners and suppliers become part of a wider supply chain, and new regulations enforce ever higher standards of data protection. There is a high probability you will find that the simplistic approach you start with will not meet the organization's ongoing needs. This is where Titus wins, and it is key that IT decision-makers understand the importance of planning ahead to futureproof their data protection.

For the reasons identified above, organizations need to think about future classification needs upfront, not as an afterthought.

Why you need more than just MIP

4. Your technology ecosystem is more than just Microsoft

Given the pivotal role of data classification, it is critical to most organizations for a classification solution to integrate and interoperate with a wide range of complementary security and data management solutions. This ecosystem is broader than Microsoft's environment, meaning MIP is disconnected with all your other security and data management solutions, increasing management overhead, reducing your security effectiveness, and lowering your return on technology investment. MIP can integrate with third party solutions but only at a low level "one-size-fits-all."

Adding in Titus enables organizations to capitalise on the heavy investment put in to creating strong end-to-end integrations, from OEM partnerships to metadata integrations. Titus data classification's best-of-breed functionality enables CISOs to create a tailored data protection environment that supports their wider governance, compliance, and security requirements.

From mainstream vendors like Forcepoint, McAfee, and Microsoft to niche solution providers, Titus strives to create plug and play technology that allows you to introduce new services, or change security solution provider, without negatively impacting your business or users.

5. Business requirements must remain a priority

During the planning process, an organization will set out a list of requirements that they need a tool to adhere to. While some of these may align to regulatory compliance, others may be solely for internal and departmental use. It is important that during the implementation of a data classification solution that the business requirements of the tool remain a priority – they have been drawn up for a reason.

Microsoft MIP's labeling functionality is limited, and as a result, organizations are often required to reduce down their business requirements in order to fit their policy into the software. No organization should have to sacrifice a requirement to fit in to a solution, but instead should build on the MIP estate with additional functionality, such as Titus, which has the power and flexibility spoken about earlier to mould the solution to fit the business requirement. The increase in global data protection regulations mean that policies are only ever going to require further granularity, something MIP will struggle to deliver alone. Titus offers data classification that can not only be built to the desired level of granularity upon installation, but is also capable of expansion as and when the organization needs it.

Why you need more than just MIP

6. You need coverage beyond basic Office applications

MIP only provides classification coverage for some products in MS Office suite. Titus brings classification to the widest range of productivity tools on the market – from deep into MS Office (including Visio and Project), MS SharePoint (including SP Online), MacOS and Google Workspace, through to specialist CAD tools.

Why is it important to cover so many applications and platforms? Regulatory compliance is not just about protecting your MS office files. If you simply rely on MIP (or other classification providers) to provide holistic data classification services across your entire data estate, MIP's file type limitations will result in piecemeal or fragmented coverage at best. In short you will only achieving a part of your compliance obligation. Furthermore, without complete coverage for all your unstructured data, you won't get the value and ROI from your classification solution.

Why you need more than just MIP

7. Pay for incremental value

As stated previously, MIP is just a part of the wider Microsoft proposition and the tool comes with a certain amount of limitations when it comes to classification. These can leave organizations exposed when it comes to newly mandated data privacy controls and compliance obligations. It is, therefore, a worthwhile exercise to consider if MIP gets you to where you need to be, or is it a case of spending more to build in additional functionality to create more granular solution.

It may also appear that MIP comes for "free" with the wider enterprise-wide Microsoft license, which can be seen as appealing. The reality is of course, that there is still a charge for data classification – the costs are simply embedded within the broader deal. Since there is a cost, the cost-effectiveness of MIP needs to be considered.

There are, of course, instances where using MIP alone will provide an effective solution to an organization's data classification requirements. However, many industries are seeing legislation becoming an increasingly determinant driver governing the way processes have to become more stringent in the way data is controlled and protected. Requirements are becoming focused at a much more granular level at both a local and international level. Therefore, it is important to evaluate whether you are really getting suitable value for money from using MIP alone.

8. You need increased visibility of user actions

Adding Titus data classification empowers administrators with an extensive reporting module, enabling you to drill down into how and where your classifications are being applied. Titus data classification comes with a range of common report templates, simplifying analysis to help you to understand where rules could be appended or automated. Titus' reporting dashboard is ideal for communicating trends and usage regularly to senior management. Titus data classification also directly integrates with third party analytics tools such as Splunk, for example.

9. Looking at the bigger picture

It's important that organizations look at the bigger picture when thinking about their requirements of a data classification solution, rather than getting bogged down in the minutiae.

Organizations need a solution that delivers a fully customizable experience, ensuring data is protected exactly how it needs to be in order to maintain regulatory compliance, which as we have previously stated, is now not a "nice to have," but critical. Titus' roadmap agility and responsiveness to change requests is something that our customers value. This might be feature led enhancements, or support for a completely new platform or application. Titus has over 35 years' experience in working with customers to rapidly develop software products that meet both their exacting needs, and those of an increasingly demanding and regulated marketplace.

Detailed use cases

The following use cases provide just a sampling of what is possible when using a best-of-breed data classification solution to enhance the framework provided by Microsoft MIP. With a Titus deployment, the scope of your data security program is limited only by your imagination and willingness to protect your investments.

Classify on print

It's not uncommon for internal bad actors to copy sensitive content, paste it into Word, and then print that document – either to a physical printer or to PDF – in an attempt to circumvent corporate security policies. In this situation, Titus will apply markings, metadata, and even rights management, while MIP does not have the ability to run against this event.

Calendar invitations

Attaching sensitive files to an Outlook calendar invitation can provide an accidental loophole in your security posture. Titus has the flexibility to run policy in this situation and provide a myriad of actions. MIP does not have the ability to run in calendar invitations.

The two use cases above are examples beyond MIP's capabilities. Below we will explore 3 further use cases where Titus can provide additional capability on top of the MIP framework.

Ethical wall

This use case often comes up in banking where the brokerage business and the banking business are prohibited from exchanging information. More commonly, there are cases where material of a sensitive nature can only go to one external domain at a time. Titus can be configured to detect, warn, or even prevent information going to multiple domains based on the specific requirements of an organization's ethical walls.

Sensitivity drift

Titus can automatically adjust the sensitivity of files, documents, and emails with or without rights management, based on certain dates. For example, a major event in which all material goes from Restricted to Public upon launch, such as press releases, data sheets and other related documents. Titus can further provide a fail-safe approval where the date to be met is reached, but the final approval still rests with a senior manager, if required.

Other use cases

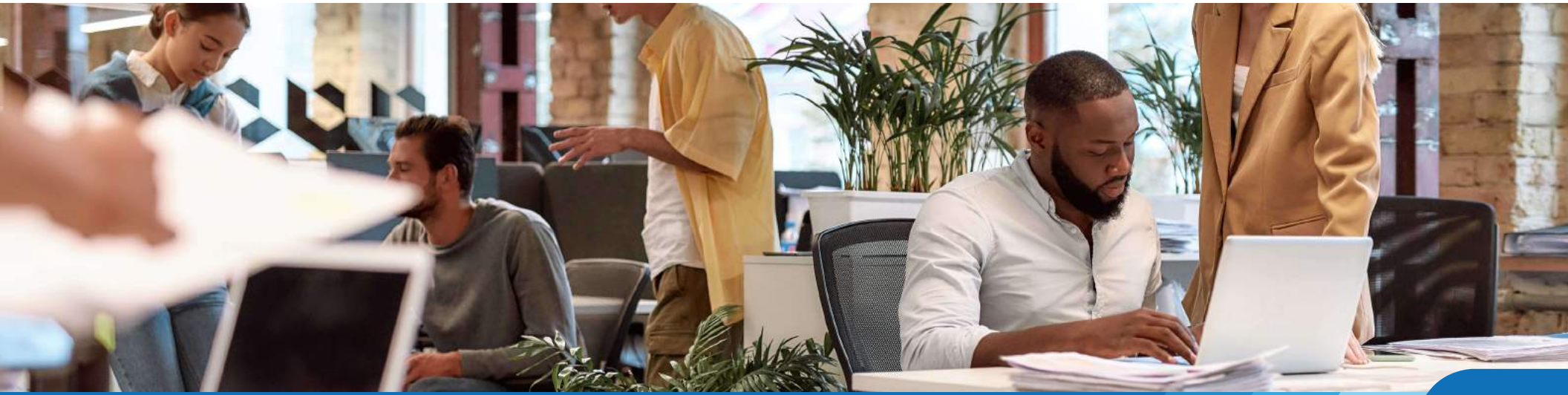
Optical character recognitions, completely automated detection of sensitive information with natural language processing, expert systems decision trees with guided selection for users can all be created with Titus. Titus can easily be extended to support new platforms for extensibility. Support for a variety of rights management vendors and the ability to trigger from metadata on a cloud platform other than OneDrive are among the use cases in which Titus enhances MIP.

Conclusion

Titus data classification is fully compatible and interoperable with MIP, adding significant value to the labeling, meaning that organizations can incorporate elements of MIP if they wish, but then enhance that functionality with Titus. This approach, by combining the best of a mass-market product in MIP, incorporating Azure RMS, and best-of-breed classification in Titus provides organizations with significant added value; advanced classification policy, coverage for the widest range of Microsoft and non-Microsoft applications and access to an extended technology ecosystem being just a few examples.

MIP provides a level of data classification which may be satisfactory for current levels of legislation, particularly if a business is localised or active in an industry where data protection is not highly regulated. If this is currently the case (which is becoming increasingly unlikely even now), there is something of an expectation that all business over time will have to comply with some form of data protection legislation at some point in the future. As many organizations are now finding out, historical standards are rapidly becoming redundant against modern-day data protection requirements. With a multitude of existing, and the increasing emergence of new data protection regulations, organizations need to be asking themselves if the functionality MIP provides suits current and ongoing needs when it comes to remaining compliant. This is especially important when considering the business-crippling fines that are being levied against organizations found to be non-compliant with the regulations set by governing bodies. For example, GDPR sets a maximum fine of €20 million or 4% of annual global turnover – whichever is greater – for infringements, with examples of significantly upward of €100m for large businesses being seen.

Taking a combined approach to enterprise information protection with enhanced data classification at the core enables policy issues and integration requirements to be tackled together to deliver maximum value for your business – ensuring organizations can meet the classification challenges identified today, plus those that will be introduced around the corner.



titus

by HelpSystems

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

© HelpSystems, LLC. All trademarks and registered trademarks are the property of their respective owners.

tt-gd-0621-ml