FORTRA

WHITE PAPER (Titus)

Improve Your Privacy Strategy

Extend Microsoft Azure Information Protection Capabilities Using Titus Accelerator for Privacy.

In today's interconnected and cloud-centric world, the need to secure sensitive information is more evident than ever. Ineffective privacy protection programs expose your organization to significant financial and legal risks, including regulatory fines and stock price drops, as well as liability to customers and shareholders.

The fact is most organizations are unaware of how much sensitive data they have, the value of that data, where it resides and how it's being used. Understanding the context of sensitive data is the critical first step in building a culture of privacy and overcoming these challenges for businesses of all sizes in all industries.

The challenge is real, and it is complex. Sensitive data breaches can happen as the result of internal handling or, in some cases, from the scaling back of security policies to fit the capabilities of a particular technology being used to help with security. It's a real a catch-22! Creating a privacy ecosystem requires a deep understanding of the risks associated with handling and storing personal data in internal systems, as well as overcoming challenges such as human error, workflow bottlenecks and inadequate privacy technologies.

As an IT professional, part of your job is to limit the exposure of personal data, build reports on activities and threat levels, and educate end users about best practices around personal data handling. In addition, you've got to ensure that the business meets the growing list of regulatory compliance mandates set out around privacy, while demonstrating to employees, customers and shareholders that their personal data is protected. These requirements make for a complicated IT landscape.

Finding the Right Privacy Solution

You've got Microsoft Azure Information Protection, so you're good, right? Not so fast. While most organizations understand the need to protect personal data, many often 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 opt to simply add on Microsoft's data protection tool, the Azure Information Protection solution.

Azure Information Protection is a cloud-based solution that helps organizations label, classify and protect their documents and emails. Labels — also called "tags" — are attached to files and emails to alert users to the level of sensitivity of the information contained within. For example, a file might include credit card information, and thus, would be given a visual marking and a "Confidential" label. Classification refers to metadata inserted into emails and files, and it contains more details about the document type, the information contained within the file as well as how it should be handled. Azure Information Protection can apply labels and 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 one of five different labels: for example Non-business, Public, General, Confidential or Highly Confidential. Each top-level label can have one sub-level label, such as Directory Groups, FTEs, Custom Lists or Anyone — No Protection. Azure Information Protection can 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.

Azure Information Protection scans documents that reside on network endpoints, servers and in the cloud, identifying structured data such as credit card numbers and social security numbers. The solution's built-in capabilities include a set of basic scanning tools, such as those used by most data loss prevention (DLP) solutions but which lack the ability to understand context. The ability to evaluate context is crucial for locating sensitive personally identifiable information (PII) written in a more narrative format. For companies new to privacy protection, Azure Information Protection offers a great 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.

Titus complements Azure Information Protection

Titus Accelerator for Privacy can extend and improve the capabilities of Azure Information Protection by enabling your users to label documents and emails at creation. In addition, Titus Accelerator for Privacy takes data categorization a step further by looking at the context around your organization's sensitive information using deep learning technologies, a type of machine learning. This complementary solution accurately identifies PII both at creation and in motion and helps users determine how to handle such information.

Titus Accelerator for Privacy enhances Azure Information Protection by adding the ability to do the following:

- Identify data at creation and in motion
- Identify unstructured data using deep learning technologies
- Help educate users on privacy and information handling best practices

How It Works

Labelling has many variables, and users have to make a lot of decisions about how information needs to be handled. Titus Accelerator for Privacy acts as a safety net on top of Azure Information Protection, taking a more thorough look as users create new documents or attach existing files to new emails. Titus Accelerator for Privacy considers words and phrases to better understand the context of data to fine-tune the sensitivity level and also to reduce the potential of falsely identifying information as sensitive.

When launching a data protection solution, many organizations encounter issues with workflow bottlenecks and lack of understanding among end users. Titus Accelerator for Privacy allows you to seamlessly guide the categorization of data by providing personal attributes from a growing list of global privacy concerns. This capability increases efficiency, creates a simplified experience and educates users at the same time.

This lightweight solution can be quickly configured and deployed, making it an ideal starting point for organizations beginning their privacy journey. Titus Accelerator for Privacy can be used as a standalone solution for identifying data at creation and in motion, but if you're already using Azure Information Protection, adding Titus Accelerator for Privacy helps take your data protection strategy further. As privacy and security ecosystems grow and form, Titus Accelerator for Privacy becomes an integral part of your program, ensuring all pieces of your ecosystem work as a fully optimized data privacy solution.

Azure Information Protection is designed to deliver labeling solutions for a broad set of identifiers, aimed at a wide audience with modest customization needs. Organizations with complex data privacy requirements often have to downgrade their security policies to use the solution.

Titus Accelerator for Privacy, on the other hand, leverages machine learning technologies to offer a dedicated and highly targeted data privacy solution that extends your labelling capabilities to allow for more granular control, with fully customizable categories that let you accurately identify information as required by various privacy regulations.

Titus Accelerator for Privacy Improves Your Privacy Protection

Deploying a full-fledged data classification suite with robust, customizable functionality requires you to first develop a comprehensive data handling policy, which in turn requires input and time commitment from IT, legal, R&D, executive

leadership, business units and others within the organization. The process could take months. That's why deploying Titus Accelerator for Privacy by itself or on top of your existing Azure Information Protection implementation is an attractive first step. You gain an additional layer of privacy protection without a heavy internal lift. Titus Accelerator for Privacy also gives you visibility into what needs to be protected using a broad array of detection capabilities.

Here are some of the key benefits you'll see by adding Titus Accelerator for Privacy to your Azure Information Protection deployment:

Reduced Risk. Titus Accelerator for Privacy dramatically enhances privacy protection and reduces risk by accurately and efficiently detecting unstructured personal data through the use of machine learning. Unstructured data makes up more than 80% of most business' information and it can be difficult to get a handle on.

Titus Accelerator for Privacy enables you to identify sensitive unstructured data as it's created or shared using Windows-based applications, helping users understand what kinds of information need to be better protected. By evaluating words within the surrounding context, Titus Accelerator for Privacy can accurately predict what constitutes personal data and automatically alert users to potential risk.

Prebuilt Data Models for Fast and Easy Deployment. Titus offers out-of-the box configurations that target a number of sensitive information types. These were designed with production deployments in mind.

You can choose between three levels of data privacy:

- **Personal Data Analytics** — The solution can perform personal data analytics with no need for user interaction. Titus Accelerator for Privacy looks for personal data and logs the details so that IT admins and business leaders can gain a deeper understanding of their sensitive data.

- **Privacy Enforcement** — Get personal data analytics plus send user alerts when there is a potential for a data breach. For example, Titus Accelerator for Privacy might detect that employee addresses are being sent externally and send an alert to the user as well as to your IT admin. The user can decide how to act given the alert, and the IT admin will be kept informed of the activity.

- **Privacy awareness —** Get both personal data analytics and privacy enforcement plus apply visual markings to files and emails when personal data appears within them to increase awareness throughout your organization.

Titus consultants are available to answer sizing and scaling questions and to help you with a fast and easy deployment.

Support for Multiple File Types. When it comes to non-Microsoft files such as Adobe Creative Suite files, Titus Accelerator for Privacy extends your labelling capabilities. With Azure Information Protection, tagging non-Microsoft files requires users to turn on additional protection capabilities, which means all tagged files will be encrypted. Wholesale encryption of all tagged files can wreak havoc on organizational processes and workflows. For example, many files might need to be tagged "General Business" but don't need to be encrypted.

Digital rights management tools, in this case RMS, limit how a file can be used, stored and sent through email. Users would need an encryption key to open the file. If someone forwards an email with an encrypted file attached and the recipient doesn't have the key, business slows to a crawl, or stops completely, as they try to troubleshoot the issue. In frustration, many users will simply turn encryption off so they can forward files to colleagues who need to view them. These workarounds, however, can put sensitive data at risk of a breach if truly sensitive files are then forwarded to unintended recipients. Again, it's a catch-22 with no easy answer for Azure Information Protection users. Titus Accelerator for Privacy allows you to label non-Microsoft files and apply encryption to only those that truly need that additional layer of protection.

Rich Context-building. Machine learning in Titus Accelerator for Privacy helps your users understand the context around their data, ultimately supporting your overall security and privacy strategy. Titus Accelerator for Privacy can embed metadata into your files at creation based on the context of

the data in them, but it must work with a designated client agent to do so. When using Titus Accelerator for Privacy with Azure Information Protection as a client, you'll need to use the Azure Information Protection SDK to program this additional capability. One drawback with this approach, however, is that Titus Accelerator for Privacy must then limit itself to the precise Azure Information Protection metadata format using a narrow set of parameters. (To get the full benefit of Titus Accelerator for Privacy's metadata capability, use it with Titus Classification Suite or Titus Illuminate — see below for more on these solutions).

If you do work with the Azure Information Protection SDK to embed metadata into your organization's files, you'll get seamless integration with the rest of your privacy and security ecosystem. Third-party security solutions can easily leverage Titus' technology-agnostic metadata as part of a fully interoperable, data security ecosystem.

Even without the metadata functionality, Titus Accelerator for Privacy features robust privacy detectors that can identify personal details such as name, address, birthdate; health information; security information such as usernames and passwords; and financial information such as credit card numbers and bank account details. Using deep learning, Titus Accelerator for Privacy categorizes data by scanning for specific words and phrases as well as their context to identify PII and also to help reduce false positives on sensitive information.

Adding the context of why something is sensitive is important in helping users understand the implications of exposure. Consider a scenario where you just had a breach and cybercriminals stole some data labelled simply "Sensitive." Was it customer PII, employee health data, financial data or business information? Perhaps it was combination of all these types of data. With Titus Accelerator for Privacy, you can identify data on a more granular level using context, adding multi-layered tags and suggestions for how to handle sensitive information. This level of identification and tagging helps reduce the overall likelihood of a breach in the first place.

After scanning for context on a file labelled "Sensitive" by Azure Information Protection, Titus Accelerator for Privacy might actually determine that the information contained in the file is not sensitive. For example, an employee might write an email to a colleague that says, "I about had a heart attack when I saw the score from last night's game." Another email might say, "John Smith had a heart attack over the weekend and will not be coming into the office for three weeks."

Some solutions might see the first email and flag it as personal health information because of the words "heart attack," resulting in a false positive identification of PII. Azure Information Protection may not flag either of these emails since they are made up of unstructured data rather than simpler, more structured data. Titus Accelerator for Privacy has the ability to scan the context around these two sentences and determine that the first one does not contain any PII but the second one does and should be flagged as confidential.

Automated Data Protection. Data security solutions often require end users to spend too much time and energy ensuring that data is protected. These added tasks cause frustration and workflow delays. Titus Accelerator for Privacy works behind the scenes to automatically scan emails before they are sent. If personal data is detected, Titus Accelerator for Privacy can send an alert to the user suggesting an action that best meets your enterprise rights and encryption requirements. You'll limit human error within your organization and ultimately reduce the risk of a data breach overall — because a large percentage of breaches result from mistakes or accidental sharing of sensitive information.

Titus Accelerator for Privacy provides a seamless user experience, alleviating a common barrier to successful data protection and allowing for optimized organizational workflows and improved productivity. Your users experience no workflow interruptions, and your data is categorized correctly and protected based on your organizational policies. You'll also increase your ROI on security investments and boost confidence that your data is secure.

Ensure Privacy Compliance. To protect individuals, many industries and governments have created privacy regulations that require organizations to identify and secure their data. As these regulations increase in numbers and scope, it can be difficult for IT teams to understand requirements and ensure compliance across an entire organization. Nearly every mandate requires that you have a solution in place for the identification of personal data. Noncompliance can mean serious consequences, including hefty fines. Many regulations have multiple levels of protection that must be applied to documents and emails. With only one tag allowed per file in Azure Information Protection—either a top-level value or a sub-level value—organizations are immediately limited, and many privacy regulations cannot be met.

Most organizations, however, have to comply with multiple regulations simultaneously. If your privacy solution only allows for one label per file and you must comply with two very different privacy regulations, you are likely to run into issues. Your only option would be to generalize the label selection, thus losing the specificity needed to provide adequate protection—and in some cases, you might not actually meet regulatory compliance.

Titus Accelerator for Privacy offers a flexible policy engine to help you seamlessly achieve compliance with existing, changing and new regulations within your industry. Enable your organization to easily adapt to mandatory policies as they evolve and ensure that your workforce experiences minimal workflow bottlenecks caused by policy changes and restrictions.

Getting your organization to come into compliance can seem complicated. The first thing is to begin to understand what information is private and then what you need to do to protect that information. Titus Accelerator for Privacy lets you set very detailed, customized parameters for the types of data to scan for as well as the types of alerts and suggestions to make for handling that data. The ability to identify more granular, unstructured information and apply multiple labels to files enables you meet a wide range of industry regulations and internal privacy policy requirements.

Accelerate Cloud Adoption. Many organizations are concerned about accidentally putting PII up into the cloud and violating certain regulations, or worse, experiencing a data breach where customer and employee PII is stolen. In fact, because of these concerns, some organizations put off moving anything to the cloud at all.

Because Titus Accelerator for Privacy identifies PII while files and emails are being created, you can more easily avoid putting sensitive information into the cloud. In addition, you'll gain the confidence you need to move your non-sensitive information to the cloud sooner.

Want to Take Your Security Strategy Further?

Titus Accelerator for Privacy alerts users when a new email or document contains personal information, but if you want to actually classify that information, you'll need to pair the solution with a client agent such as Titus Classification Suite, Titus Illuminate or Azure Information Protection.

Titus Accelerator for Privacy deployed with Titus Classification Suite and Titus Illuminate can take your privacy strategy much further than simply adding Titus Accelerator for Privacy onto Azure Information Protection. The Titus trio provides a fully automated, more flexible, customizable, no-touch data privacy solution. Titus Accelerator for Privacy identifies PII in documents and emails at creation and in motion, and Titus Classification Suite injects rich metadata to specify the category of PII, creating a unified and simplified language for the entire security ecosystem. Titus Classification Suite also classifies the file or email (Sensitive, Restricted, etc.) and applies specific data handling policies (Send with Encryption, Don't Send, or any number of custom actions your policies mandate). Titus Illuminate scans data at rest on your on-premises servers and stored in cloud repositories, looking for context and enabling the same metadata capabilities. Titus Accelerator for Privacy plus Titus Classification Suite and Titus Illuminate can handle your entire privacy protection program without user input or disruption to daily workflows.

Titus Classification Suite enables you to embed metadata attributes into email, documents and files at every stage of the content life cycle and automatically adds visual

markings to help organizations meet compliance and legal requirements. In addition, Titus Classification Suite can encryption technologies to protect your most sensitive personal information.

Titus Classification Suite offers flexible and customizable classification metadata schema, giving your data even deeper context so people understand how to handle the information. This rich metadata is automatically accessible by all of your other third-party security solutions, such as data loss prevention and encryption technologies, ensuring a seamless, integrated privacy protection ecosystem. Azure Information Protection, on the other hand, integrates with other solutions only via Microsoft's own SDK, which further ties customers to the Microsoft universe and limits their flexibility to build a data protection solution using best-in-class components.

Titus enables you to carry out a more robust, enterprise-grade data security strategy, based on custom policies that are unique to your business. You'll have streamlined classification tools to clearly inform both your people and your policies on what information should be secured and how to handle it.

Improve Your Privacy Strategy

Privacy and data protection solutions can be cumbersome, ineffective and costly. Titus Accelerator for Privacy is a scalable and highly accurate data identification solution. It integrates seamlessly with existing security products and offers an effective way to immediately reduce risk. Any organization in need of protecting sensitive personal data can enhance and optimize their privacy solution with the use of Titus Accelerator for Privacy — both for today's security needs and tomorrow's.

Whether your approach to data security is to implement a labelling solution or a deeper classification strategy, Titus is here to help make it possible.

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.