Data Control

Monitor sensitive data across endpoints and servers

Real-time security, visibility and control over personal data. Simplify GDPR compliance.

May 2018 will see the coming into force of the European Union's General Data Protection Regulation (GDPR). This new regulation, aimed at improving data protection and treatment, will force all organizations without exception to **strengthen the security of all the Personally Identifiable Information (PII)** they store and/or process, especially data held, used or transmitted on **employees' and collaborators' devices.**

WHY DO YOU NEED TO PROTECT YOUR ORGANIZATION'S PERSONAL AND SENSITIVE DATA?

Companies must ready themselves to comply with GDPR, which comes into force in May 2018 and will bring with it 'dissuasive' fines of up to 20 million euros or 4 percent of a company's global annual turnover, whichever is greater, in the event of breach.

The GDPR will impact all companies, industries and regions, including those outside the EU, which collect and store personal data of any EU citizens.

Also, companies must be ready to avoid the reputational damage caused by a data leak, and its negative effects on the confidence of employees as well as current and potential customers.

Organizations are facing some major challenges to comply with the upcoming regulation. Mainly, they need to be able to:

- **Reduce the proliferation of uncontrolled and unstructured data.** Unstructured data held on servers as well as on employees' and collaborators' (partners, consultants, etc.) endpoints and devices makes up roughly 80 percent of all business related data. As the volume of unstructured data doubles every year, so does the risk posed to businesses[1].

- **Fight off the exponential increase in exfiltration cases.** The number of cases where poorly managed and secured data is exfiltrated from computing systems is increasing every day. Often the affected organization is not even aware that this is happening. These data thefts are usually due to external attacks, malicious insiders driven by lucrative objectives or revenge, or simply negligence.

THE SOLUTION: PANDA DATA CONTROL

Data Control is a data security module fully integrated into the Panda Adaptive Defense platform. Data Control is designed to assist organizations in complying with data protection regulations, as well as discovering and protecting personal and sensitive data both in real time and throughout its lifecycle on endpoints and servers.

Panda Data Control discovers, audits and monitors **unstructured[2] personal data** on endpoints: from data at rest to data in use and data in motion.

Figure 1 – General view of the files that contain personal information and the users that have accessed to them.

KEY BENEFITS

Discover and audit

Identify files with Personally Identifiable Information (PII) as well as users, employees, collaborators, endpoints and servers in your organization that are accessing this personal data.

Monitor and detect

Implement proactive measures to prevent access to PII with the help of reports and real-time alerts on the unauthorized and suspicious use, transmission and exfiltration of personal data files.

Simplify management

The Panda Data Control module is native in Panda Adaptive Defense and Panda Adaptive Defense 360. It doesn't require organizations to deploy any additional software or hardware, and can be easily and immediately activated without cumbersome configurations. The Data Control module is enabled and managed from the cloud platform.

Demonstrate compliance with applicable regulations to senior management, the DPO[3], all other employees in your organization, and the Supervisory Authorities. Show the strict security measures in place to protect PII at rest, in use and in transit between endpoints and servers.

PII SECURITY AND GOVERNANCE

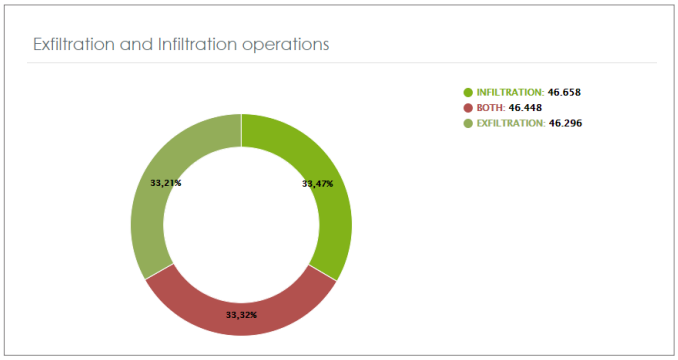
Organizations protected by **Panda Adaptive Defense** can rest assured that their endpoints and servers won't be compromised by malicious programs coming from external sources, and therefore won't fall victim to external data exfiltration attacks.

Panda Adaptive Defense's **classification service categorizes 100 percent of all applications** running on the protected endpoints and servers, returning a verdict on their trustability or malicious nature by using **machine learning** techniques supervised by Panda Security's malware specialists. This system ensures that **only those applications classified as goodware** are allowed to run.

The **Data Control module** leverages the solution's Endpoint Detection and Response (EDR) capabilities to continuously monitor the protected endpoints in the organization, discovering and protecting the unstructured personal data held and transmitted across the network.

Finally, the Data Control **alerts and reports** can be customized and adapted to the specific needs of each company.

Figure 2 - Operations with files at risk of exfiltration and infiltration: The charts allow you to monitor and assess the risk of the operations performed on PII files by users and machines. This way, Data Control helps organizations adopt measures to prevent and control data exfiltration operations.



KEY FEATURES

Data Discovery:

Creates an indexed inventory of all files that store unstructured personal data (data at rest), with the number of occurrences of each type of data. It classifies all information automatically.

The classification combines different techniques and algorithms of machine learning that optimize the results while reducing false positives and resource consumption on devices.

Data Monitoring:

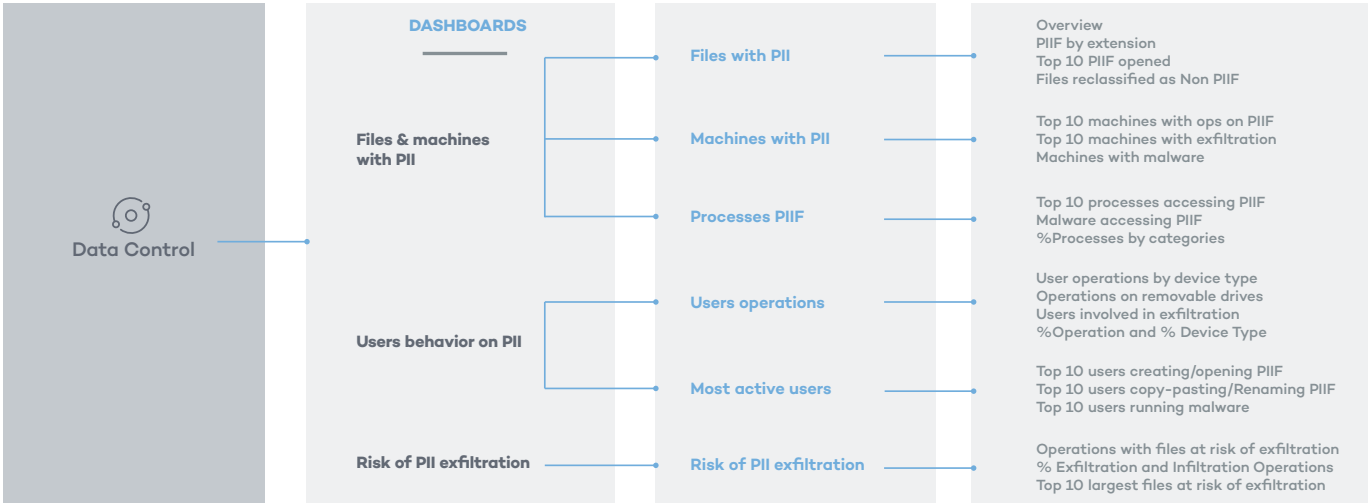
Monitors the various types of operations performed on unstructured files (data in use), while keeping the personal data file inventory fully up to date. Any attempt to copy or move any of these files out of the network via email, Web browsers, FTP or removable storage (data in motion) is recorded by the module.

Data Visualization:

The results of the data monitoring and discovery tasks are continuously synced on the Adaptive Defense platform and in its module Advanced Visualization Tool. This module provides tools for investigating all events affecting data at rest, in use and in motion, both in real time and retrospectively throughout its lifecycle on devices.

Data Control's dashboards and predefined reports and alerts help to cover use cases and ensure security governance of the unstructured personal data held on the organization's protected devices.

Figure 3 – Panda Data Control – Dashboards, sections, charts and predefined queries.



HOW PANDA DATA CONTROL ASSISTS WITH GDPR COMPLIANCE

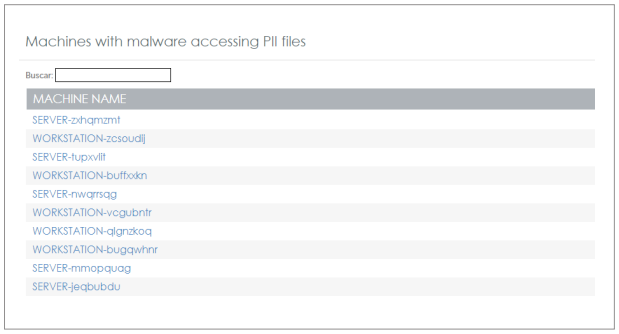
GDPR Article	Panda Data Control feature
Art. 32: Security of processing. *«The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.»*	Panda Data Control provides tools for organizations to assess, both in real time and retrospectively, whether the personal data files stored on their network are accessed only by authorized personnel and whether the security policies in place are adequate or not. Available reports include: • Machines with PII, PII Files (PIIFs), Machines with most operations on PIIFs and Malware processes accessing PIIFs, in the Files and machines with PII dashboard. • Distribution of types of operations on PII, Users involved in Personal Data operations, and Users running malware, in the User operations on PII files dashboard.
Art. 33: Notification of a personal data breach to the supervisory authority. *«In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent. This notification shall describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.»*	Panda Data Control offers, in addition to the detailed graphs for compliance with article 32, includes a series of reports specially focused on PII exfiltration: • Operations with files at risk of exfiltration and infiltration. • Largest files at risk of exfiltration. • Users/machines involved in exfiltration operations in the panel: Risk of PII exfiltration.
Art. 35: Data protection impact assessment. *«Where a type of processing in particular is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.»*	The Data Control module aims at identifying those files that store personal information, as well as monitoring the actions taken on them and the users involved. This data enables organizations to discover the volume, type and use of the personal information residing on their network, so that they can assess the impact and risk of processing such information. The aforementioned dashboards and reports apply to this article as well.
Art. 39: Tasks of the data protection officer (DPO). *«The data protection officer shall have at least the following tasks:* *· To monitor compliance with this Regulation.* *· To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35.»*	All of the aforementioned dashboards and reports, especially those referring to article 35, are essential tools to help the DPO fulfil their duties.

PANDA DATA CONTROL DASHBOARDS

Art. 32: Security of processing.

Files and machines with PII Data Control Dashboard - Machines with malware accessing PII files:

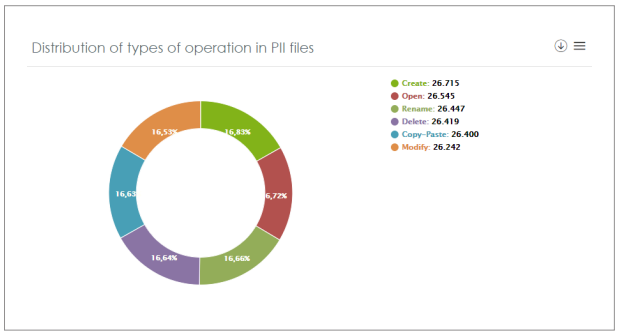
This dashboard shows the top 10 computers where malicious processes have been detected accessing personal data. This information allows security administrators to detect recurrent malware infections and persistent threats on certain computers, as well as to assess the impact of these threats on the personal data held by the organization as required by the GDPR.



Art. 33: Notification of a personal data breach to the supervisory authority.

User operations on PII files Data Control Dashboard – Distribution of types of operation in PII Files:

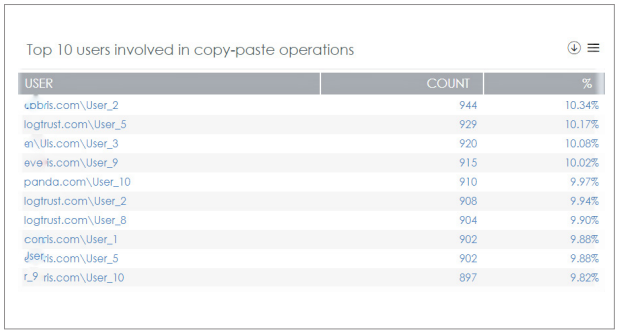
This dashboard displays the types of operations performed on the personal and sensitive data files handled by your organization. A significant increase or decrease in the number of any of these operations might indicate a data security incident or event.



Art. 35: Data protection impact assessment.

User operations on PII files dashboard – Top 10 users involved in copy-paste operations:

This dashboard lists the top users who performed copy-paste operations on files with personally identifiable information (PII). Data Control monitors other types of operations as well: accessing, creating, opening, renaming, deleting, etc.

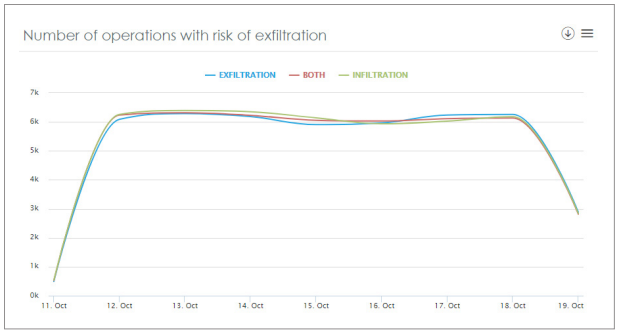


Art. 39: Tasks of the data protection officer (DPO).

Risk of PII exfiltration dashboard - Number of operations with files at risk of exfiltration:

This graph helps organizations monitor personal data flows by displaying the number of exfiltration operations performed on sensitive data files across the network.

This information enables the DPO to determine the usual number of exfiltration operations, and detect deviations caused by security incidents.



[1] Carla Arend. IDC Opinion - March 2017.
[2] Unstructured data refers to data that does not reside in a database or any other data structure. Unstructured data can be textual or non-textual. Panda Data Control focuses on the textual unstructured data held on endpoints and servers.
[3] DPO (Data Protection Officer): The person responsible for overseeing the data protection strategy in an organization.