FORTRA

WHITE PAPER (Titus)

Data Protection in the Enterprise

Titus Classification Suite or Azure Information Protection?

Every organization is challenged by exponential data growth. In fact, data now forms the very core of many business endeavors. At the same time, cybercrime continues to increase and has only become more sophisticated. Hackers want to obtain critical business data but also personal information belonging to organizations' employees and customers.

Because of this increase in data-related crimes, organizations must take special precautions to protect their sensitive data. Legislation such as the General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA) help ensure that individuals' personal information is protected by requiring organizations to comply with increasingly strict rules for handling data.

Unfortunately, many organizations don't even realize they are at risk because they don't know what sensitive data they have or where it is located. Taking stock of your data is the first step toward protecting one of your most critical business assets.

Data identification technologies help you understand the types of data you have and where it resides. Understanding more about your organization's data enables you to set information handling policies and educate users. Redundant, obsolete or trivial data, aka "ROT," can often be safely discarded under a defensible deletion policy. If it's personal information or sensitive business data, however, you need to take measures to protect it and ensure that users know how to handle it.

A data classification solution not only helps identify the data in your IT environment, but it monitors your data at creation and as it moves throughout your organization. These solutions apply labels — or classifications — to emails and documents and also help put your data handling policies into action. You can configure settings to delete old data, encrypt sensitive data when it's sent outside of your organization, and ensure that you are in compliance with regulations.

When it comes to implementing a data classification solution, you have several options and it's critical to find one that supports your unique business needs. If you want to develop a stronger privacy strategy, start by establishing your secure information handling policies and then find the technologies you need to enforce them. Don't alter your policies to fit the technology.

This white paper considers why some organizations might select Microsoft's Azure Information Protection for their data classification needs and explains why Titus Classification Suite is a far better option for all but the most basic use cases.

An Easy Option?

While most organizations understand the need to protect personal data, many don't have the people or mechanisms in place to execute a privacy solution that works. Because so many businesses use Microsoft products — from Office applications to developer tools to cloud technologies — many end up using Microsoft's data protection tool, Azure Information Protection, by default. For companies new to privacy protection, Azure Information Protection offers a way to begin to understand what constitutes sensitive data and how to categorize it. However, if your organization generates a complex range of data types and must meet growing privacy regulations, the capabilities in Azure Information Protection may be too narrow.

Let's take a closer look. This cloud-based solution helps organizations label, classify and protect their documents and emails. For Microsoft customers, it may seem like an easy way to implement a data classification strategy because the solution often comes bundled with other Microsoft products. Many organizations already own it.

Azure Information Protection can scan documents that reside on network endpoints, servers and in the cloud to identify well-defined patterns such as credit card numbers and social security numbers. Similar to those found in most data loss prevention (DLP) solutions, these built-in scanning tools lack the ability to understand context. And the ability to evaluate context is crucial for locating sensitive personally identifiable information (PII), which is often written in a more narrative format.

Azure Information Protection attaches labels — also called "tags" — to files and emails to alert users to the level of sensitivity of the information contained within. For example, a file including credit card information could be given a "Confidential" label. The solution also can apply metadata to emails and files to help classify information. Metadata contains details about the document type, the information contained within the file as well as how it should be handled. Azure Information Protection can apply classifications automatically based on rules and conditions defined by administrators at your organization or manually by your users.

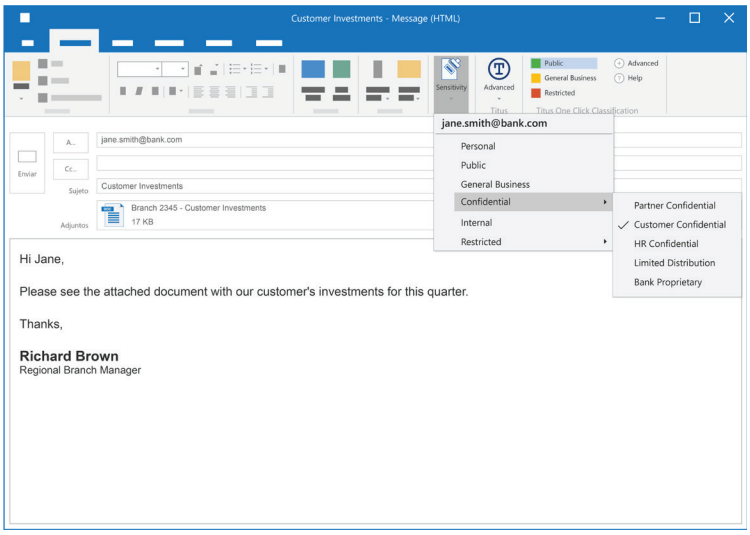
With Azure Information Protection, users can tag a file with only two levels of customizable identification. The top-level tags relate to the sensitivity level — for instance, Non-business, Public, General, Confidential, and Highly Confidential. Each top-level label can have one sub-level label, such as Directory Groups, FTEs, Custom Lists or Anyone/No Protection. For all but the most basic data protection scenarios, two labels may not be enough, however.

Azure Information Protection can also assign a Rights Management System (RMS) policy based on any particular label set, but the policy options are limited to those defined within the Azure Information Protection system. The solution

"The ability to evaluate context is crucial for locating sensitive personally identifiable information."

can apply encryption, access control, usage policies and auditing to files. This functionality works well with Microsoft Exchange, SharePoint and OneDrive for Business. However, only authorized users can open files and only from devices with software that can enforce the policies. Recipients of encrypted files who lack an Office 365 or Azure AD identity would need to sign up for Microsoft's Rights Management Service (RMS) for individuals and install the Azure Information Protection client or mobile device app. This process can be pretty cumbersome, especially when you simply want to share a project file.

If an organization truly wants to use a single vendor for all of their IT needs, Azure Information Protection does offer the bare minimum requirements for data classification. You can configure the program to classify documents with the two-level limit on details. Azure Information Protection allows you to embed metadata and trigger RMS, but again, those policies are solely pre-configured and Microsoft-based. You do not have the ability to customize your own deeper policies and rules or apply them at a very granular level. In addition, actually getting it up and running in a way that will meet all of your privacy and data protection needs can be cost prohibitive.



Azure Information Protection offers only two levels of data classification, which may not be granular enough to truly protect your sensitive customer, employee, and business data. The program often requires custom development to integrate with your other security technologies, and its very basic classification capabilities might not be flexible enough to close potential security gaps in your daily workflow.

A Better Option

Titus Classification Suite offers sophisticated data identification and classification capabilities, including a highly flexible policy engine driven by machine learning and extensive security ecosystem integration. You get the flexibility to tailor a data classification solution to meet your organization's specific needs, both in terms of the underlying schema for how the technology is built and in terms of policy customization.

The rich metadata capabilities within the Titus Classification Suite enable unlimited detail and contextualization for the information contained in files. The solution corpus is created from context gleaned from emails and documents, a batch data steward built into the solution as well as from user input, giving you flexibility and ultimately greater confidence that your data is being handling according to your business requirements.

This precision allows you to specify policies and actions on a much more granular level, ultimately leading to greater protection of your most sensitive data and greater freedom in the way you use your public information. Along the way, with guidance from this robust solution, your users become experts in handling your organization's data.

Titus also enables you to maintain ongoing awareness of user and application behavior to ensure compliance with your policies as well as external regulations.

Flexible Data Schema. Titus offers unlimited levels of metadata to help you classify the information in your organization. You can designate as many fields within the system as necessary to categorize your data. In addition to an unlimited number, the Titus Classification Suite offers a wide variety of field types as well.

Azure Information Protection supports two levels of classification, which is extremely limited. Users can enter a single value at each level, which means categorization generally defaults to sensitivity. To specify parameters such as retention date and so on, you need to employ a separate unified labeling product.

Having unlimited options for identifying and categorizing your data helps your organization meet today's regulatory demands outlined by the GDPR and CCPA as well as any potential future privacy legislation. Field types available in the Titus Classification Suite include the following:

- **Single Selection.** Select from an ordered or non-ordered list, such as Public, Internal, Secret, Top Secret or other categories of your choosing, to indicate the level of sensitivity of information contained within a file or email.
- **Multiselect.** Select multiple designations to specify who should view information, how it can be used or unlimited other granular designations. For example, you might want

to send an email to your HR, Finance and Engineering groups, but only to Senior Management. Multiselect is especially useful for military agencies, where users need to label information according to its "releaseability." Users could select multiple nations from a list to indicate where certain information can be shared.

- **Type-in Fields.** Input unique information into a document's metadata to inform users and other technologies integrating with Titus as information moves within and outside of your organization.
- **Date Fields.** Set expiration dates and implement a defensible deletion strategy to automatically delete files when they are no longer useful, or indicate dates when files can be made public. This field is particularly useful in legal settings or for fulfilling data retention period regulations.

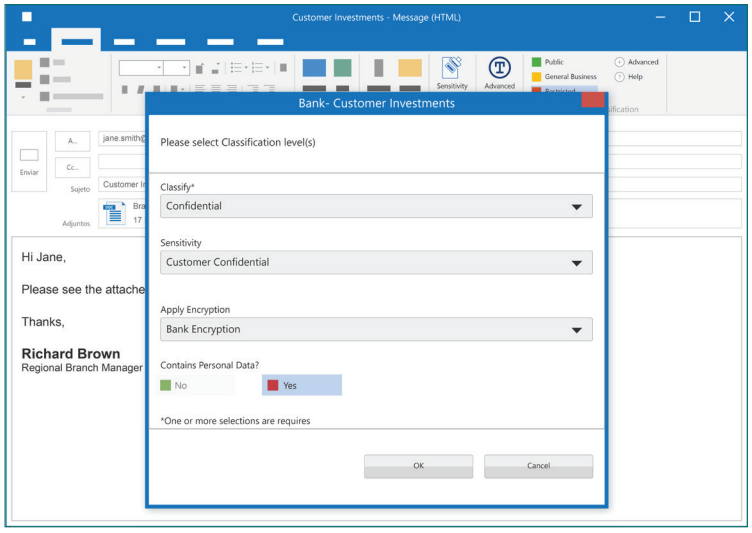
Flexible Policy Engine. The Titus Classification Suite policy engine maps to any business requirement, providing unlimited choice and flexibility. A simple user interface provides powerful scripting-like capabilities that work within user workflows without disruption.

As users send emails, save documents, print documents and perform a range of other daily actions, the Titus Classification Suite works behind the scenes to evaluate the context of data contained in every file or email. The solution then suggests user actions based on that context in relation to the organization's defined policies. The Titus Classification Suite can also be configured to perform some actions automatically. Azure Information Protection does not have the ability to evaluate context and cannot perform as many actions.

Build policy based on your business requirements, not on technology limitations. The Titus Classification Suite helps you implement policies based on your unique business needs as well as on regulation rules outlined by the GDPR, CCPA, SEC and other legislation. Titus enforces your policies by warning users or blocking risky activity completely. The solution helps build a security culture within your organization by including users in the process and continually educating them on best practices for handling data.

Intelligent classification allows you to build policies based on specific user attributes as well as on data identity, content and context.

Policy Extensibility. The Titus extensibility framework allows you to add additional context to your policy evaluation (Custom Conditions) and leverage your other security investments to perform actions (Custom Actions).



When a user writes an email and hits send, Titus Classification Suite scans for sensitive information and suggests classification levels based on your organization's information handling policies. The solution also applies metadata to inform your other security technologies, ensuring that information is protected as it moves within and outside your organization's walls.

A rules-based policy engine allows you to dynamically control the user experience. You can set any of the following parameters as conditions: Active Directory Attributes or Group Membership, recipients, author, environment, existing metadata, machine learning, and more.

The following extensibility features are not available within Azure Information Protection:

- Zero-friction classification with high confidence using machine learning
- Global recognition of personally identifiable, health and financial information
- Expert systems decision trees for guided selection
- The ability to save complex sets of selections as favorites
- The ability to apply conditions on anything other than content
- Classification upon printing to prevent leakage
- Classification of calendar items
- The ability to manage or compartmentalize beyond groups and users by applying Active Directory attributes.
- Restriction of documents from being opened by anyone outside corporate facilities
- Management of sensitivity drift (For example, you can keep a press release or quarterly earnings report classified as Internal prior to a specific date and then make it External.)

Freedom of Choice. Titus brings to the table a long list of strategic technology partnerships, all participating in an open security ecosystem. Because Titus is not tied to one platform, the company's solutions are better positioned to help you realize the full potential of your other security investments — and fill your security gaps.

Titus Classification Suite metadata informs a range of actions across this open ecosystem, integrating with your DLP and encryption technologies, cloud access security brokers (CASBs) and other security products.

Titus offers three levels of ecosystem integration:

- Solution interoperability where metadata is shared in any definition (as opposed to only matching the format of Azure Information Protection labelling)
- External processing to support the invocation of a broad array of rights management solutions, instead of only Microsoft's AD RMS or Azure RM (Titus does support both Microsoft flavors and many others.)
- Applicable APIs to allow third-party applications to apply correct metadata, which further extends the investment you've already made in security technologies

The rich metadata within Titus Classification Suite helps reduce false positive identification of sensitive data by your other security solutions. False positives can restrict your ability to get business done if rules are implemented inaccurately.

As mentioned earlier, Microsoft Azure Information Protection does not integrate well with other security vendors. It cannot run on G Suite for Enterprise and offers a very limited solution for Mac or mobile platforms. In addition, Azure Information Protection can trigger only RMS for encryption, which can be limiting if you need to share information externally. Titus solutions integrate with virtually every encryption vendor. Even if your organization uses an obscure encryption technology, Titus experts can custom-tailor the solution to meet your needs.

With Titus Classification Suite serving as the hub in your security ecosystem, you can have peace of mind that your privacy and data handling policies are consistent and integrated across your entire IT landscape.

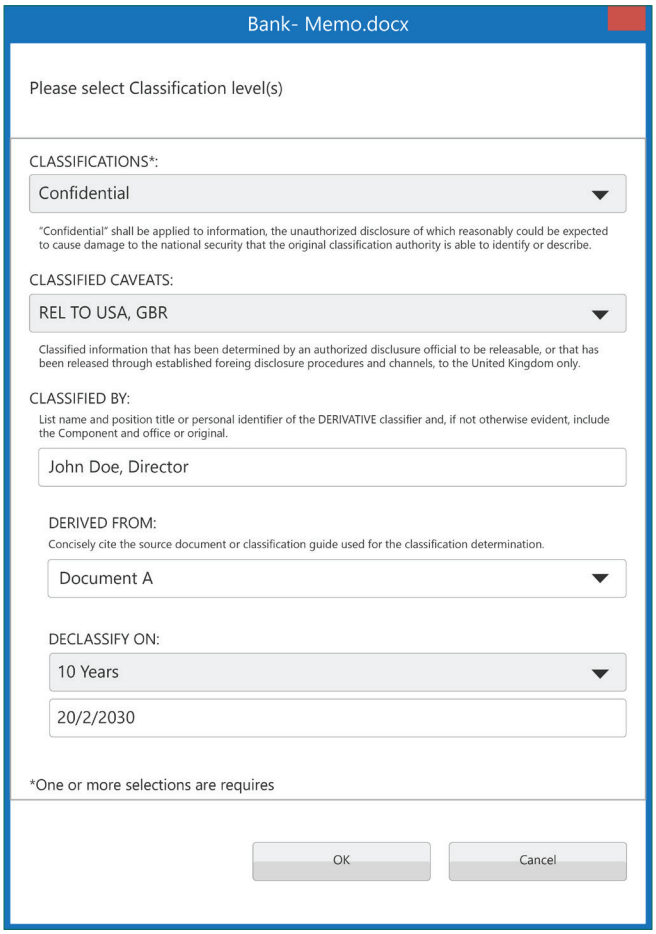
Rest Easy When It Comes to Compliance

Organizations of all kinds are grappling with how to understand and comply with a growing list of stringent privacy regulations. The extensive identification and classification features in Titus Classification Suite help you meet compliance requirements for your on-premises and cloud-based data at rest and in motion.

The first step toward ensuring compliance with the GDPR and the CCPA is to discover your sensitive, personal information in both structured and unstructured scenarios. From there, you've got to determine where to store the different levels of information and how it can be used. The Titus team can guide organizations going through this process to develop a coherent data classification strategy that covers both unstructured and structured information.

For example, all data privacy legislation includes the "right to be forgotten," which means consumers have the right to request that your organization delete any information about them you have obtained. If you don't comply, your organization could get hit with an enormous fine. Knowing where that information is stored and its sensitivity level is critical.

Titus can help you understand your requirements and then apply technologies to ensure that nothing falls through the cracks.



Titus Classification Suite offers virtually unlimited levels of classification, and the rich, persistent metadata it applies to documents helps you categorize your organization's data according to your unique business and policies. In addition to an unlimited number of levels, the Titus Classification Suite offers a wide variety of field types as well, so you can select from drop-down menus, type in details, establish date and time parameters, and more. All classification parameters can be customized for your specific organization.

The Bottom Line

Azure Information Protection cannot compete with the robust features in Titus Classification Suite. The powerful Titus policy engine keeps pace with your business, providing flexible, deep data classification and identification. With Titus, you'll truly understand what kind of data your organization has. You'll also know its value and how best to classify files to mitigate your exposure to risk.

Titus Classification Suite is a far better option for any organization that needs scalable privacy policies for protecting a complex data landscape. Titus empowers your employees to work confidently and productively, knowing their emails, documents and sensitive information are protected.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.