Data Control

Panda Data Control Administrator's Guide

Version: 1.1.00-00

Author: Panda Security

panda

pandasecurity.com

1. Preface

Who is this guide aimed at?

Icons

1.1. Introduction

This guide offers the information and procedures necessary to benefit fully from the Panda Data Control service.

1.2. Who is this guide aimed at?

This documentation is aimed at technical personnel in IT departments of organizations that have contracted the **Panda Data Control** service for **Adaptive Defense** and **Adaptive Defense 360**.

This manual includes the procedures and settings required to interpret and fully benefit from the security information provided by the **Panda Data Control** platform.

All the procedures and instructions in this guide apply both to **Adaptive Defense** and **Adaptive Defense 360**. The term "Adaptive Defense" is used generically to refer to both of these advanced security products.

1.3. Icons

The following icons are used in the guide:

Additional information, such as an alternative way of performing a certain task.

Suggestions and recommendations.

Important advice regarding the proper use of the options available in the **Panda Data Control** service**.**

See another chapter or section in the guide for more information.

2. Introduction

2.1. Introduction

The evolution of data protection regulations, along with a considerable increase in the amount of advanced threats in circulation, have combined to generate greater interest in overhauling the security protocols that protect the personal information of companies' customers and employees.

This personal data, regardless of its status (data in use, data in motion or data at rest) has to comply with new security requirements, which derive from:

- **Compliance with new European regulations**: From May 2018, the GDPR will issue fines of up to €20 million or 4% of a previous year's turnover for failure to comply with the regulations. All companies within the EU that compile and store the personally identifiable data (PII) of customers, employees and suppliers resident in the EU are subject to these rules.
- **The greater volume of unstructured data in companies**: Data stored in office application files (Word, Excel, text files, HTML, etc.) represents 80 percent of the data handled by organizations, and is spread, with no real control, across the servers, desktops, laptops and other devices of employees, partners and contractors, etc.
- **The publication of confidential data**: It is increasingly common for IT attacks to reveal massive amounts of personal data of customers. Such attacks can be perpetrated by financially motivated outsiders or negligent or disgruntled insiders, among others.

Good data security governance practices are key to mitigating these risks and ensuring compliance with the regulations.

2.1.1 Personal data protection requirements

This new personal data protection scenario gives rise to high-level requirements for organizations, including:

- Controlling the personal data stored in files, with no internal structure, on computers and servers and accessed by hundreds of authorized employees.
- Demonstrating compliance with the legislation and any given time via continuous monitoring.
- Notifying any data leaks to the authorities (DPA - Data Protection Authority) and affected customers within 72 hours.

These requirements however, must be met without increasing the complexity of the products and tools used by the organization to manage IT security.

2.2. What is Panda Data Control? Main benefits

It is a security module integrated in **Adaptive Defense** that supports regulation compliance and provides visibility and supervision of the personal data (*PII*) stored on corporate IT infrastructures.

Panda Data Control visualizes, audits and monitors, in real time, the complete lifecycle of PII files: from data at rest, operations carried out on them and their external transfer.

2.2.1 Main benefits

Visualization and audits

Using dashboards, reports and alerts, documents with PII are identified along with the operations carried out by the users of corporate computers and servers.

The risk of leaks is reduced by evaluating the efficacy of existing security policies, offering key information to improve and adapt, and inform users of good practices and other measures.

Monitoring and detection

It implements proactive measures for accessing and acting on PII files with reports and alerts in real time about their use and any suspicious or unauthorized exfiltration/infiltration.

To avoid fines or damage to corporate reputation, alerts immediately notify of any possible theft of personal data. The information collected in the Data Control tables, the dashboards and the predefined reports allow real-time analysis of the complete lifecycle of an incident: who carried out each action, when, where, on which computer or server, and what media was used.

Simplified management

Panda Data Control is a module of **Panda Adaptive Defense** and **Panda Adaptive Defense 360** and therefore does not require any additional deployment. It is activated immediately, without intervention from the administrator and managed quickly and simply from the same cloud platform.

2.3. Panda Data Control and the General Data Protection Regulation (GDPR)

The GDPR (General Data Protection Regulation) is the new legal framework in the EU that replaces the previous data protection directive.

Its aim is to protect personal data and provide a reference point for developing safe procedures for processing, storing and, where necessary, destroying personal data handled by organizations. The law grants eight specific rights to individuals regarding how companies can use the data that is directly and personally related to them.

It also sets out very strict rules that govern what happens if the rules regarding access to personal data are violated and the consequences (fines) that organizations may suffer.

2.3.1 GDPR articles related to the Panda Data Control features

Panda Data Control helps comply with the following articles of the GDPR:

Article 32: Security of processing

This requires the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk. It also requires the evaluation of the risks of processing data and the implementation of measures for controlling data usage and access.

Panda Data Control provides information about how PII files are distributed on the network and their access by users: the computers used and the types of actions being carried out. This makes it possible to verify that the data is accessed only by authorized personnel, and if the company security policies are correct, to assess the risk in the management of PII.

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

This requires that the competent authority is notified within 72 hours whenever there is a breach of security regarding personal data, if it may represent a risk to the rights and freedoms of natural persons.

Panda Data Control analyzes the incident to assess its impact, showing which computers, users and files have been compromised and identifying the type of leak: if it was caused by malware, by unauthorized external communication of data (exfiltration) or by actions from within the company (infiltration).

Article 35: Data protection impact assessment

This requires an assessment of the impact of data processing operations on the protection of personal data where it is likely that such processing, due to its nature, scope, context or purpose, represents a high risk to the rights and freedoms of natural persons.

Panda Data Control automatically identifies files containing personal data and monitors the actions taken on them, and the users who execute them. As such it is possible to know the quantity, type, volume or use of personal information so that the impact and risk of processing can be evaluated.

Article 39: Tasks of the data protection officer (DPO)

This establishes the figure of the DPO (data protection officer) to monitor compliance with the regulation and offer advice regarding data protection impact assessment and monitor its performance.

Panda Data Control offers the DPO graphical tools to support the supervision, assessment and understanding of the risks associated with the processing of personal data.

2.3.2 Panda Data Control features related to the GDPR

The basic information from which **Panda Data Control** constructs the security intelligence for the processing of personal data is summarized as follows:

- Discovery/automatic classification of files without an internal structure as either PII files or not PII files
- Information about PII files:

  - Name
  - Type
  - Extension
  - Size
  - Type of personal information in the file
- Classification of processes acting on the PII files:
  - Malware
  - Pending classification
  - Goodware
- Type of action taken on the PII files.
  - Create
  - Open
  - Rename
  - Delete
  - Copy – Paste
- Classification of actions taken on PII files:
  - Data leaking or communication actions (*data exfiltration*)
  - Data introduction operations (*data infiltration*)
- Users that take actions on the PII files.
- Location of computers with PII files within the corporate IT infrastructure.

2.4. Panda Data Control service features

Panda Data Control deploys technology on computers that is specifically designed to collect detailed information about any PII files discovered. This information is received by the **Threat Intelligence Platform**, where it is processed and enriched to be sent to the **Advanced Visualization Tool** for advanced visualization and presentation.

2.4.1 Features

Data Discovery

Creation of an inventory thanks to the automatic classification of unstructered files containing personal data, along with the number of times that each type appears.

Panda Data Control uses a combination of rules, regular expressions and machine-learning algorithms, among other techniques, that optimize the classification results, minimizing false positives and the consumption of resources on computers and servers.

Data Monitoring

Monitoring of the actions carried out on files without an internal structure (data in use), keeping up-to-date the inventory of personal data files on corporate computers (data at rest). When these files are to be copied or transferred from the computer (data in motion), this action is recorded indicating its origin (mail clients, browsers, FTP, etc.).

Data Visualization

The result of the discovery and continuous monitoring is synchronized in real time on the **Adaptive Defense Platform**. The **Advanced Visualization Tool** module provides tools to interpret events recorded on personal data at rest, in use and in transit, both in real time and retrospectively throughout is lifecycle on corporate computers.

2.5. Main components of the Panda Data Control architecture

Below you can see the general architecture of the **Panda Data Control** service and its principal components:

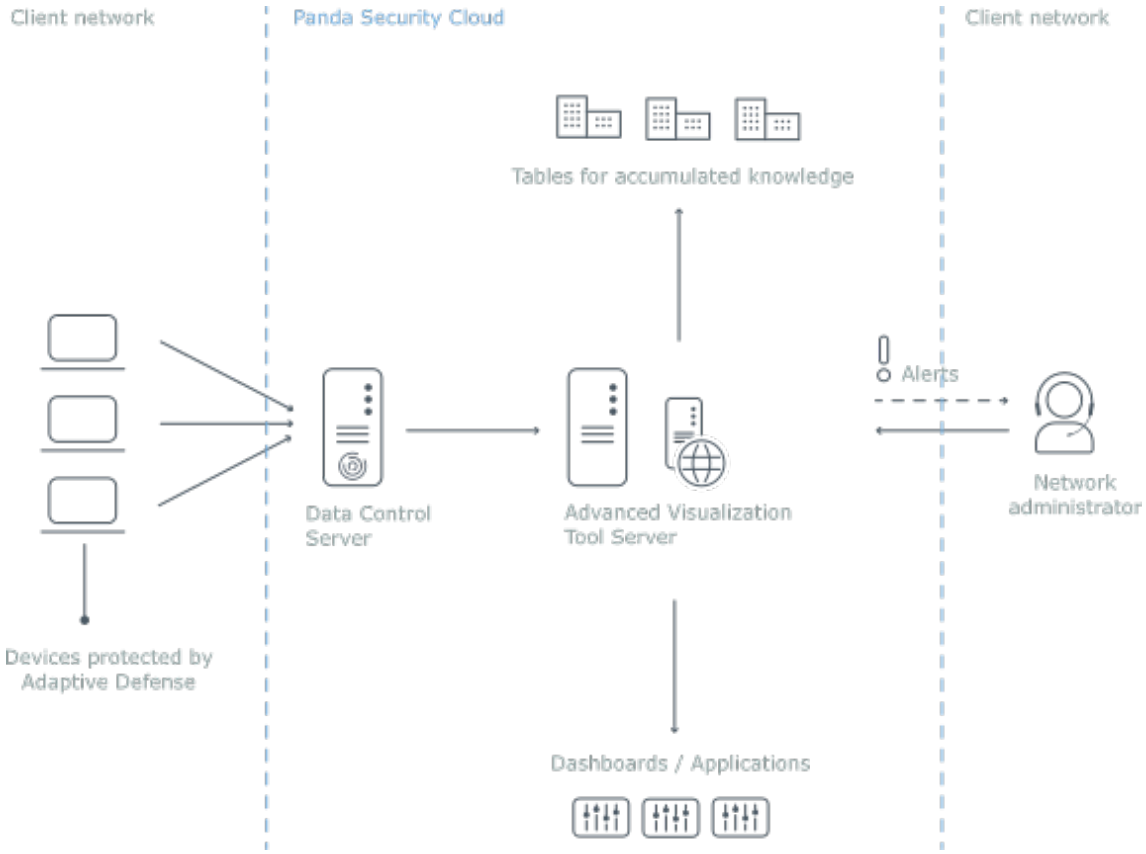


Figure 1: general architecture of Panda Data Control

Panda Data Control comprises the following components:

- Panda Data Control server.

- Computers monitored by Adaptive Defense or Adaptive Defense 360.
- Advanced Visualization Tool server and Web management console.
- Network administrator computer for managing the service.
- Applications / Dashboards.
- PII knowledge table.

2.5.1 Cloud-hosted infrastructure

All the infrastructure directly involved in the service (**Advanced Visulization Tool** server, **Panda Data Control** server, **Adaptive Defense** server) is deployed in the Panda Security cloud, with the following advantages:

- **No maintenance costs for the customer**

As the servers do not have to be physically installed on customers' premises, customers can forget about the costs arising from the purchasing and maintenance of hardware (warranty management, technical problems, storage of spare parts, etc.).

Neither will they have to worry about costs associated with operating systems, databases, licenses or other factors associated with on-premises solutions.

Similarly, the outlay derived from needing specialized personnel to maintain the solution also disappears.

- **Access to the service from anywhere at any time**

The service is accessible from any computer, overcoming any problems that could occur in companies with an infrastructure spared across various sites.

For this reason, it is not necessary to have specific communication deployments, such as VPNs, or special router configurations to enable access to the management console from outside the customer's local network.

- **Service available 24/7 - 365 days a year**

This is a high availability service, with no limit on the number of monitored computers. Customers do not need to design or implement complex redundant infrastructure configurations. Nor do they require specific technical personnel to maintain service availability.

2.5.2 Panda Data Control server

This is a high-availability server farm that harvests all the events related to PII files generated on users'

computers and servers. Its main functions are to:

- Collect the information continuously monitored and gathered by the **Adaptive Defense** agents in real time.
- Store all the data in a table that can be easily accessed by the administrator.
- Build the data sources to feed the charts displayed by **Advanced Visualization Tool** in the management console.
- Generate configurable alerts for situations that could potentially jeopardize personal data.

2.5.3 Computers protected by Adaptive Defense and Adaptive Defense server

Users' computers continually send the actions executed by processes to the cloud-hosted **Adaptive Defense** server. This server automatically generates security intelligence through Machine Learning technologies on Big Data repositories. The security intelligence is added to the events collected from the computers protected by **Adaptive Defense** and sent directly to the **Panda Data Control** server. This operational structure offers the following advantages:

- The information received by the **Panda Data Control** server is already processed by the **Adaptive Defense** server, and as such contains the security intelligence that will help identify if the process acting on PII files is goodware or malware.
- Data packets are only sent once from the protected computers protected by **Adaptive Defense**, saving bandwidth and the need to install SIEM servers locally in every location, which would be much more complex and expensive to maintain.
- No additional configuration is required, neither in the **Adaptive Defense** console, nor on the protected computers. The **Adaptive Defense** servers will automatically and transparently send all necessary information to the **Panda Data Control** server.

To classify unstructured files, **Panda Data Control** requires Microsoft Office 2007 with Microsoft Filter Pack or later.

Refer to Appendix 3 Panda Data Control requirements for a full list of requirements. See the FAQ https://www.pandasecurity.com/spain/support/card?id=50116 for installing Microsoft Filter Pack

2.5.4 Advanced Visualization Tool server and Web management console

This generates the widgets, dashboards and graphical applications that display the collected data in an ordered and easy-to-understand way.

The Web server also hosts the management console, accessible from any place at any time through any ordinary compatible browser.

Advanced Visualization Tool implements functions through the tools and resources described below:

- A wide range of widgets that enable visualization of the actions taken on the PII files.
- Dashboards that can be configured by the administrator with information for the IT department.
- Configurable alerts that are generated in real time to reveal potentially dangerous situations.
- Graphical resources to view and work with the **PII knowledge table** with details of the actions taken on files with personal data.
- Advanced tools for searching and processing the information stored: filters, groupings, advanced operations with data, generation of new widgets with information, etc.

2.5.5 Applications / Dashboards

The most relevant information for the IT team is displayed through three applications accessible from the Web management console:

- **Files and machines with PII**: Identifies PII files on the network, showing the computers they are on and the actions taken on them.
- **User operations on PII files**: Shows the operations that users take on the PII files, detailing the physical device they are on (hard disk, USB drive, etc.)
- **Risk of PII extraction**: Displays actions that could represent a leak of personal data.

2.5.6 PII Knowledge table

Panda Data Control stores the PII information in a single table with the following features:

- **Raw data storage**: This is the result of the monitoring of computers and servers, along with the security intelligence information generated by the **Adaptive Defense** server.
- **Continuous storage**: All processes are continuously monitored and the information sent for storage.
- **Real-time storage**

The **PII Knowledge Table** is the base for generating the applications and charts in **Adaptive Visualization Tool,** allowing the filtering and transformation of data (grouping, organization, searches, etc.).

See Chapter 7 for more information about the PII knowledge table and the meaning of each field

2.6. How does Panda Data Control work?

To fulfill confidentiality requirements, **Panda Data Control** implements the service via three different processes that run on different components of the architecture shown in point 2.5:

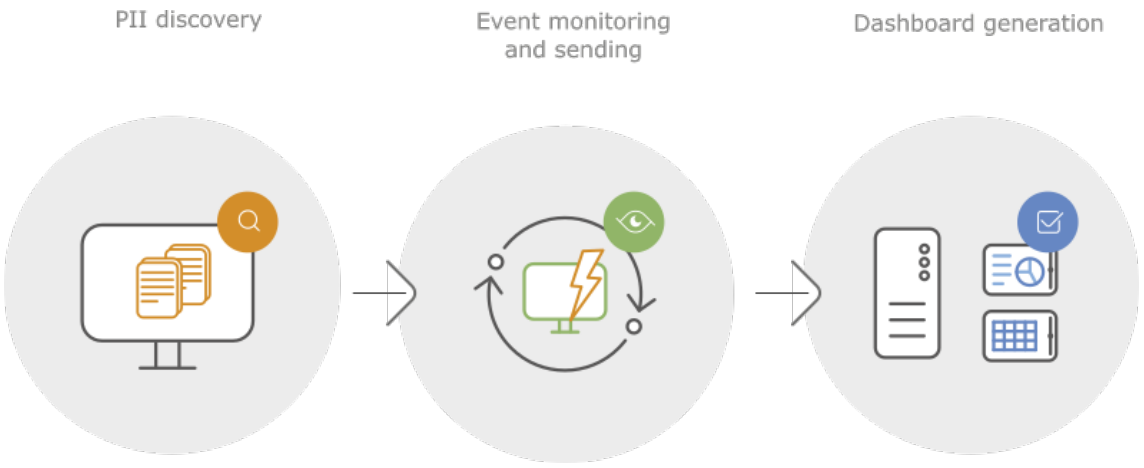


Figure 2: complete flow of processes in Panda Data Control

- Discovery of personal information on computers
- Monitoring of operations on PII files on computers
- Communication and organization of the information in dashboards / applications and in the **PII Knowledge Table.**

2.6.1 Discovery of PII on computers

This process runs on the computers protected by **Adaptive Defense**. The agent scans all mass storage devices connected to the computer or server (local hard drives, external hard drives, USB drives, network drives and RAM disks) for files without an internal structure that contain personal information.

This search is launched automatically when the **Panda Data Control** module is enabled for the first time from the **Adaptive Defense** management console.

See the Adaptive Defense online help for details on enabling Panda Data Control from the management console.

Types of personal information supported

Adaptive Defense applies Machine Learning algorithms and regular expressions to each compatible

file discovered in order to detect personal information. The data recognized as PII are as follows:

- Credit card numbers
- Bank account numbers
- Personal and fiscal ID numbers
- Driving license numbers
- Passport numbers
- Social security numbers
- First names and last names
- Locations (cities) and countries
- Addresses and postcodes
- Phone numbers
- IP addresses

Supported countries

The format and content of PII data differs depending on the country of origin of the person. Currently the following countries are supported:

- Germany
- Spain
- France
- Sweden
- UK

Mass storage devices supported

The files can be on any of the following mass storage devices:

- Local hard disks
- Remote hard disks (remote network drives)
- USB storage devices
- Virtual RAM drives
- CDROMS, DVDs, Blu Ray, etc.

File types supported

Panda Data Control searches for data on the following file types:

- Office

- OpenOffice
- PDF
- TXT
- HTML
- CSV

For the complete list of file extensions supported, see Appendix 1: Extension list.

Data confidentiality

Once the scan is complete, **Adaptive Defense** only sends the **Panda Data Control** server the number of times it found each of the supported PII file types.

Neither the data file nor its partial or complete content is sent to the Panda Data Control server and consequently never leaves the computer on which it is hosted.

Once the search and classification process is complete, **Adaptive Defense** monitors all the actions taken on PII files and reports them to the **Panda Data Control** server.

2.6.2 Monitoring actions on PII files

With the exception of the events generated during the initial scan on enabling the service, the rest of the actions follow the sequence below:

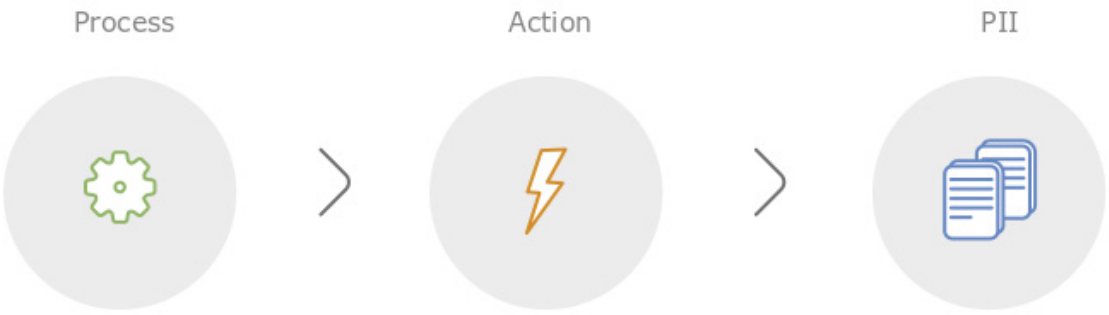


Figure 3: parameters defining Panda Data Control events

For every action that a process takes on a PII file, a single event is stored with detailed information concerning the elements involved. Each generated event is defined by three parameters:

- Parent process responsible for the action.
- Action taken.
- Hash of the file containing personal data.

Process that takes the action

Panda Data Control stores the following information about the process that took the action on the PII file:

- User that launched the process.
- Process name and path.
- Hash of the process.
- Name of the computer on which the process was run and its IP address.
- Classification of the process (goodware, malware, in the process of classification) to assess whether it is a potential case of data theft.

PII file that received the action

Panda Data Control stores the following data about the PII file affected:

- File name and path.
- Hash of the file.
- Host device (local hard disk, external hard disk, USB memory, mapped network drive, virtual RAM drive).

Type of action

Panda Data Control detects several types of actions that can affect PII files:

- Create.
- Open.
- Delete.
- Edit.
- Copy and paste of the file.
- Rename.

2.6.3 Filtering and grouping of the information

Depending on the information sent by the **Adaptive Defense** agents, the **Panda Data Control** server evaluates whether the reported files contain personal data. If it is actually a PII file, all events received are accumulated to feed the various widgets in the applications.

In addition, **Panda Data Control** dumps all the raw data received in the **PII Knowledge Table**.

2.6.4 Classification of the action taken on PII files

When **Adaptive Defense** monitors the actions taken by processes that could send or receive data,

the machine learning algorithms implemented in **Panda Data Control** assess the probability that those operations are part of an unauthorized data exfiltration/infiltration attempt. In such cases, **Panda Data Control** assigns a classification (**Infiltration** or **Exfiltration**) to the operation, indicating the high probability of a security incident to the administrator.

See Appendix 2: Process list for a list of the programs that can form part of an incident associated with the exfiltration or infiltration of personal data.

2.7. Panda Data Control user profile

This service is primarily aimed at the IT department of organizations, and in particular the DPO, who can carry out some or all of the tasks below:

- Audit users' computers and servers looking for PII files.
- Monitor actions taken on PII files.
- Evaluate if there is a risk of data leakage, based on the user, process (goodware or malware) and the type of operation on the PIIF.
- Detect trends that could help anticipate potential security breaches that could lead to the infiltration/exfiltration of PII files.
- Enable compliance with the GDPR.

3. The Web management console

General structure of the Web console

3.1. Introduction

This chapter describes the general structure of the Web management console and its components.

The Web console is the main tool for administrators to view the security status of their network. As a centralized Web service, it offers a series of features that positively affect the way the IT department can work with it:

- **A single tool for leveraging data about PII**

The Web console provides preconfigured graphical tools that allow administrators to easily view all the collected information about the PII files found on the network.

This information is delivered via a single Web console, enabling the integration of various tools and removing the complexity of using products from different vendors.

- **Access to consolidated information without the need to support infrastructure across all locations**

As the server that hosts the Web console is hosted by Panda Security, there is no need to install or maintain specific infrastructure on customers' premises.

Moreover, as it is hosted in the cloud, the server can be accessed from all customers' offices, presenting consolidated data from a single repository. This simplifies data interpretation and speeds up decision making.

3.1.1 Requirements for accessing the Advanced Visualization Tool Web console

In order for you to access the Web console, your system must meet the following requirements:

- Have a certified/supported browser (others may be compatible)
  - Mozilla Firefox
  - Google Chrome

Other browsers may also work, but some of their versions may not be supported. As such it is advisable to use one of the browsers listed above

- Internet connection and communication through port 443
- Minimum screen resolution 1280x1024 (1920x1080 recommended)
- A sufficiently powerful computer to generate charts and lists in real time
- Sufficient bandwidth to display all the information collected from users' computers in real time

3.1.2 Accessing the Advanced Visualization Tool Web console

The **Advanced Visualization Tool** Web console can be accessed via SSO from the **Adaptive Defense** management console, with no need to enter new credentials.

To access this environment, click the **Advanced Visualization Tool** link from the top menu in **Adaptive Defense.**

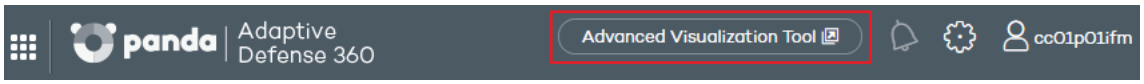


Figure 4: accessing the Advanced Visualization Tool service from the Adaptive Defense console

3.2. General structure of the Advanced Visualization Tool Web console

The Web console is designed to deliver a uniform and coherent experience to administrators, both in terms of visualization and the search for information as well as configuring custom data widgets. The end goal is to deliver a simple yet powerful and flexible tool that allows administrators to rapidly view the status of the personal data stored in the organization's unstructured files without a steep learning curve.

3.2.1 Side menu overview

The side menu is located to the left of the screen and can be accessed at any time.

Initially, this menu only displays the icons for each option. By moving the mouse pointer to the left of the screen, or clicking a free section of the side menu, a description of each icon is displayed.

Below you can see the main options of the side menu:

Home 

This takes users back to the Home page of the Web console.

Data Search 

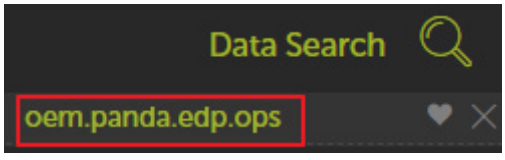


Figure 5: shortcut to the knowledge table

This lets you access the accumulated knowledge table. From here, administrators can view the data as it has been sent from the computers protected by **Adaptive Defense**.

As administrators access the knowledge tables, they appear under the Search option as shortcuts, to make it easier to access them.

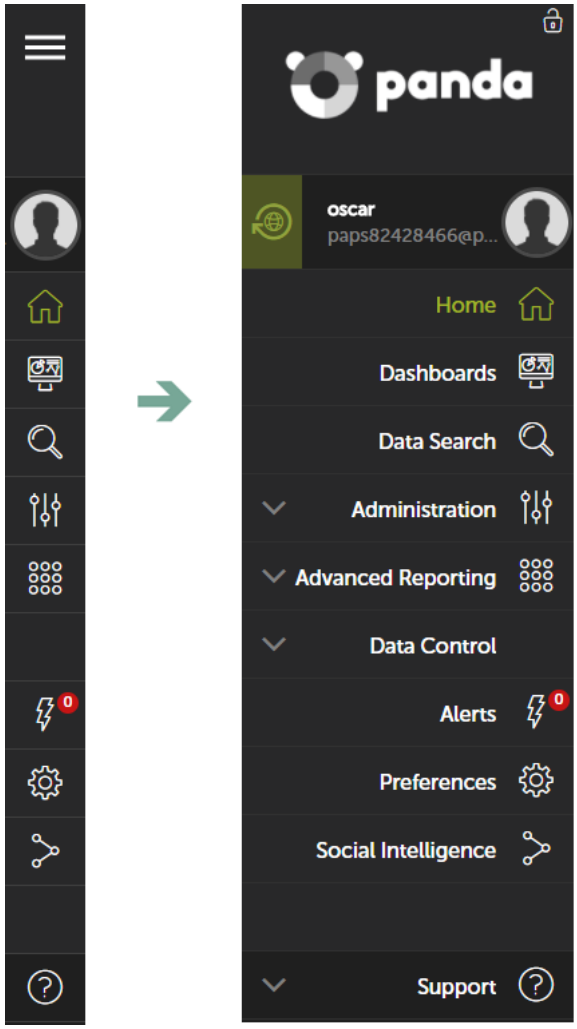


Figure 6: side menu in the Panda Data Control console

See chapter 7 Knowledge table for more information about the fields included in the accumulated knowledge table

Administration

This lets you configure new alerts.

For more information about pre-configured alerts, see Chapter 5: Configured applications.
For more information about how to create and configure new alerts, see Chapter 6: Alerts

Advanced Reporting 

Drop-down menu with the available applications for **Advanced Reporting Tool**.

For more information, refer to Advanced Reporting Tool guide

Data Control

This includes the three applications described below:

- **Files and machines with PII**: This displays the workstations and servers that contain PII files, the PII files found on the network, and the processes that have performed operations on them.
- **User operations on PII files**: This displays the actions taken by users on PII files, and the physical device where the personal data resided (internal hard drive, USB drive, etc.)
- **Risk of PII extraction**: Suspicious operations that could lead to a personal data breach.

Alerts 

This displays a window with information about the alerts received.

For more information about pre-configured alerts, see Chapter 5: Configured applications.
For more information about how to create and configure new alerts, see Chapter 6: Alerts

Preferences 

This section offers a series of options that can be configured for the logged-in user and for others that access the service.

Log out 

Here you can log out of the **Panda Data Control** console. It then displays the IDP (Identity Provider) login screen.

4. Introduction to the applications

Resources and common items on the dashboards
Preconfigured alerts
Generation of new charts

4.1. Introduction

The dashboards are preconfigured applications that provide the network administrator with specific information about the network.

The three dashboards included in the Web console are as follows:

- Files and machines with PII
- User operations on PII files
- Risk of PII extraction

All the dashboards have a common layout, described later in this section, in order to facilitate data interpretation.

The applications also generate alerts that warn administrators in real time of potential problems.

> *To create new alerts in addition to those that are already configured in the applications, see Chapter 6: Alerts*

4.1.1 Accessing the dashboards/applications

Access to the dashboards is available through the side menu, in the **Data Control** section.

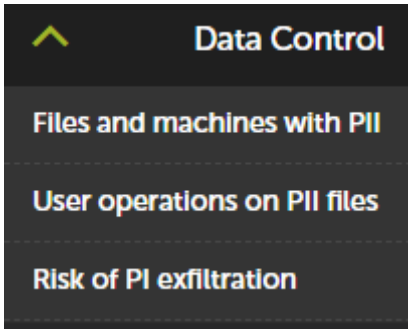


Figure 7: data Control drop-down menu

4.1.2 Accessing the alerts

Access to the alerts is available through the side menu, via **Administration**, **Alerts Configuration**.

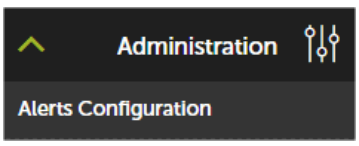


Figure 8: option in the Administration menu to set up the preconfigured alerts

The **Alerts Subscription** screen is used to look for configured alerts, to assign policies, and enable and disable individual alerts.

4.2. Resources and common dashboard items

4.2.1 Time periods for the data displayed

Each application has two controls for defining the time period for the data displayed on screen:

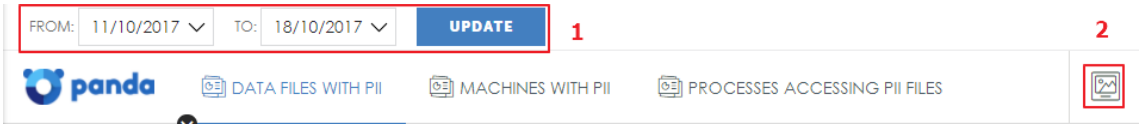


Figure 9: date range picker

- **Date range (1):** This lets you set the time period displayed in the widgets of the selected dashboard. The period will apply to the widgets of all the tabs on the dashboard.
- **Screenshot (2):** This opens an independent window with the content of the tab in graph format so it can be downloaded and printed.

The browser pop-up protection may prevent you from seeing the new window. Disable this feature in the browser in order to see the window

The browser pop-up protection may prevent you from seeing the new window. Disable this feature in the browser in order to see the window.

4.2.2 Tabs

Figure 10: console tabs

The tabs divide the information into different areas according to the level of detail of the data displayed: general information or more detailed reports and data breakdowns.

Each tab offers access to the tools displayed below:

- **Tab name (1):** This describes the information contained in the tab. To select a tab, simply click on the name. The **Detailed information** tabs contain data tables that can be used in reports.
- **Shortcut menu (2):** Click the arrow to display a drop-down menu that takes you directly to any section within the tab.

4.2.3 Sections

The information within a tab is divided into sections. Each section is a group of widgets with related information.

Click the arrow button to display or hide a complete section.

Figure 11: accessing a tab's sections

4.2.4 Widgets

These are controls that display the data using tables and advanced graphs.

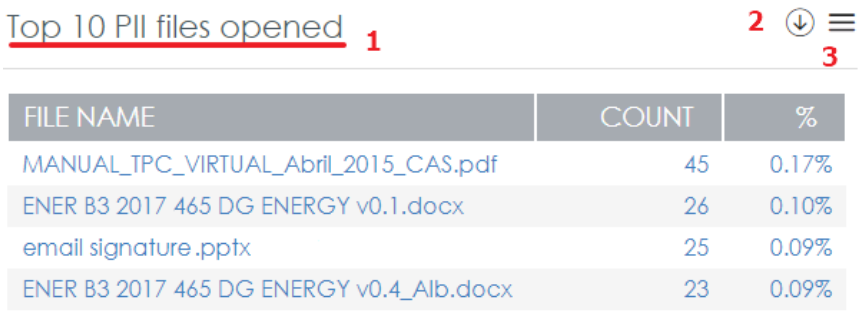


Figure 12: console widget

Each widget comprises several items:

- **Widget name (1)**: This indicates the type of information displayed.
- **Display/hide button (2)** : This lets you hide or display the widgets you want.
- **Widget menu (3)** : This contains three options:
- **Screenshot**: This opens the widget content on a new page so it can be saved as a graph, printed, etc.

> *The browser pop-up protection may prevent you from seeing the new window. Disable this feature in the browser in order to see the window*

- **Download Data**: This downloads the data viewed with the widget. The data is downloaded in .CSV format separated by commas, so it can be imported into other applications.
- **Go to query**: This displays the knowledge table associated with the widget and which is the source for its data, along with the settings for the filters, groups and operations.

The Go to query option lets you see the precise configuration of the data source that feeds the widget, including the selected time period. This way, administrators can experiment with the chart displayed using the SQL statement. More information is available later in this chapter.

- **Support** : Support window with hotkeys assigned to the widgets to browse the data displayed.
- **Information**: These are the different tables and charts that display the information.

4.2.5 Tables and charts

The data is represented through a range of charts (Voronoi diagram, line and bar charts, pie charts, etc.) and more detailed data tables.

Calendar charts

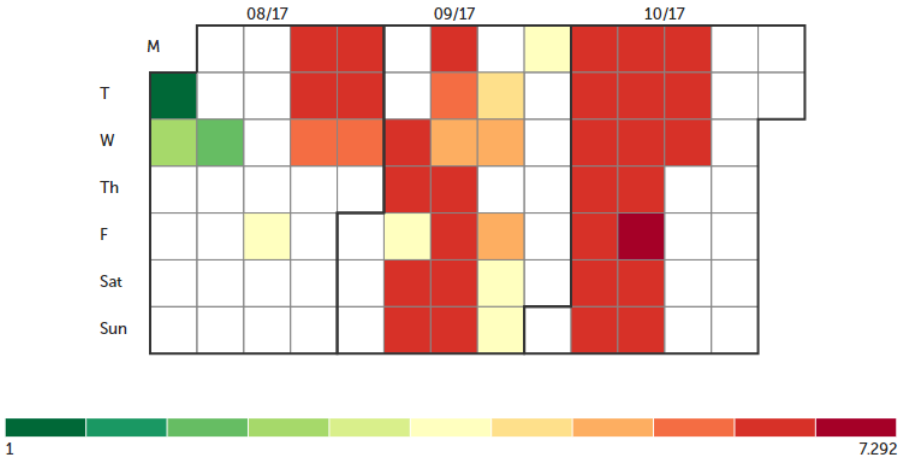


Figure 13: calendar chart

This represents the real values of the events detected throughout a year.

Each box represents a day in each month. The boxes are grouped into blocks that represent the months of the year.

In turn, each box is colored according to the number of events in the day. The color range (green - red) lets you quickly compare days against each other, thereby giving a better view of the development of the indicators monitored.

Move the mouse pointer over a box to see the corresponding color in the key, and a tooltip with the date and the exact number of events.

Bar chart

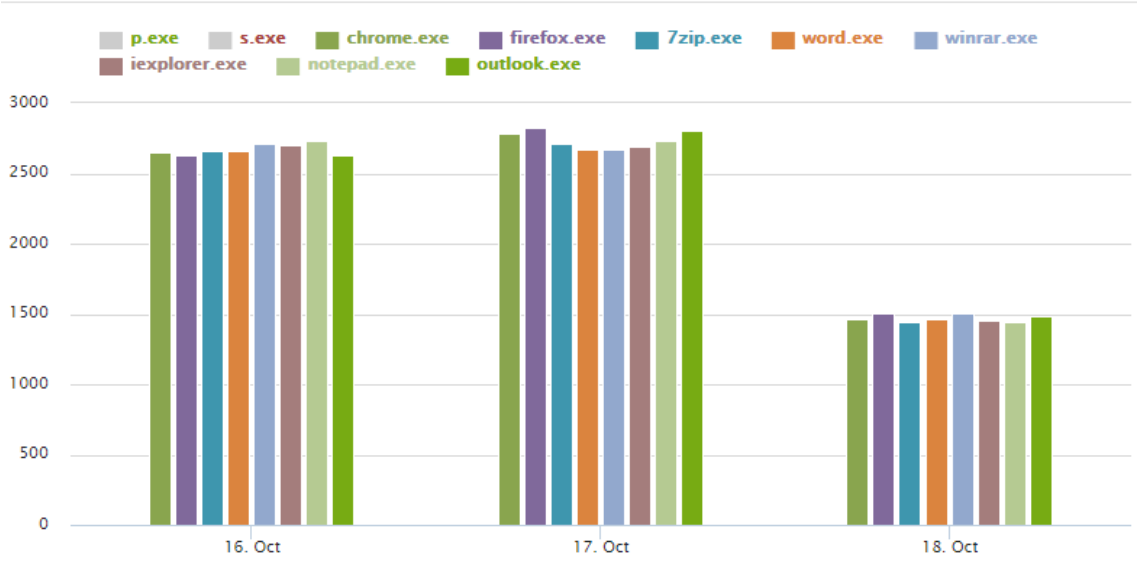


Figure 14: bar chart

Bar charts let you see, in a single chart, the development of several different concepts, represented by different colors in the key at the top of the chart.

Place the mouse pointer over the data and a tooltip will indicate the date and time of the measurement and the value of the concept at that moment.

Line chart

Shows the development or evolution of one of several concepts, represented by different colors in the key at the top of the chart.

Place the mouse pointer over the data and a tooltip will indicate the date and time of the measurement and the value of the concept at that moment.

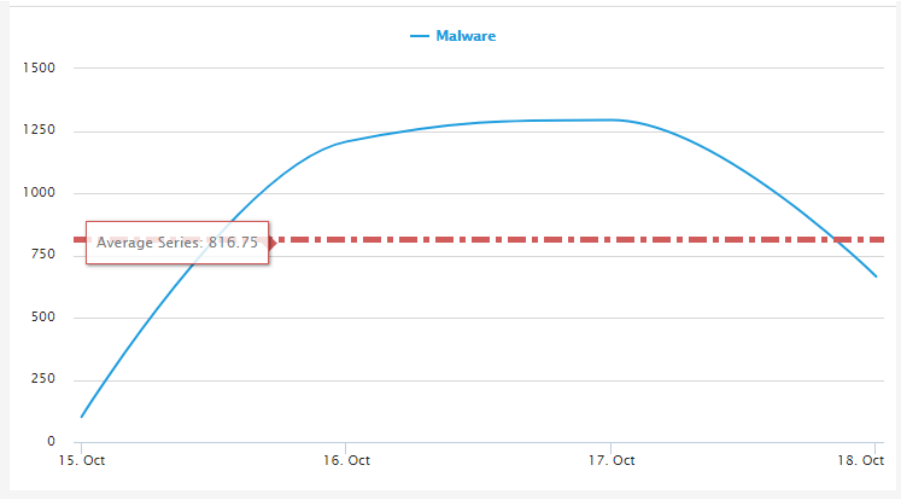


Figure 15: Line chart

Voronoi diagram

A Voronoi diagram shows information from the corresponding knowledge table in the form of groups of data. It uses polygons of various shapes and sizes whose area represents a relative (percentage) number of items shown inside.

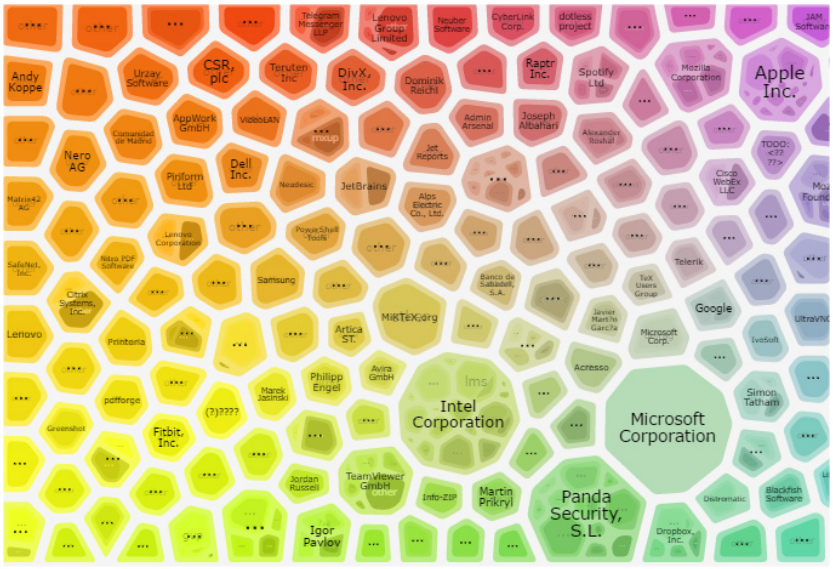


Figure 16: voronoi diagram and Thiessen polygons

- **Navigating a Voronoi diagram**

A polygon can comprise other polygons representing groups of lower-level data.

As such there is a hierarchy of levels of groups ranging from the more general to the more specific. Voronoi diagrams allow you to navigate through the different levels of data groups:

- Double-click using the left mouse button on a group of data to access the lower level.
- From there, double-click using the right mouse button to return to the previous level.

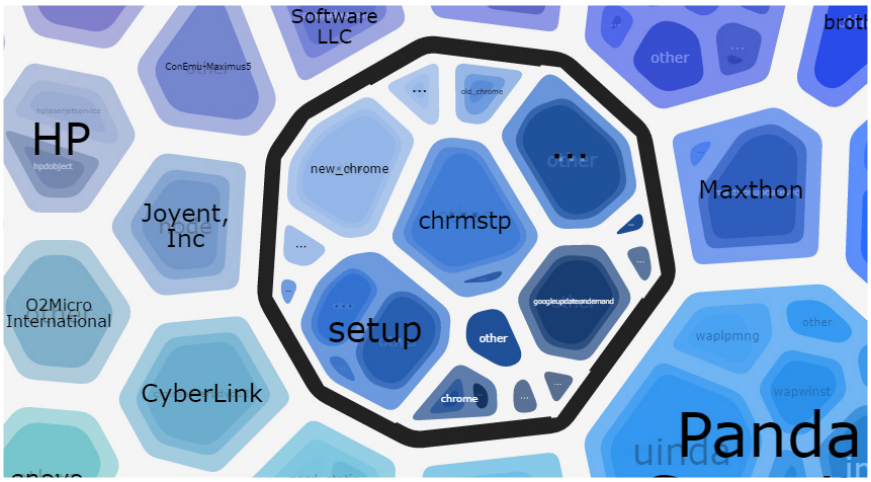


Figure 17: zooming in into a polygon by double-clicking on it

Place the mouse pointer on a group to display the number of items in the group and the percentage that they represent of the total.

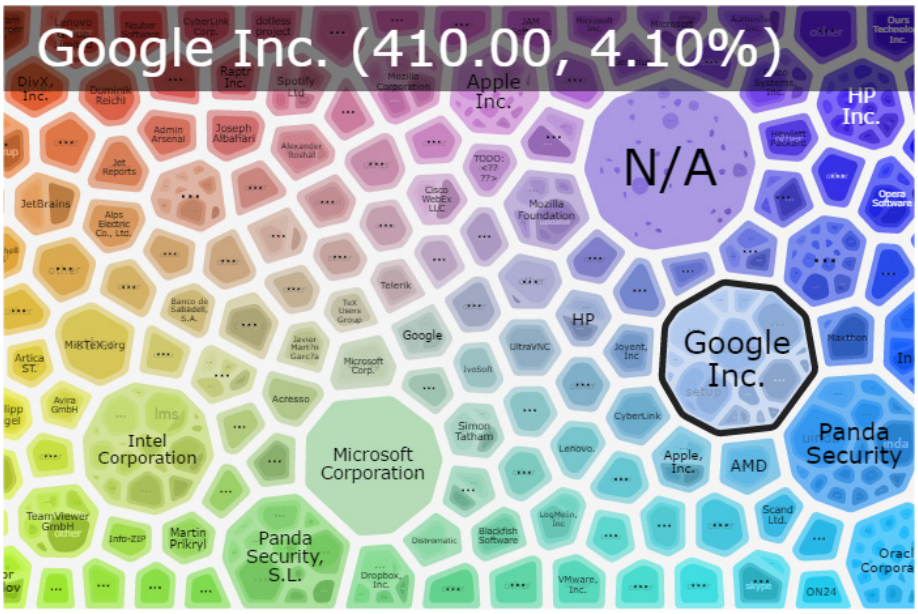


Figure 18: data displayed within a polygon

- **Diagram controls**

A widget containing a Voronoi diagram offers the following controls:

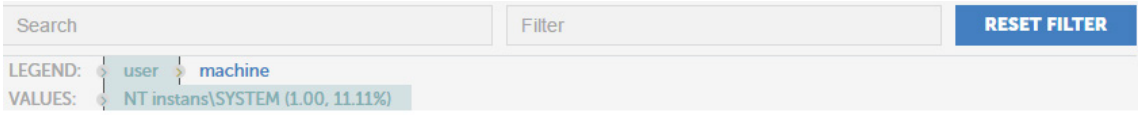


Figure 19: controls for configuring the data displayed in a Voronoi diagram

- **Search**: This finds a polygon in the Voronoi diagram, and expands it to show the groups it comprises. This is the same as double clicking with the left mouse button on a polygon in the diagram. To undo a search, double-click with the right mouse button.
- **Filter**: This shows the polygons that contain groups coinciding with the filter criteria.
- **Reset filter**: This clears the filter. It does not undo searches. To undo a search, double-click with the right mouse button.
- **Legend**: This indicates the knowledge table fields used to group the information displayed. The order of the fields indicates the group hierarchy and can be altered simply by dragging them to the left or right to establish a new hierarchy.
- **Values**: In combination with the fields shown in the **Legend** control, this indicates the value of a specific field. By selecting a polygon, either with the search tool, or by double-clicking it, the **Values** field will take the value of the search or the selected polygon.

When navigating a Voronoi diagram, the highlighted field in **Legend** will take the value of the selected polygon. The adjacent fields will indicate the data layer that will be accessed upon double-clicking it using the left mouse button (drill down to the value shown on the right of the highlighted field), or upon double-clicking it using the right mouse button (exit to the value shown on the left of the highlighted field).

- **Example of a Voronoi diagram**

The following example illustrates how a Voronoi diagram works.

Depending on the **Legend,** the starting point is a chart that groups the data in the following order:

- **Level 1 AlertType**: Indicates the type of threat detected on the network.
- **Level 2 Machinename**: Indicates the name of the computer where the threat was detected.
- **Level 3 executionStatus**: Indicates whether or not it was executed.
- **Level 4 itemPath**: Indicates the file path and name.
- **Level 5 itemName**: Indicates the name of the threat.

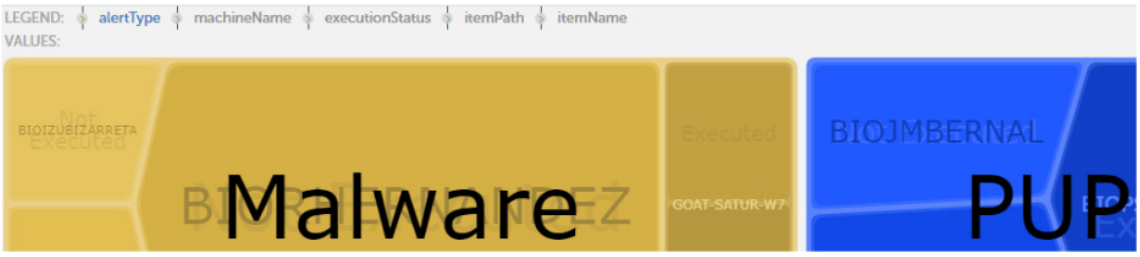


Figure 20: example of the first data layer in a Voronoi diagram

At first, the diagram displays Level 1: the data grouped by **AlertType**, the first **Legend** field, highlighted in blue.

The second legend field is **MachineName,** so by double-clicking on one of the **AlertType** groups in the diagram (e.g. Malware) the second level will be displayed grouping the data according to **MachineName**. The Voronoi diagram will look like this:

The **Values** field is refreshed displaying the Level 1 selection (**AlertType=Malware**) and its content, the Level 2, with the data grouped by M**achineName**, highlighted in blue.

Follow this process to navigate through the Voronoi diagram up to the last level, or move backwards through the diagram by double-clicking with the right mouse button.

If you want to establish an alternative order of grouping, simply drag the fields shown in **Legend** to the left or to the right in order to set the new order.

Figure 22: example of the second data layer in a Voronoi diagram

For example, if you want to first determine which computers have run some type of malware and then the name of the threat -in order to determine its characteristics-, then finally the computers on which it was executed, you can configure the grouping order as follows:

- Level 1 ExecutionStatus
- Level 2 ItemName
- Level 3 Machinename

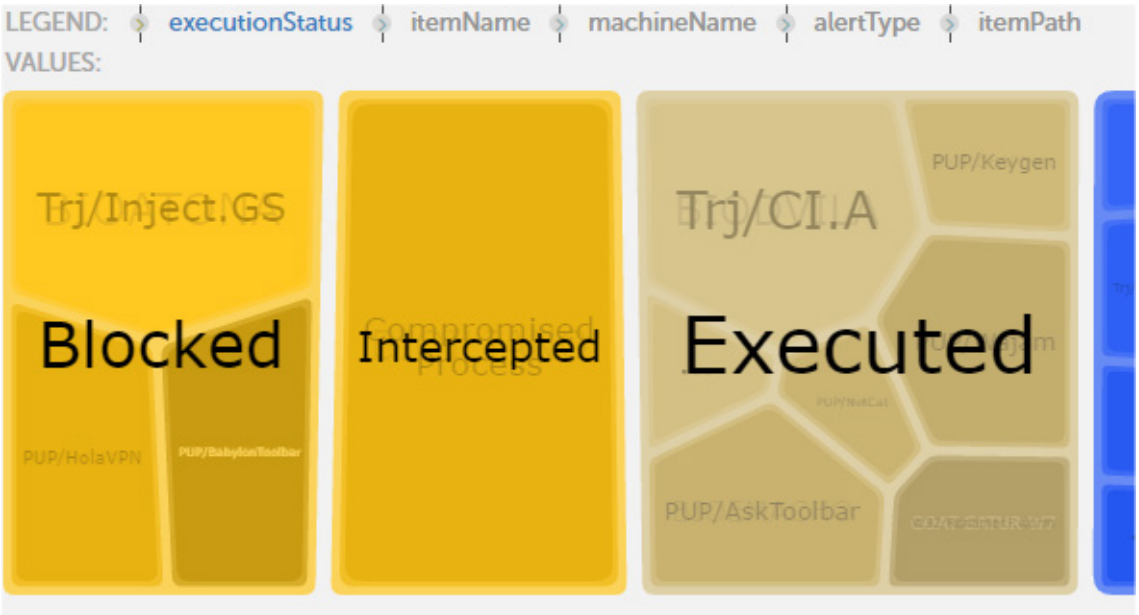


Figure 21: new configuration for an alternative order of grouping

By double-clicking **Executed** in the Voronoi diagram, you can see the names of the items run; clicking one of these will display the computers on which it has been executed.

4.3. Generating new charts based on the widgets provided

By clicking the icon in each widget and selecting **Go to Search,** the corresponding knowledge table that feeds that widget will open.

Each knowledge table has a series of transformations, filters and groups designed to present the most important data clearly and accurately. These transformations are in SQL language and can be edited to adapt to the customer's needs.

It is not possible to overwrite the widgets provided, but you can generate new widgets using the original ones as a base.

4.3.1 Modifying the SQL statement associated with a widget

Once you are in the knowledge table associated with a widget, click the icon in the toolbar. A window with the preset SQL statement will open. After editing the statement, click **Run** to test the execution. The data in the table will be updated immediately.

You can also modify the SQL statement by adding new filters, groups and data transformations via the toolbar.

4.3.2 SQL statement favorites

After changing the SQL statement and ensuring that the generated data is correct, it can then be saved for later access, by marking it as a **Favorite**. To do this, follow these steps:

- Opening a knowledge table will display a new entry in the sidebar, below the **Search** icon.
- A heart icon will be displayed to the right of the name of the entry.
- Click this icon and the SQL statement will be marked as **Favorite**, and will appear in the list of favorites.

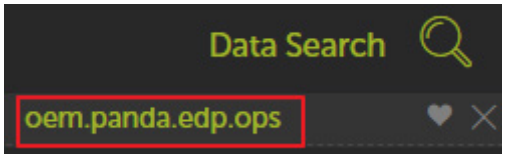


Figure 22: icon for marking alerts as Favorite

Favorites can be found in the side menu **Administration**, **Alerts Configuration.**

5. Configured applications

Files and machines with PII
User operations on PII files
Risk of PI exfiltration

5.1. Introduction

This chapter describes how the three applications provided with **Panda Data Control** operate, both regarding the interpretation of charts and tables as well as the operation of the preconfigured alerts.

5.2. Setting the time period

The three applications provided have a control option at the top of the screen to allow you to set the data time period.

Figure 23: date range picker

Administrators must select the most appropriate time interval to view the status of the personal data held by the company. The various widgets and time intervals will help the administrator spot suspicious trends.

Wider date ranges

When the date range set is wider (months or days), the data will be displayed as a history or an evolution of activity over time.

Narrower date ranges

By selecting a narrower range of dates, such as the current day, administrators can determine the current status of the personal data held by the company, but will lose the perspective of data over time.

5.3. 'Files and machines with PII' application

Finds those files and computers on the network that store confidential information, and shows those processes that act on it. It is divided into three tabs: **Data files with PII**, **Machines with PII** and **Processes accessing PIIF**. Each of these tabs is described below.

5.3.1 Data files with PII

Shows the personal data files found on the organization's workstations and servers.

It is divided into two sections:

- **General View**: Shows a summary of the PII files found, the computers that store them and how they have been used.
- **Files reclassified as not having PII**: Shows those PII files that have undergone a change of

status.

General view

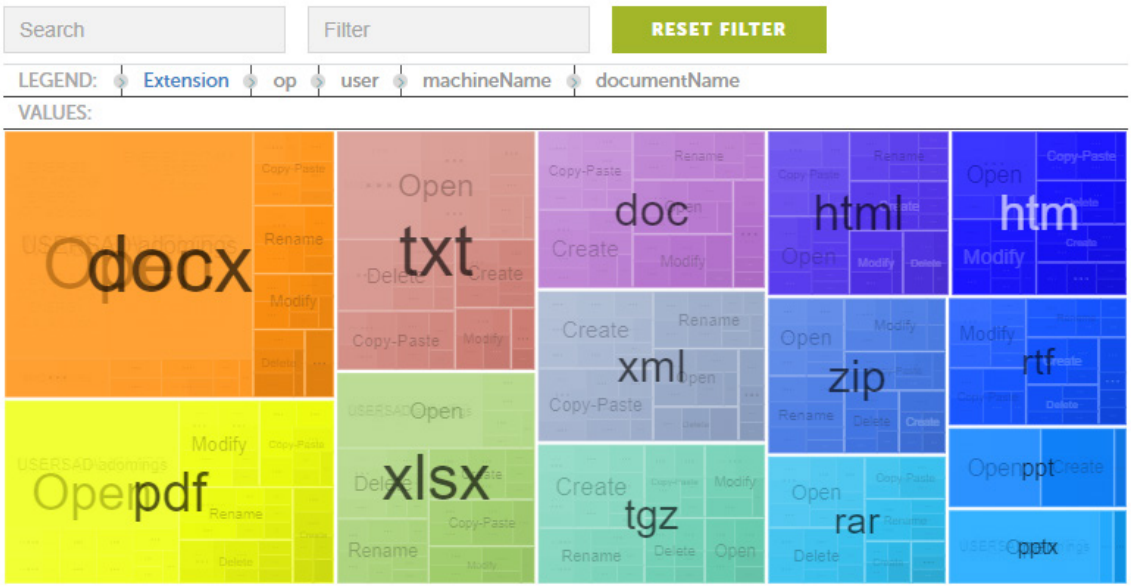


Figure 24: 'General view' widget

- **Aim**: To give an overview of those computers in the organization that store most PII files.
- **Type of widget**: Voronoi diagram.
- **Data displayed**:
  - **First level (machineName)**: Workstation/server name.
  - **Second level (user)**: Name of the computer user.
  - **Third level (op)**: Type of operation performed on the PII file.
  - Fourth level (Extension): PII file extension.
  - Fifth level (documentName): PII file name.
- **Grouping**: Computer, user, operation, extension, name.

This diagram shows those computers on the network that contain most personal data files, and provides additional information such as users, files and operations performed. The Voronoi diagram lets you drill down into each computer to access the various information layers.

Distribution of PII files by extension

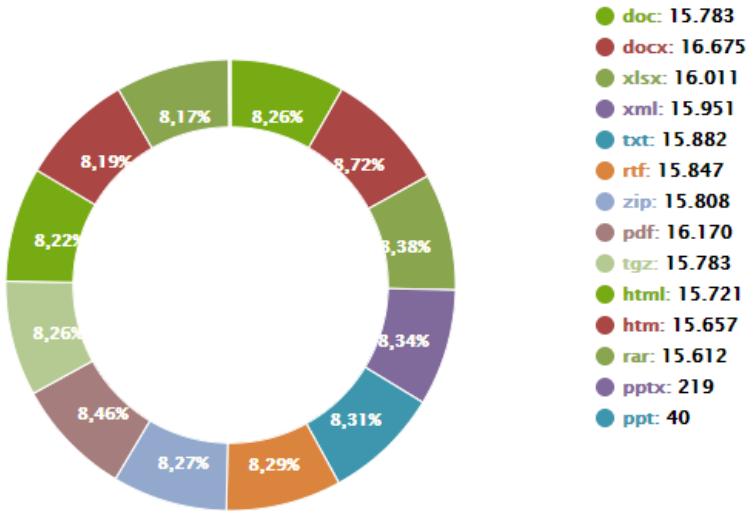


Figure 25: 'Distribution of PII files by extension' widget

- **Aim**: To show the format of the files where personal data is most frequently found.
- **Type of widget**: Pie chart.
- **Data displayed**: PII files grouped by extension.
- **Grouping**: File extension.

This widget shows the types of personal data files most used in the organization. This information can be used to update corporate security policies in order to prevent the use of certain file formats deemed not safe enough to store customer or user information.

Top 10 PII files opened

FILE NAME	COUNT	%
[redacted]	45	0.17%
[redacted]	26	0.10%
[redacted]	25	0.09%
[redacted]	23	0.08%
[redacted]	23	0.08%
[redacted]	23	0.08%
[redacted]	23	0.08%
[redacted]	22	0.08%
[redacted]	6	0.02%
[redacted]	6	0.02%

Figure 26: 'Top 10 PII files opened' widget

- **Aim**: To show those files most frequently accessed and which contain personal data.
- **Fields**:

- **File name**: PII file name.
- **Count**: Counter showing the number of events.
- **%:** Accesses to the file as a percentage of the total accesses to PII files on the network.

This widget shows the PII files most frequently accessed over the selected time period. It helps administrators identify frequently accessed files that may need additional security measures or access restrictrions.

5.3.2 Machines with PII

This tab shows the computers on the network with most activity on personal data files. The information is divided into two sections:

- **Most active machines**: Shows the workstations and servers with most activity on PII files.
- **Machines with malware**: Shows the workstations and servers with PII files accessed by processes classified as malware by **Adaptive Defense**.

Top 10 machines with operations on PII files

MACHINE NAME	COUNT	%
[redacted]	315	0.17%
[redacted]	13	0.01%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%

Figure 27: 'Machines with PII' widget

- **Aim**: To show the 10 computers with most operations on PII files.
- **Fields**:
  - **Machine name**: Workstation/server name.
  - **Count**: Number of PII file operations performed over the selected period.
  - **%:** Number of PII file operations performed on the computer as a percentage of the operations performed on all computers on the network.

This widget shows the 10 computers where most PII file operations have taken place regardless of the type of action (open, copy, move, etc.). It allows administrators to identify the computers where most personal data files are accessed in order to establish specific control measures.

Top 10 machines with exfiltration operations

MACHINE NAME	COUNT	%
[redacted]	5	0.01%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%
[redacted]	2	0.00%

Figure 28: 'Top 10 machines with exfiltration operations' widget

- **Aim**: To show the computers from which most personal data files have been sent out of the network.
- **Fields**:
  - **Machine name**: Name of the workstation or server from which personal data has been extracted.
  - **Count**: Number of exfiltration events.
  - **%:** Exfiltration events per machine as a percentage of the total number of exfiltration events registered on the entire network.

This widget shows the 10 computers that have sent most personal data files out of the network. This information allows administrators to detect massive data leaks from certain computers.

Machines with malware accessing PII files

Aim: To show the computers where most personal data files have been accessed by processes classified as malware.

- **Fields**:
  - **Machine name**: Workstation/server name.
  - **Count**: Number of accesses.
  - **%:** Accesses per computer as a percentage of the total number of accesses detected on all computers on the network.

This widget shows the 10 computers where most malicious processes have been detected accessing personal data. This information allows administrators to detect infected computers and assess the impact of any incident affecting personal data, as demanded by the GDPR.

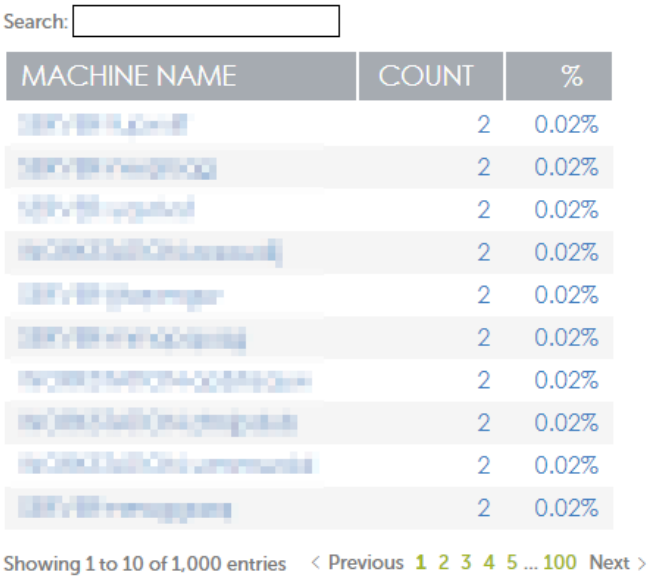


Figure 29: 'Machines with malware accessing PII files' widget

5.3.3 Processes accessing PII Files

This tab is divided into two sections:

- **Processes accessing PII**: Shows the processes found on the network that have accessed personal data files.
- **Malware processes**: Shows the processes that have accessed personal data and have been classified by **Adaptive Defense** as malware.

Top processes accessing PII files

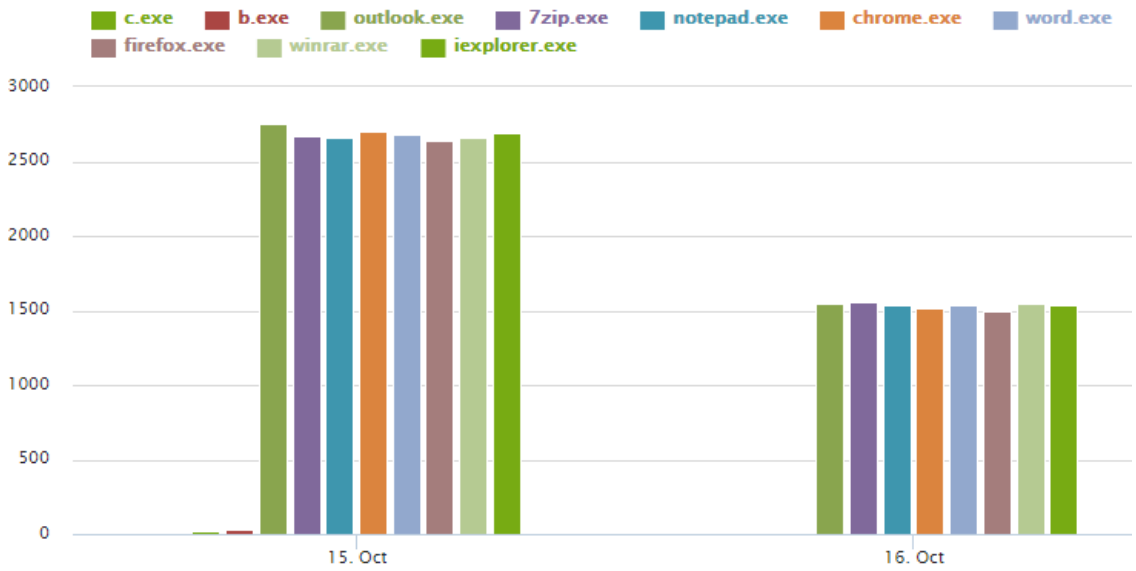


Figure 30: 'Processes accessing PII files' widget

- **Aim**: To show the 10 processes most frequently used to operate on PII files.
- **Type of widget**: Bar chart.
- **Data displayed**: History of the number of operations performed on PII files, grouped by the top 10 processes used to perform them.
- **Grouping**: Process.

This widget shows a history of the processes that have performed most operations on PII files. This information allows administrators to detect anomalous increases in the number of operations that may indicate a massive data exfilttration/infilltration attack.

Number of malware processes accessing PII files

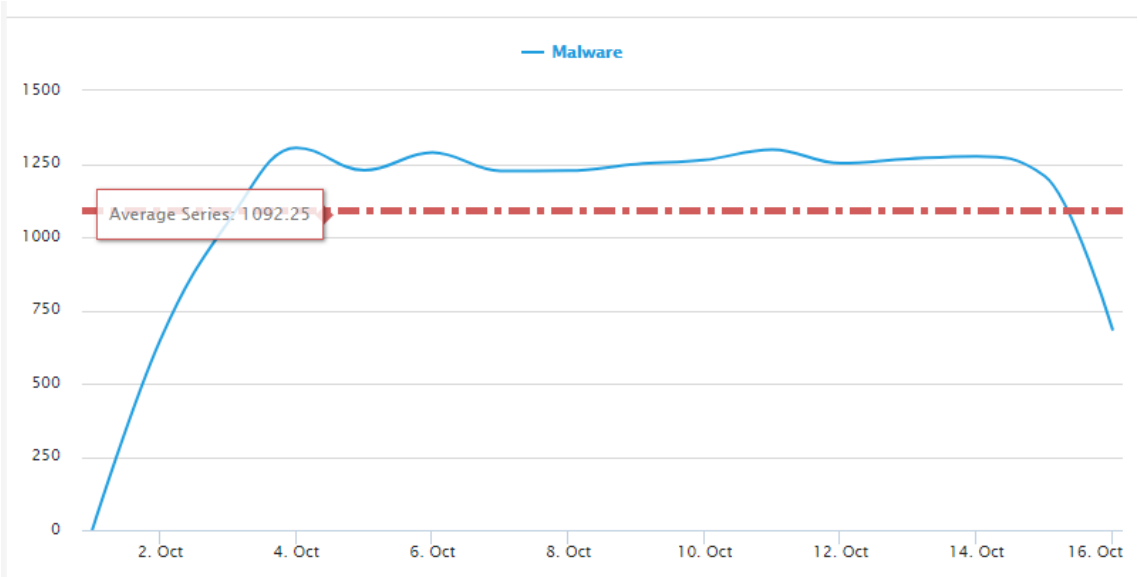


Figure 31: 'Number of malware processes accessing PII files' widget

- **Aim**: To show the evolution of the number of accesses to PII files by processes classified as malware by **Adaptive Defense**.
- **Type of widget**: Line chart.
- **Data displayed**: Evolution of the total number of operations performed on PII files. Monthly access average.
- **Grouping**: Processes classified as malware.

This widget allows administrators to anticipate security incidents associated with data theft (by Trojans, APTs) or data hijacking (ransomware).

Distribution of processes by category

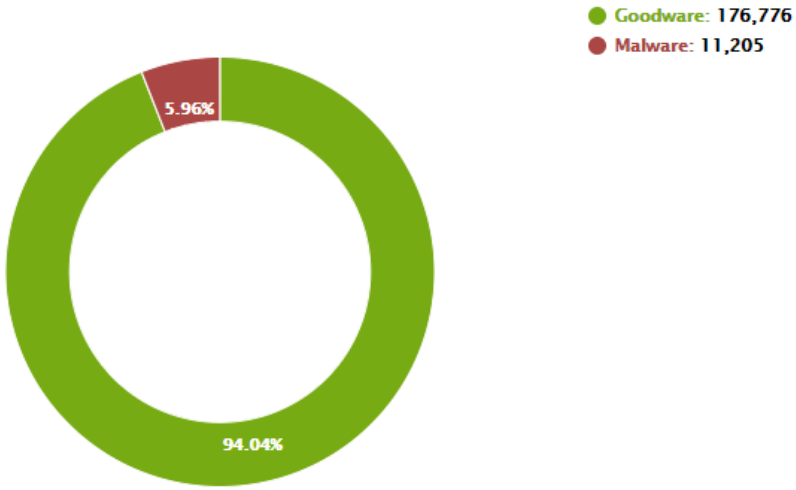


Figure 32: 'Distribution of malware vs legitimate processes' widget

- **Aim**: To show the number of processes classified as malware compared to the rest of processes.
- **Type of widget**: Pie chart.
- **Data displayed**: Percentage of safe vs malicious processes.
- **Grouping**: Process classification (malware, goodware, monitoring).

This widget compares the number of safe processes to the number of malware processes, allowing administrators to detect deviations that may indicate an attack on the organization.

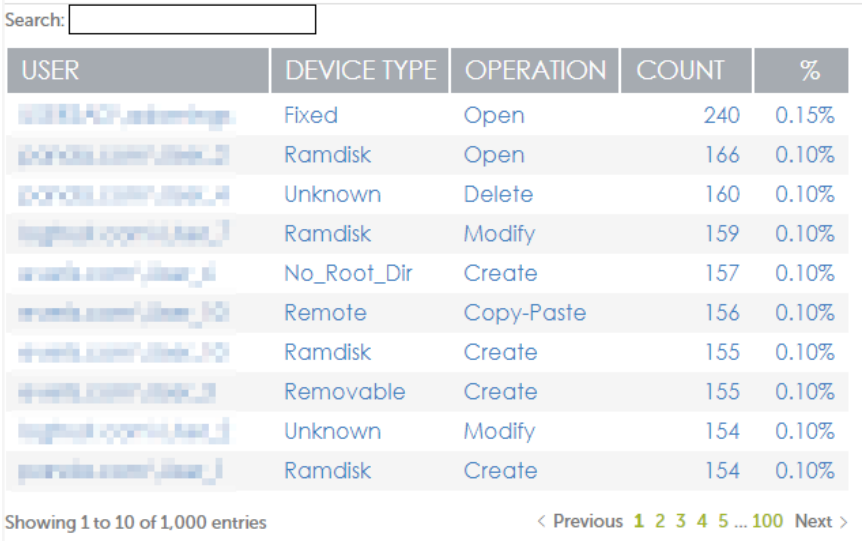
5.4. User operations on PII files

Shows the types of operations performed on the personal data files run in the organization as well as the type of device that contained the data (fixed or mobile device).

5.4.1 User operations

- **User operations**: Shows the types of operations performed on personal data files, and the users involved in data exfiltration/infiltration operations.
- **Types of operations**: Shows the types of operations performed on personal data files, as well as the type of device that contained the data (fixed or mobile device).

User operations on PII files by device type


Search:

USER	DEVICE TYPE	OPERATION	COUNT	%
[redacted]	Fixed	Open	240	0.15%
[redacted]	Ramdisk	Open	166	0.10%
[redacted]	Unknown	Delete	160	0.10%
[redacted]	Ramdisk	Modify	159	0.10%
[redacted]	No_Root_Dir	Create	157	0.10%
[redacted]	Remote	Copy-Paste	156	0.10%
[redacted]	Ramdisk	Create	155	0.10%
[redacted]	Removable	Create	155	0.10%
[redacted]	Unknown	Modify	154	0.10%
[redacted]	Ramdisk	Create	154	0.10%

Showing 1 to 10 of 1,000 entries < Previous 1 2 3 4 5 ... 100 Next >

Figure 33: 'User operations on PII files by device type' widget

- **Aim**: To show the users that have performed operations on personal data files as well as additional information.
- **Fields**:
  - **User:** User account who ran the program that accessed the personal data file.
  - **DeviceType:** Type of device that contained the accessed file. Refer to chapter 7 PII knowledge table for more information about the **DeviceType** field and the values it can take.
  - **Operation:** Operation performed on the PII file. Refer to chapter 7 PII knowledge table for more information about the **Operation** field and the values it can take.
  - **Count:** Number of operations performed by the user of the relevant type and on the relevant type of device.
  - **%:** Operations as a percentage of the total number of registered operations.

This widget shows a full list of the users that have handled PII files stored on any type of device in the organization. This information enables administrators to establish additional security measures for those users who use most personal data or store it on mobile devices.

Calendar of user operations on removable drives

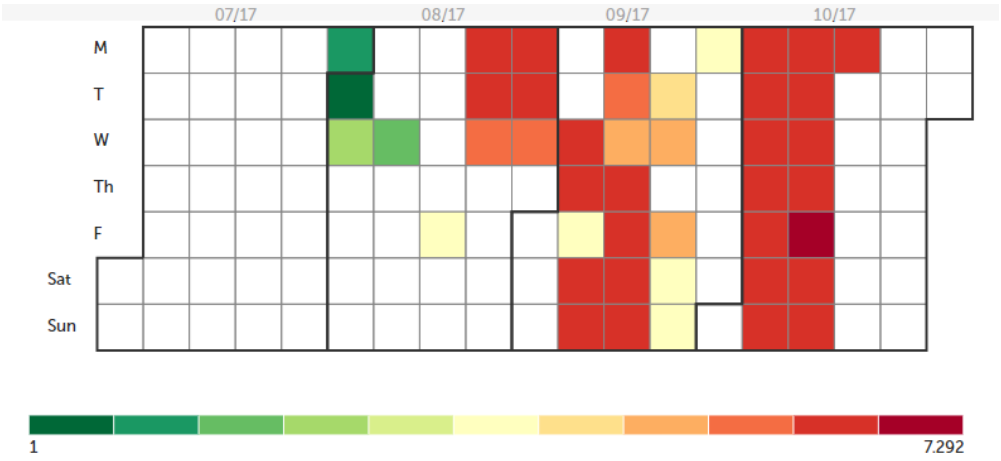


Figure 34: 'Calendar of user operations on removable drives' widget

- **Aim**: To show the evolution of the operations performed on personal data files residing on external storage devices.
- **Type of widget**: Calendar chart.
- **Data displayed**: Number of operations performed on PII files residing on external devices, grouped by day of the month.
- **Grouping**: Day of the month.

This widget monitors the operations performed on personal data files residing on removable drives, showing their evolution over the last month. This information can be used to identify potential data leaks since the devices monitored in the widget are removable.

Users involved in exfiltration operations

Search:

USER	EXFILTRATION FLAG	COUNT	%
[redacted]	BOTH	1727	1.84%
[redacted]	EXFILTRATION	1661	1.77%
[redacted]	EXFILTRATION	1634	1.74%
[redacted]	EXFILTRATION	1633	1.74%
[redacted]	BOTH	1630	1.73%
[redacted]	EXFILTRATION	1625	1.73%
[redacted]	BOTH	1621	1.72%
[redacted]	EXFILTRATION	1620	1.72%
[redacted]	BOTH	1616	1.72%
[redacted]	EXFILTRATION	1616	1.72%

Showing 1 to 10 of 63 entries < Previous 1 2 3 4 5 6 7 Next >

Figure 35: 'Users involved in exfiltration operations' widget

- **Aim**: To show the number of data exfiltration/infiltration operations per user.
- **Fields**:
  - **User:** User account who ran the program that exfiltrated/infilltrated personal data files.
  - **Exfiltration flag:** Indicates whether the operation performed on the PII file was data exfiltration or infiltration.
  - **Count:** Number of registered operations of the relevant type.
  - **%:** Operations as a percentage of the total number of registered operations.

This widget shows the number of data exfiltration/infiltration operations per network user. This information allows administrators to identify those users who are accessing and using personal data unlawfully.

Distribution of operation types on PII files

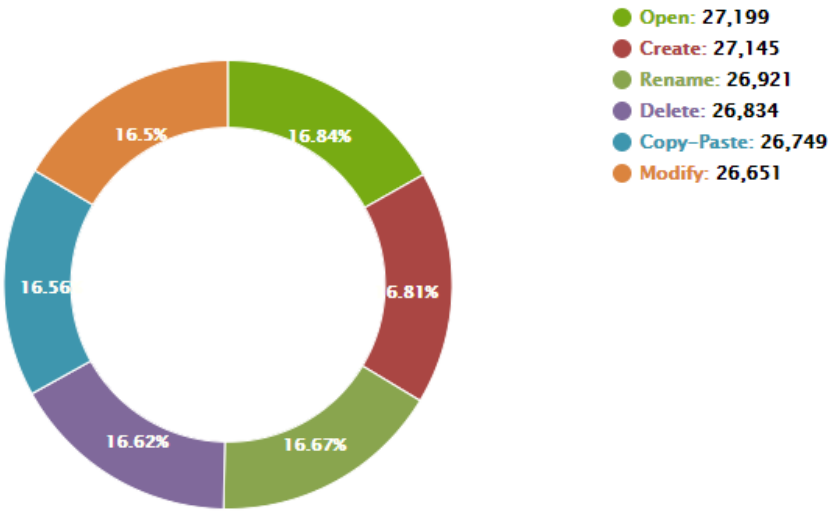


Figure 36: 'Distribution of operation types on PII files' widget

- **Aim**: To show the percentage of the various types of operations performed on personal data files.
- **Type of widget**: Pie chart.
- **Data displayed**: The percentage of each type of operation.
- **Grouping**: Operation type.

This widget shows the most common operations performed on personal data files. This information enables administrators to identify deviations from the usual number of operations that may indicate a security breach.

Distribution of operations on removable devices

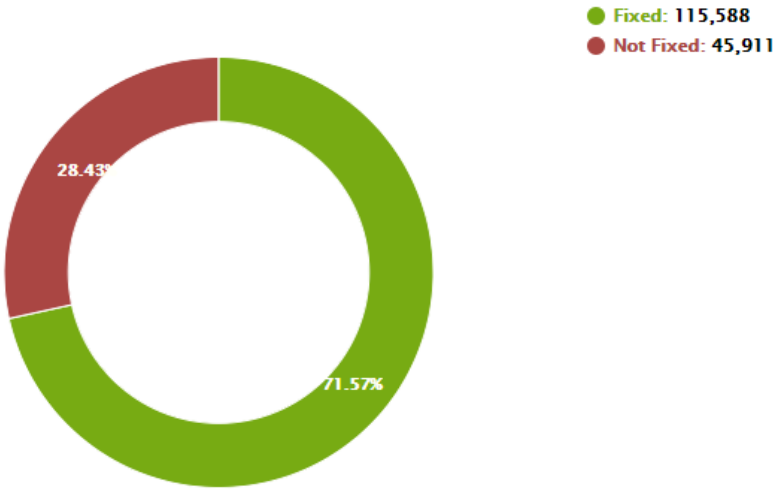


Figure 37: 'Distribution of operations on removable devices' widget

- **Aim**: To compare the percentage of operations performed on personal data files residing on removable devices with the percentage of operations performed on personal data files residing on fixed devices.
- **Type of widget**: Pie chart.
- **Data displayed**: Percentage of operations performed on fixed and removable devices.
- **Grouping**: Type of device.

This widget gives an indication of the danger level of the operations performed on personal data files. If the higher percentage of operations takes place on removable devices, the administrator will be able to take measures aimed at reducing the likelihood of a data breach.

5.4.2 Most active users

Shows the users in the organization most likely to be responsible for a data breach based on the number of operations they perform on personal data files and the malware run on their devices.

- **Active users by operation type**: Shows the users that have performed most operations on PII files.
- **Top users running malware**: Shows the users that have run most processes classified as malware.

Top 10 users involved in create operations

USER	COUNT	%
[redacted]	945	3.48%
[redacted]	937	3.45%
[redacted]	930	3.43%
[redacted]	928	3.42%
[redacted]	920	3.39%
[redacted]	918	3.38%
[redacted]	916	3.37%
[redacted]	911	3.36%
[redacted]	910	3.35%
[redacted]	910	3.35%

Figure 38: 'Top 10 users involved in create operations' widget

- **Aim**: To show the users that have created most personal data files.
- **Fields**:
  - **User:** User account who ran the program that created the personal data file.
  - **Count:** Number of registered operations of the relevant type.
  - **%:** Operations as a percentage of the total number of registered operations.

This widget helps administrators identify those users who have generated most unstructured personal data files in the organization.

Top 10 users involved in open operations

USER	COUNT	%
[redacted]	945	3.48%
[redacted]	937	3.45%
[redacted]	930	3.43%
[redacted]	928	3.42%
[redacted]	920	3.39%
[redacted]	918	3.38%
[redacted]	916	3.37%
[redacted]	911	3.36%
[redacted]	910	3.35%
[redacted]	910	3.35%

Figure 39: 'Top 10 users involved in open operations' widget

- **Aim**: To show the users who have accessed most personal data files.

- **Fields**:
  - **User:** User account who ran the program that opened the personal data file.
  - **Count:** Number of registered operations of the relevant type.
  - **%:** Operations as a percentage of the total number of registered operations.

Top 10 users involved in copy-paste operations

USER	COUNT	%
[redacted]	945	3.48%
[redacted]	937	3.45%
[redacted]	930	3.43%
[redacted]	928	3.42%
[redacted]	920	3.39%
[redacted]	918	3.38%
[redacted]	916	3.37%
[redacted]	911	3.36%
[redacted]	910	3.35%
[redacted]	910	3.35%

Figure 40: 'Top 10 users involved in copy-paste operations' widget

- **Aim**: To show the users who have performed most copy-paste operations with personal data files.
- **Fields**:
  - **User:** User account who copied-pasted the personal data file.
  - **Count:** Number of registered operations of the relevant type.
  - **%:** Operations as a percentage of the total number of registered operations.

Top 10 users involved in rename operations

- **Aim**: To show the users that have renamed most personal data files.
- **Fields**:
  - **User:** User account who renamed the personal data file.
  - **Count:** Number of registered operations of the relevant type.
  - **%:** Operations as a percentage of the total number of registered operations.

USER	COUNT	%
[redacted]	945	3.48%
[redacted]	937	3.45%
[redacted]	930	3.43%
[redacted]	928	3.42%
[redacted]	920	3.39%
[redacted]	918	3.38%
[redacted]	916	3.37%
[redacted]	911	3.36%
[redacted]	910	3.35%
[redacted]	910	3.35%

Figure 41: 'Top 10 users involved in rename operations' widget

Top 10 users running malware

USER	COUNT	%
[redacted]	945	3.48%
[redacted]	937	3.45%
[redacted]	930	3.43%
[redacted]	928	3.42%
[redacted]	920	3.39%
[redacted]	918	3.38%
[redacted]	916	3.37%
[redacted]	911	3.36%
[redacted]	910	3.35%
[redacted]	910	3.35%

Figure 42: 'Top 10 users running malware' widget

- **Aim**: To show the users who have performed most operations on personal data files using processes classified as malware.
- **Fields**:
  - **User:** User account who ran the malware that accessed personal data.
  - **Count:** Number of registered operations of the relevant type.
  - **%:** Operations as a percentage of the total number of registered operations.

This widget shows the users that use infected workstations or servers and launch processes classified as malware with their credentials, either voluntarily or involuntarily (botnets, accidental infections, etc.).

5.5. Risk of PII exfiltration

Shows the operations performed on personal data files that **Panda Data Control** classifies as involving a risk of data exfiltration/infiltration.

5.5.1 Risk of exfiltration

Number of operations with files at risk of exfiltration

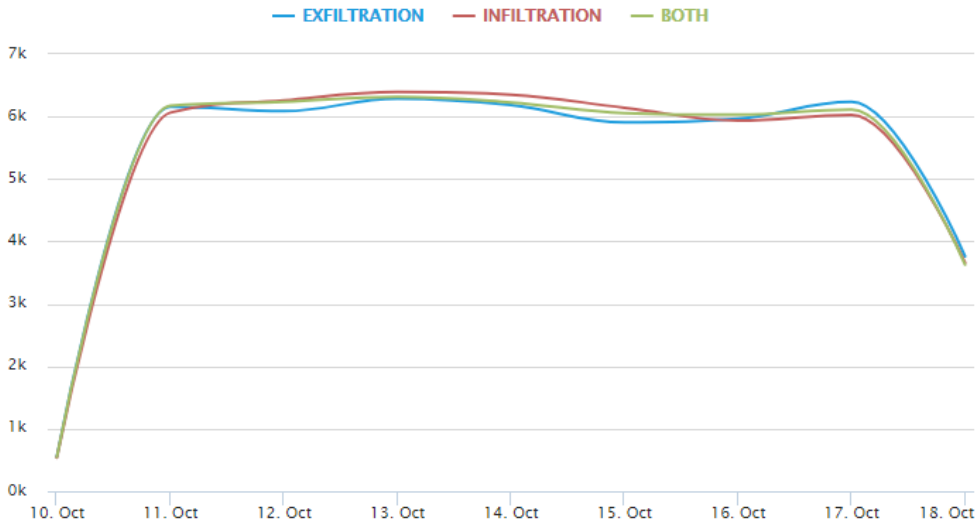


Figure 43: 'Number of operations with files at risk of exfiltration' widget

- **Aim**: To show the evolution of accesses to PII files classified as data infiltration, exfiltration or both.
- **Type of widget**: Line chart.
- **Data displayed**: Operations classified as unauthorized exfiltration or infiltration of data.
- **Grouping**: Action type (infiltration, exfiltration, both).

This widget shows the evolution of the accesses to personal data files classified by **Panda Data Control** as unauthorized data exfiltration/infiltration. A sudden spike on the chart may represent a data breach in the organization.

Operations with files at risk of exfiltration and infiltration

- **Aim**: To compare the percentage of data exfiltration operations, data infiltration operations and operations combining both data exfiltration and infiltration.
- **Type of widget**: Pie chart.
- **Data displayed**: Percentage of each type of operation.
- **Grouping**: Operation type.

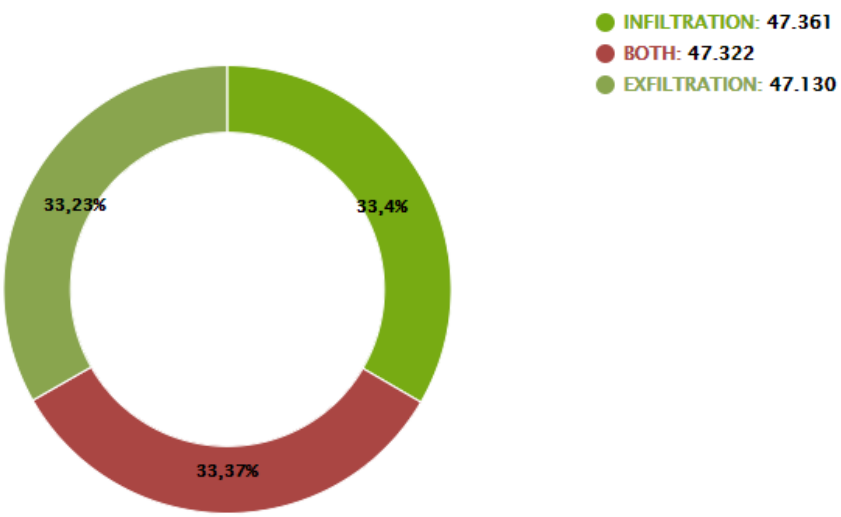


Figure 44: 'Operations with files at risk of exfiltration and infiltration' widget

Top 10 largest files at risk of exfiltration

DOCUMENT NAME	MACHINE IP	MACHINE NAME	DOCUMENT SIZE (MB)	USER
randomDoc_jgvtfn.rtf	10.138.11.217	SERVER-bmwbpucl	25.1	
randomDoc_fx.rtf	10.39.9.229	WORKSTATION-pwrywpot	25.1	
randomDoc_jmosecxh.zip	10.89.115.62	WORKSTATION-fjplzpnw	25.09	
randomDoc_lc.txt	10.231.8.76	SERVER-suljlpdp	25.09	
randomDoc_vvitc.htm	10.131.251.26	WORKSTATION-udkjoezd	25.09	
randomDoc_jqqgrhta.xlsx	10.234.230.14	SERVER-hsqryuwd	25.09	
randomDoc_lcvm.tgz	10.151.151.205	SERVER-snylnrsp	25.09	
randomDoc_xqnpufho.rtf	10.104.229.53	WORKSTATION-ydlxsomy	25.09	
randomDoc_kdwrdol.doc	10.107.155.16	WORKSTATION-zcmtwqfc	25.09	
randomDoc_icke.htm	10.100.21.11	SERVER-oaijrgxf	25.09	

Figure 45: 'Top 10 largest files at risk of exfiltration' widget

- **Aim**: To show a list of the largest personal data files that have been accessed in your organization.
- **Fields**:
  - **Document name:** Name of the PII document.
  - **User:** User account who accessed the document.
  - **Machine IP:** IP address of the computer where the PII file resides.
  - **Machine Name:** Name of the computer where the PII file resides.
  - **Document size (MB):** Document size (in megabytes).

Operations performed on large personal data files pose a bigger threat as they may result in a massive data breach. These operations must be monitored and controlled very closely.

6. Alerts

Alert system architecture
Creating alerts

6.1. Introduction

The **Panda Data Control** alert system allows administrators to keep up-to-speed with events that take place on the network that require their attention, without having to go to the Web console. It is therefore a key module in minimizing the reaction time of the IT department when faced with potential data exfiltration situations in the organization.

The alert system is fully configurable by the network administrator, including the frequency for sending alerts, the conditions required for generating them and the delivery method used.

6.2. Alert system architecture

The **Panda Data Control** alert system comprises several fully configurable modules. The sequence of processes involved in the generation of alerts is as follows:

Figure 46: modules participating in the alert generation flow

- **Generation of events**: Each entry in a knowledge table generates a unique event that can later be converted into one or more alerts.
- **Alert module**: The events that meet certain criteria defined by administrators in the alerts module will generate an alert.
- **Antiflooding module**: This prevents the problem of a 'storm of alerts', allowing the alert generation module to be temporarily disconnected from the generation of events on exceeding a certain threshold defined by the administrator. This prevents the generation of a flood of alerts.
- **Post filter ing module**: This handles the alerts once they are generated, changing their properties or even selectively eliminating them in line with the criteria established by the administrator.
- **Delivery module**: This allows the delivery of the alerts to administrators in a number of ways.

6.2.1 Process for configuring the alerts

Setting up a new alert requires a series of steps, some of them mandatory, some of them optional, in order for the alert to work correctly.

These steps are listed below along with a brief description of the process.

1. **Creating the alerts (mandatory)**: Creating an alert requires you to define the type of event you want from the knowledge table, and to establish that it will generate an alert.
2. **Editing the alert subscription (optional)**: This lets you enable or disable the newly created alert. Alerts are enabled automatically when they are created.
3. **Set the delivery criteria (mandatory for the first alert)**: The delivery settings allow you to determine the delivery method and specify associated information. For example, if you specify delivery by email, you must indicate the recipient's email account.
4. **Creating an antiflooding policy (optional)**: This sets maximum thresholds for generating alerts in order to avoid mass mailings. Administrators who prefer to receive all generated alerts shouldn't use any antiflooding policy.
5. **Creating a new delivery policy (mandatory for the first alert)**: The delivery policy lets you define the following parameters for delivering alerts:
    a. **Assigning the antiflooding policy** (point 4).
    b. **Assigning the delivery schedule**: Alerts will only be sent in line with the calendar settings.
    c. **Delivery method** (point 3).
6. **Assigning a delivery policy** (point 5) to the alert created (point 1).
7. **Creating post filter s (optional)**: If you want to edit the alert before it is sent you have to create a post filter .

The block diagram that comprises an alert is as follows:

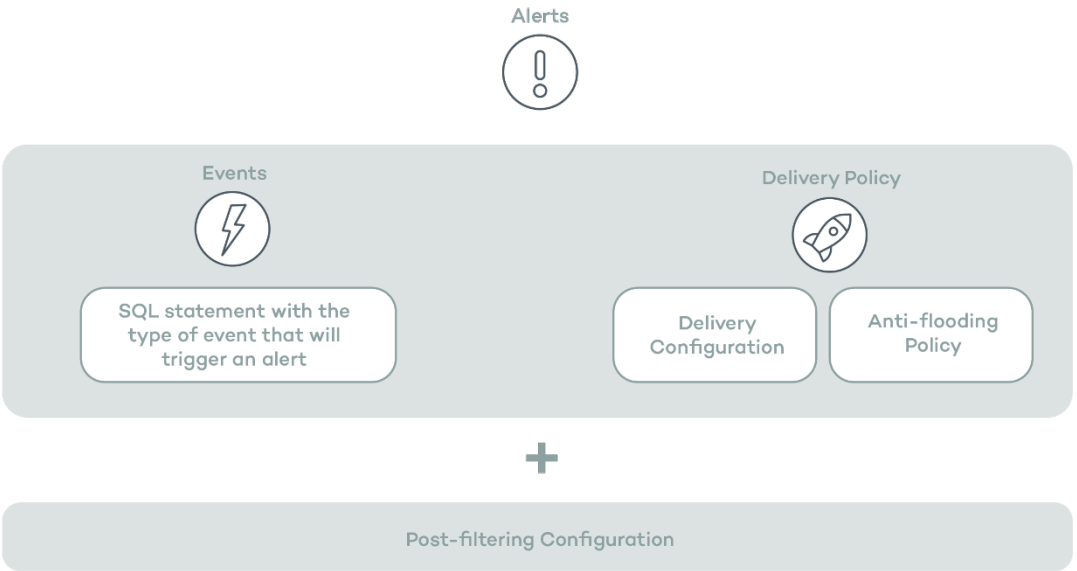


Figure 47: logical components of an alert

6.3. Creating alerts

Alerts are created from the associated knowledge table. To create an alert, follow these steps.

1. Select the corresponding table in the **Search** side menu.

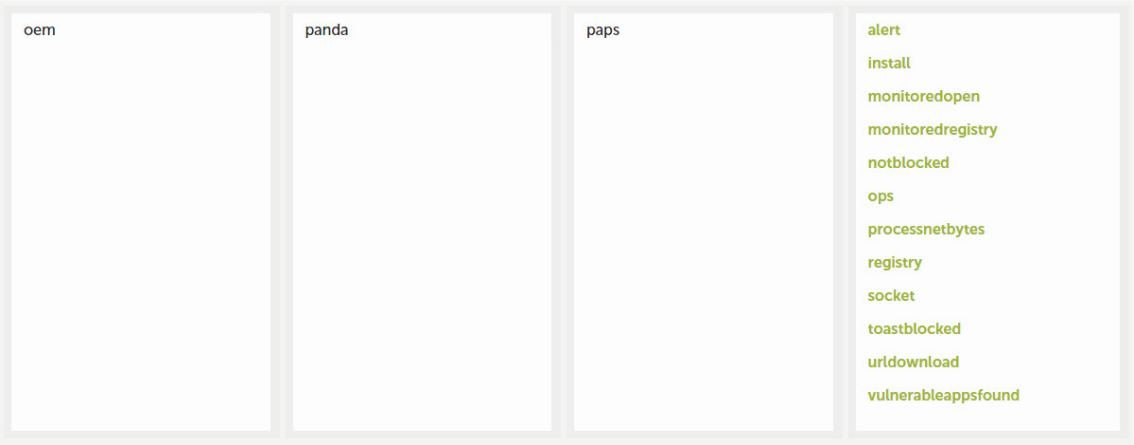


Figure 48:table search tool by tag

2. Apply the filters and data transformations required to generate the information you want and click the icon on the toolbar.
3. Set the alert parameters.
    a. **Subcategory**: Tag that classifies the alert and enables later searches or filters.
    b. **Context**: Tag that classifies the alert and enables later searches or filters.
    c. **Message**: The alert subject.
    d. **Description**: The alert content.
4. Alert generation frequency.
    a. **Each**: Generate an alert for each event entry in the table.
    b. **Several**: Lets you define the frequency and thresholds for generating alerts.
    c. **Period**: Time period to which the threshold applies.
    d. **Threshold**: This determines the number of events in a given period that will trigger the sending of an event.
    e. **Counters**: This lets you add columns from the knowledge table to the alert. The contents of a counter field can be incorporated into the subject or description of the alert simply by putting the field name preceded by the $ symbol.

If, for example, a **Period** of 5 minutes is set and a **Threshold** of 30, no alert will be sent until there are 30 events. Event 60 will generate a second warning and so on until the five-minute period has concluded, at which time the event counter is reset to 0.

During the process of creating alerts, the volume of alerts generated according to the settings is checked. If the alert will generate more than 60 alerts per minute, the alert settings are invalid. In this case, increase the Threshold field to lower the number of alerts generated per minute

Once the alert is created, the system will begin generating entries as the events defined in the alert occur. To view the generated alerts log, see the Alert Management section later.

6.3.1 Alert management

The generated alerts can be managed by clicking the **Alerts** side menu. Click the **Alerts panel** tab to display the following sections: **Alerts Overview** and **Alerts History.**

Alerts Overview

This view displays the alerts generated by the system through various charts. The charts can be configured by the administrator using several tools.

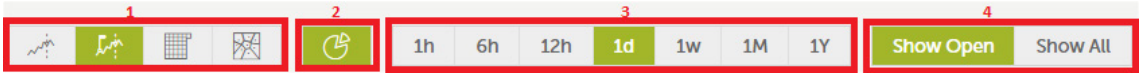


Figure 49: alert list configuration toolbar

- **Type of chart (1)**: This lets you choose the way that the alerts will be represented:
  - Line chart.
  - Timeline.
  - Calendar chart.
  - Voronoi diagram.
- Enable/disable pie chart (2)
- Time period represented in the chart (3).
  - 1 hour.
  - 6 hours.
  - 12 hours.
  - 1 day.
  - 1 week.
  - 1 year.
- Filter by alert status (4)
  - **Open:** Only open alerts are displayed.
  - **All alerts:** All alerts are displayed.

See Chapter 4 for more details about each type of chart

Alert History

This section shows a list of the alerts generated. Each alert has a number of fields that the system fills in as configured by the administrator when creating the alert:

- **Status**: Watched; not read.
- **Type**: Type of alert, taken from the Message field in the alert settings, described in the section on **Creating alerts** earlier in the chapter.
- **Detailed Information**: Extract from the alert text taken from the **Description** field, described in the section on **Creating alerts** earlier in the chapter. Click **Detailed Information** in the alert to display the content.
- **Category**: Alert category taken from the **Subcategory** and **Context** fields, described in the section on **Creating alerts** earlier in the chapter.
- **Priority**: All alerts are generated with normal priority by default. To change the priority of an alert (**very low, low, normal, high, very high**) you have to configure a postfilter. Refer to the point on **Configuring post filters** later in this guide.
- **Created**: Date and time of creation and the time elapsed since the alert was generated.
- **Menu**: The final column in the **Alerts History** table displays a menu with options for each alert:
- **View alerts details**: This lets you see all the information associated with the alert in a new window.
- **Create annotation**: This lets you add a text to the alert. Completing the form will add an  icon to the alert indicating that a technician made a comment about the alert. You can also convert a note into a task if the alert requires action over a period of time.
- **New filter**: This lets you create postfilters as described in the following section.
- **Mark as closed**
- **Delete**

Establishing filters in the alert history

Click the **Type**, **Category** or **Priority** fields of a specific alert to set a filter that will only display alerts that match the criteria set.

The applied filters will be shown in the filter bar.

6.4. Creating post filters

Post filters allow you to edit the features of the generated alerts before they are sent, as well as deleting them if they coincide with certain criteria.

The post filter s are created from the **Alerts** section in the side menu. Click the ooo icon of an alert that has been generated to display a drop-down menu with actions available.

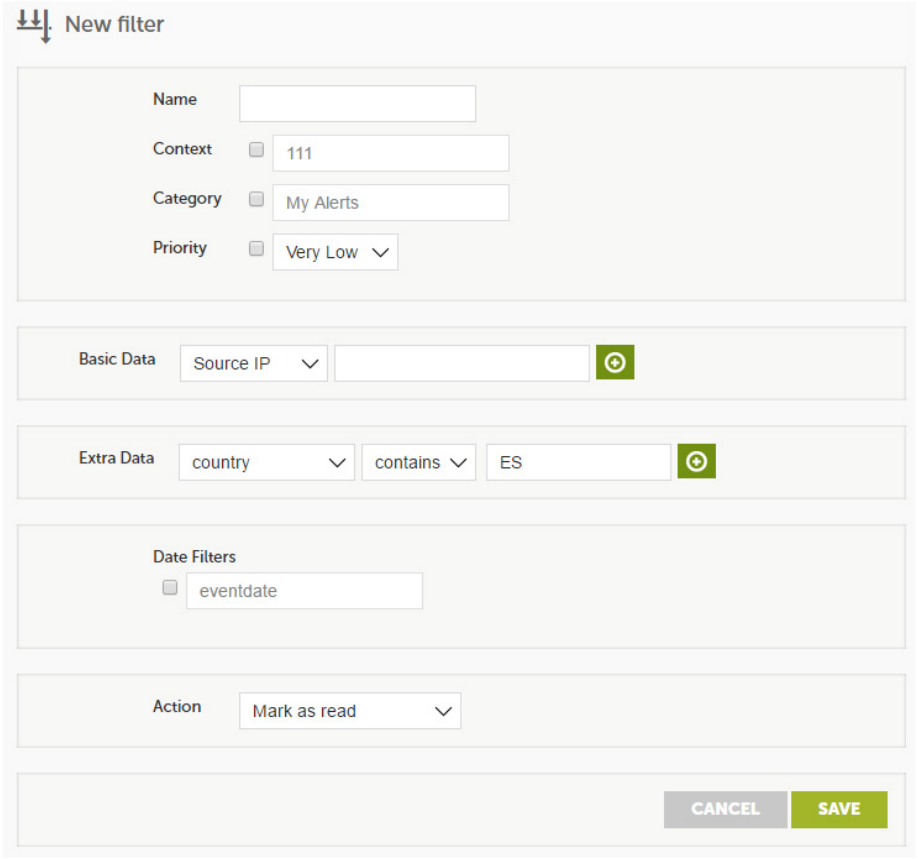


Figure 50: post filter creation window

The post filter screen comprises five sections:

Section 1: Description

This section specifies the name and criteria that alerts have to match for the filter to apply.

- **Name**: Name of the filter.
- **Context**: This sets the context of the alert as a filter condition.
- **Category**: This sets the category of the alert as a filter condition.
- **Priority**: This sets the priority of the alert as a filter condition.

Section 2: Basic data

This section is not used.

Section 3: Extra data

In this section you can set criteria based on the content which alerts must meet for the post filter to be applied.

In the process of configuring an alert, a series of columns can be established in the **Counter** field. The contents of these columns is accessible from the alert body when it is generated using the $ symbol. The Extra data section allows you to choose from the dropdown menu those counters that you want to include as a filter condition.

Section 4: Filter dates

You can set one or more date ranges to act as a criteria. The post filter will not apply to alerts generated outside the established period.

Section 5: Action

- Mark as read.
- Change priority.
- False positive.
- Change notify method.
- Delete.

6.4.1 Post filter management

You can manage post filters from the **Alerts** side menu, by clicking **Post filters**.

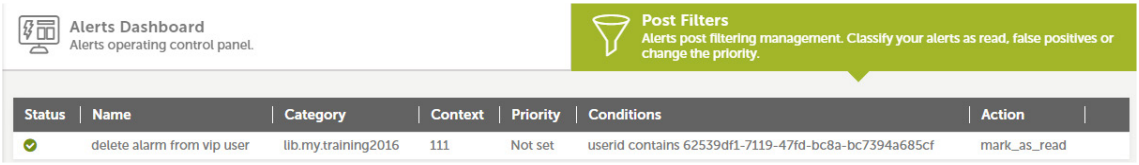


Figure 51: post filter management tab

This window displays a list of the post filters configured with the following information:

- **Status**: Enabled or disabled.
- **Name**: Name given to the post filter when it was created.
- **Category**: Category that determines whether the post filter is applied.
- **Context**: Context that determines whether the post filter is applied.
- **Priority**: Alert priority that determines whether the post filter is applied.
- **Conditions**: Alert content that determines whether the post filter is applied.
- **Action**: Internal command that the alert will apply.

6.5. Creating delivery conditions

The delivery conditions are created through the side menu **Administration**, **Alerts Configuration**, then select the tab **Delivery methods**.

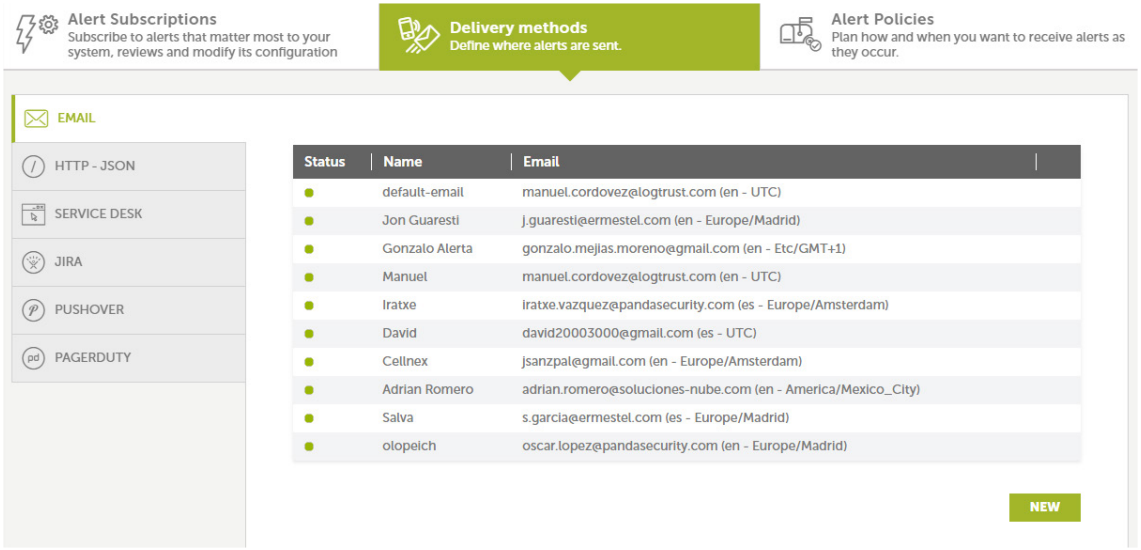


Figure 52: delivery method creation window

Select the delivery type in the left panel. The options are as follows:

- **Email**: The alerts are sent via email.
- **HTTP-JSON**: The alerts are sent via JSON objects.
- **Service desk**: The alerts are sent via Service Desk.
- **JIRA**: The alerts are sent via Jira server.
- **Pushover**: The alerts are sent in a Pushover account.
- **Pagerduty**: The alerts are sent in a PagerDuty account.

Once the type of delivery is selected, click the **New** button to set up a new type of delivery.

Email

This enables the sending of real-time alerts to email accounts.

The required fields are:

- **Name**: Name of the delivery method.
- **Email**: Email account of the recipient.
- **Timezone**: Sets the time and date for sending the email.
- **Language**: The language in which the alert is received.

HTTP-JSON

This enables the sending of real-time alerts via HTTP or HTTPS using JSON objects with POST method.

To improve security, in addition to using the HTTPS encryption protocol you can also enable Digest authentication.

The required fields are:

- **Name**: Name of the delivery method.
- **URL**: URL of the target server, specifying the protocol (HTTP or HTTPS) and the port (e.g. `http://localhost:8080/index.php`).
- **Timezone**: Sets the time and date for sending the email.
- **Language**: The language in which the alert is received.
- **User:** This is only used when the **Authenticated** checkbox is selected.
- **Password**: This is only used when the **Authenticated** checkbox is selected.

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of JSON Delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

Service desk

This enables the real-time sending of alerts to Service Desk Plus servers, using two different methods: REST and SERVLET.

The required fields are:

- **Name**: Name of the delivery settings.
- **URL**: URL of the target server.
- **REST:** `http://[SERVER]:[PORT]/sdpapi/request/`
- **SERVLET**: `http://[SERVER]:[PORT]/servlets/RequestServlet`
- **Delivery method**: REST or SERVLET
- **User**: Name of the technician assigned.
- **Technician Key**: Technician key generated in the Service Desk administration panel.
- **Timezone**: Sets the time and date for sending the message.
- **Language**: The language in which the alert is received.

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of Service Desk delivery methods, the new configuration will be displayed preceded by a red

dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

JIRA

This enables the real-time sending of alerts to Jira servers.

The required fields are:

- **Name**: Name of the delivery settings.
- **URL**: URL of the target server (e.g. `http://localhost:8090/rest/api/2/issue`).
- **User:** JIRA user name.
- **Password:** JIRA password.
- **Issue Type:** The type of task to be created in Jira. In the server URL, there will be a Json object with the projects created. The variable *issuetypes* will list the types of incidents permitted by the project.
- **Project key:** Identifier of the project where the alert will be created. In the server URL, there will be a Json object with the projects created and their identifiers. The Key tag contains the identifiers of each project.
- **Timezone**: Sets the time and date for sending the message.
- **Language**: The language in which the alert is received.

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of JIRA delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

Pushover

This enables the real-time sending of alerts to PushOver servers.

The required fields are:

- **Name**: Name of the delivery method.
- **Token Application**: API Key of the application created in https://pushover.net/apps
- **User/group**: API Key of the user or group to whom the alerts will be sent.
- **Device (optional)**: Name of the device to which the alerts will be sent.
- **Title (optional)**: Text that appears in the alert.
- **URL (optional)**: Link sent in all alerts.
- **Url Title (optional)**: Text that links to the URL above.
- **Sound (optional)**: Type of notification to be sent.

- **Timezone**: Sets the time and date for sending the message.
- **Language**: The language in which the alert is received.

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of PushOver delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

Pagerduty

This enables the real-time sending of alerts to PagerDuty accounts.

The required fields are:

- **Name**: Name of the delivery method.
- **Service Key**: API Key of the PagerDuty service that receives the alert.
- **Client**: Name or identifier that appears in the alert.
- **Client URL**: Link sent in all alerts.
- **Timezone**: Sets the time and date for sending the message.
- **Language**: The language in which the alert is received.

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of PagerDuty delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

6.5.1 Delivery method management

Each of the Delivery methods created has a menu that allows it to be edited and/o deleted.

When editing a delivery method already created, a window is displayed with editing options.

6.6. Creating antiflooding policies

An antiflooding policy allows complete, temporary suspension of alert generation when the rate of alerts exceeds a certain threshold defined by the administrator in the policies.

Antiflooding policy creation is done from the side menu **Administration**, **Alerts Configuration**, then go to the **Alert Policies** tab, then the **Antiflooding Policy** tab.

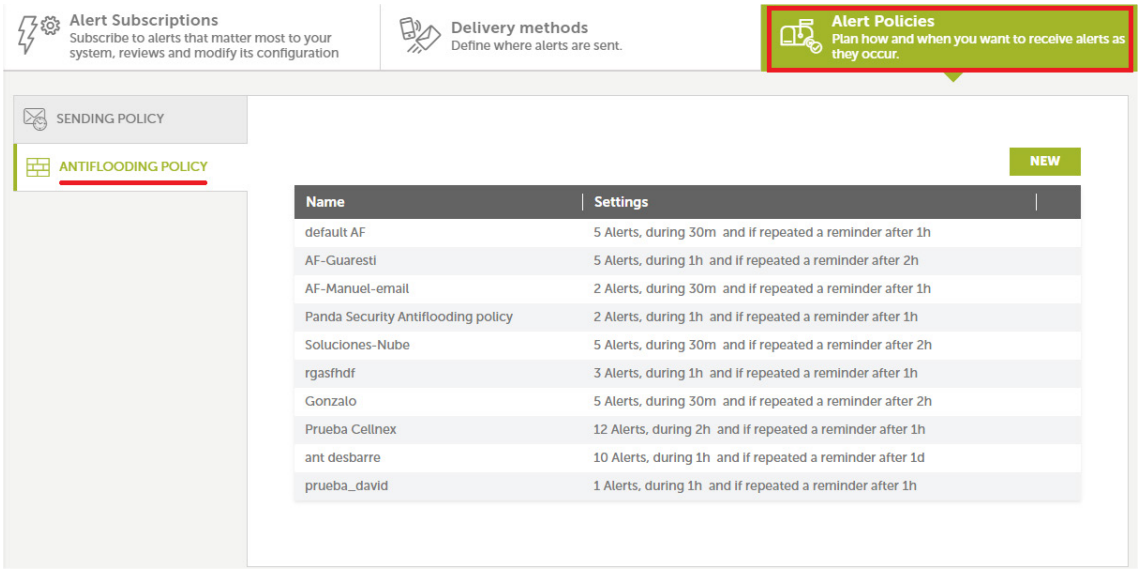


Figure 53: antiflooding policy creation window

Click **New** to display a window with the complete settings options of the policy.

Here you can set:

- Maximum number of alerts that can be received.
- Time period to which the previous criteria applies.
- A reminder if the alert is repeated after the established time period.

6.6.1 Editing antiflooding policies

Each of the antiflooding policies created has an associated menu that allows it to be edited and/or deleted.

When editing antiflooding policies already created, a window is displayed with editing options.

6.7. Creating alert policies or delivery methods

Alert policies, also called sending policies, let you define how the alerts generated are sent.

A sending policy is the nexus of the policies defined above (antiflooding policy and delivery methods).

Creating sending policies is carried out through the side menu **Administration**, **Alerts Configuration**, then go to the **Alert Policies** tab, then the **Sending Policy** tab.

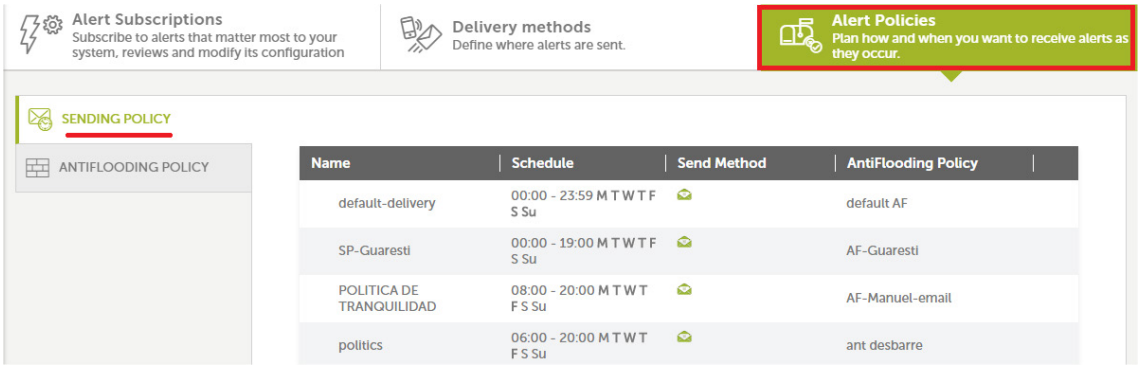


Figure 54: sending policy creation window

Click **New** to display a window with the complete settings options of the sending policy:

- **Name**: Name of the sending policy.
- **Default**: This indicates whether the policy is to be treated as a default policy. If there are alerts that don't have a sending policy assigned, this will be assigned by default.
- **Antiflooding policy**: This specifies the antiflooding policy to apply.
- **Schedule**: This indicates the time period when the policy will be active.
- **Send method**: This indicates the methods of delivery configured earlier that will be used to deliver the alert.

6.7.1 Editing sending policies

Each of the sending policies created has an associated menu that allows it to be edited and/or deleted. When editing sending policies already created, a window is displayed with editing options.

6.7.2 Configuring an alert sending policy

Sending policies are assigned to alerts through the side menu **Administration**, **Alert Configuration**, then go to the **Alert Subscriptions** tab.

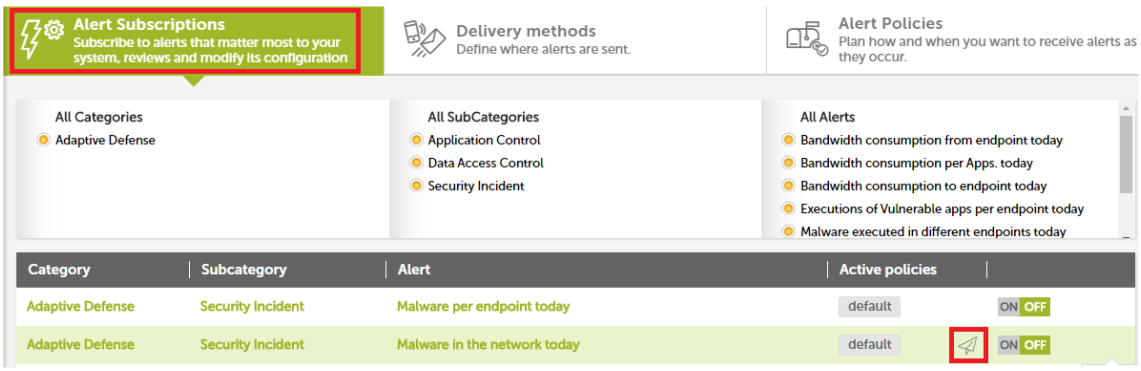


Figure 55: sending policy configuration window

Each alert has an  icon which lets you select a sending policy.

7. PII knowledge table

Table description

7.1. Oem.panda.edp.ops table description

Adaptive Defense collects information about the processes run on all workstations and servers across the network, whether goodware or malware. If those processes access PII files, the information is sent to the **Panda Data Control** server, where it is organized into an easy-to-read table.

Each line of the table is an event monitored by **Panda Data Control**, and provides information such as when the event occurred, the computer where it took place, its IP address, etc.

7.1.1 Edp.ops table

Name	Description	Values
evendate	Date when the event was logged on the **Panda Data Control** server	Date
serverdate	Workstation/server's date when the event was generated	Date
machineName	Workstation/server name	String
machineIP	Workstation/server IP address	IP address
User	User name of the process that operated on the file	String
ExfiltrationFlag	Indicates whether the file has been the subject of an operation classified as data exfiltration, data infiltration, or both	INFILTRATION EXFILTRATION BOTH
DocSize	Size of the PII file (in bytes)	Numeric
Operation	Operation performed on the PII file	Create Modify Open Delete Rename Copy-Paste OnDemand: Search launched from the console by the administrator
FatherHash	MD5 of the process that operated on the PII file. This field will be empty if **operation** is **On Demand**	String
FatherPath	Path of the process that operated on the PII file. This field will be empty if **operation** is **On Demand**	String
FatherCategory	Category of the process that operated on the PII file. This field will be empty if **operation** is **On Demand**	Goodware Malware Monitoring: Unknown process in the process of classification PUP: Unwanted program
DocumentPath	Drive where the PII file that was operated on resides, along with its path, in the following format: DEVICE TYPE|PATH	String
DocumentName	Name of the file that was operated on. In rename operations, this field displays the **DocumentName** value of the original file, and the **DocumentName** value of the renamed file, in the following format: TARGET_NAME|ORIGINAL_NAME	String String | String
DocumentHash	Hash of the file that was operated on	String

DeviceType	Drive where the PII file that was operated on resides	0: UNKNOWN 1: NO_ROOT_DIR: The path is invalid or does not exist 2: REMOVABLE: Mobile device (external hard drive, card reader, USB device, etc.) 3: FIXED: Internal hard drive 4: REMOTE: Network drive 5: CDROM 6: RAMDISK | String
CreditCardCount	Number of credit card numbers found in the PII file	Numeric
AccountCount	Number of bank account numbers found in the PII file	Numeric
IDCount	Number of ID card numbers found in the PII file	Numeric
DriveLicCount	Number of driver's license numbers found in the PII file	Numeric
PassPortCount	Number of passport numbers found in the PII file	Numeric
SSIdCount	Number of social security numbers found in the PII file	Numeric
EmailCount	Number of email addresses found in the PII file	Numeric
FiscalIDCount	Number of taxpayer identification numbers found in the PII file	Numeric
IPCount	Number of IP addresses found in the PII file	Numeric
NameCount	Number of first and last names found in the PII file	Numeric
AdressCount	Number of physical addresses (street name, house number) found in the PII file	Numeric
CityCount	Amount of location data (cities) found in the PII file	Numeric
PostalCodeCount	Number of postal codes found in the PII file	Numeric
PhoneCount	Number of phone numbers found in the PII file	Numeric
UserStringRule	Unused	Null
UserStringRuleCount	Unused	Null
UserRegex	Unused	Null
UserRegexCount	Unused	Null
Reclassified	True: The file contained PII but doesn't	Boolean

	contain it any more False: The file has not been reclassified and therefore contains PII

Table 1: description of the actions taken on PII files

8. Appendix 1: Extension list

Supported extensions

8.1. Supported extensions

Panda Data Control searches for personal data in files with the following extensions:

Suite name	Product	Extensions
Office	Word	DOC DOCX DOCM RTF
	Excel	XLS XLSM XLSX XLSB
	PowerPoint	PPT PPS PPSX PPSM SLDX SLDM POTX PPTM
OpenOffice	Writer	ODM OTT STW SXG SXW
	Draw	ODG OTG STD
	Math	ODF SXM
	Base	ODB
	Impress	OTP STI SXI
	Calc	OTS SXC
Plain text		TXT
Web browsers	Internet Explorer Chrome Opera Etc.	HTM HTML MHT OTH
Mail client	Outlook Outlook Express	EML
Other	Adobe Acrobat Reader	PDF
		XML
	Contribute	STC
	ArcGIS Desktop	SXD

Table 2:files in which Panda Data Control searches for PII

9. Appendix 2: Process list

Monitored processes

9.1. Monitored processes

When **Panda Data Control** comes to assessing whether an operation forms part of an incident classified as exfiltration or infiltration of personal data, the solution's machine learning algorithms look at the following subset of processes:

Type	Program name	Binary name
Web browser	Microsoft Edge	browser_broker.exe microsoftedge.exe microsoftedgecp.exe
	Google Chrome	chrome.exe
	Comodo Dragon	dragon.exe
	Mozilla Firefox	firefox.exe
	Microsoft Internet Explorer	iexplore.exe msimn.exe
	Opera	opera.exe
	Yandex	yandex.exe
	Mozilla Prism	zdclient.exe
	Torch	torch.exe
	Apple Safari	safari.exe
Mail messaging	Microsoft Outlook	outlook.exe
	Mozilla Thunderbird	thunderbird.exe
	Windows Live Mail	wlmail.exe
	Yahoo Zimbra Desktop	zdesktop.exe
Chat messaging	Microsoft Skype	skype.exe
	Facebook Whatsapp	whatsapp.exe
File storage	Dropbox	dropbox.exe
File transfer	PuTTY SFTP	psftp.exe
	WinSCP	winscp.exe
Windows administration	Putty	pscp.exe putty.exe
	Netcat	nc.exe
	Microsoft BITSAdmin Tool	bitsadmin.exe
Interpreter/Compiler	Microsoft Scripting Host	mshta.exe
	Java	java.exe javaw.exe
Database	Firebird SQL Server	fbserver.exe
Miscellaneous	Miscellaneous	browser.exe

Table 3: processes monitored in data exfiltration discovery tasks, along with the program's trade name and software type

10. Appendix 3: Panda Data Control requirements

Console access requirements
Internet access requirements
Hardware and software requirements

10.1. Management console access requirements

In order for you to access the Web console, your system must meet the following requirements:

- Have a certified/supported browser (others may be compatible)
  - Mozilla Firefox
  - Google Chrome

Other browsers may also work, but some of their versions may not be supported. That's why we recommend that the aforementioned Web browsers be used.

- Internet connection and communication through port 443.
- Minimum screen resolution 1280x1024 (1920x1080 recommended).
- Enough processing power to generate the module's charts and lists in real time.
- Enough bandwidth to display all the information collected from users' computers in real time.

10.2. Internet access requirements

To install and work with **Panda Data Control** correctly, the computers where the module is to be installed must be able to access a number of URLs.

If you have a firewall, a proxy server or other network connection restrictions in place, make sure to allow access to the following URLs:

Web management console

- https://www.pandacloudsecurity.com/
- https://managedprotection.pandasecurity.com/
- https://pandasecurity.logtrust.com

Updates and upgrades

- http://acs.pandasoftware.com/member/installers/
- http://acs.pandasoftware.com/member/uninstallers/
- http://enterprise.updates.pandasoftware.com/pcop/pavsig/
- http://enterprise.updates.pandasoftware.com/pcop/files/
- http://enterprise.updates.pandasoftware.com/pcop/nano
- http://enterprise.updates.pandasoftware.com/pcop/sigfiles/sigs
- http://acs.pandasoftware.com/free/
- http://acs.pandasoftware.com/sigfiles

- http://acs.pandasoftware.com/pcop/uacat
- http://enterprise.updates.pandasoftware.com/pcop/uacat/
- http://enterprise.updates.pandasoftware.com/updates_ent/
- https://pcopsupport.pandasecurity.com
- http://pcoplinux.updates.pandasecurity.com/updates/nanoupdate.phtml (Linux systems)
- http://pcoplinux.downloads.pandasecurity.com/nano/pavsignano/nano_1/ (Linux systems)
- http://www.intego.com (OS X systems)

Communications with the server

- https://mp-agents-inst.pandasecurity.com
- http://mp-agents-inst.pandasecurity.com/Agents/Service.svc
- https://mp-agents-inst.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-sync.pandasecurity.com/Agents/Service.svc
- https://mp-agents-sync.pandasecurity.com/AgentsSecure/Service.svc
- http://mp-agents-async.pandasecurity.com/Agents/Service.svc
- https://agentscomp.pandasecurity.com/AgentsSecure/Service.svc
- https://pac100pacprodpcop.table.core.windows.net
- https://storage.accesscontrol.pandasecurity.com
- https://prws.pandasecurity.com
- http://beaglecommunity.appspot.com (Panda Cloud Cleaner)
- http://waspproxy.googlemail.com (Panda Cloud Cleaner)

Communications with the Collective Intelligence servers

- http://proinfo.pandasoftware.com
- http://proinfo.pandasoftware.com/connectiontest.html

If the product cannot connect to the aforementioned URLs, it will try to connect to http://www.iana.org

- https://euws.pandasecurity.com
- https://rpuws.pandasecurity.com
- https://rpkws.pandasecurity.com/kdws/sigs
- https://rpkws.pandasecurity.com/kdws/files
- https://cpg-kw.pandasecurity.com
- https://cpp-kw.pandasecurity.com

- https://cpg-fulg.pandasecurity.com
- https://cpp-fulg.pandasecurity.com
- https://cpg-fusm.pandasecurity.com
- https://cpp-fusm.pandasecurity.com
- https://cpg-fuo.pandasecurity.com
- https://cpp-fuo.pandasecurity.com
- https://ows.pandasecurity.com

Ports 18226 TCP and 21226 UDP (customer intranet) must be open to allow correct communication between the **Panda Data Control** communications agents. Ports 443 and 80 must also be open on the proxy.

If you have perimeter security devices such as advanced firewalls, which inspect and block communications based on their content, we recommend that you add additional rules to allow traffic to the aforementioned URLs.

10.3. Hardware and software requirements

- Processor: Pentium 1 GHz
- RAM: 1 GB
- Free space for installation: 650 MB

- **Workstations**

- Operating systems: Windows 10, Windows 8.1, Windows 8, Windows 7 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows XP (32-bit and 64-bit) SP2 or later.

- **Servers**

- Operating systems: Windows Server 2003 (32-bit and 64-bit) SP1 or later, Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2, Windows MultiPoint Server 2012.
- Windows Core operating systems: Windows Server Core 2008, 2008 R2 and 2012 R2 (GUI installation not required).
- RAM: 1 GB

- **Other supported systems**

- VMware ESX 3.x, 4.x, 5.x and 6.x
- VMware Workstation 6.0, 6.5, 7.x, 8.x, 9.x, 10.x, 11.x and 12.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008, 2008 R2, 2012, 2012 R2 and 2016 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer and XenApp 5.x and 6.x

- **Installed libraries**

- Microsoft Filter Pack: MS Office 2007 or later