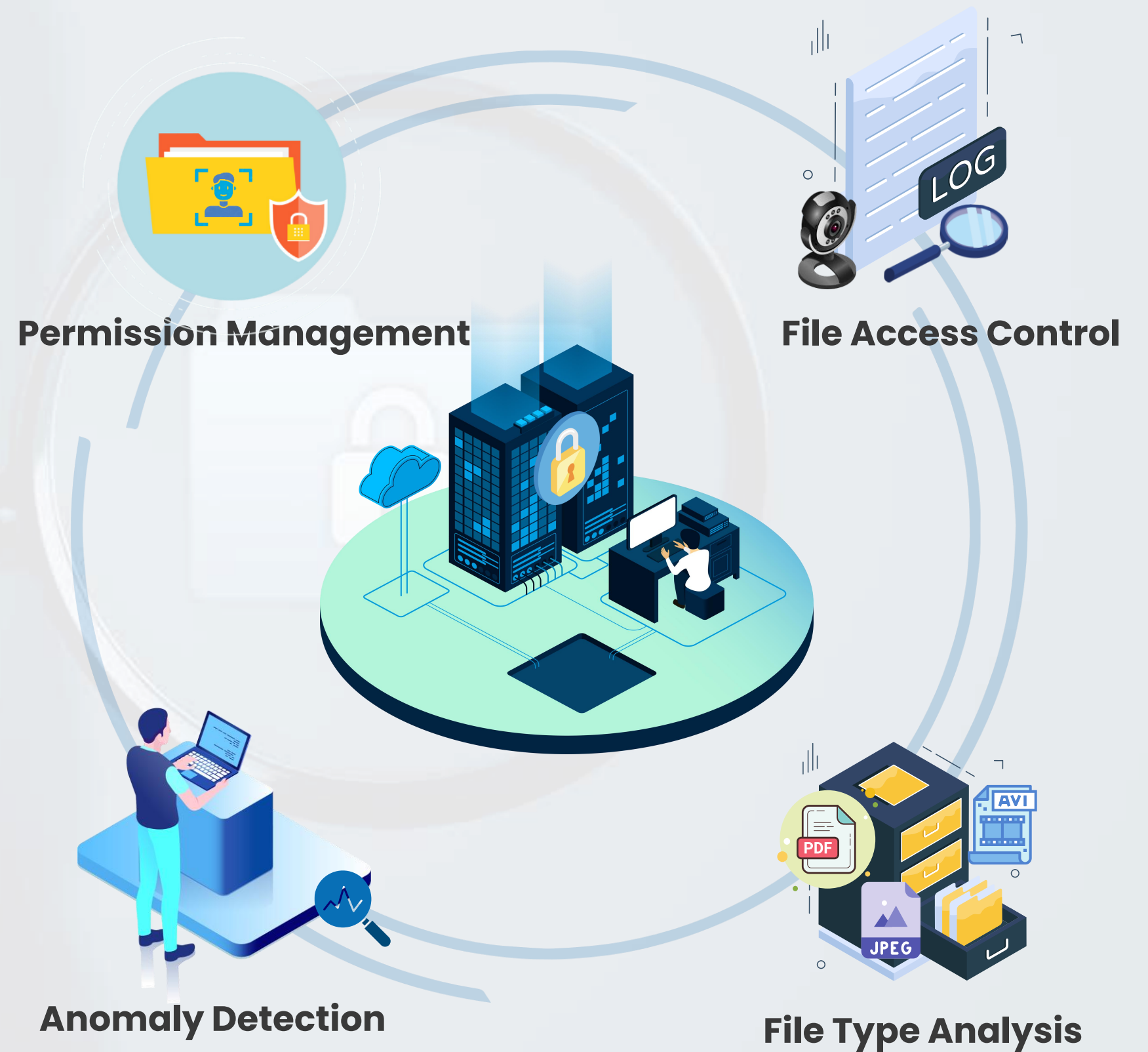




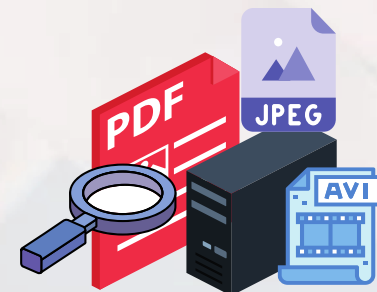
# Report and Manage Cyber Security Risks on the File Server



The management of file servers is important for securing files and maintaining data integrity. However, misconfiguration or inadequate management of file servers can introduce a number of risks. FolSec offers 4 perspectives to the IT administrator to identify risks on file sharing servers, provide visibility and ease of management. With FolSec

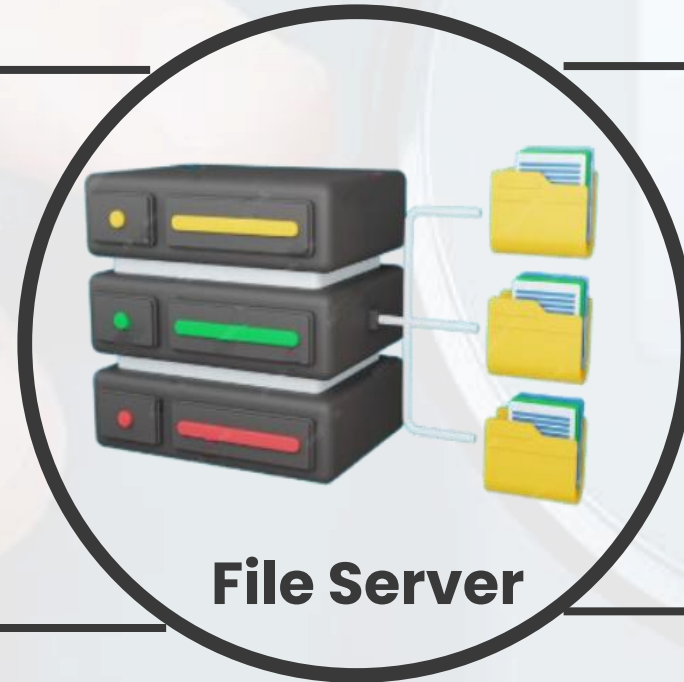
## NTFS Permission Reporting & Management

It manages user permissions on the file server from the web interface, thus ensuring that only authorized people can access the files. With FolSec



## File Type Analysis

It analyzes the types of files on its server, identifies potentially dangerous or incompatible files and takes precautions against them.



## File Access Control

It monitors and audits file activities so you can report intrusionable access statuses.



## Anomaly Detection

Anomalies on the file server are detected and responded to quickly, thus preventing possible security breaches in advance.

# What you cannot report or measure you cannot manage the system.

folder  
permission  
risks!

Risk of not being able to detect  
whether users have unnecessary  
permissions



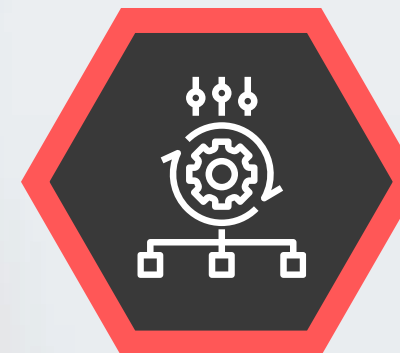
It cannot be reported  
instantly which folders the  
Everyone group has access  
permission to.

No restore option in case  
folder permissions are  
corrupted



Granting permissions on a  
user-based basis rather  
than Active Directory  
Groups

Inability to manage access  
requests to critical folders



Lack of reporting in folder  
permission processes

# FolSec permissions of NTFS folders Report and manage from the web interface.

Perspective  
Features of  
permission



**Permission Reporting and Management**



**Leave Request Management**

Users can make folder permission requests themselves



**Active Directory Security Group Management**

You can add and edit groups from the FolSec web interface.



**Leave Management**

You can Add Permission - Delete - Clone - Move - Allow for a period of time - Assign scheduled permission..



**Backup and restore folder permissions**

# You can't manage the risk you can't see:

## File Server Access Risks

Failure to monitor file access and activity increases the risk of security breaches going undetected



Not tracking what users do and what files they access makes it difficult to detect **unauthorized activity**

Failure to detect malicious or suspicious activity prevents early detection of **vulnerabilities or breaches**



Failure to monitor devices running on the system makes early detection of **malware** difficult.

Not tracking changes to files makes it difficult to detect **data loss or unauthorized changes**



# Reporting and alarming of user access opportunities on the file server.

File Access  
Perspective  
Features



Reading from event logs, deleting, creating, moving, changing permissions, editing files, changing file ownership, deleting event logs, etc. Makes access logs meaningful with



Reports **process activities** in file access logs



Makes suspicious user activities **visible**



Provides **instant notifications** by reporting file activities and generating customizable alarms



Provide reporting of **user activities**

# Failure to detect dangerous or unwanted file types can lead to security risks.

File Type Risks!

Failure to automatically manage old or unnecessary files can **increase** data management costs and unnecessarily take up storage space



Failure to detect unwanted or unnecessary files can cause storage space and **data crowding problems.**

Failure to detect multiple copies of the same data may result in inefficient use of storage resources



Incomplete file categorization can lead to data management and **compatibility issues**

# Provide detailed reporting and management of the properties of the files on the file server

File Type  
perspective  
properties



Reporting of file extensions. How many of each file type are there, who owns them, and what is their size?

You can **detect** waste files

With file aging, you can delete, copy and move files **according to options** such as desired extension, access date and file ownership.

**Reporting** of file categories

**You can report which user and which path** the known Ransomware extensions are on and take action to delete them.

You can **clean data by reporting** duplicated files.



# You can perform anomaly behavior and user risk assessment on the file server.

Anomaly  
Detection  
Features



**You can detect suspicious user activities.** For example: Deleting, moving, changing permissions, etc. 100 files in 1 minute.



**Detection of suspicious Ransomware activity.** For example: If 100 file reading, deleting and creating events occur simultaneously within 1 minute, it will be reported as a suspicious activity.



**Alarms can be created according** to event types in a folder you can specifically specify. Ex. If 10 files in the c:\data\finance folder are deleted at the same time within 5 minutes, an alarm will be generated.



FolSec permission **control can report risky users** with access control file type control modules.

# Permission Perspective Overview

The screenshot displays the FOLSEC Folder Security Management interface. The top navigation bar includes the FOLSEC logo and several menu items: Dashboards, Folder Perspective (selected), User Perspective, Permission Logs & Restore, Backup & Restore, Report, User & Group Management, and Configuration. The main content area is titled "Folder Perspective" and shows a tree view of folders on the left, including fileserver01.folsec.local and folsecemc.folsec.local. The right pane displays the "Folder Permissions" for the path folsecemc.folsec.local, listing users and groups with their respective access levels and actions.

**Folder Perspective**

Path: folsecemc.folsec.local  
Folder Owner:  
Folder Permission Manager:

**Folder Permissions**

User&Group ↑	Access	Inherited	Actions
<input type="checkbox"/> CREATOR OWNER	Full Control	Disable	
<input type="checkbox"/> NT AUTHORITY\SYSTEM	Full Control	Disable	
<input type="checkbox"/> BUILTIN\Administrators (Local User)	Full Control	Disable	
<input type="checkbox"/> BUILTIN\Users (Local User)	Special	Disable	
<input type="checkbox"/> FOLSEC\ismail	Full Control	Disable	
<input type="checkbox"/> FOLSEC\Finans	Read & Execute	Disable	
<input type="checkbox"/> FOLSEC\Tubitak_BT	Read	Disable	
<input type="checkbox"/> FOLSEC\tevfik	Modify	Disable	

# Audit Perspective Overview

## Audit Logs

Date Filter: All Time
 File Server: folsecdc.folsec.local
 Archive

Record Time ↓	Account Name	Event	Event ID	Record ID	Object Name	Process Name	Record Info
25.03.2024 14:05	ismail	Rename	4656	1192400772	C:\newshare\New WinRAR arşivi.rar		Audit Success
25.03.2024 14:05	ismail	Modify	4663	1192400763	C:\newshare\New WinRAR arşivi.rar		Audit Success
25.03.2024 14:05	ismail	Create	4656	1192400762	C:\newshare\New WinRAR arşivi.rar		Audit Success
25.03.2024 14:04	ismail	Modify	4663	1192400706	C:\newshare\New Rich Text Document.rtf		Audit Success
25.03.2024 14:04	ismail	Create	4656	1192400705	C:\newshare\New Rich Text Document.rtf		Audit Success
25.03.2024 13:52	tevfik	Modify	4663	1192400528	C:\newshare\New Text Document (2).txt		Audit Success
25.03.2024 13:52	tevfik	Create	4656	1192400526	C:\newshare\New Text Document (2).txt		Audit Success
25.03.2024 13:52	tevfik	Create	4656	1192400511	C:\newshare\New folder (2)		Audit Success
25.03.2024 00:02	tevfik	Create	4656	1192387906	C:\Windows\System32\dsa.msc	C:\Windows\System32\mmc.exe	Audit Failure
24.03.2024 22:10	tevfik	Create	4656	1192386224	C:\Windows\System32\dsa.msc	C:\Windows\System32\mmc.exe	Audit Failure
23.03.2024 00:25	ismail	Permission Change	4670	1192348004	C:\newshare\New folder		Audit Success
23.03.2024 00:25	ismail	Permission Change	4670	1192348001	C:\newshare\New folder\New folder		Audit Success

# File Type Perspective General View



- Dashboards ▾
- File Analysis**
- File Duplicate Analysis
- File Action Policy
- Folder Analysis
- Folder Size Analysis
- Folder Size Logs
- Task Report
- Configuration

## File Analysis

File Server:  Extension:

- Show/Hide Filters ▾
- Clear Filters ▾
- Actions ▾
- Refresh
- Export ▾

Name	Category	Extension	Size	Created At	Updated At	Last Access Date	Owner	Tag	Doc. Last Author	Doc. Author	Full Path
New Text Document.txt	Text Files	.txt	0.00 KB	22.03.2024 16:14	22.03.2024 16:14	22.03.2024 16:14	FOLSEC\tevfik				\\fileserver01.folsec.local\FileServer03Share\New Text Document.txt
New Text Document - Copy (2).txt	Text Files	.txt	0.00 KB	19.03.2024 11:28	19.03.2024 11:28	19.03.2024 11:28	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer02Share\New folder (2)\New Text Document - Copy (2).txt
folsec-windows-interface.zip	Compressed Files	.zip	189.07 MB	13.03.2024 16:21	13.03.2024 16:19	13.03.2024 16:21	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer01Share\folsec-windows-interface.zip
new_test_file_100.txt	Text Files	.txt	0.00 KB	04.03.2024 19:13	04.03.2024 19:13	04.03.2024 19:13	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer02Share\audit_testing\119\new_test_file_100.txt
new_test_file_101.txt	Text Files	.txt	0.00 KB	04.03.2024 19:13	04.03.2024 19:13	04.03.2024 19:13	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer02Share\audit_testing\119\new_test_file_101.txt
new_test_file_102.txt	Text Files	.txt	0.00 KB	04.03.2024 19:13	04.03.2024 19:13	04.03.2024 19:13	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer02Share\audit_testing\119\new_test_file_102.txt
new_test_file_103.txt	Text Files	.txt	0.00 KB	04.03.2024 19:13	04.03.2024 19:13	04.03.2024 19:13	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer02Share\audit_testing\119\new_test_file_103.txt
new_test_file_104.txt	Text Files	.txt	0.00 KB	04.03.2024 19:13	04.03.2024 19:13	04.03.2024 19:13	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer02Share\audit_testing\119\new_test_file_104.txt
new_test_file_105.txt	Text Files	.txt	0.00 KB	04.03.2024 19:13	04.03.2024 19:13	04.03.2024 19:13	BUILTIN\Administrators				\\fileserver01.folsec.local\FileServer02Share\audit_testing\119\new_test_file_105.txt

# Anomaly Perspective General View

**FOLSEC**  
FOLDER SECURITY MANAGEMENT

Dashboards ▾ Anomaly Events General Summary **User Risk Analysis** Configuration

User Risk Analysis fileserver01.folsec.local Export Calculate User Risk Scores Configuration

### Top 5 Risky Users

User	Risk Score
tevfik	100
ismail	100
tevfik2	0
Folsec0101	0
selcukkibar	0

### User Risk Scores

Search Refresh Overall Risk Score ↓

User	Overall Risk Score
tevfik	100
ismail	100
tevfik2	0
selcukkibar	0
Folsec0101	0
Administrator	0
newuser	0
setuser	0

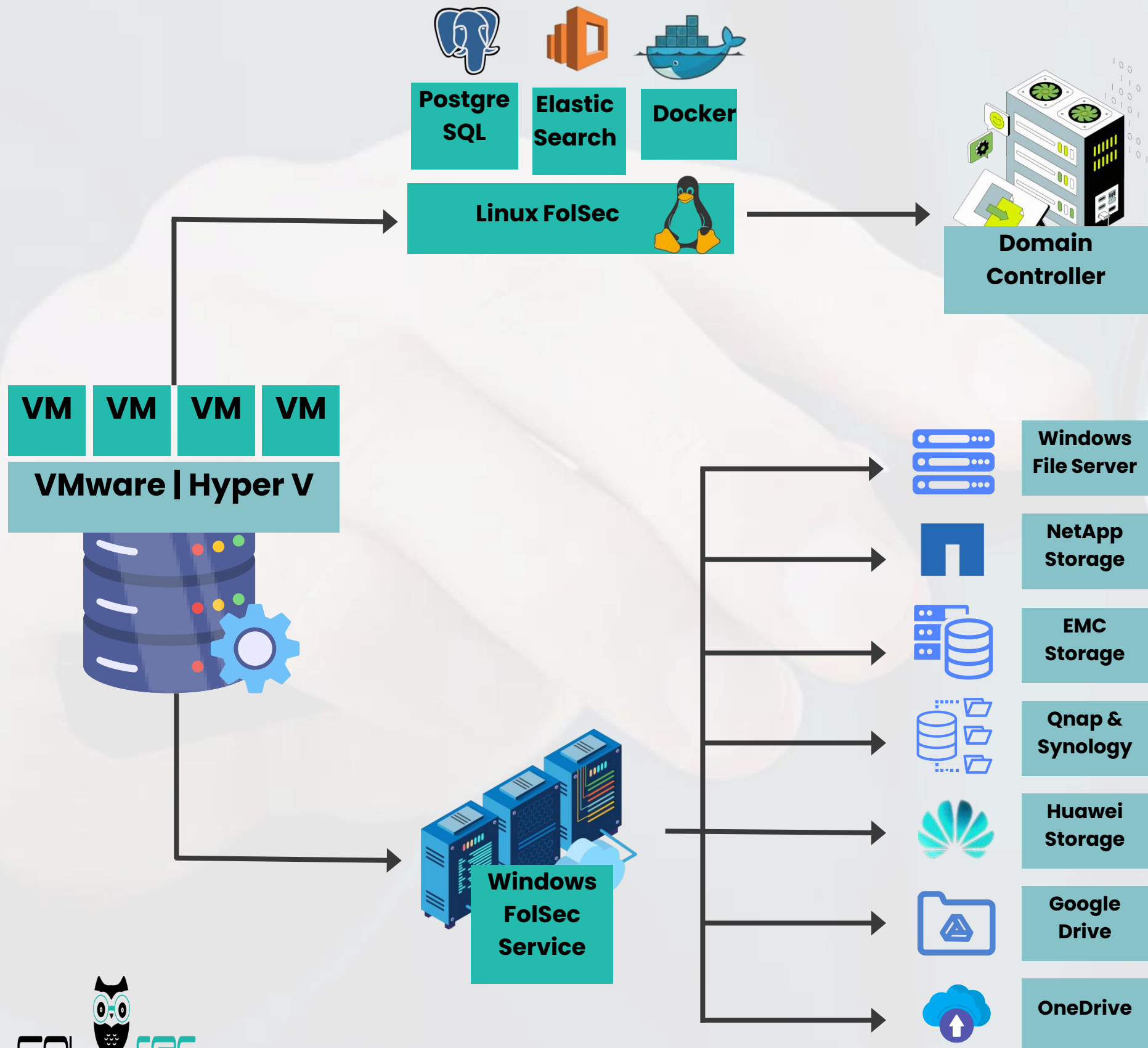
Items per page: 10 1-10 of 20

### User Risk Elements

Anomaly Risk Score: File Type Risk Score: Permission Risk Score: Audit Risk Score: Overall Risk Score:

Name	Risk Type	Value	Description
<input type="text" value="Search"/>	<input type="text" value="Search"/>		

# FolSec Topology



## Requirements


- ①
  - FolSec Linux (FolSec will be provided by.)
  - Cpu: Minimum 8 Core
  - Disk: Minimum 500GB (SSD Recommended)
  - Ram: Minimum 24GB
- ②
  - Windows 2016,2019 or 2022 Standard Server (1 piece ) Must be included in the domain.
  - Cpu: Minimum 8 Core
  - Disk: Minimum 500GB (SSD recommended)
  - Ram: Minimum 24GB

## Authorizations of FolSec Active Directory and File Server Service Account

- ① The FolSec user must be added to the "Account Operators" group on Active Directory in order to save the users and groups in the domain to the FolSec db.
- ② In order to read Windows event logs, it must be included in the "Event Log Readers" Group on the relevant file server..
- ③ In order to read permissions, file types, file sizes, etc. information, the FolSec service account must have at least "read, premission read and permission change" privileges in all folders..



## FolSec (Folder Security Management)

 0 533 215 73 95

 [info@folsec.com](mailto:info@folsec.com)

 [folsec.com](http://folsec.com)

