HUAWEI OCEANSTOR AND SEARCHINFORM FILEAUDITOR INTEGRATED SOLUTION

PROBLEM

○ **Identification** of confidential files in document flow or storage and categorisation of them

○ **Control** of access, monitoring files available to specific users/usergroups

○ **Making** of shadow copies, ensuring recovery of lost information and saving history of file revisions

○ **Detection** of employee operations in the file system

Large data storage systems capable of managing massive data arrays and allowing for access for multiple users are unavoidable nowadays. The issue is that such storages require impeccable compliance with security rules and ensuring a high level of data protection.

In order to store your data safely and be aware of where your confidential information is located, who uses it or makes any changes, it is important to equip your system with smart analytics and accompany the storage with a file auditing tool.

SEARCHINF@RM

RISK AND COMPLIANCE MANAGEMENT

The essence of integration

Huawei OceanStor and SearchInform Risk Monitor – HOW DOES IT WORK?

✓ Logging at Huawei OceanStor level

✓ SearchInform FileAuditor reads logs from Huawei OceanStor file system

✓ Logs are read, standardised, processed and analysed by the SearchInform system

✓ Data is checked in accordance with security policies, information security incidents are detected

✓ Content of the files is scanned and tagged according to the preset categories

✓ Current access rights to the specified files get identified

HUAWEI

SEARCHINF⊙RM
RISK AND COMPLIANCE MANAGEMENT

Search

- **Search by dictionaries** – identify documents on specific topics: trade secret, GDPR, etc.

- **Search by attributes** – file name, type and size, etc.

- **Search by regular expressions** – look for documents containing data of the same type, for example, phone numbers, passport numbers and series, bank details, personal names, etc.

- **Basic search algorithms** – search by words and phrases.

- **Search by operations** – creation, removal, modification, opening, etc.

Alerts

- Security policies can be created based on search criteria

- The checking against the security policies can be scheduled

- In case an event matches the criteria a specialist will be alerted to an incident

Classification

- Tags every file depending on the type of information it comprises

- Classifies files by personal data, credit card numbers, trade secret, etc.

- Allows creation of a "library" of sensitive data with detailed catalog

Reports

Reporting function allows quick creating visual analytics and receiving details about any aspect you're interested in.

The default configuration includes basic templates, and the report wizard allows you to create custom reports not limited by any criteria.

- RelationsChart report

- Content routing report

- User productivity report

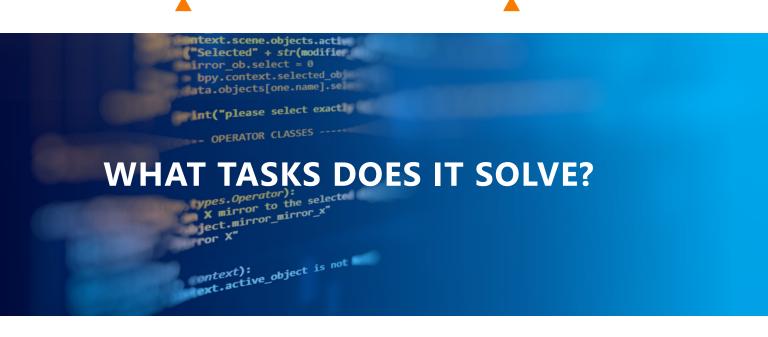- Software and hardware report

- etc.

Blocking

Abnormal activity blocking. File tags help control editing, reading, uploading, and other actions which are suspicious. Configuration of restrictions for users and PCs is flexible and easy.

Classification of vulnerable data

Finds files in a document flow that contain critical information, and assigns a certain type to each file: personal data, trade secret, credit card numbers, etc.

Access rights audit

Facilitates confidential information access control – automatically monitors open resources, files available to a specific user or group, privileged accounts.

WHAT TASKS DOES IT SOLVE?

Critical documents archiving

Makes shadow copies of critical files found on a PC, server or network folders, saves the history of their revisions. Confidential data archive helps in incident investigation and ensures recovery of lost information.
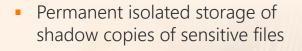
User activity monitoring

Audits user operations in a file system. The specialists responsible for risk mitigation always have their information about changes made to a file updated (creating, editing, moving, deleting, etc.).

SEARCHINF@RM
RISK AND COMPLIANCE MANAGEMENT

BENEFITS

- You get a single solution as SearchInform FileAuditor and Huawei OceanStor are smoothly integrated

- No need to deploy third-party solutions and make them work together

- Built-in options of audit of operations with information and access control list

- Automated categorisation of stored data based on its content

- Permanent isolated storage of shadow copies of sensitive files

- Detection of storage violations and access misuse

HUAWEI

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

ABOUT SEARCHINFORM

SearchInform was founded in 1995, since then the company has been developing information security solutions for businesses as well as has been active in the ERM market for 15 years already. In 2017 SearchInform solution was recognised by Gartner and included into the Gartner Magic Quadrant.

Today the company provides
more than **3000** clients in **20** countries
with the software and services protecting
over **2 000 000** computers all over the world.

SEARCHINF@RM

RISK AND COMPLIANCE MANAGEMENT

searchinform.com