FORTRA

WHITE PAPER *(Titus)*

Can You Handle Your Data?

Improve information handling practices to better protect sensitive data and comply with increasingly strict data regulations.

The modern world is swimming in data, with no signs of that changing any time soon. Personal information, confidential business data, highly sensitive government information — it's all increasing in volume and importance. Threats to the security of this sensitive data have increased in number and sophistication. As a result, industry and geographic data regulations are highly complex and stricter than ever. Non-compliance can lead to hefty fines and damage to a company's brand and reputation.

There's a clear trend to provide additional protections to individuals around both privacy and the use of their data. In Europe, for example, the General Data Protection Regulation (GDPR) mandates that organizations must implement "right to erasure" policies on individuals' personal data. Also known as "right to be forgotten," this policy gives people the right to have their personal data deleted if there is no longer a reason for an organization to keep it. The GDPR also gives individuals the "right of access," which means they have the right to access their personal data, along with information about how it's being processed, shared and used. Without proper data labeling, though, just finding the data in question could be an enormous task, depending on the size of the organization, what kinds of data they store and what systems they use to store it.

Providing these rights to individuals is a daunting challenge, but noncompliance is an expensive proposition. Penalties for GDPR noncompliance can be up to €20 million, or 4 percent annual global turnover — whichever is higher — of an organization's worldwide annual revenue.

Other regions have data regulations that are equally strict. The California Consumer Privacy Act (CCPA) contains sweeping data protection for consumers. It requires organizations to disclose to individuals the types of information they have stored and gives people the right to request deletion and to access personal information in a "readily useable format." The trend is to provide consumers with increasingly specific rights around how their data is handled.

These regulations are only partially about protecting sensitive personal and business data; they're equally about information handling — because it's difficult to protect without first addressing the ways data is kept and handled. Many organizations struggle to accurately identify data as employees use and share it in their day-to-day work.

How can you protect something if you don't even know you have it?

Manual processes for identifying, classifying and protecting data can be cumbersome when dealing with large volumes of data. In addition, many people don't know how to treat the various types of data they encounter. Some people are unclear of classification expectations. And others are simply unfamiliar with the content. When data handling processes seem too tedious, many people will find workarounds that put sensitive data at risk.

Digital tools for data identification and classification can help organizations meet all of these challenges efficiently and accurately. This paper explores how organizations can improve information handling practices to better identify, classify and protect their sensitive data and comply with information rights regulations using these tools.

Identify, Classify, Secure

Managing your complex data environment, meeting strict data regulations and protecting sensitive information all require detailed information handling practices that start with data identification, classification and labeling. But it also requires organizations to change the way they think about data.

Every document, every file, every email has the potential to affect business outcomes. Some are obviously more benign than others. A person emailing a co-worker to ask what they are doing for lunch, for example, is not as sensitive as financial or customer information being sent from inside the organization to someone outside of the organization. Those are extreme scenarios. But what about a transcription of an interview with a subject matter expert (SME) going over the technical features in a soon-to-be-announced product? Would it be a big deal for a marketing manager to send that to a freelance writer under NDA outside of the organization who's working on marketing materials?

People need to learn what different types of data mean to an organization and why it's important to protect them. They also need processes to help them identify sensitive data and understand how to protect it in the midst of a busy work day. Most people have far too many tasks on their to-do list. That marketing manager just needs the freelance writer to help get a job done. If the freelance writer doesn't have access to the organization's network, emailing background materials is the easiest way to keep the project moving. But what if that interview accidentally got into a competitor's hands?

People need tools to help them identify sensitive data and understand how to protect it within the flow of day-to-day work. Identifying, labeling and classifying individual assets is at the heart of good data protection and, when possible, doing this when content is created can go a long way in protecting it down the line.

Digital tools can help organizations identify unstructured data using automatic content-matching and validation. Some tools can analyze files at rest in your IT environment, and others can identify data at creation and while it is in motion — i.e., when sending as an email attachment or uploading to a server. Advanced technologies, such as machine learning, can even help organizations identify company-specific content types, enabling an even more efficient and accurate data protection program.

These tools can help organizations inventory their data by identifying specific content types and then classifying and labeling content according to company data security policies.

Powerful Policy Manager

People need to be able to share information securely and easily. Technologies that support a policy-driven foundation for identifying, classifying and securing sensitive data are key. A configurable policy management platform allows organizations to decide the rules and level of enforcement — including which tools and technologies the policies will control.

A good policy manager is activated within user workflows and can educate users via alerts and suggestions that help them make decisions about the data they're working with. The implementation of data policies is triggered by specific events, such as sending an email, saving a new document, uploading a document to the Cloud and other activities.

For example, when a user hits send on an email, the data classification tool will loop through the attachments, recipients and email content to ensure data policies are being followed. An alert stops the send and tells the user why it was stopped — perhaps that SME interview mentioned above is attached to the email and, according to data policies, contains information that should not be sent outside of the organization. Users then have the option to change the classification, remove the attachment from the email before sending or just hit send it anyway to this particular recipient.

Powerful Policy Manager

GUIDED SELECTION

The complexity of today's information handling requirements makes it difficult to expect users to know how to map a given piece of information to classification, retention schedule, and other required labeling and metadata. Some organizations may want to start with simple labels such as Public or Personal, Unclassified, Confidential, Restricted or Internal Use only, and Secret. These simple labels, however, may not address all of the data security regulations out there today.

Policy managers that include guided selection capabilities can help users determine more detailed classification and labeling of data. These capabilities provide a series of questions within user workflows to help people determine a document's sensitivity level and other specific information.

Presented with a limited number of choices outlined in easily understood terms, users can make informed decisions about content and use the system to more accurately map data from hundreds or even thousands of possibilities. Basic questions help users determine whether content is approved for public use, whether it can be shared with all employees within an organization and whether it would cause significant harm if it were leaked outside the company.

Taking a three-question approach can provide a large number of possible classification options. If each question in the series has 15 possible answers, leading to another question with 15 possible answers, there would be 3,375 permutations to be mapped to correct information handling. That becomes pretty granular when it comes to data labeling. Yet, the process remains relatively simple because users are only exposed to three questions at a time with a total of just 45 items to choose from.

SOPHISTICATED SCHEMAS

Taking a three-question approach can provide a large number of possible classification options. If each question in the series has 15 possible answers, leading to another question with 15 possible answers, there would be 3,375 permutations to be mapped to correct information handling. That becomes pretty granular when it comes to data labeling. Yet, the process remains relatively simple because users are only exposed to three questions at a time with a total of just 45 items to choose from.

It's critical that information-handling procedures have the ability to evolve over time, as business needs evolve. For example, collateral for a new product introduction, announcements of financial results, or merger and acquisition details are all cases in which information is very sensitive up to a certain date when it becomes public. Keeping some of this information restricted until that date is critical to avoid violating regulations and losing competitive go-to-market momentum. Being able to tag this content with metadata such as dates and other project attributes, enables organizations to not only avoid those risks but also avoid having to reclassify the content manually once it becomes public information.

Once the information does become public, the sensitivity level can be downgraded and data handling policies can be adjusted accordingly. The sophisticated metadata schema settings allow classification levels to automatically change over time, a capability known as "metadata conversion."

Without the metadata tags, it would be easy for a bad actor to change a document's classification level and send it outside of the organization before the information has been made public. Or even for a user to change the classification level by accident.

CONTEXT-SETTING

Some policy managers have the ability to take things a step further to look at content, existing metadata, environment, Active Directory details, attachments, recipients and other custom dynamic properties programmed by an organization. Being able to set a broad context for information handling that is specific to a particular organization provides a higher level of data protection.

Organizations have virtually unlimited options when it comes to building policies that make use of company-specific information to perform analysis and set the context for data at creation, at rest, and in motion. The ability to extract data attributes from Active Directory, indicating for example that an employee has resigned, could go a long way in terms of making sure data is handled correctly.

How Machine Learning Can Help

Policy managers with built-in machine learning capabilities can make information handling more efficient, more accurate, and more secure. Machine learning uses analytical models to give computer systems the ability to learn from data, without being explicitly programmed or fed that data. There are different types of machine learning, including supervised, unsupervised and deep learning, and each can be used in a number of different ways.

Supervised machine learning can help users make better decisions about how information is handled, using automated or recommended data classifications based on organization-specific categories and policies. This technology leverages proven algorithms to build a company-centric model that can predict classification categories for emails and documents. Based on the model, the program then either suggests or automatically applies classifications to unknown documents, enabling greater security and staff productivity.

Using supervised machine learning for categorization allows organizations to efficiently train a model, or corpus, for data identification, without requiring massive resources or data. Basically, you feed the corpus your categorized examples, and it learns to recognize those similarities in documents to inform classification suggestions. This methodology reduces risk by improving accuracy and efficiency of data identification, classification and protection. When confidence levels increase, machine learning can automatically apply data policies for an additional layer of security. The end result? Machine learning can simplify the decision-making process for end users with recommended classifications and take it out of the equation with automated classification.

Unified Security Ecosystem

No single technology vendor is currently providing a sophisticated suite of solutions to handle all aspects of a comprehensive cybersecurity program. Setting up policies within individual tools that provide various data protection capabilities is bound to create conflicts and inconsistencies.

Ideally, the data classification tools you implement will provide an open solution that can put your policies into action and also communicate with the other security technologies in your system, such as data loss prevention (DLP), cloud access security brokers (CASB), enterprise digital rights management (EDRM) and whatever other tools you employ in your data protection strategy. If your metadata can be easily read by these other technologies to facilitate proper information handling, your data security policies can be appropriately followed across your organization. For example, let's say a user classifies an email as "General Business" using a data classification tool, encrypts it using a particular encryption tool, and then attaches a document classified as "Internal." In a world where your cybersecurity ecosystem is unified, the encryption tool would raise a flag and not let the document be sent.

The best data classification tools let organizations set their policies and then help unify the ecosystem by ensuring that the policy is applied consistently across all tools.

Conclusion

With today's increased data security regulations and increasingly sophisticated cyberthreats, organizations need better information handling and data governance policies — and they need the right tools to help them implement their policies consistently and efficiently across all areas of their business.

Establishing a policy-driven foundation to help facilitate the identification and classification of sensitive data at creation, in motion or at rest is key to applying the right level of protection. With a configurable policy management platform, organizations can automatically apply policies based on classification and categorization.

Titus offers a comprehensive data protection and information handling solution that covers data at rest, at creation, and in motion. Designed with an open ecosystem in mind, Titus solutions integrate easily with an organization's existing software systems, giving customers the freedom to deploy the technologies that best fit their business requirements without disrupting user workflows. Security solutions work better together, enabling consistent policy enforcement and unlocking the value of an organization's technology investments.

Book a free demo to see how Titus provides an open, intelligent and flexible solution to help simplify data handling within your organization.

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.