Get Control of Your Unstructured Data | Security Compliance Productivity

Fasoo Data Radar

Unified Approach for Unstructured Data

Discover and Classify
Encrypt and Restrict Access
Trace and Audit

Fasoo Data Radar can discover, classify, and protect sensitive data with smart "Pac & Tag" technology in a single automated workflow on file servers, desktops, laptops and connected drives. An agent installed on each device applies policies defined by administrators using the web-based console. Files matching your unique definition of sensitive data can be tagged, encrypted and restricted (Pac) according to policy, without the need for user intervention, or allow users to choose which files to protect. A unique identifier (Tag) is embedded with each file so it's never out of your control and provides deep traceability for regulatory audit requirements. Data Radar is linked to a user profile through integration with Active Directory or other LDAP-based directory services.

Discover

- Automatically scan file servers, desktops, laptops and connected drives for unstructured data
- Define sensitivity level by matching patterns, dictionary terms, regular expressions and thresholds
- Capture file name, location, size, time accessed and detected patterns
- View detected files at the centralized console and locally for the user to view

Classify

- Add classification tags as metadata to identify files containing sensitive data
- Automatically classify files or allow users to add tags manually
- Indicate how files should be protected and used based on classification tags
- View how local files are classified in a local viewer or within each file

Encrypt and Restrict Access

- Encrypt files automatically based on level of sensitivity and classification
- Restrict file access to unauthorized users
- Maintain encryption and control when files are shared or copied outside your network
- Quarantine or delete files to eliminate redundant, trivial or obsolete data

Trace and Audit

- Trace discovered files, their locations and the sensitive data found in them
- Revoke access to sensitive file derivatives and renamed copies wherever they reside
- Demonstrate compliance with internal policies, customer requirements, and government mandates
- Review trends to understand how data grows and changes

Fasoo 7315 Wisconsin Avenue, Bethesda, MD 20814 (732) 955-2333 inquiry@fasoo.com www.fasoo.com

System Requirements

Server

Hardware

CPU: Xeon 2.5GHz Quad Core or higher

RAM: 16GB or higher (recommend 32GB)

HDD: 100GB or higher

Software

OS: Linux, Windows Server 2008 R2 or later

DBMS: Microsoft SQL Server 2008 or higher, MySQL, MongoDB

Client

Hardware

CPU: 2GHz or higher

RAM: 3GB or higher

Operating System

Microsoft Windows 7 or later

Microsoft Windows Server 2008 R2 or later

Apple macOS High Sierra

Linux

File types supported

Microsoft Office (doc, docx, eml, mdb, msg, ppt, pptx, rtf, xls, xlsx)

Open Office (odp, ods, odt, ott, stc, stl, sxc, sxi, sxw)

Adobe Reader (pdf)

Text (txt)

CAD (dwg)

Image (jpg, png, bmp, tif, tiff, gif)

Adobe Photoshop (psd)

Web Browser (chm, htm, html, mht, xml, xps)

Archive (7z, alz, bz2, gz, rar, tar, zip)

Others as defined by customer

Categorize and protect sensitive data

Administrators can use Data Radar to identify and protect sensitive data on network storage locations, desktops and laptops, ensuring persistent data protection and visibility.

STEPS

1. Create filters with one or more data patterns.
2. Group filters and set thresholds to detect sensitive data that meet regulatory and corporate governance needs.
3. Create labels to classify detected files.
4. Define encryption level or remediation applied to a file when it meets the definition of sensitive data.
5. Assign policies to servers, users, groups, roles or job titles that classify and protect files on a schedule or as users or systems create and modify them.
6. View details of detected files and sort them by classification type, level of sensitivity and remediation actions.