DATASHEET

WATCHGUARD DATA CONTROL

Monitor sensitive data across your endpoints

REAL-TIME DATA SECURITY, VISIBILITY AND CONTROL IN ONE PRODUCT

Uncontrolled access to your company's personal and sensitive data is an everyday security threat that may lead to serious financial loss and reputational damage. Are you willing to take that risk?

PROTECT YOUR PERSONAL AND SENSITIVE DATA

Companies are forced to strengthen or adopt new measures to protect the personal or sensitive data stored by the organization. The most important factors that motivate this transformation are:

- **Exponential increase in exfiltration cases and data leaks**. Data thefts are usually due to external attacks, malicious insiders aiming to make money or get revenge, or simply negligence, and affected organizations are often not even aware that this is happening.
- **Regulatory compliance with laws such as the GDPR,** violation of which can lead to having to pay large fines or a percentage of a company's global turnover.
- **Unstructured data grows massively.** Unstructured data makes up roughly 80% of an organization's entire data set, and the volume of unstructured data tends to double each year.

THE SOLUTION: WATCHGUARD DATA CONTROL

WatchGuard Data Control is a data security module fully integrated into WatchGuard EDR and WatchGuard EPDR. It is designed to help organizations comply with data protection regulations.

WatchGuard Data Control discovers, audits and monitors unstructured[1] personal data on endpoints: from data at rest to data in use and data in motion. Its powerful custom search engine allows administrators to find any file in the organization with data to control (copyrighted materials, confidential information, etc).

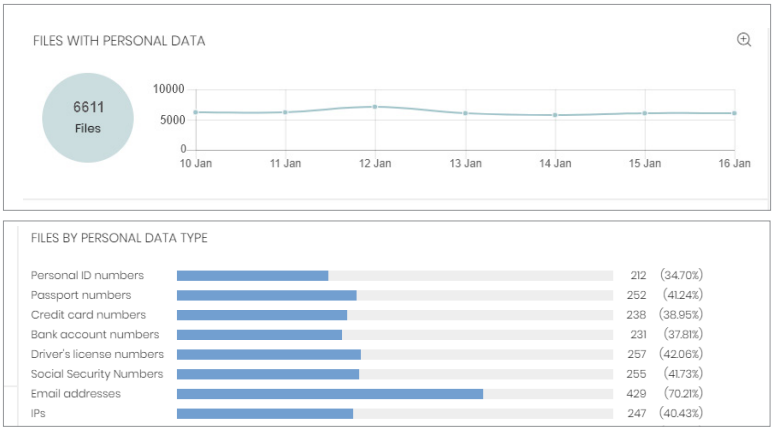


Figure 1: Main dashboard. Access to different panels to visualize files containing Personal Data, Computers With Personal Data, and Files By Personal Data Type.

KEY BENEFITS

Discover and Audit

Automatically identify files with personal data as well as the users, employees, collaborators, workstations and servers in your organization that are accessing personally identifiable information (PII[2]).

Monitor and Detect

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

Demonstrate Compliance

Show compliance with applicable regulations to senior management, the DPO,[3] and all other employees in your organization. Demonstrate the strict security measures in place to protect PII in workstations and servers.

Find Any Kind of Data to Control

Run custom searches to find any kind of data in the files on your network. Find duplicated personal files and delete them to reduce the risk of data exfiltration.

Simplify Management

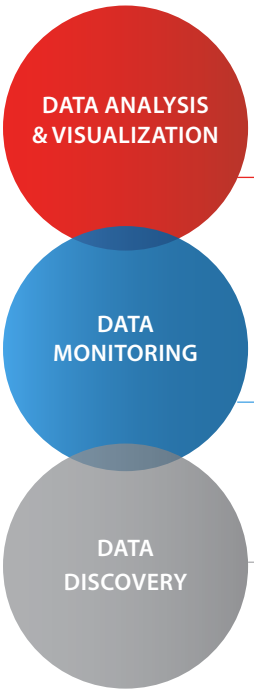
It doesn't require organizations to deploy any additional software or hardware and can be easily and immediately activated without cumbersome configurations. Once activated, the module is enabled and managed from the Cloud platform.

BUSINESS DATA GOVERNANCE

Strong data governance allows organizations to answer any questions related to the personal data handled by employees: What data is stored on employees'endpoints? Who can access that data and what actions are taken on it? Are those actions aligned with your corporate policies?

- Discover and understand unstructured personal data. Tag, group and classify this data according to its criticality.
- Establish security and access policies to control data access and use by authorized users.
- Educate your staff to ensure they handle data according to external regulations and internal policies.
- Use dashboards, reports, and custom and predefined alerts to demonstrate data governance.
- Analyze the causes of a personal data breach and adjust corporate policies. Establish the sequence of actions performed in a breach of personal information.

WATCHGUARD DATA CONTROL MAIN FEATURES



Visibility and insights into personal data at rest, in use and in transit, in real time and retrospectively

Pre-configured dashboards and alerts

Monitoring operations[4] for data in use

Monitoring of inbound and outbound[5] operations for data in motion

Monitor PIIF[6] and files matching User Defined Rules

Free custom searches to find files that match the search criteria (PIIF and non PIIF)

Exportable report with the results of the custom search

Classification of PII (data at rest) with machine-learning techniques

Inventory of files with PII available in WatchGuard Cloud

Supported Countries of WatchGuard Data Control

Available in Spain, Germany, UK, Sweden, France, Italy, Portugal, Netherlands, Finland, Denmark, Switzerland, Norway, Austria, Belgium, Hungary, and Ireland.

[1]**Unstructured data** refers to data that does not reside in a database or any other data structure. Unstructured data can be textual or non-textual. WatchGuard Data Control focuses on the textual unstructured data held on endpoints and servers.
[2]**PII (Personally Identifiable Information):** Personal ID, driver's license, passport, social security number, email, fiscal ID, IPs, first names, last names, phone numbers, bank accounts, credit cards
[3]**DPO (Data Protection Officer):** The person responsible for overseeing the data protection strategy in an organization
[4]**Data in use.** Monitoring of actions on PIIF: access, opening, creation, editing, deleting, renaming, copy and paste
[5]**Data in motion** with risk of leakage via Outlook, Web browsers, FTP, external USB drives
[6]**Files (PIIF):** Unstructured files with PII such as Office, OpenOffice, PDF, TXT, etc

FEATURES

Data Discovery

Automatically classifies and creates an indexed inventory of all files, including duplicates, that stores unstructured personal data (data at rest), with the number of occurrences of each type of data. These files can be deleted from the inventory. The Scheduler feature determines when the full disk analysis is launched (required for inventory and searches).

The classification process uses a combination of rules, regular expressions, and machine-learning techniques, among others, optimizing classification results while reducing false positives and resource consumption on devices.

Data Search

Run free custom searches to find files with specific content. **WatchGuard Data Control** will generate a list of all files containing the information, with the option to export it for easier management.

Data Monitoring and Control

Monitor the various types of operations performed on unstructured files (data in use), while keeping the personal data file inventory fully up to date. Any attempt to copy or move any of these files out of the network via email, web browsers, FTP or removable storage (data in motion) is recorded by the module. Control writing information in removable storage drives only if they are encrypted.

Data Visualization

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

WatchGuard Data Control's dashboards and predefined reports and alerts help to cover many use cases and ensure security governance of the unstructured personal data.

Supported platforms and systems requirements of WatchGuard Data Control

Compatible with the following solutions:
WatchGuard EPDR and WatchGuard EDR

Supported operating systems: Windows.

List of compatible browsers:
Google Chrome and Mozilla Firefox (others may be compatible).