Arctera™
Dark Data Assessment

Analysis for ACME Roadrunner Suply

Delivered by The SE Community

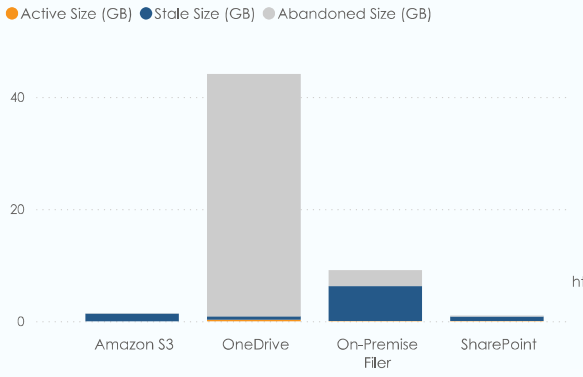
Revision 2.02 | November 2024

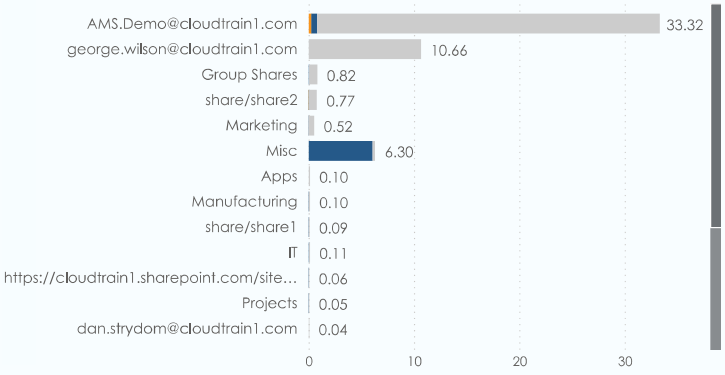
Arctera Dark Data Assessment

All

Environment Summary

Stored Data	Repositories	File Items	Control Points
67.43GB	53	14.23K	41
on 5 data source types	16 found as exposed / open	466 tagged as sensitive	2 found as permissive

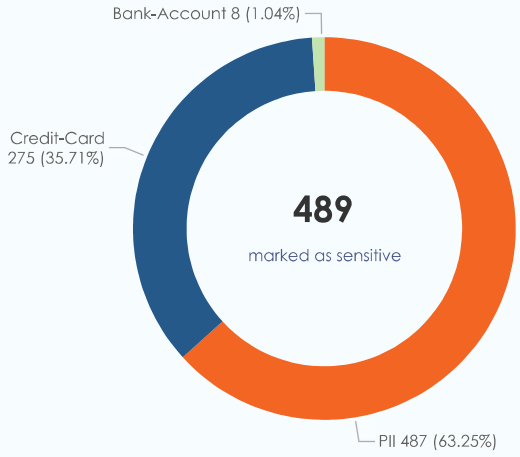




Sensitive Data Summary

Filter by Classification Tags

- Bank-Account
- Credit-Card
- DI_SYSTEM_PWD_PROTE...
- PII
- US-Drivers-License
- US-HIPAA
- US-SSN



357
sensitive files on open shares

487
files containing PII data

275
files containing PCI-DSS data

Recommendations

Delete Highly Sensitive and Regulated PII Files

No files containing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, or genetic / biometric data were found.

Such data profilings are forbidden by law (i.e: GDPR Art.9 rule), liaise with department owner to delete those files and review processes to prevent future special category captures.

Review Files containing PII on Open Shares

Out of 487 files containing personal identifiable information, 355 are specifically located on open shares!

You should consider with business owner to move those files to more controlled shares. It will reduce the surface risks of data leaks.

Review Files containing PCI/DSS on Open Shares

Out of 275 files containing credit card information, 246 are specifically located on open shares!

You should consider with business owner to move those files to more controlled shares. It will reduce the surface risks of data leaks.

arctera

Arctera Dark Data Assessment

All

Cost Analysis

15% Mission Critical Data

33% ROT Data

48% Classified Data

52% Dark Data

The Real Cost of Clutter

The Vulnerability Lag Report (Arctera / Vanson Bourne)

Cost Analysis for Doing Nothing

Based on your custom projected figures, are you comfortable spending close to **$765,000** on low to no value data?

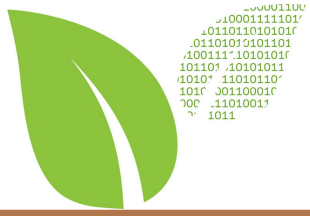
Mission Critical Data:	$162,000
ROT Data:	$297,000
Dark Data:	$468,000

Reset to initial findings

Projected Storage (TB)	300
TCO for 1TB/year	$3,000

Carbon Footprint Analysis

67.43GB Stored Data	**2.17kg** CO2e per year



345.MB Active Data	**0.01kg** CO2e per year
9.61GB Stale Data	**0.35kg** CO2e per year
49.64GB Abandoned Data	**1.81kg** CO2e per year

Reset to initial findings

Projected Storage (TB)	300
kg CO2e for 1TB/year	40

Impact for Keeping Everything

The current climate change is a consequence of our significant emissions of various greenhouse gases. We can measure these emissions with a simple index: kilograms of CO2 equivalent (kg CO2e).

Based in your custom figures, the data not being modified in the last 3 years impacts for **10,000 kg CO2e per year**

The Impact of old data on Green IT Initiatives

The carbon footprint of distributed cloud storage (arxiv.org)

Recommendations

Data Disposition

Hoarding older data with limited value to organisation can not only lead to hard storage costs & increased carbon footprint but also costs associated with various operations & risks associated with data leak.

Review the Abandoned, non-business data & dispose off anything not required for the business.

Data Tiering / Migration

Data not accessed often can be safely moved to lower tier storage so save costs.

Either move data using tools or employ tiering techniques to automatically tier data based on data age & content.

Data Retention

Any important data that needs to be retained for any regulatory or corporate compliance should ideally moved to specialized archive solutions with WORM capabilities.

Such data needs to be classified and reviewed periodically to ascertain expiry based on ever changing compliance policies.

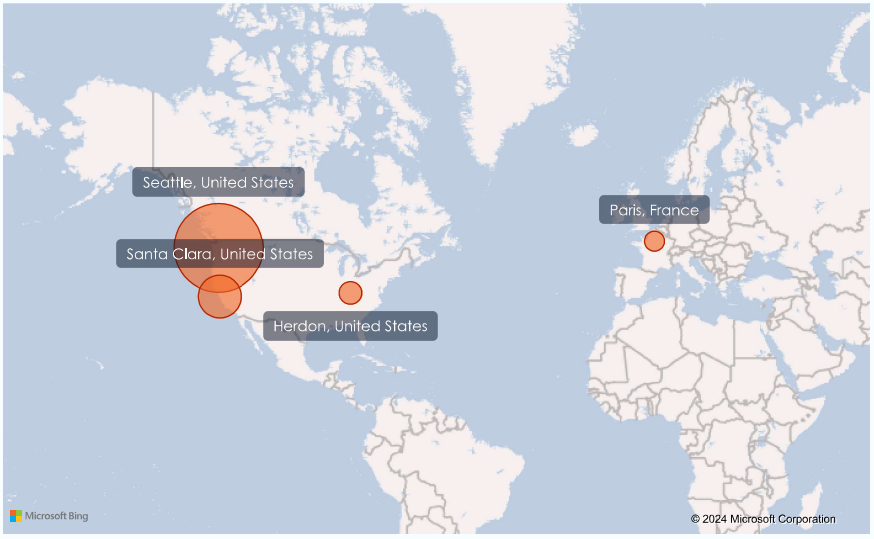
arctera

Arctera Dark Data Assessment

All

Storage Analysis

Stored Data per Location

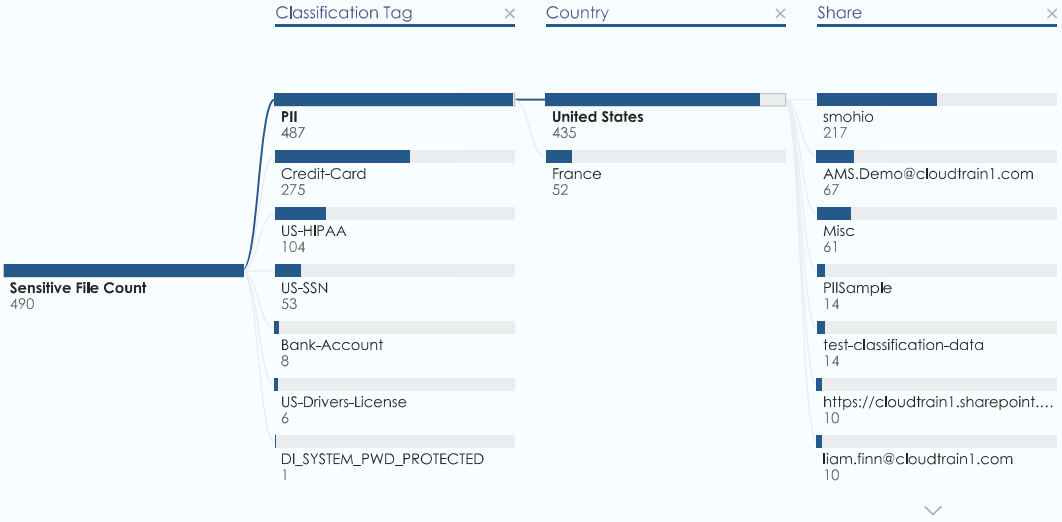


$3,000 Total Cost of Ownership per TB

67.43GB Stored Data	$ 162.6 per year
345.MB Active Data	$ 0.9 per year
9.61GB Stale Data	$ 26.2 per year
49.64GB Abandoned Data	$ 135.4 per year

Sensitive Data Storage Analysis

354.MB Sensitive Stored Data



22.46MB Sensitive Active Data

43.52MB Sensitive Stale Data

287.98MB Sensitive Abandoned Data

Recommendations

Review Data Storage

Periodically review stored data based on the local regulations & compliance requirements.

Understand what kind of data is consuming the most storage & why.

Data Locality / Sovereignty

Presence of personal data (PII) & other sensitive personal data on the systems warrants a detailed review of the PII information. As per various data protection laws OR regulations requirements, citizens data must reside in servers in certain jurisdictions.

Review the storage of files containing PII information.

Review Total Cost of Ownership

Review the Total Cost of Ownership of your stored data based on type of technologies leveraged and plan data reduction, migration projects based on the above insights.

arctera

Arctera Dark Data Assessment

All

Private Mode not Enabled

Cost of a Data Breach

$4.35M Average total cost of a data breach

45% of breaches occured in the cloud

Cost of a Data Breach

As of 2022, the cost per stolen record in data breaches worldwide amounted to **$164**.

Are you comfortable spending **millions** for data breaches with limited insights into sensitive data, access and usage?

12.7% increase since 2020
11% involved ransom
Remote work increased risks

The Real Cost of a Data Breach

Cost of a Data Breach Report (IBM / Ponemon)

487

files containing PII data

Loose PST Files

170

PST File Count

File Path	File Size (GB)	Permitted Users
\\cloudtrain1-my.sharepoint.com\AMS.Demo@cloudtrain1.com\albert_meyers_000_1_1.pst	0.03	0
\\cloudtrain1-my.sharepoint.com\AMS.Demo@cloudtrain1.com\andrea_ring_000_1_1.pst	0.18	0
\\cloudtrain1-my.sharepoint.com\AMS.Demo@cloudtrain1.com\andrew_lewis_000_1_1.pst	0.16	0
\\cloudtrain1-my.sharepoint.com\AMS.Demo@cloudtrain1.com\andy_zipper_000_1_1.pst	0.52	0
\\cloudtrain1-my.sharepoint.com\AMS.Demo@cloudtrain1.com\andy_zipper_001_1_1.pst	0.26	0
\\cloudtrain1-my.sharepoint.com\AMS.Demo@cloudtrain1.com\benjamin_rogers_001_1_1.pst	0.40	0
Total	**10.34**	

Recommendations

Review & Protect Sensitive Data

The presence of sensitive data in the unstructured repositories opens up risks for data breaches and leaks.

Periodically review sensitive data, need of storing these, access controls, protection & backup / recovery mechanisms.

Educate & Train

Majority of data breaches occur because of inefficient implementation of policies & procedures to safeguard data.

Educate & train your employees on data collection, storage & protection, data threats & data security best practices and periodically review and update policies, procedures & processes governing sensitive data.

Monitor Data Access & Exposure

Understand if the sensitive data is exposed to right individuals, monitor user activity to understand anomalous behaviours, attacks & unwarranted permission changes.

You should consider with business owners to move those files to more controlled shares. It will reduce the surface risks of data leaks.

arctera

Arctera Dark Data Assessment

Ransomware Risk

All

Private Mode not Enabled

7

Potential Ransomware Files

6/7/2021 4/19/2023

All

Clear all slicers

Probable Infection	Last Accessed	File Path	Users with File Access
July 1, 2021	March 10, 2022	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/4a-313.wpd.locky	4
June 7, 2021	June 7, 2021	\\fileserver.evlab.local\Group Shares\Accounting\Credit card\american-express.txt.asasin	6
June 7, 2021	June 7, 2021	\\fileserver.evlab.local\Group Shares\Accounting\Expense-policy.txt.cry	6
June 7, 2021	June 7, 2021	\\fileserver.evlab.local\Group Shares\CXO\FY20-Report.docx.locky	5
June 7, 2021	June 7, 2021	\\fileserver.evlab.local\Projects\Project_X\project-overview.pptx.asasin	8
June 7, 2021	June 7, 2021	\\fileserver.evlab.local\Projects\Project_Y\samples.rtf.locky	8
June 7, 2021	June 7, 2021	\\fileserver.evlab.local\users\Mike.Smith\Personal\WP_20160107_14_22_48_Pro.jpg.cry	3

Recommendations

Reduce Attack Surface Area

Apart from implementing various security principles, fixing vulnerabilities, training employees etc. devise a plan to manage privileges and access in an efficient way for data servers and cloud repositories, especially where sensitive data is stored.

Detect Anomalies

Employ various technologies that work together to understand anomalies in production environments to timely detect any infection or attack. This may include user behaviour analytics and backup anomaly detection among other techniques.

Remember that ransomwares are increasingly becoming sophisticated and detecting exfiltration or double extortion cyberattack requires multiple toolsets to provide timely detection.

Formulate a Robust Backup Strategy

Once cyberattack is detected, impact is established and threat is neutralised, successfully recovering data to a last known state is the most important step.

For that, organisations need to deploy a robust backup & recovery strategy.

Arctera Dark Data Assessment

All

Private Mode not Enabled

Sensitive Files

490
Sensitive File Count

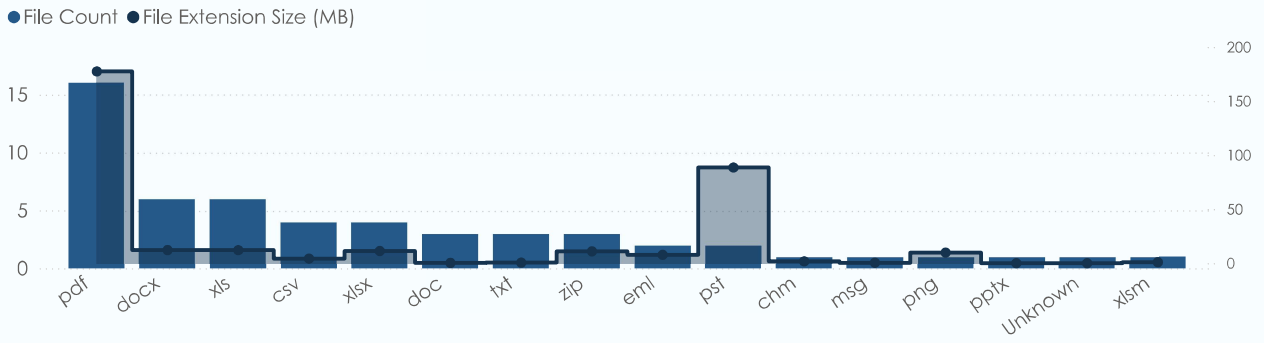
0 114

All

Clear all slicers

File Path	Classification Tags	Permitted Users
\\fileserver.evlab.local\Medical\General\087754.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\General\108615.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\General\486600.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\General\600738.pdf	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Medical\General\621153.pdf	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Medical\Medical Detail\226603.pdf	PII	114
\\fileserver.evlab.local\Medical\Medical Detail\551163.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\Medical Detail\653108.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\Medical Detail\Medical_Form.docx	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Medical\Medical Detail\Medical_Form-update.docx	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Misc\Credit card\Delimited and non-delimited.docx	PII | Credit-Card	114
\\fileserver.evlab.local\Misc\Credit card\Delimited.docx	PII | Credit-Card	114
\\fileserver.evlab.local\Misc\HIPAA matches\General\087754.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Misc\HIPAA matches\General\108615.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Misc\HIPAA matches\General\486600.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Misc\HIPAA matches\General\600738.pdf	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Misc\HIPAA matches\General\621153.pdf	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Misc\HIPAA matches\Medical Detail\226603.pdf	PII	114
\\fileserver.evlab.local\Misc\HIPAA matches\Medical Detail\551163.pdf	PII | US-HIPAA	114

Sensitive Files by File Types



Recommendations

Periodically Classify Your Unstructured Estate

Visibility into content of unstructured data is usually overlooked and that's where sensitive data risk lurks and is susceptible to breaches and leaks.

Ensure your organisation has a scalable and robust classification program in place for efficient data governance, protection & security.

Review & Prevent Exposure

In case there is a business need to store sensitive data in unstructured repositories, ensure that the data is adequately protected and only legitimate persons have access.

Build programs to periodically review access & exposure plus maintain permission hygiene.

Promote Accountability

Understand real data ownership and promote accountability of sensitive data with data custodians.

Involve business in decision making around data management, access governance, data protection and privacy.

arctera

Arctera Dark Data Assessment

User Activity

All

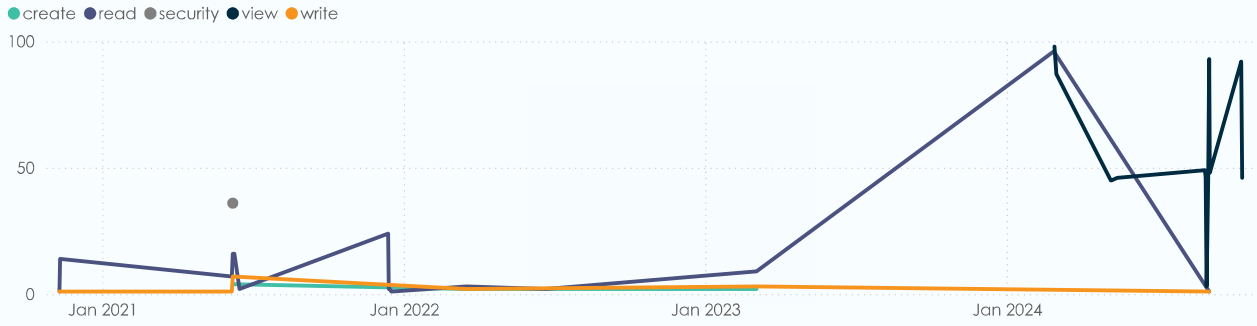
Private Mode not Enabled

190
Event Count

11/10/2020 10/12/2024

All

Clear all slicers



Time Stamp	Event Type	User Name	Full Path
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/10 - Copy.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/10.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/AC_Test.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/AL DDA Lab.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Anne Test 10302023.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Another Copy.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/bank-account.xlsx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Book.xlsx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Chambers.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/DDA_Taiwan_Training_For_Partner.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/DITest.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document10.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document11.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document12 - Copy.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document12.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document13.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document14.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document15.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document16.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document17.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document18.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document19.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Document20.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/DocumentFred.docx
10/12/2024 3:05:00 AM	view	app@sharepoint	https://cloudtrain1.sharepoint.com/sites/ditest1/Shared Documents/Documentqc.docx

Recommendations

Monitor User Activity

Continuously monitor user activity on unstructured data for forensics, investigations & meeting compliance needs.

User Activity monitoring also benefit operationally to keep the visible data estate up-to-date using "true" incremental scanning & classification.

Build Policies to Detect Malicious or Rogue Behaviour

Create policies to get alerts on unusual activity in the environment, be it an employee on a copying spree or a malware renaming and encrypting documents.

Give special care for any permission changes in the environment as those can inadvertently cause exposure of sensitive data leading to data leaks and breaches.

Leverage Usage Information to Certify Access

User entitlements should be reviewed regularly to ensure that right permissions are granted to right users and that ensures the risk is minimised from insider threat.

Historical user activity information should also be used in this activity to make permissions decisions and resolving challenges for additional context.

arctera

Arctera Dark Data Assessment

All

Private Mode not Enabled

Permissions Risk

2
Permissive Control Points

0 — 114

All | All | Clear all slicers

Permissive Control Point	Group Trustees	Permissions	Permitted User Count
\\fileserver.evlab.local\Medical\General	Administrators	Full Control	114
\\fileserver.evlab.local\Medical\General	Administrators	Read-Execute	114
\\fileserver.evlab.local\Medical\General	Administrators	Write	114
\\fileserver.evlab.local\Medical\General	Creator Owner	Full Control	114
\\fileserver.evlab.local\Medical\General	Creator Owner	Read-Execute	114
\\fileserver.evlab.local\Medical\General	Creator Owner	Write	114
\\fileserver.evlab.local\Medical\General	Everyone	Full Control	114
\\fileserver.evlab.local\Medical\General	Everyone	Read-Execute	114
\\fileserver.evlab.local\Medical\General	Everyone	Write	114
\\fileserver.evlab.local\Medical\General	Local System	Full Control	114
\\fileserver.evlab.local\Medical\General	Local System	Read-Execute	114
\\fileserver.evlab.local\Medical\General	Local System	Write	114

Sensitive and Permissive

73
Sensitive & Permissive Files

0 — 114

All | Clear all slicers

File Path	Classification Tags	Permitted Users
\\fileserver.evlab.local\Medical\General\087754.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\General\108615.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\General\486600.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\General\600738.pdf	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Medical\General\621153.pdf	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Medical\Medical Detail\226603.pdf	PII	114
\\fileserver.evlab.local\Medical\Medical Detail\551163.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\Medical Detail\653108.pdf	PII | US-HIPAA	114
\\fileserver.evlab.local\Medical\Medical Detail\Medical_Form.docx	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Medical\Medical Detail\Medical_Form-update.docx	PII | US-HIPAA | US-SSN	114
\\fileserver.evlab.local\Misc\Credit card\Delimited and non-delimited.docx	PII | Credit-Card	114
\\fileserver.evlab.local\Misc\Credit card\Delimited.docx	PII | Credit-Card	114
\\fileserver.evlab.local\Misc\HIPAA matches\General\087754.pdf	PII | US-HIPAA	114

Recommendations

Maintain Permission Hygiene

Overtime, businesses goes off best practices adding various access control entries and using all possible combinations of permissions for quick & dirty fixes to provide access. This can lead to over-exposure in the unstructured repositories.

Organisations need to review access hygiene on filesystem control points and directory services time to time.

Classify Data to Understand Toxic Combination

Permissive and sensitive data is a toxic combination as it's asking for trouble from insiders & cyber-attacks.

Along with visibility into permissions and exposure, classification is key to differentiate between valuable and non-valuable data and ensuring right controls are put in place to protect important data.

Govern Access

Regularly review entitlements / permissions to employees and other user accounts. Involve business users and promote accountability in keeping permissions up-to-date and minimising risk of over exposure.

Get permission recommendations and performing what-if analysis for permission changes before making those changes.

arctera

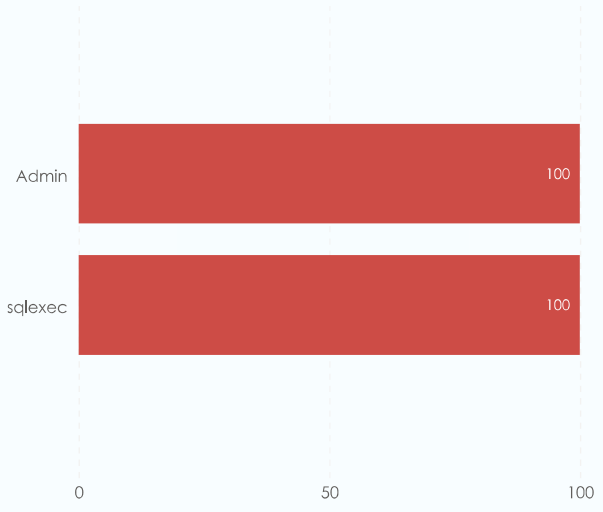
Arctera Dark Data Assessment

All

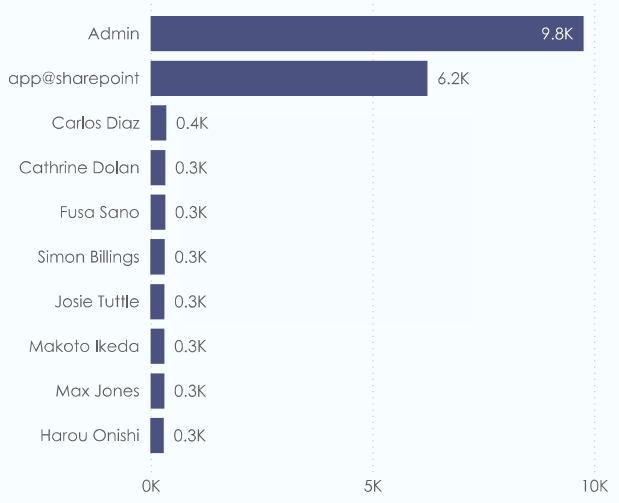
Private Mode not Enabled

Top 10 - Users

Riskiest Users

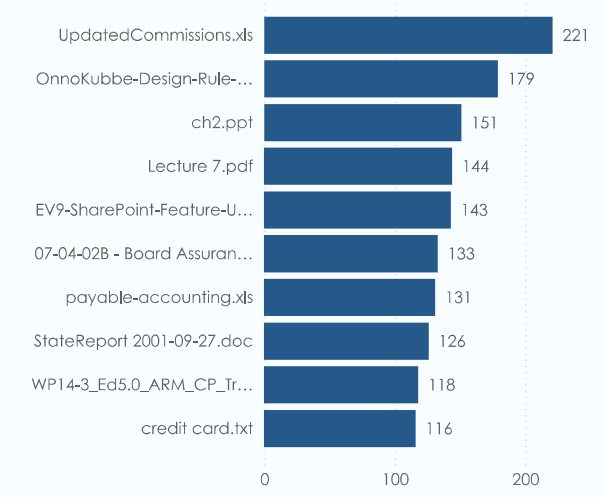


Most Active Users

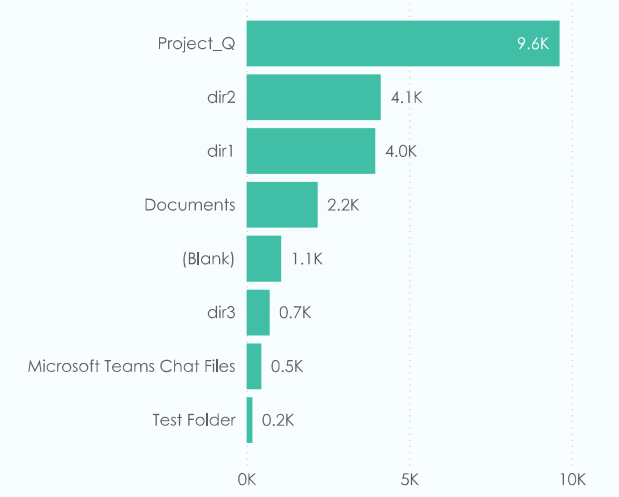


Top 10 - Most Accessed

Most Accessed Files



Most Accessed Folders



Recommendations

Review Riskiest & Active Users for Potential Threats

Users become risky if they get access to large number of files, have anomalous behaviour and have access polivy violations generated against them.

Review if certain applications need to move out of unstructured space or their activity need to be excluded from monitoring. Folder usage can provide insights into certain directories being accessed more than often and can be candidate for file and access control reviews.

Review File Type & Folder Usage

Understand if there are any unexpected file types having most activity which can lead to investigations & finding rogue users or applications.

Review if certain applications need to move out of unstructured space or their activity need to be excluded from monitoring. Folder usage can provide insights into certain directories being accessed more than often and can be candidate for file and access control reviews.

Reduce Access

One way to reduce unwanted accesses is to control permissions as per business need.

Leverage context, content and metadata to enable data-driven access controls.

arctera

Arctera Dark Data Assessment

All

Private Mode not Enabled

Directory Services

217

users across 188 groups

User Name	Deleted	Disabled
$R51000-FACLD2F2P7EO		✕
da arai	✕	
DefaultAccount		✕
Discovery Search Mailbox		✕
E4E Encryption Store - Active		✕
Guest		✕
HealthMailbox-Exchange-DB01	✕	
HealthMailbox-Exchange-Mailbox-Database-0960622640	✕	
it arai	✕	

Groups with disabled users
Denied RODC Password Replication Group
Domain Guests
Domain Users
Guests
None
Remote Desktop Users
System Managed Accounts Group
Users

Circular Groups

There are no matching items

Department Usage / Chargeback

Recommendations

Maintain Directory Services Hygiene

Stale or duplicate accounts & Groups can become unmanageable over time adding overheads and potential issues with access control.

Clean up the directory services accounts as per best practices and organisation policies to ensure that stale accounts or departed user accounts are disabled or removed from the system time to time and directory services hygiene is maintained.

Minimize Privileged Group Membership

Privileged groups are those to which powerful rights, privileges, and permissions are granted that allow them to perform nearly any action in an organization's Active Directory.

Because most advanced attacks rely on the exploitation of privileged credentials, providing users the minimum possible levels of access drastically decreases the cyberattack surface.

Promote Accountability for Department Usage

Showback or Chargeback is an effective way to show or bill data usage back to business. The context from Directory services and "real" ownership can pin-point on usage by department to show real usage of data across disparate groups in the organisation.

This can ensure we tie in the usage with real activity data and get the real owners to own the capacity consumption.

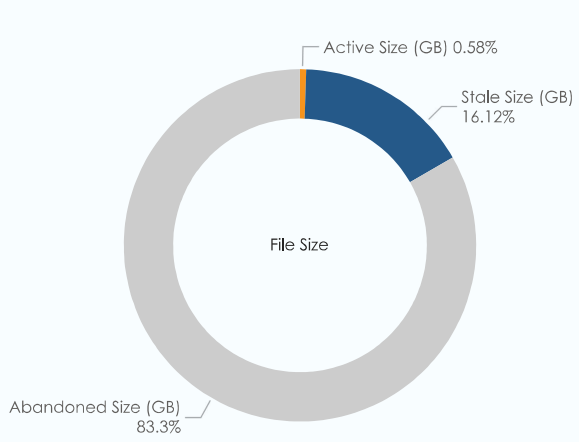
arctera

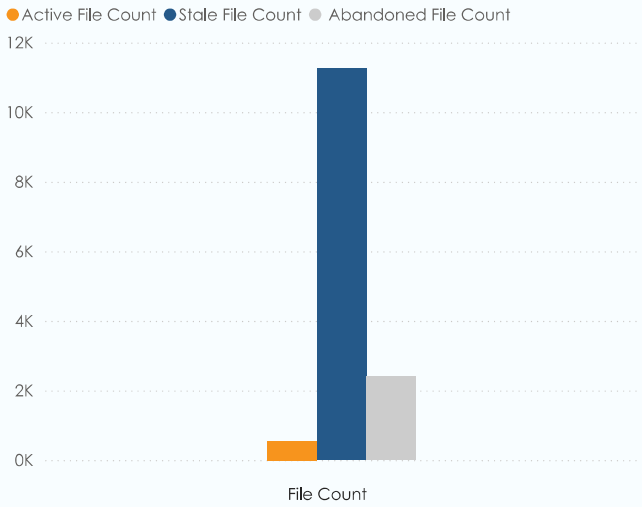
Arctera Dark Data Assessment

All

Data Age

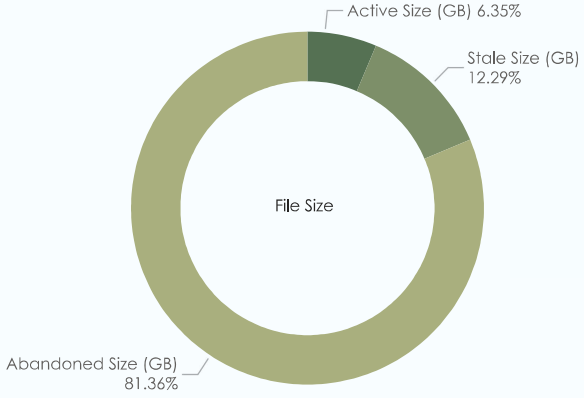
Last Modified | Last Accessed

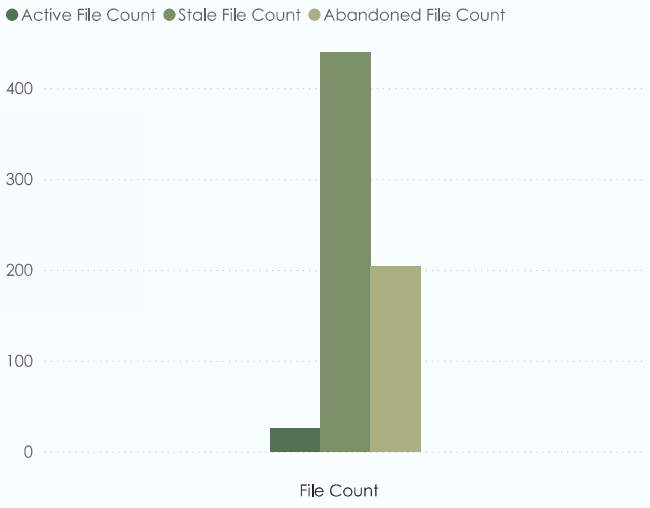




Sensitive Data Age

Last Modified | Last Accessed





Recommendations

Delete Abandoned Files

Files not modified and accessed for long time are simply lying around, are largely having little business value increasing storage costs and increasing risks.

Review such abandoned files and initiate a data deletion process across the environment as per organisation and compliance policies. Make it defensible by involving data custodians and leveraging content analysis.

Delete / Archive Stale Files

Stale files on the other hand may be of importance to organisation and should be reviewed more carefully. Periodically enable workflows to govern such data and choose best resting place based on content and context.

Understand whether it contains sensitive data, records, data required for compliance and archive based on the merit and regulatory requirements. If data is non-business, initiate a data deletion review.

Review Activity on Sensitive Data

Sensitive data on the other hand has to be reviewed very carefully. Who has been touching such data? Are those legitimate people having access? Is the sensitive data stored at the right place? Is the right protection applied to such data?

Can this data be safely moved or deleted? Finding answers to all these questions can ensure adherence to data storage, protection, privacy and security principles.

Arctera Dark Data Assessment

Large Files

All

Private Mode not Enabled

1
File Count

5.33 5.33

All

Clear all slicers

Last Modified Date	File Path	File Size (GB)
Thursday, March 10, 2022	\\fileserver.evlab.local\Misc\VM_SERV1_x64-apps.vmdk	5.33
Total		**5.33**

Recommendations

Review & Delete Large Files

Large files on unstructured repositories, although limited are not uncommon. More often than not, these may be non-business media files or archive files or application install files / images. In some cases, there can be databases or VMware images found on unstructured repositories.

Most of these can be safely deleted after a cursory review and help in not just saving storage costs but costs associated with operations of managing and backing up such big files.

Migrate PST Files

It's not uncommon to find PST and other email files. These can grow to multiple Gigabytes and poses risk to the organisation since emails tend to contain sensitive & business data. If left unchecked, these can get on hands of malicious actors and can cause big losses to organisations.

Consider leveraging archive toolsets to securely store such data as per compliance requirements and make the data discoverable for investigations and eDiscovery purposes.

Migrate or Tier Large Business Files

Systematically migrating to cloud or lower tier storage based on access types can help reduce cost associated with storage and operations.

arctera

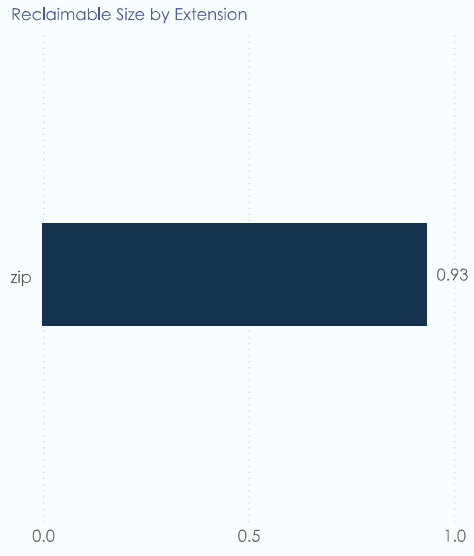
Arctera Dark Data Assessment

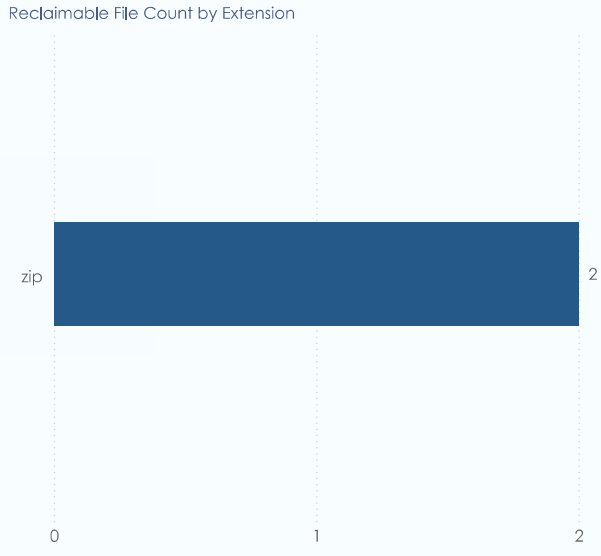
All

Potential Duplicates

There are no matching items

Potential Duplicates by File Types





Recommendations

Review & Delete Duplicates

Duplicate files can take up unnecessary storage and impact storage costs and operations. Review such files and associated permissions to delete duplicates and ensuring the right individuals have access to the remaining files.

This is an easy way to reclaim storage and reduce costs.

Archive Files

Archiving files has many benefits. Apart for retaining documents / records for compliance purpose, it helps move files to lower tier and doing a single-instancing reducing storage.

Consider leveraging Arctera solutions to archive with placeholders to reduce storage, ensure compliance and still providing access to individuals accessing such duplicates.

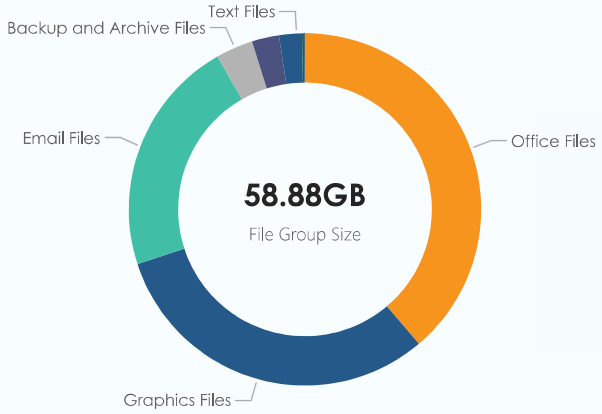
Adopt Collaboration Systems

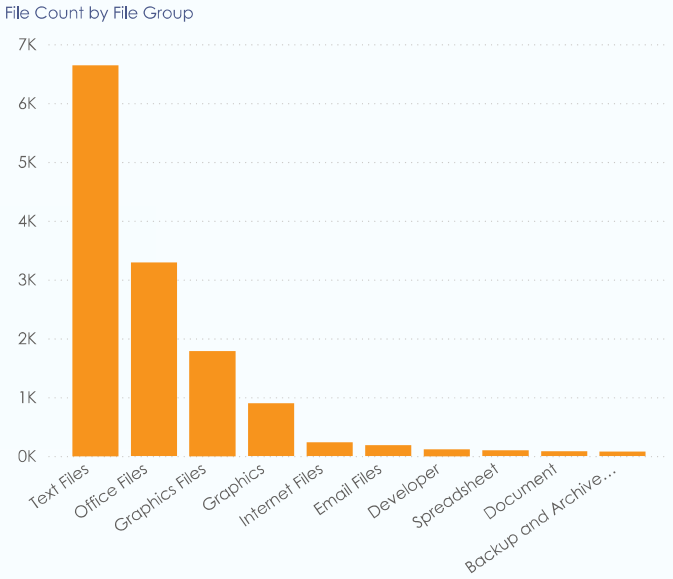
Consider leveraging collaborative solutions for storing and sharing documents. Many such solutions enable versioning and ensure there are not many unnecessary copies created.

Arctera Dark Data Assessment

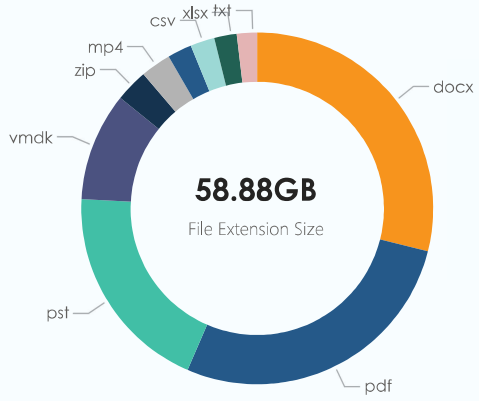
All

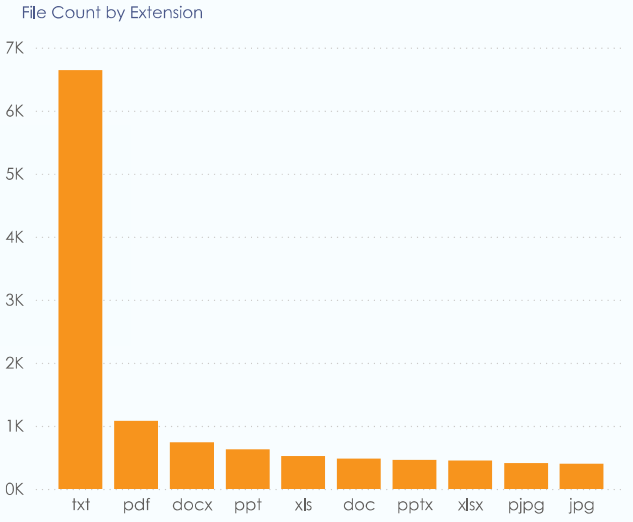
Top 10 - File Groups





Top 10 - Files Extensions





Recommendations

Review Big Sized File Groups / Types

There are certain kind of files that may not have business reasons to be on shared repositories or shares & takes up the most storage.

Review such file types and associated applications / users to remediate.

Large Number of Small Files

It's not uncommon to find a very large number of small sized files. These can often be associated with application logs or temporary files unnecessary taking storage & impacting operations.

Review such files to reduce storage and operations overhead.

Unexpected File Groups / Types

Review file groups / types data for any unexpected or unknown files. There can be file types not associated with a known group or even residue from a past cyber-attack.

Understanding all kind of file types stored on collaborative repositories is important to have a robust data-centric strategy.

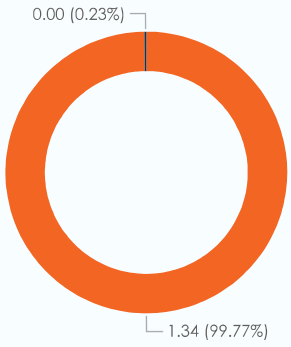
arctera

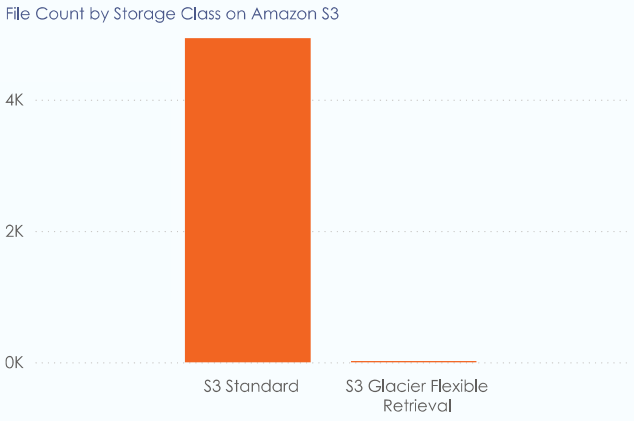
Arctera Dark Data Assessment

All

Amazon S3

1.44GB
on 2 buckets





Bucket Details

Bucket Name	Device	Is Private	Bucket Size (GB)	File Count	Sensitive File Count
smohio	DIQAUser	No	1.31	4,740	217
test-classification-data	DIQAUser	No	0.03	194	15
Total			**1.34**	**4,934**	**232**

Recommendations

Review Big Sized File Groups / Types

There are certain kind of files that may not have business reasons to be on shared repositories or shares & takes up the most storage.

Review such file types and associated applications / users to remediate.

Large Number of Small Files

It's not uncommon to find a very large number of small sized files. These can often be associated with application logs or temporary files unnecessary taking storage & impacting operations.

Review such files to reduce storage and operations overhead.

Unexpected File Groups / Types

Review file groups / types data for any unexpected or unknown files. There can be file types not associated with a known group or even residue from a past cyber-attack.

Understanding all kind of file types stored on collaborative repositories is important to have a robust data-centric strategy.

Arctera Dark Data Assessment

All

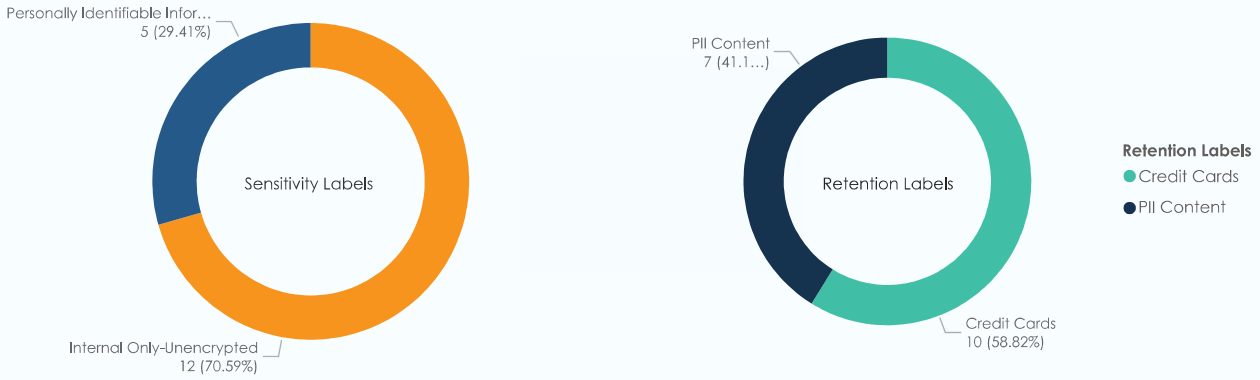
Private Mode not Enabled

Microsoft 365 Labels

45.07GB
on Microsoft 365

Sensitivity Labels:
Labeled File Count Unlabeled File Count

1198 1215



Mislabeled Sensitive Documents

There are no matching items

Recommendations

Review Big Sized File Groups / Types

There are certain kind of files that may not have business reasons to be on shared repositories or shares & takes up the most storage.

Review such file types and associated applications / users to remediate.

Large Number of Small Files

It's not uncommon to find a very large number of small sized files. These can often be associated with application logs or temporary files unnecessary taking storage & impacting operations.

Review such files to reduce storage and operations overhead.

Unexpected File Groups / Types

Review file groups / types data for any unexpected or unknown files. There can be file types not associated with a known group or even residue from a past cyber-attack.

Understanding all kind of file types stored on collaborative repositories is important to have a robust data-centric strategy.

About Arctera

Arctera helps organizations around the world thrive by ensuring they can trust, access, and illuminate their data from creation to retirement. Created in 2024 from Veritas Technologies, an industry leader in secure multi-cloud data resiliency, Arctera comprises three business units: Data Compliance, Data Protection, and Data Resilience. Arctera provides more than 75,000 customers worldwide with market-leading solutions that help them to manage their most valuable assets: data.

Learn more at **www.arctera.io.** Follow us on X **@arcteraio**

arctera.io

For global contact information visit:
arctera.io/contact

A0152 10/24