ITsMine™

Meeting CCPA Requirements With ITsMine Beyond DLP™

Introduction

The California Consumer Privacy Act (CCPA) has emerged as a blueprint for data protection regulations in the US. Inspired by the EU's General Data Protection Regulation (GDPR), the CCPA has adapted the new international standard set by the European legislation to a distinctly American context.

The CCPA is a consumer privacy law regulating how businesses handle customer information. Based on the General Data Protection Regulation (GDPR) and due to recent data breaches, CCPA aims to empower consumers with new rights in order to protect their privacy. Business transparency is encouraged and gives consumers a certain amount of control over how their personal information is used with the goal of reducing misuse.

Any company that collects data about California residents should start evaluating whether it is subject to new obligations and liabilities under the California Consumer Privacy Act (CCPA). Even businesses that meet the requirements of the EU General Data Protection Regulation (GDPR) will have more to do to prepare for the CCPA.

The CCPA went into effect on January 1, 2020. Enforcement by the California Attorney General will begin July 1, 2020 at the latest. Enforcement will begin earlier if regulations are issued speedily.

The CCPA gives California consumers enhanced rights to their personal information, including knowing what personal information is being collected, how it is being used, whether their information has been disclosed or sold to third parties, to whom, and the right to oppose the sale of their information to third parties. Because the CCPA is an entirely different piece of legislation than the GDPR, affected companies should not assume their GDPR compliance efforts will satisfy the requirements of the CCPA.

Which Entities Need to Comply With the CCPA?

The most important definition in the CCPA is that of "Personal Information," since all of the CCPA requirements emanate from whether a Business is collecting or processing such information.

"Personal Information" is defined as information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household.

The CCPA applies to any for-profit entity that (i) does business in California, (ii) collects personal information of California residents (or has such information collected on its behalf), (iii) determines, on its own or jointly with others, the purpose and means of processing that information, and (iv) meets one or more of the following criteria:

- has annual gross revenues in excess of $25 million, adjusted for inflation; or
- annually buys, receives for commercial purpose, sells or shares the personal information of 50,000 or more consumers, households or devices; or
- derives 50 percent or more of its annual revenues from selling consumer information.

As personal data is at the heart of the Privacy Regulation and its use is becoming more and more regulated across the world, Data Loss Prevention (DLP) has emerged as an indispensable tool in data protection strategies. Covering a blind spot in traditional security frameworks, DLP protects data against employee negligence or malice, whether a computer is located in or outside the company network. Without a technical solution for monitoring collection, processing and storage of personal data, enterprises run the risk of falling foul of strict regulation. And it's not enough to simply monitor. Companies need to protect and educate their end users at the same time.

In order to ensure compliance, it is essential that companies are equipped with a Data Loss Prevention (DLP) system capable of protecting all the data and processes across all devices, departments and software. While this may be easier said than done, there are practical steps that can be taken to ensure organizations are protected from all types of data loss.

Obligations under CCPA

Personal information is defined under the CCPA as the following:

Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following (if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household):

A) Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.

B) Characteristics of protected classifications under California or federal law.

C) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies.

D) Biometric information.

E) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement.

F) Geolocation data.

G) Audio, electronic, visual, thermal, olfactory, or similar information.

H) Professional or employment-related information.

I) Education information that is not publicly available or personally identifiable.

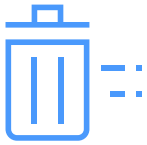
J) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Any information that data controllers have on the data subject, such as date of birth, address, salary, and rent would therefore all constitute protected personal data under the CCPA.

Any organization that acts as a controller has several obligations under this regulation. The main ones include:

Data visibility

One of the basic requirements for any compliance strategy is knowing where your data is. You cannot protect data if you don't know where it is. Each controller will have the responsibility to determine what types of consumer PI its business collects, shares, and/or sells. Therefore, each controller or processor will have the responsibility to maintain records of all categories of processing activities carried out by himself or on behalf of a controller.



Right to deletion

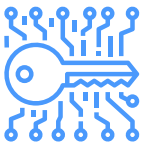
CCPA allows individuals to request the deletion of their personal information unless exceptions apply. Under the CCPA, the right applies to personal information that has been "collected" from the consumer. To that end, there is a need to develop a way to identify, track, and control the collection, retention, and deletion of consumer PI.

Sensitive data

Once you identify your data, you need to classify it properly. Sensitive data discovery is a critical step in any effective data security program. Data loss prevention solutions provide always-on monitoring to control data in near real time. When a file is created, copied, edited, detached from an email, extracted from an archive, retrieved from cloud storage or otherwise modified, it is instantly searched, classified, and reported.

Security

The CCPA does not directly impose data security requirements but instead relies on existing California law to "establish a right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk arising from existing California law." You need to review your network security to ensure that standards are reasonable, particularly with regard to the collection and maintenance of consumer PI.



Pseudonymize or Pseudonymization

The processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures, to ensure that the personal information is not attributed to an identified or identifiable consumer. It is recommended that the encryption travel with the data so that it is protected end-to-end, regardless of where it is shared.

Protecting data on the move

Data is most vulnerable when it is leaving the security of a company network. Nowadays the workforce is becoming increasingly mobile. Many companies offer their employees to work remotely part of or all the time. With many organizations now operating across borders, travel between company offices is inevitable as are industry events and on-site client meetings. The organization is being required to understand how data moves within it. Documenting the way information flows in your company by making an inventory helps demonstrate that the organization is being compliant. Mapping the flow of data will also help to identify areas that could cause CCPA compliance problems.

Data accuracy

Organizations should take all reasonable steps to ensure the personal data that they hold is not incorrect or misleading. To that end, 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 any data centers, it requires that the organization be able to access, report and remove personal information from all those systems when required by consumers or regulators. To satisfy CCPA requirements, you must be able to track the movement, or lineage, of a contacts personal data – where it was first acquired, whether consent was obtained, where it moves over time, where it resides in each of your systems, and how it gets used. The connections between those systems and silos are key to tracking the complex path that personal data follows through your enterprise.

Personal data breach

The CCPA introduces a requirement for all organizations to report personal data breaches to the relevant supervising authority. Organizations should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will aid decision-making as to whether or not you need to notify the relevant authority and affected individuals. Beyond that, the organization must keep a record of any personal data breaches, regardless of whether or not it requires notification.

Data Loss Prevention

Much of the focus on the California Consumer Privacy Act (CCPA) has been on the new rights it affords California consumers, including the right to access, delete, and opt out of the sale of their personal information. But arguably the greatest risk to covered businesses involves data security, as the CCPA creates a private right of action with substantial statutory penalties for breaches involving a consumer's personal information.

The CCPA allows consumers to sue businesses when their *"non encrypted or non redacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."* Violations of this provision are subject to statutory penalties of $100 to $750 per incident, additional actual damages, and injunctive relief. Judges may consider a defendant's "assets, liabilities, and net worth" in determining the precise penalty.

The CCPA does not define the exact security measures that should be implemented. CCPA defines "reasonable" security based on the nature of the personal information a company holds. A key first step for many organizations is to map the data held by the organization in order to determine the most "reasonable" set of controls to best protect it.

In addition, given that the CCPA's private right of action is partially conditioned on any compromised data being "non redacted" or "non encrypted," businesses are well-advised to assess whether appropriate redaction and encryption methods are employed and operating effectively.

To that end, Data Loss Prevention (DLP) solutions offer unparalleled insight into a company's data, allowing admins to set strict rules concerning specific sets of sensitive data while allowing employees liberty to freely manage data outside of these categories. It is an easy way to add an additional layer of security to a company's network and ensure that human error or malicious intentions do not invite the wrath of the DPA upon a business. In the era of the CCPA, there will be no more excuses for companies to suffer 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 data to be classified into three DLP functional types: "Data In Use" (DIU) DLP, "Data In Motion" (DIM) DLP and "Data At Rest" (DAR) DLP.

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

Additionally, the criterion of real-time protective actions for all data states must include practically all local channels on endpoint computers, 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 block, remediate, alert, log, shadow-copy, and more.

ITsMine Next Generation DLP Solution

DLP solutions are uniquely situated to provide not only informational support but also tools that can help meet the strict regulations listed in the CCPA. Among those requirements are data discovery services which help the organization understand where personal data is stored, meet the restrict personal data usage requirement through data in use monitoring, prevent personal data tampering and loss, and maintain personal data security standards.

But today, these capabilities are not enough. State of the art DLP generation products must be simple to deploy and simple to use, automatically classify and track data, restrict who has access and be able intervene in real time if data is sent to the wrong person, all while consistently reporting back to data owners, end users and security analysts, using prevention mode with no false positives and short term implementation processes with rich forensics abilities. The new DLP generation takes into account the need for data deletion, encryption (in case of Ransomware, for example) and modification.

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

ITsMine™ covers two unique use cases to help any organization meet the following

requirements:

1. Find about data breaches and get critical forensics information

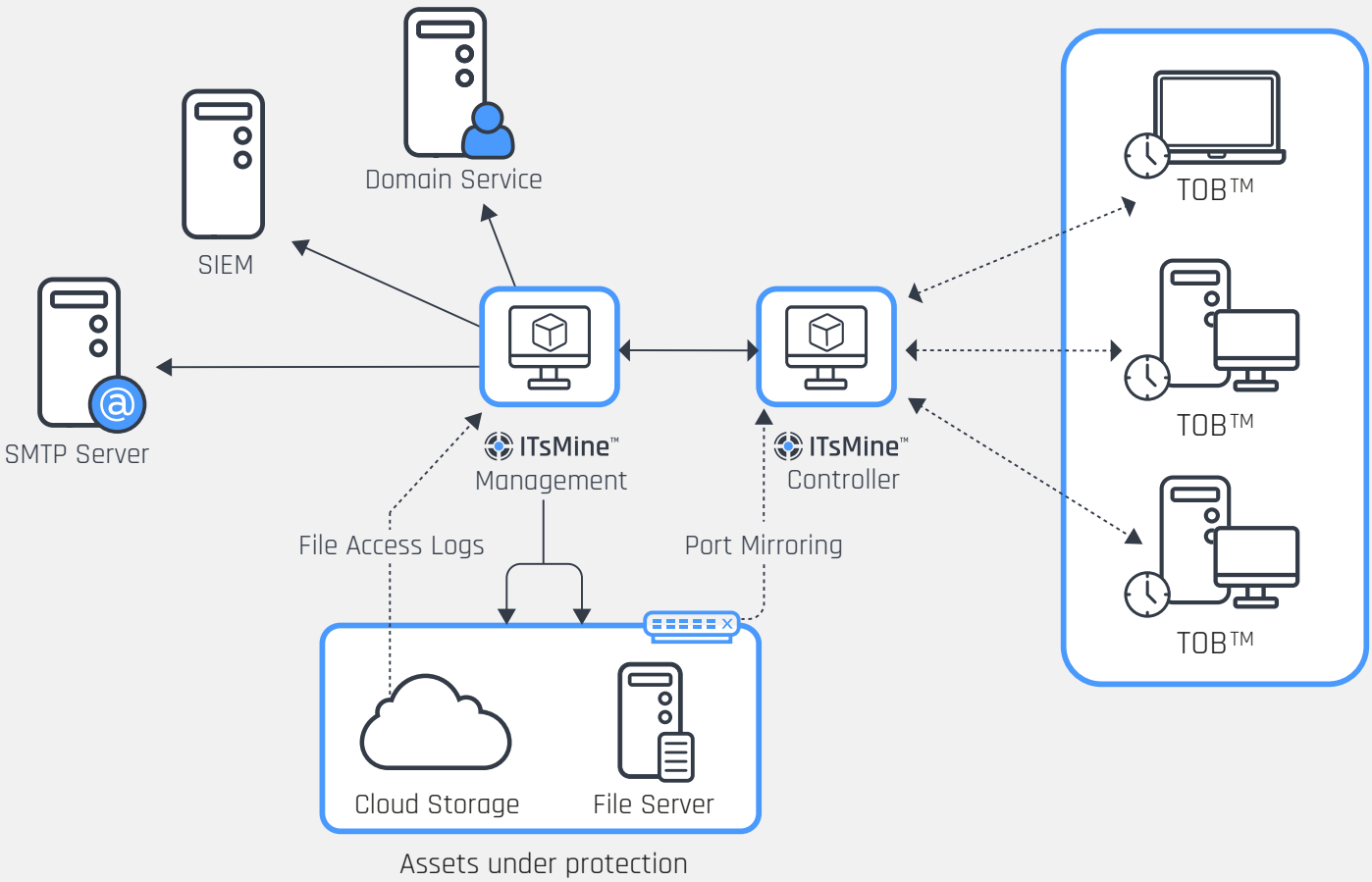
2. Track extremely important files when in use; both inside and outside the organization

The Technology

ITsMine™ offers an innovative approach to data loss prevention. Initially, the software automatically creates a HeatMap of the organizational file storage areas, classifying the folders by their degree of importance as well as based on daily user access. Second, 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 in each SoftwareMine. The "minefield" changes on a daily basis. Additionally, an administrator can mark specific files or folders that they wish to track using ITsMine™ manual policy.

Thirdly, 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 behavior, the system will actively check if the vector of attack is external or a rogue employee and classify the risk level of the "security event" and will automatically decide whether to educate the user, block a specific activity or even 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 would not remain on the endpoint and will be saved only on the file storage (Endpoint Sanitation).

When taking into consideration the need for a DLP solution and trying to comply with the CCPA requirements, it is important to review ITsMine main implementation benefits:

CCPA requirement	Traditional DLP	ITsMine DLP
Data discovery and mapping (1798.100)	Yes – but it might cause huge numbers of false positives	**Yes +** finding the most interesting areas in the company's file storage and protecting them.
Track sensitive personal data (1798.100)	Yes	**Yes +** full review on data flow and ability to warn users accessing certain sensitive areas.
Data security (1798.105, 1798.140, 1798.81)	Yes	**Yes +** a layer of data protection restricting the transmission of personal data outside the network and recognizing its flow. Further adds the ability to ensure a level of security appropriate to the risk.
Data accuracy (1798.115, 1798.110)	No	**Yes +** there is a need to take all reasonable steps to ensure the personal data that companies hold is not incorrect or misleading.
Data breach (1798.150)	Yes – but not the main goal	**Yes +** Find about data breaches and get critical forensics information.
Right to deletion (1798.105)	No	**Yes +** an option to identify, track, and control the collection, retention, and deletion of consumer PI.

Conclusions

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

Neither DLP nor any other technology alone can be a "silver bullet" for the CCPA. A whole slew of various complementary information security and privacy enhancing technologies must be assembled to ensure full compliance. Even so, DLP is one of the critical pieces of the CCPA compliance puzzle in terms of data breach.

ITsMine attempts to drastically change the way enterprises engage with DLP solutions by approaching the problem from a different angle. ItsMine provides a DLP solution that is easy to implement, easy to automate, requires minimal maintenance, is non-intrusive, uses minimal resources, and is capable of providing more information than ever before in the event of a breach. The end product aims to satisfy the listed objectives while providing equivalent or greater protection than the competition. ItsMine provides end-to-end data-centric protection that prevents unauthorized access, maintains CCPA compliance by using encryption and granular access controls protect consumer data as it's collected, processed, and shared, ensuring consumer data privacy while allowing your organization to continue developing innovative data strategies to support growth.