ITsMine™

Meeting GDPR Requirements With ITsMine Beyond DLP™

Introduction

Personal data is at the heart of the EU General Data Protection Regulation (GDPR), and one of the key criteria of the new GDPR legislation is the need to keep data secure. There are several steps that can be taken to ensure companies meet GDPR and technology plays a critical role. Without a technical solution for monitoring the collection, processing and storage of personal data, enterprises run the risk of not being compliant with the strict regulations. And it's not enough to just monitor, you also need to protect and educate your end users, at the same time.

Ensuring your IT infrastructure is capable of protecting all the data it holds and processes across all devices, departments and software with a Data Loss Prevention (DLP) system, and being able to prove the security of your infrastructure is essential to compliance. While this may be easier said than done, there are practical steps you can take to ensure your organization is protected from all types of data loss.

Controller/Processor Obligations Under GDPR

Any information that data controllers have on the data subject and any data that is being processed by the processor, such as date of birth, address, salary, and rent would all constitute protected personal data under the GDPR. Any organization that acts as a controller or a processor has several obligations under this regulation. The main ones include:

Records of processing

Each controller is responsible for maintaining records of all the processing activities which take place within the organization. Therefore, each processor is responsible for maintaining records of all categories of processing activities carried out on behalf of the controller.

Data mapping

The organization is required to understand how data within its organization moves. Documenting the way information flows in your company by taking inventory helps demonstrate that the organization is being compliant. Mapping the flow of data will also help to identify areas that could cause GDPR compliance problems.

Data accuracy

Organizations should take all reasonable steps to ensure the personal data that they hold is not incorrect or misleading. Organizations must carefully consider any challenges to the accuracy of personal data.

Tracking personal data

Since personal data usually resides in many different applications or services, servers, cloud or data centers, the organization is required to be able to access, report and remove personal information from all systems when required by consumers or regulators. To comply with GDPR requirements, you must be able to track the movement, or lineage, of a contact's personal data – where it was first acquired, whether consent was obtained, where it moved over time, where it resides in each of your systems, and how it gets used. The connections among those systems and silos are key to tracking the complex path that personal data takes through your enterprise.

Security

Organizations must have appropriate security in place to prevent the personal data they hold from accidentally or deliberately being compromised. The organization needs to consider the security principle alongside Article 32 of the GDPR, which provides more specifics on the security of its processing: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk".

Risk management

Article 32 requires that measures implemented ensure a level of security appropriate to the risk. Risk-based security ensures that priorities are established and decisions are made through a process of evaluating data sensitivity, system vulnerability and the likelihood of threats. This is a key component of knowing your current state and is essential for building an appropriate GDPR compliant program.

Personal data breach

The GDPR requires all organizations report certain types of personal data breaches to the relevant supervisory authority. Organizations must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without delay. Also, the organization should ensure that it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision making about whether or not they need to notify the relevant supervisory authority and the affected individuals. On top of it all, the organization must also keep a record of any personal data breaches, regardless of whether it is required to notify those involved or not.

Data Loss Prevention

Looking at the security and data breach report obligations results in two main takeaways :

The GDPR does not define the security measures that should be implemented. It requires having a level of security that is "appropriate" to the risks presented by processing data. There is a need to consider this in relation to the state-of-the-art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, a personal data breach is whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorization; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. So, on becoming aware of a breach, organizations should try to contain it and assess the potential adverse consequences on individuals, based on how serious or substantial these are, and how likely they are to happen.

Data Loss Prevention (DLP) solutions offer unparalleled insights into a company's data, allowing admins to set strict rules concerning specific sets of sensitive data while giving employees the liberty to manage data outside of these categories freely. It is an easy way to add an extra layer of security to a company's network, ensuring that human error or malicious insider intentions do not bring down the wrath of the DPA upon a business. In the era of the GDPR, there are no longer reason for companies to suffer from data loss.

So, what should an organization expect from a DLP solution?

In order to protect digital data in its three fundamental states, DLP solutions require three functional DLP types be implemented: "Data In Use" (DIU) DLP, "Data In Motion" (DIM) DLP and "Data At Rest" (DAR) DLP.

The first, and the most important, is the ability to automatically analyze and classify the informational content of transmitted, used, and stored data of various formats and types. These must include not only files and emails, but also instant messages, social media posts, web forms and webmails, raw textual data and, in some scenarios, even metadata and binaries.

Secondly, the criterion of real-time protective action for all data states must include all local channels on endpoint computers, the most risky network communications, as well as various data storage devices, systems, and repositories. Specifically, DLP components can apply a whole set of protective actions, such as blocking, remediating, alerting, logging, shadow-copying, and more.

Another essential DLP capability is controlling data operations based on their context. Context is indispensable for preventing data leakage or loss in a multitude of use cases when the detection of security policy violations does not require content analysis, which can be quite CPU-intensive and take a considerable amount of time to complete.

ITsMine Beyond DLP™ - Next Generation DLP Solution

DLP solutions are uniquely situated to provide not only informational support, but also tools to help meet strict GDPR regulations. Among the requirements we can find data discovery services which assist organizations in understanding where personal data is stored, helping them meet the strict personal data usage requirements through data in use monitoring, preventing personal data tampering and loss and maintaining personal data security standards.

But today, this offering is not enough. There is a need for next generation DLP products to be simple to deploy and simple to use, out-of-the-box, automatically classify and track data, restrict who has access to data and intervene in real-time if data is sent to the wrong person, constant reporting back to data owners, end users, and security analysts, using prevention mode with no false positives, and short term implementation process with rich forensic abilities. Next generation DLP take into account the need of leakage or loss prevention that refers to data deletion, encryption (in the case of Ransomware, for example) and modification.

ITsMine™ Beyond DLP™ offers a new, unique, offensive approach for Data Loss Prevention (DLP) that requires no policies or permanent endpoint agents, while guaranteeing protection against internal and external attackers. ITsMine™ Beyond DLP™ solves the DLP challenges using a fully automated solution with negligible false positives and without affecting employees productivity.

ITsMine™ Beyond DLP™ covers two unique use cases to help organizations meet with the above requirements:

1. Find out about data breaches and obtain critical forensic information

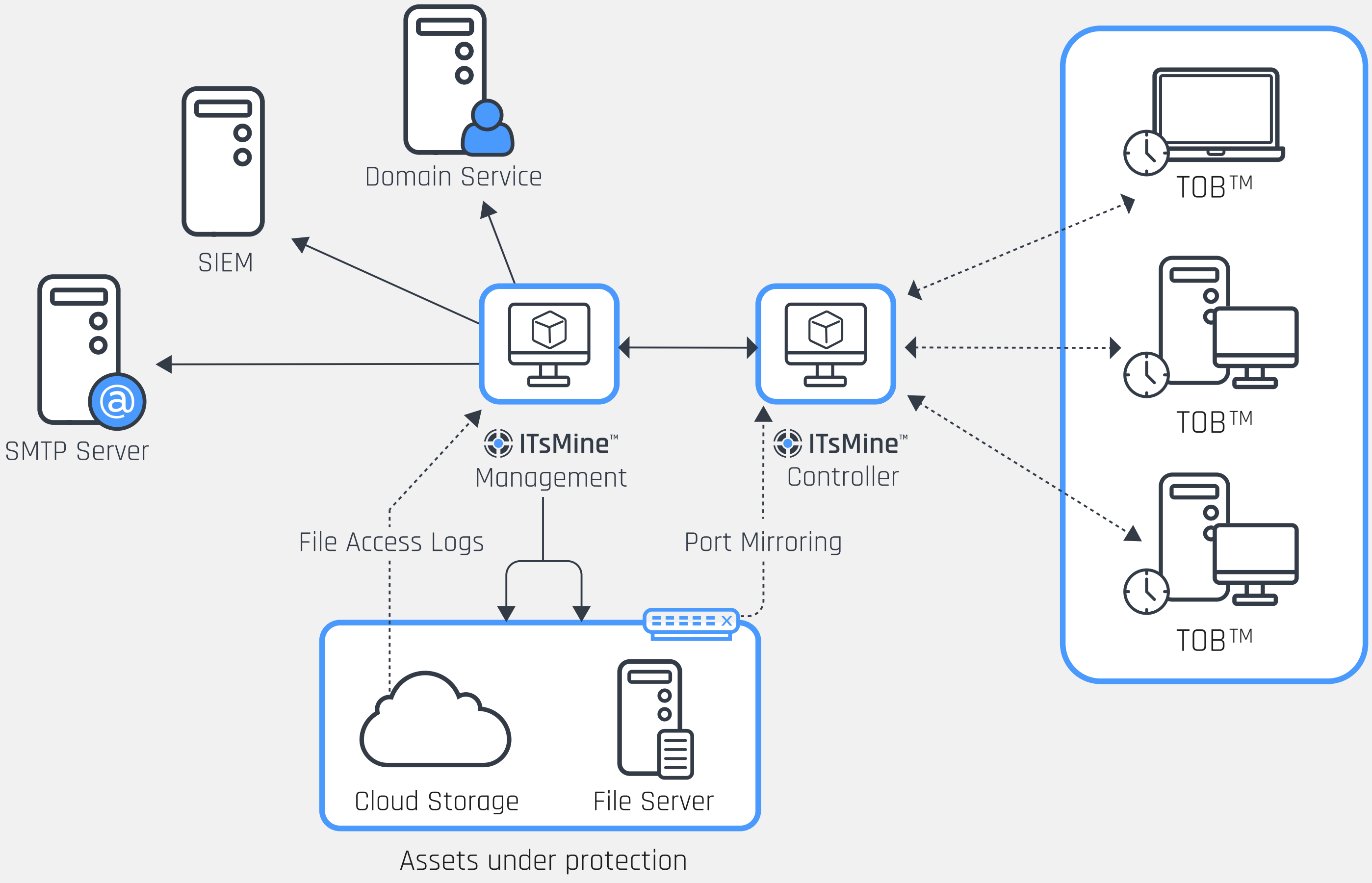
2. Track extremely important files when in use inside and outside the organization

The Technology

ITsMine™ Beyond DLP™ offers an innovative approach to data loss prevention. In the first stage, the software automatically creates a heat map of the organizational file storage areas, classifying the folders by their degree of importance, based on the access of the users on a daily basis. In the second stage, the software automatically creates files that resemble other files within a given folder (similar file name, size, document author, date created and modified), and disseminates these files throughout the company's data file storage, essentially planting SoftwareMines™ across the directory. The software also creates a Unique Identifier Number (UIN™) which is inserted into each SoftwareMine™. The "minefield" changes on a daily basis. In addition, an administrator can mark specific files or folders they wish to track using ITsMine™'s manual policy.

In the third stage, if a user steps on a SoftwareMine™, (meaning opens a fake file, tries to copy a folder containing a fake file etc.), the system zooms in on the user's computer for a limited period of time. According to the user's behavior, the system will actively check if the vector of attack is an external attacker or an internal rogue employee and classify the risk level of the "security event". It will then automatically decide whether to educate the user, block a specific activity, or send the obtained evidence to the security manager.

ITsMine™ turns the organization's file storage into a live minefield. The creation of this minefield is achieved by gathering relevant information from different sources: Characterizing the way the stored files are accessed and analyzing the organization's own file structure and permissions.



This solution offers organizations the ability to:

- Fully monitor the organizational file storage, while educating employees on responsible behavior when dealing with organizational data.
- Actively protect file storage by implementing software mines.
- Ensure sensitive data or "leftovers" of sensitive data don't stay on the endpoint and get saved only on the file storage (Endpoint Sanitation).

While taking into consideration the aspects a DLP solution needs in order to comply with GDPR requirements, it is important to review ITsMine™'s main implementation requirements:

GDPR Requirement	Traditional DLP	ITsMine DLP
Data discovery and mapping (article 2)	Yes – but it might cause a huge number of false positives	Yes + finding the most interesting areas in the company's file storage and protecting them
Track sensitive personal data (article 9)	Yes	Yes + full review of data assets flow and ability to warn users accessing certain sensitive areas
Data security (articles 25, 32)	Yes	Yes + it is a layer of data protection by restricting the transmission of personal data outside the network and recognizing its flow
Risk management (article 35)	No	Yes + ability to ensure a level of security appropriate to the risk
Data breach (article 34)	Yes – but not the main goal	Yes + Find out about data breaches and get critical forensic information
Unused privileges (data security)	No	Yes + there is a need to track what is happening with personal data across the organization and any services it is sent to goes to, and for. Including the purpose
Analysis and forensics (Article 30 + Data security)	No	Yes + Find out about data breaches and get critical forensics information
Cross border transfer (article 56)	No	Yes + Track extremely important files when in use inside or outside the organization

Conclusion

As DLP technologies are indispensable for preventing leakage or loss of personal data in IT systems, DLP is necessary for implementing the GDPR's "availability, integrity and confidentiality" principle, and achieving compliance with the regulation.

Indeed, neither DLP nor any other particular technology alone can be a "silver bullet" for the GDPR. A whole puzzle of various complementary information security and privacy enhancing technologies should be put together to ensure full compliance with the regulation. Yet, DLP is one of the critical pieces of the GDPR compliance puzzle.

ITsMine™ attempts to drastically change the way enterprises engage with DLP solutions by approaching the problem differently. With the goal of providing a DLP solution that is easy to implement, automate, requires minimal maintenance, is non-intrusive, uses minimal resources, and is capable of providing more information following the event of a breach than ever before, a unique method is required. ITsMine™'s Beyond DLP™ aims to target the required objectives while providing equivalent or greater protection than the competition.