DAR Remediator

Protirus Information Protection eXtensions

ACCELERATE YOUR DLP DATA AT REST (DAR) PROGRAM BY SAFELY AUTOMATING REMEDIATION ACTIONS

Safely Accelerate Your DLP DAR Program

Automatically quarantine / redact large volumes of sensitive documents identified by DLP based on attributes such as last accessed date - e.g. files untouched for over a year are less likely to impact the business if removed or protected. We leave clear instructions for the user detailing what has happened and the process for retrieving it safely if required.

Reduce Costs and Business Impact

DAR Remediator allows you to apply broader criteria for securing sensitive data, leading to operational cost savings, while simultaneously not impacting the business functions - this is accomplished by proactive leaving clear instructions detailing how the owner of the file can identify themselves and regain access to the file.

Automate AIP Classification and Encryption

Automatically apply AIP labels and associated encryption based on your DLP rules - identify the appropriate levels of classification and, where necessary, apply AIP encryption to limit access to over exposed sensitive data.

Multiple Repository Support

O365 OneDrive and SharePoint

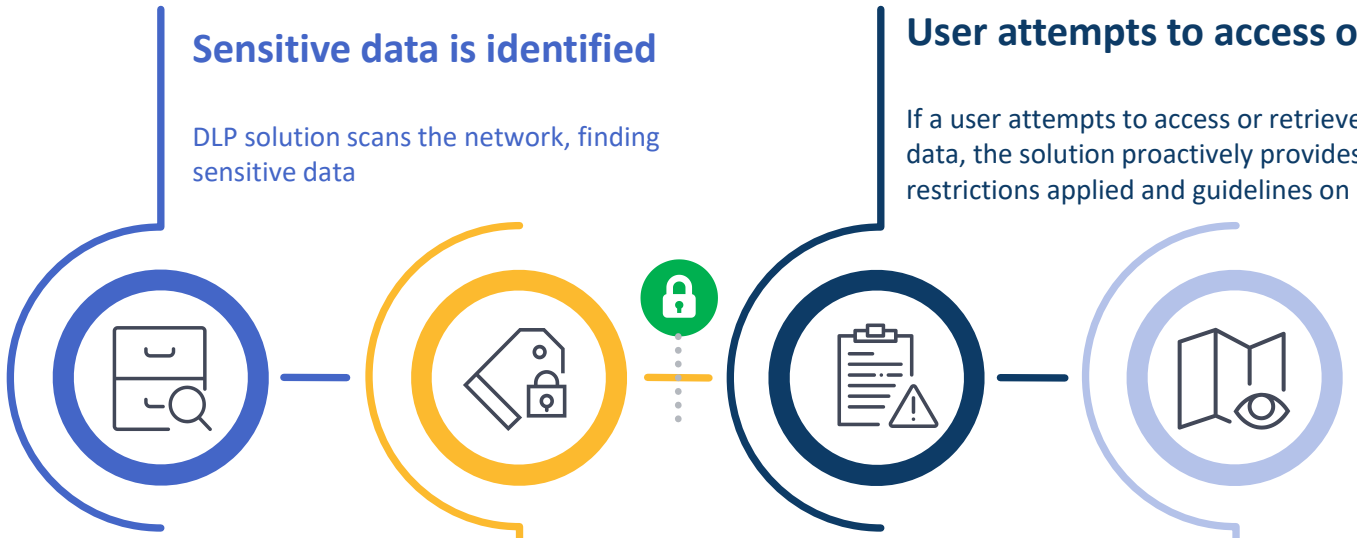
On Premise File Shares, home drives and NAS

On-premise SharePoint

PROTIRUS

PIPeX DAR Remediator

How It Works



Sensitive data is identified

DLP solution scans the network, finding sensitive data

DAR Remediator applies protection

Based on actions defined centrally, protection is applied to the sensitive data; protection mechanisms include:

- AIP Label and Encryption
- Redaction
- Quarantine

User attempts to access or retrieve data

If a user attempts to access or retrieve the remediated data, the solution proactively provides information on the restrictions applied and guidelines on how to regain access

Access to the file is returned to the user

The file is returned to the user, allowing the extraction of the detail needed and removing the offending data

PROTIRUS

PIPeX DAR Remediator

How It Addresses Your DAR Incident Remediation Challenges

Challenges	Solutions
Large volumes of files may be identified by DLP as sensitive, breaking compliance or even the law, by being stored in overly exposed areas. Correcting this is a **lengthy, manual and operationally expensive task**.	With DAR Remediator you can **automatically** apply broad controls such as **quarantine, redaction, deletion and encryption** to secure your data and remediate DLP incidents. This allows you to secure sensitive data, leading to **operational cost savings**
Manual scripted methods of DAR remediation are often **disruptive to the business**. This happens due of the use of broad remediation measures – when these are applied, they may limit users' access to data potentially relevant for their business function.	DAR Remediator allows you to apply broad criteria for securing sensitive data **without business impact** - this is accomplished by proactive leaving clear instructions detailing how the **owner** of the file can identify themselves and **regain access to it**.
Due to governance requirements, large volumes of files must be **classified** accurately with **AIP**, but the DLP solution does not provide a mechanism to achieve this.	DAR Remediator allows you to **automatically apply** 2 tiered **AIP** classification based on detailed content analysis, such as PCI, GDPR – PII + Sensitive PII.

PROTIRUS