GETVISIBILITY

Data Risk Assessment
Multi Layer Reporting

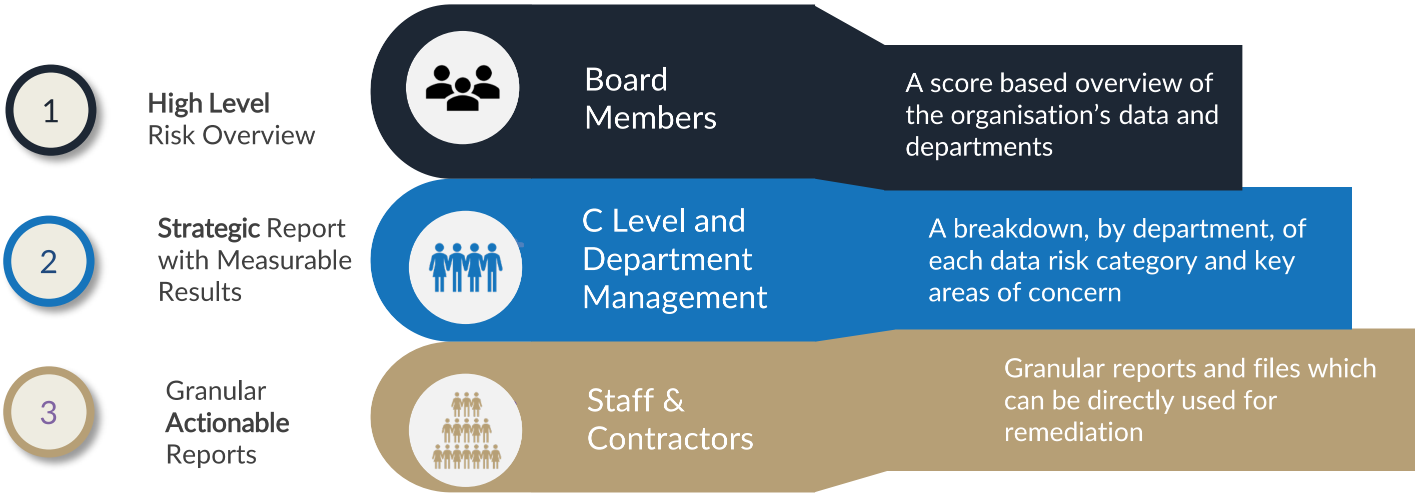
A unified view of your data landscape;

Knowing your organisation’s data, understanding your organisation’s risk, and measuring how risk changes over time is the foundation to any effective security strategy

getvisibility.com

Multi-Layer Reporting

The Getvisibility risk score enables key decision makers to quickly make informed budgeting, operational, tactical, and strategic decisions. It also allows key decision makers to measure the effectiveness of their teams and budgetary decisions, providing a framework for continuous learning and improvement.



1 **High Level** Risk Overview — Board Members — A score based overview of the organisation's data and departments

2 **Strategic** Report with Measurable Results — C Level and Department Management — A breakdown, by department, of each data risk category and key areas of concern

3 Granular **Actionable** Reports — Staff & Contractors — Granular reports and files which can be directly used for remediation

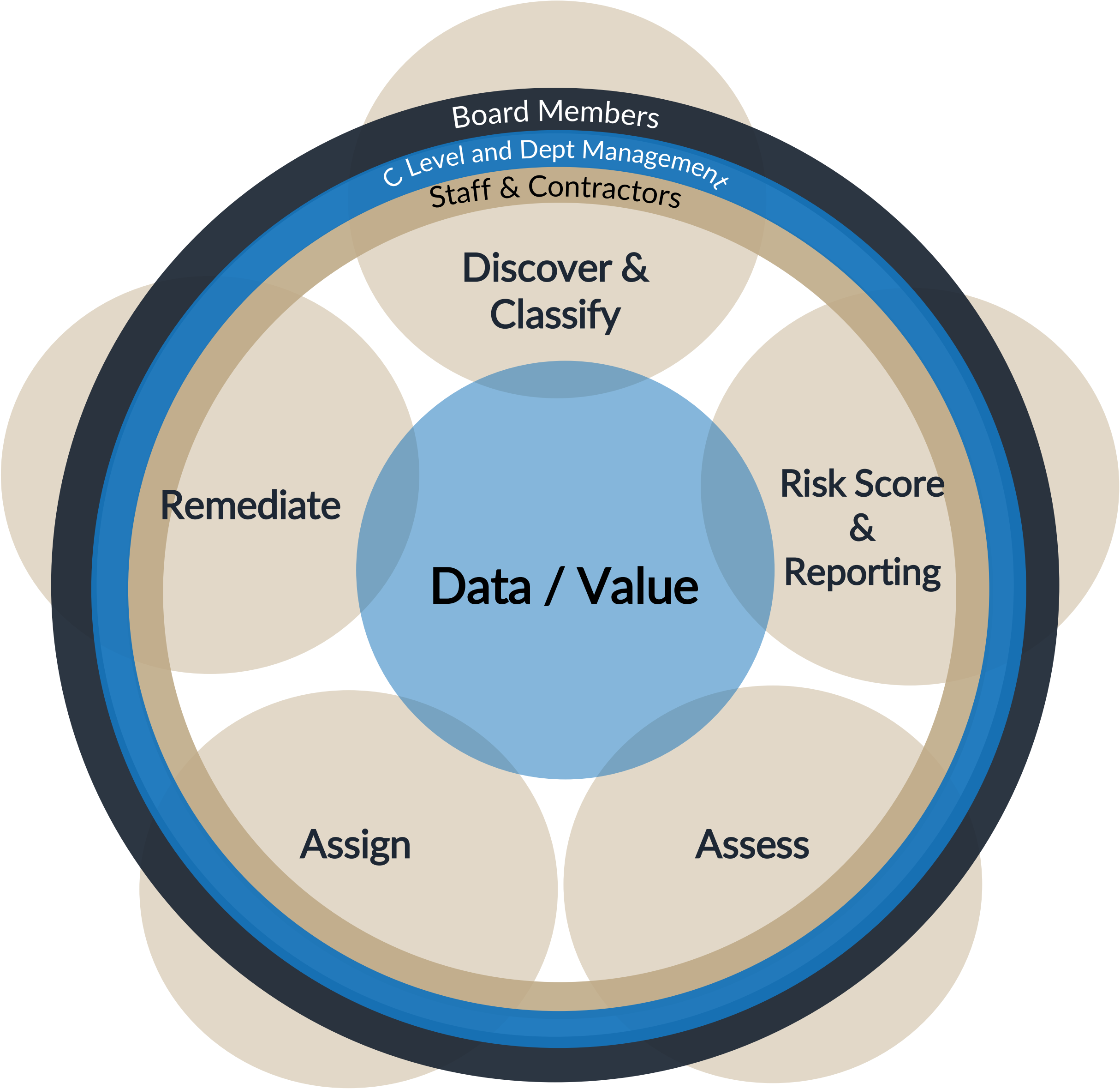
The risk score is a powerful tool for risk and security practitioners. CISOs, DPOs, and security experts now have a bench-marked mechanism for demonstrating good practice, as well as the consequences of under investment.

The Getvisibility remediation tools provide the solutions for managing and improving the data risk scores.

Data Protection and Score Review

A Key Business Process

Recurring Data Risk Assessment Reporting allows organisations to measure the compliance and effectiveness of implemented changes and remediation while monitoring their maintenance; driving further initiatives and policies.



BOARD LEVEL REPORTING

Cyber Security and data compliance have become a very important board responsibility. The impact of a cyber security breach or a data leak on an organisation has grown at a rapid rate, the likelihood of a breach has also increased. New business processes, remote working and new collaboration tools have all led to an exponentially growing volume of data and an increased attack surface.

Regulation

Appease regulators in the event of a breach as progress and continuous improvement can be demonstrated

Resourcing

Assign resources and allocate budget effectively

Prioritisation

Prioritise key high risk areas for remediation

Organisations' leadership teams and directors don’t have the time or expertise to fully assess the ever changing environment, assess the effectiveness of their companies cyber security or predict the direction of change. This makes budgeting, resource allocation and strategic decision making very difficult.

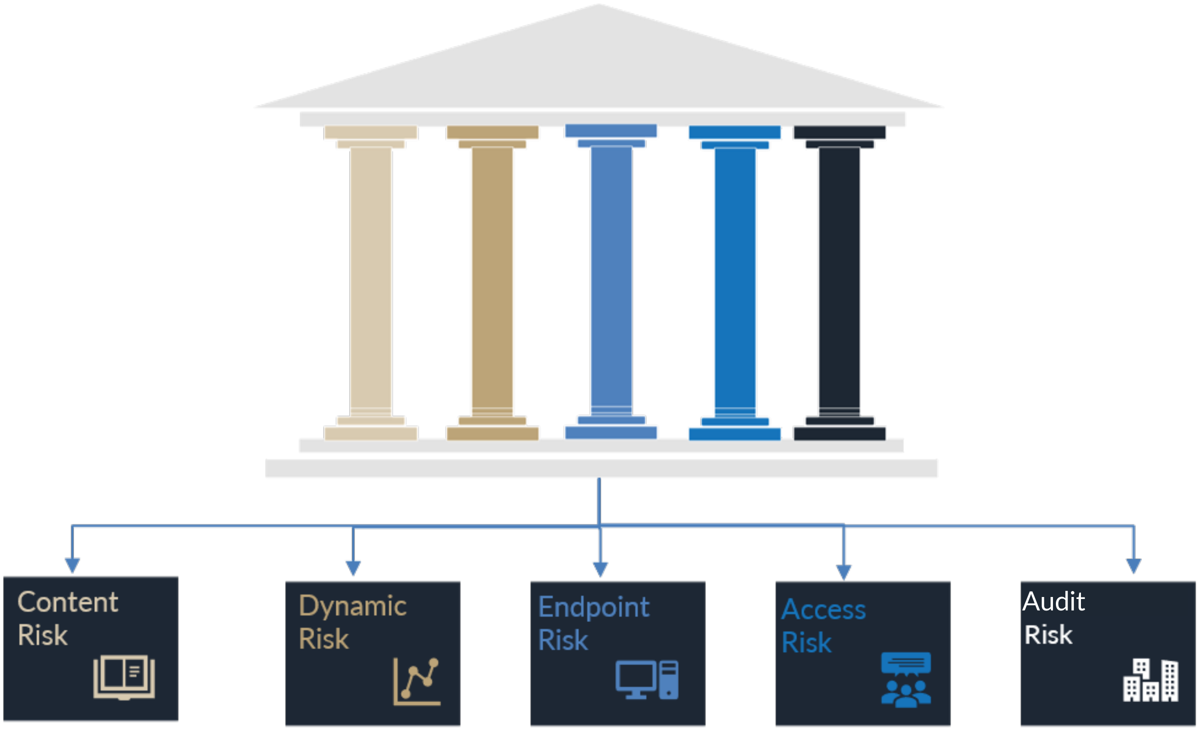
The organisation's leadership teams will get a report on a frequent basis that risk scores the key security areas. This report highlights the immediate risks, the areas of concern and how this is changing over time.

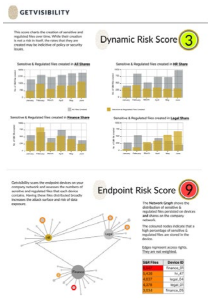
The report allows the leadership team to assign a budget in accordance with its risk tolerance, measure the impact of this budget allocation, and the effectiveness of their cybersecurity and data governance teams. The report allows for a common understanding and for strategically measurable targets for the ICT and security teams.

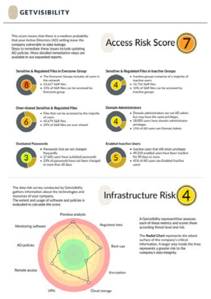
KEY PILLARS OF RISK SCORE

The Five Key Pillars of Data Risk Score

The following sections form part of the Data Risk Report and are key to assessing an organisation's data risk.



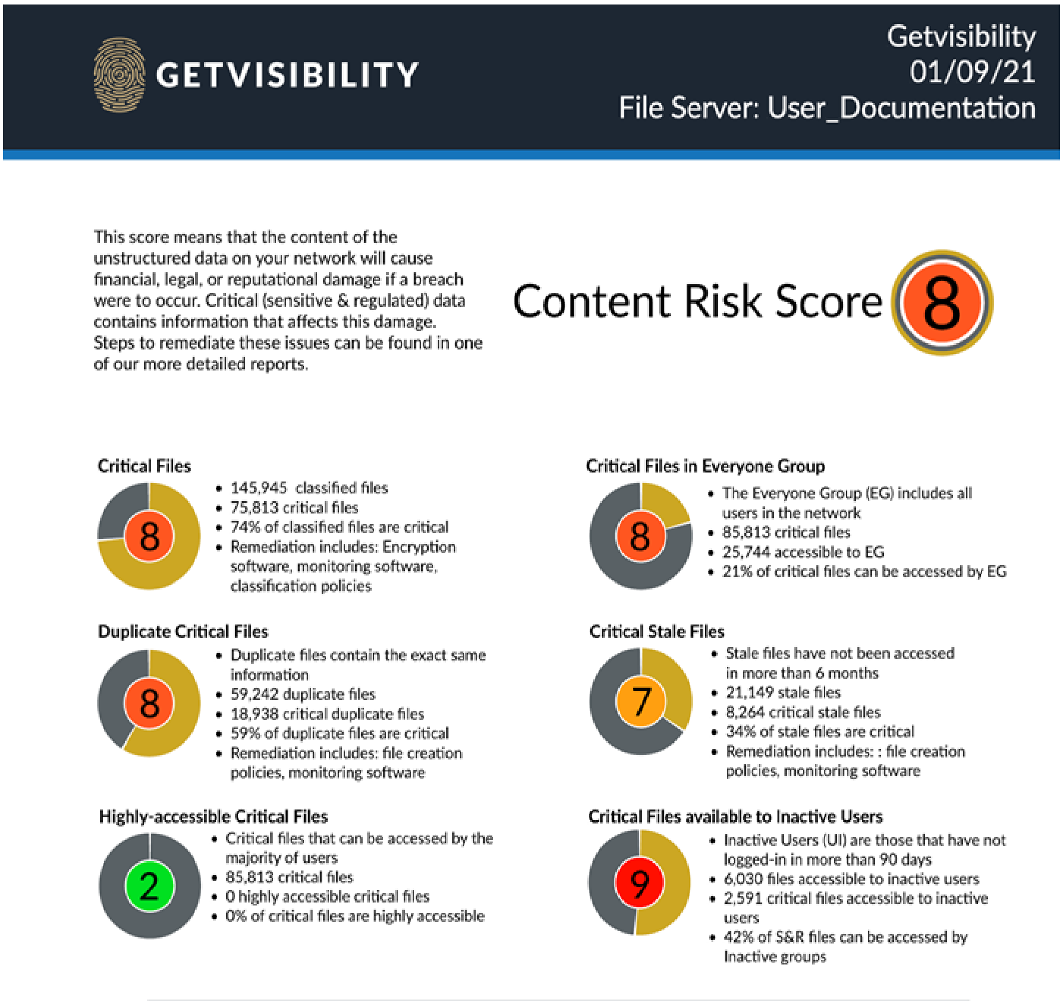




The Content Risk Score

The Content Risk Score measures the severity of risk due to: the content of the unstructured data scanned, its level of sensitivity, as a percentage of total data, and its location.

While having a high percentage of critical data in a company's system is not insecure in and of itself, it does increase the exposure potential and therefore the content risk score. This score does not take breach likelihood into account that is accounted for in the Access, Audit, and Endpoint risk scores



GETVISIBILITY

Getvisibility
01/09/21
File Server: User_Documentation

This score means that the content of the unstructured data on your network will cause financial, legal, or reputational damage if a breach were to occur. Critical (sensitive & regulated) data contains information that affects this damage. Steps to remediate these issues can be found in one of our more detailed reports.

Content Risk Score 8

Critical Files 8

- 145,945 classified files
- 75,813 critical files
- 74% of classified files are critical
- Remediation includes: Encryption software, monitoring software, classification policies

Critical Files in Everyone Group 8

- The Everyone Group (EG) includes all users in the network
- 85,813 critical files
- 25,744 accessible to EG
- 21% of critical files can be accessed by EG

Duplicate Critical Files 8

- Duplicate files contain the exact same information
- 59,242 duplicate files
- 18,938 critical duplicate files
- 59% of duplicate files are critical
- Remediation includes: file creation policies, monitoring software

Critical Stale Files 7

- Stale files have not been accessed in more than 6 months
- 21,149 stale files
- 8,264 critical stale files
- 34% of stale files are critical
- Remediation includes: : file creation policies, monitoring software

Highly-accessible Critical Files 2

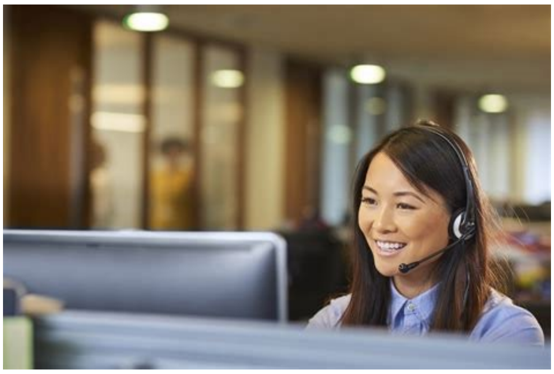
- Critical files that can be accessed by the majority of users
- 85,813 critical files
- 0 highly accessible critical files
- 0% of critical files are highly accessible

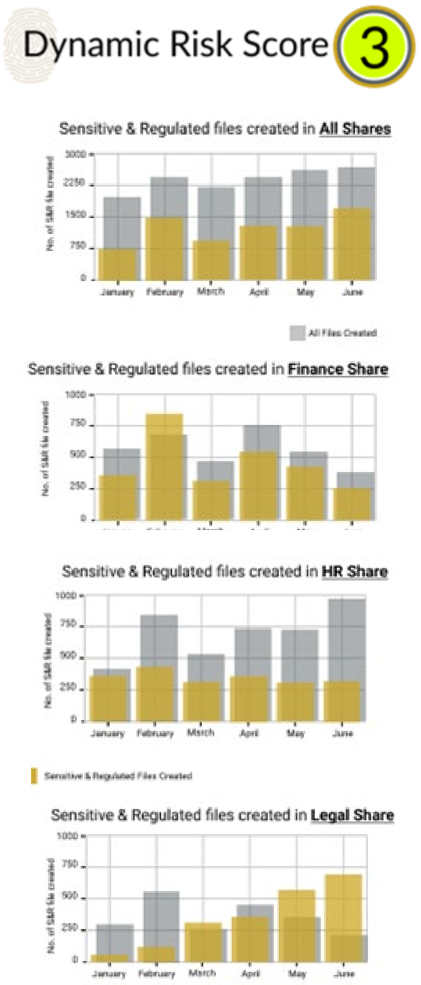
Critical Files available to Inactive Users 9

- Inactive Users (UI) are those that have not logged-in in more than 90 days
- 6,030 files accessible to inactive users
- 2,591 critical files accessible to inactive users
- 42% of S&R files can be accessed by Inactive groups

The Dynamic Risk Score

The Dynamic Risk Score monitors the creation of critical data over time. The score is an evaluation of the rate of critical data creation and indicates to the customer whether this rate has increased dramatically over a time period.





A percentage mean increase in critical document creation over this period could indicate policy change, company structural change, unintended consequences of content creation changes, or foul play. Assessing trends in critical data creation informs the risk score as to what is usual for the organisation and what is unusual.

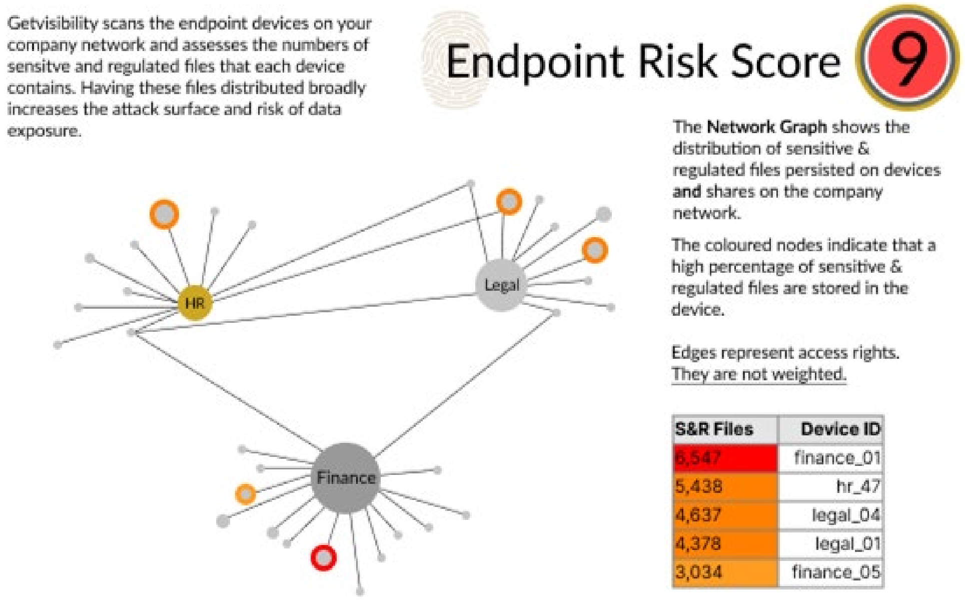
Dramatic increases in the number of critical files being created, especially if these files are not created in a secure way, provide a warning to customers about their policies. It may be the case that employees need more training in this area.

The Dynamic Risk Score is important as it indicates current trends in critical data in the company. Rather than static metrics, this metric can alert companies to unusual occurrences.

Endpoint Risk Score

Getvisibility scans the laptops, desktops, and other devices on the network, the amount of critical files in each, as well as information about each device's access to files. The addition of Getvisibility Synergy classification profiles enriches this key pillar and gives even more insight into the data at risk in each device.

Each laptop or other electronic device on a network may unknowingly contain critical information. These files can go unnoticed and potentially indicate foul play on the part of the device user. High numbers of critical files on individual devices, especially those that should not have access to them e.g. Code IP on a device with exclusively HR related access rights. When Getvisibility Synergy Pro is added, a higher risk will be given to devices that have high mis-classification ratings.



Getvisibility scans the endpoint devices on your company network and assesses the numbers of sensitve and regulated files that each device contains. Having these files distributed broadly increases the attack surface and risk of data exposure.

Endpoint Risk Score 9

The **Network Graph** shows the distribution of sensitive & regulated files persisted on devices **and** shares on the company network.

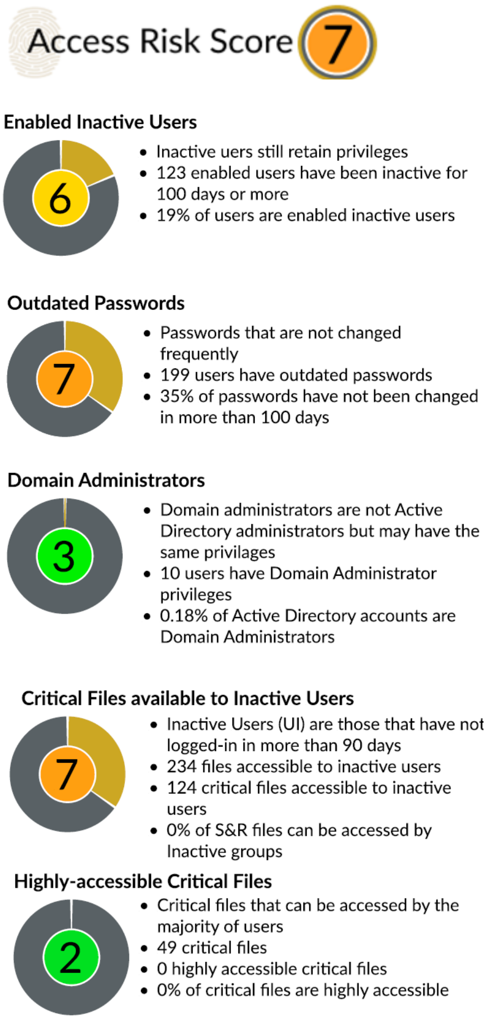
The coloured nodes indicate that a high percentage of sensitive & regulated files are stored in the device.

Edges represent access rights. They are not weighted.

S&R Files	Device ID
6,547	finance_01
5,438	hr_47
4,637	legal_04
4,378	legal_01
3,034	finance_05

The Access Risk Score

This score assess an organisations user permission policies. Identifying gaps or erroneous granting of access rights. It also scans for security risks such as: outdated passwords, erroneous domain administrators, and inactive yet enabled user accounts.



Access Risk Score 7

Enabled Inactive Users

6

- Inactive uers still retain privileges
- 123 enabled users have been inactive for 100 days or more
- 19% of users are enabled inactive users

Outdated Passwords

7

- Passwords that are not changed frequently
- 199 users have outdated passwords
- 35% of passwords have not been changed in more than 100 days

Domain Administrators

3

- Domain administrators are not Active Directory administrators but may have the same privileges
- 10 users have Domain Administrator privileges
- 0.18% of Active Directory accounts are Domain Administrators

Critical Files available to Inactive Users

7

- Inactive Users (UI) are those that have not logged-in in more than 90 days
- 234 files accessible to inactive users
- 124 critical files accessible to inactive users
- 0% of S&R files can be accessed by Inactive groups

Highly-accessible Critical Files

2

- Critical files that can be accessed by the majority of users
- 49 critical files
- 0 highly accessible critical files
- 0% of critical files are highly accessible

Data points assessed include:

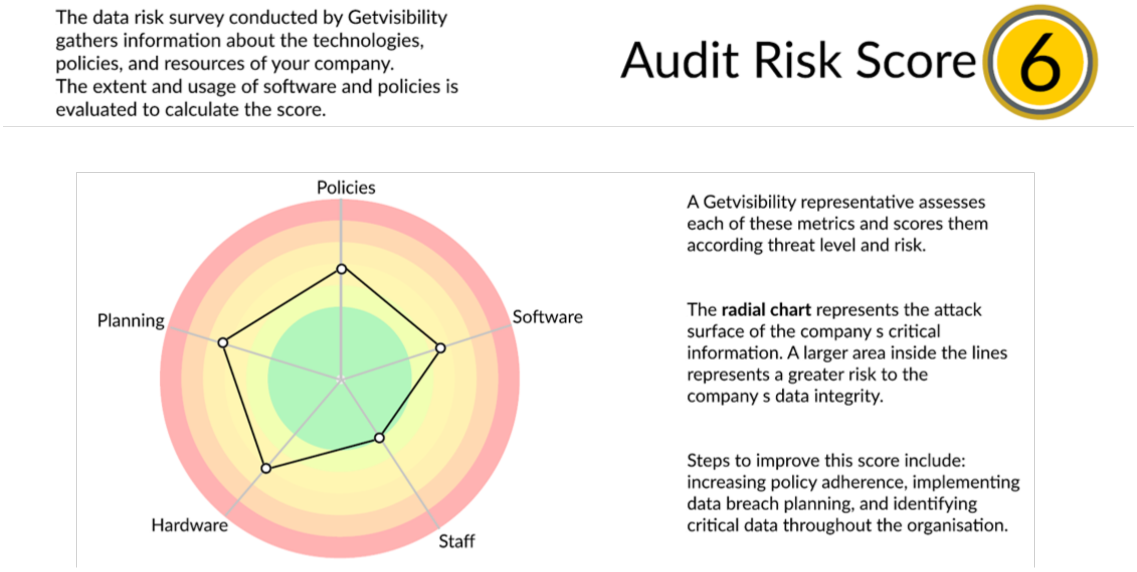
- ✓ Critical files available to all users
- ✓ Critical files available to inactive user groups
- ✓ Oer-shared critical files
- ✓ Percentage of domain administrators
- ✓ Outdated passwords
- ✓ Enabled Inactive Users

A scan of user permissions will analyse the access, password controls, and unintended permission inheritance. Analysing unintended or maliciously intended unauthorised access is vital to assess the risk potential to critical data.

Audit Risk Score

This is based on information gathered from direct engagement with the customer, collated into a survey, to assess their procedures, processes and software systems in relation to a potential data breach. Key areas include:

- ✓ Antivirus software
- ✓ Back-ups
- ✓ Back – up procedures
- ✓ Certifications
- ✓ Internal policies
- ✓ External policies
- ✓ Monitoring Software
- ✓ Security Staff and Training
- ✓ Classification Software



The data risk survey conducted by Getvisibility gathers information about the technologies, policies, and resources of your company.
The extent and usage of software and policies is evaluated to calculate the score.

Audit Risk Score 6

A Getvisibility representative assesses each of these metrics and scores them according threat level and risk.

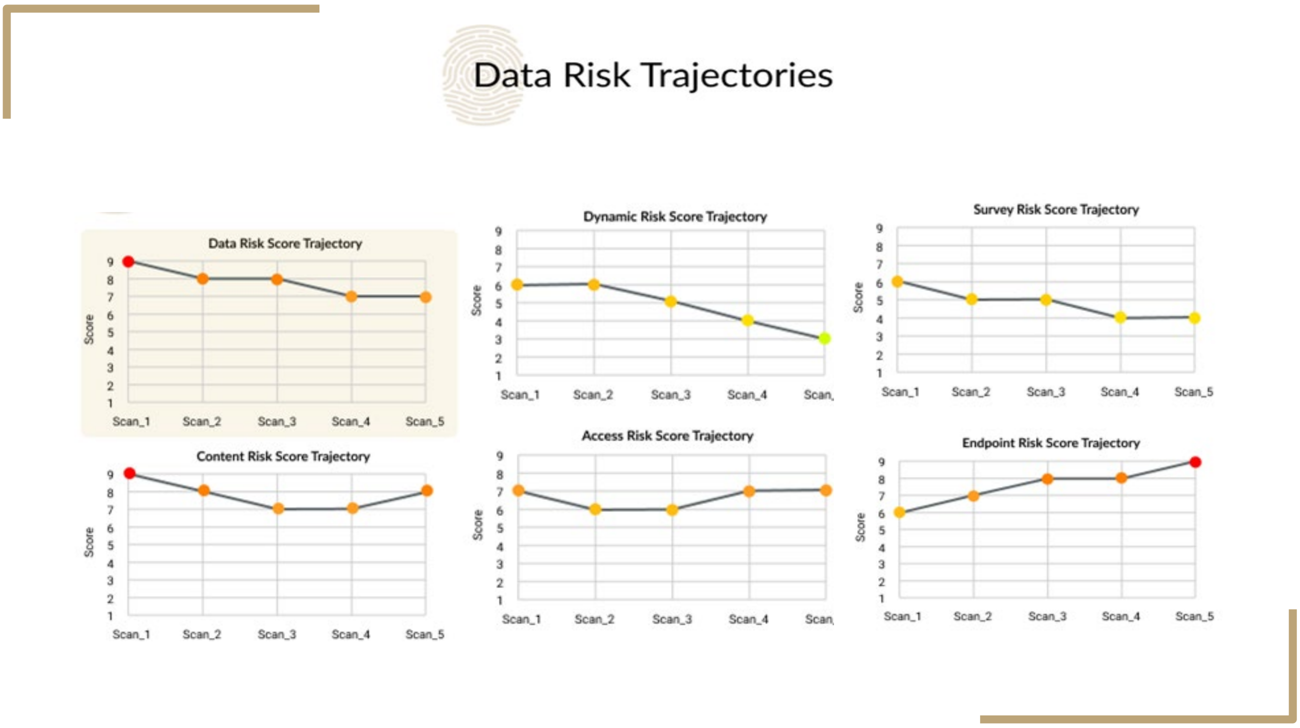
The **radial chart** represents the attack surface of the company s critical information. A larger area inside the lines represents a greater risk to the company s data integrity.

Steps to improve this score include: increasing policy adherence, implementing data breach planning, and identifying critical data throughout the organisation.

Data Risk Trajectories

This set of charts track the change in the company's data risk status over a course of Getvisibility various scans.

As policies, procedures, and software tools are put in place to address these risk scores there should be a reduction in risk over the course of a companies engagement with Getvisibility. Increases in risk could indicate changes in personnel, file-share migrations, unimplemented policies, increases in hardware devices, or foul play.
To investigate these scores in-depth, use one of Getvisibility's detailed report spreadsheets.



C Level and Department Management Strategic Reporting

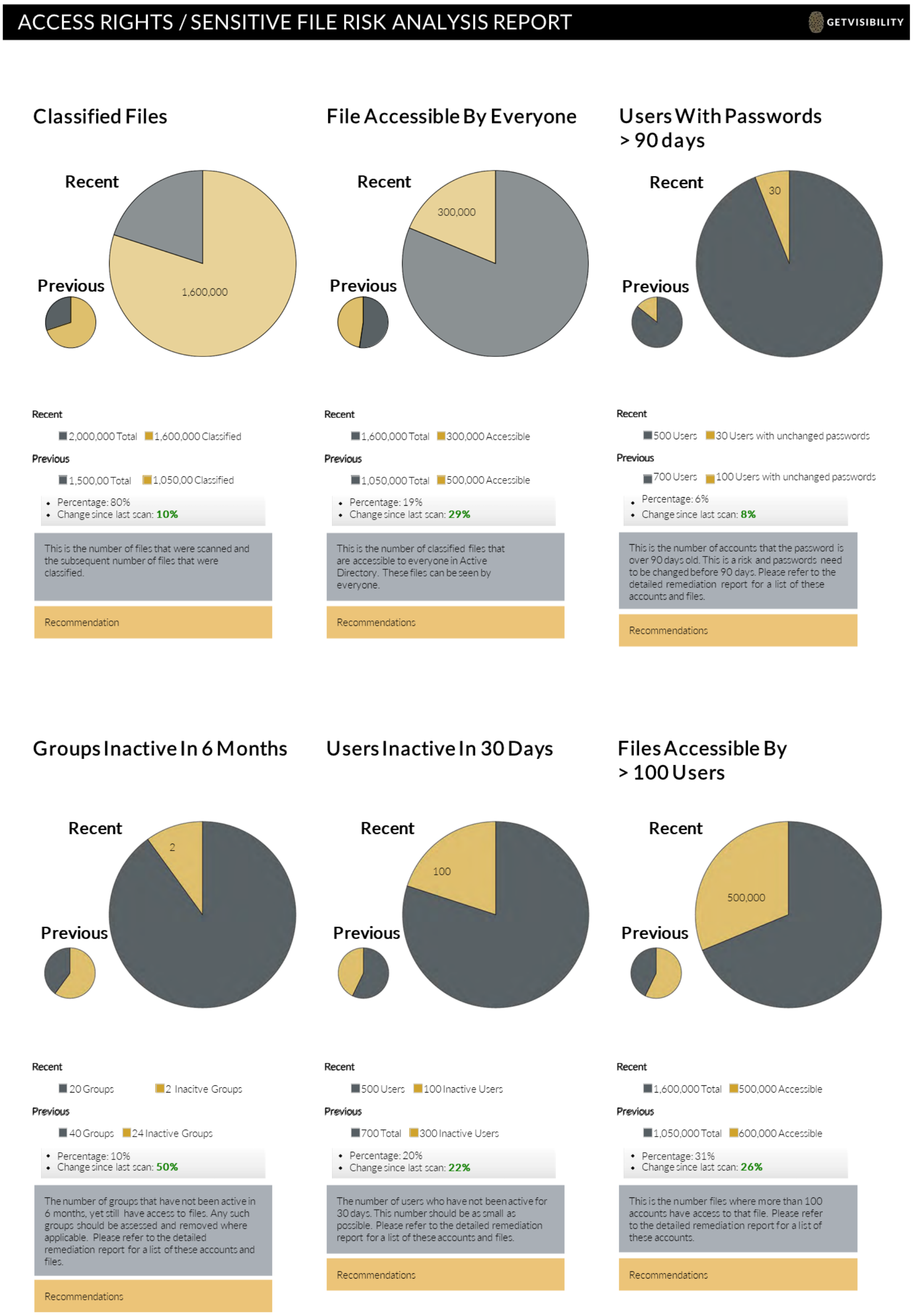
Building a cyber security strategy is becoming increasingly difficult for those tasked with data protection and compliance. Data protection regulations are becoming more stringent and new regulations are being introduced regularly across all sectors and geographies, putting pressure on organisations to comply.

Covid- 19 has amplified this issue, as new collaboration tools and an explosion in unstructured data has dramatically increased the attack surface. In parallel to this, breaches are becoming noticeably more severe as hackers are posing a larger threat to organisations through new triple extortion ransomware.

Designing an effective and compliant data protection strategy can be challenging as the nature of work is ever changing. Organisations are growing and expanding, regulations are changing and the security technology is advancing. The Getvisibility platform gives CISO/Head of Security/Data Compliance Officer a common key set of well defined metrics to everyone in the organisation. This helps them:

- Expedite budget approval
- Identify and measure risk
- Identify poorly performing departments or locations
- Identify and prioritise high risk
- Demonstrate progress and positive actions to stakeholders
- Set a detailed roadmap for the IT and Security Practice
- Build cross organisational risk awareness
- Measure and identify new risk.

Sample Strategic Access Report



ACCESS RIGHTS / SENSITIVE FILE RISK ANALYSIS REPORT

Classified Files

Recent

■ 2,000,000 Total ■ 1,600,000 Classified

Previous

■ 1,500,00 Total ■ 1,050,00 Classified

- Percentage: 80%
- Change since last scan: **10%**

This is the number of files that were scanned and the subsequent number of files that were classified.

Recommendation

File Accessible By Everyone

Recent

■ 1,600,000 Total ■ 300,000 Accessible

Previous

■ 1,050,000 Total ■ 500,000 Accessible

- Percentage: 19%
- Change since last scan: **29%**

This is the number of classified files that are accessible to everyone in Active Directory. These files can be seen by everyone.

Recommendations

Users With Passwords > 90 days

Recent

■ 500 Users ■ 30 Users with unchanged passwords

Previous

■ 700 Users ■ 100 Users with unchanged passwords

- Percentage: 6%
- Change since last scan: **8%**

This is the number of accounts that the password is over 90 days old. This is a risk and passwords need to be changed before 90 days. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Groups Inactive In 6 Months

Recent

■ 20 Groups ■ 2 Inacitve Groups

Previous

■ 40 Groups ■ 24 Inactive Groups

- Percentage: 10%
- Change since last scan: **50%**

The number of groups that have not been active in 6 months, yet still have access to files. Any such groups should be assessed and removed where applicable. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Users Inactive In 30 Days

Recent

■ 500 Users ■ 100 Inactive Users

Previous

■ 700 Total ■ 300 Inactive Users

- Percentage: 20%
- Change since last scan: **22%**

The number of users who have not been active for 30 days. This number should be as small as possible. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Files Accessible By > 100 Users

Recent

■ 1,600,000 Total ■ 500,000 Accessible

Previous

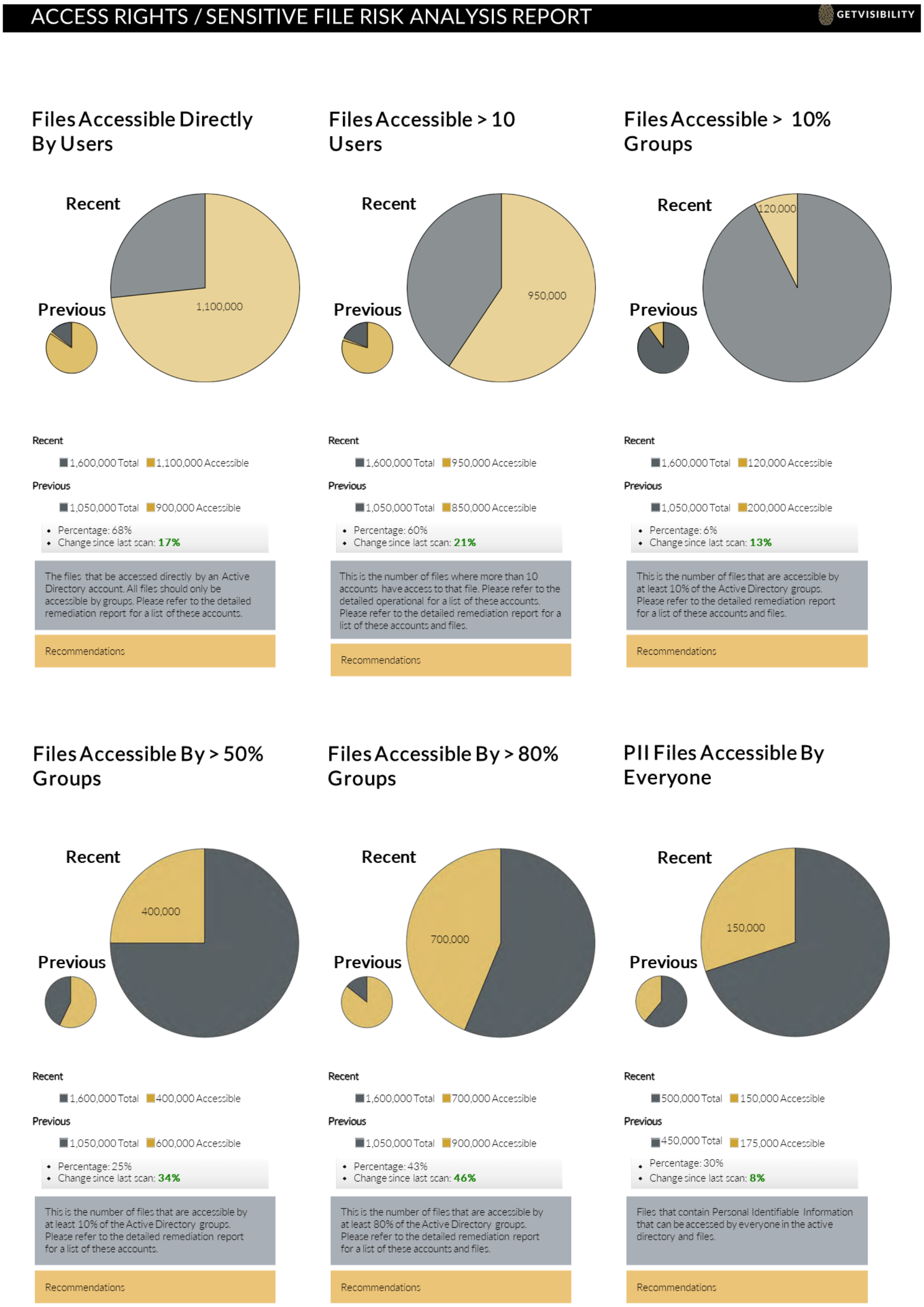
■ 1,050,000 Total ■ 600,000 Accessible

- Percentage: 31%
- Change since last scan: **26%**

This is the number files where more than 100 accounts have access to that file. Please refer to the detailed remediation report for a list of these accounts.

Recommendations

Sample Strategic Access Report



ACCESS RIGHTS / SENSITIVE FILE RISK ANALYSIS REPORT

GETVISIBILITY

Files Accessible Directly By Users

Recent

■ 1,600,000 Total ■ 1,100,000 Accessible

Previous

■ 1,050,000 Total ■ 900,000 Accessible

- Percentage: 68%
- Change since last scan: **17%**

The files that be accessed directly by an Active Directory account. All files should only be accessible by groups. Please refer to the detailed remediation report for a list of these accounts.

Recommendations

Files Accessible > 10 Users

Recent

■ 1,600,000 Total ■ 950,000 Accessible

Previous

■ 1,050,000 Total ■ 850,000 Accessible

- Percentage: 60%
- Change since last scan: **21%**

This is the number of files where more than 10 accounts have access to that file. Please refer to the detailed operational for a list of these accounts. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Files Accessible > 10% Groups

Recent

■ 1,600,000 Total ■ 120,000 Accessible

Previous

■ 1,050,000 Total ■ 200,000 Accessible

- Percentage: 6%
- Change since last scan: **13%**

This is the number of files that are accessible by at least 10% of the Active Directory groups. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Files Accessible By > 50% Groups

Recent

■ 1,600,000 Total ■ 400,000 Accessible

Previous

■ 1,050,000 Total ■ 600,000 Accessible

- Percentage: 25%
- Change since last scan: **34%**

This is the number of files that are accessible by at least 10% of the Active Directory groups. Please refer to the detailed remediation report for a list of these accounts.

Recommendations

Files Accessible By > 80% Groups

Recent

■ 1,600,000 Total ■ 700,000 Accessible

Previous

■ 1,050,000 Total ■ 900,000 Accessible

- Percentage: 43%
- Change since last scan: **46%**

This is the number of files that are accessible by at least 80% of the Active Directory groups. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

PII Files Accessible By Everyone

Recent

■ 500,000 Total ■ 150,000 Accessible

Previous

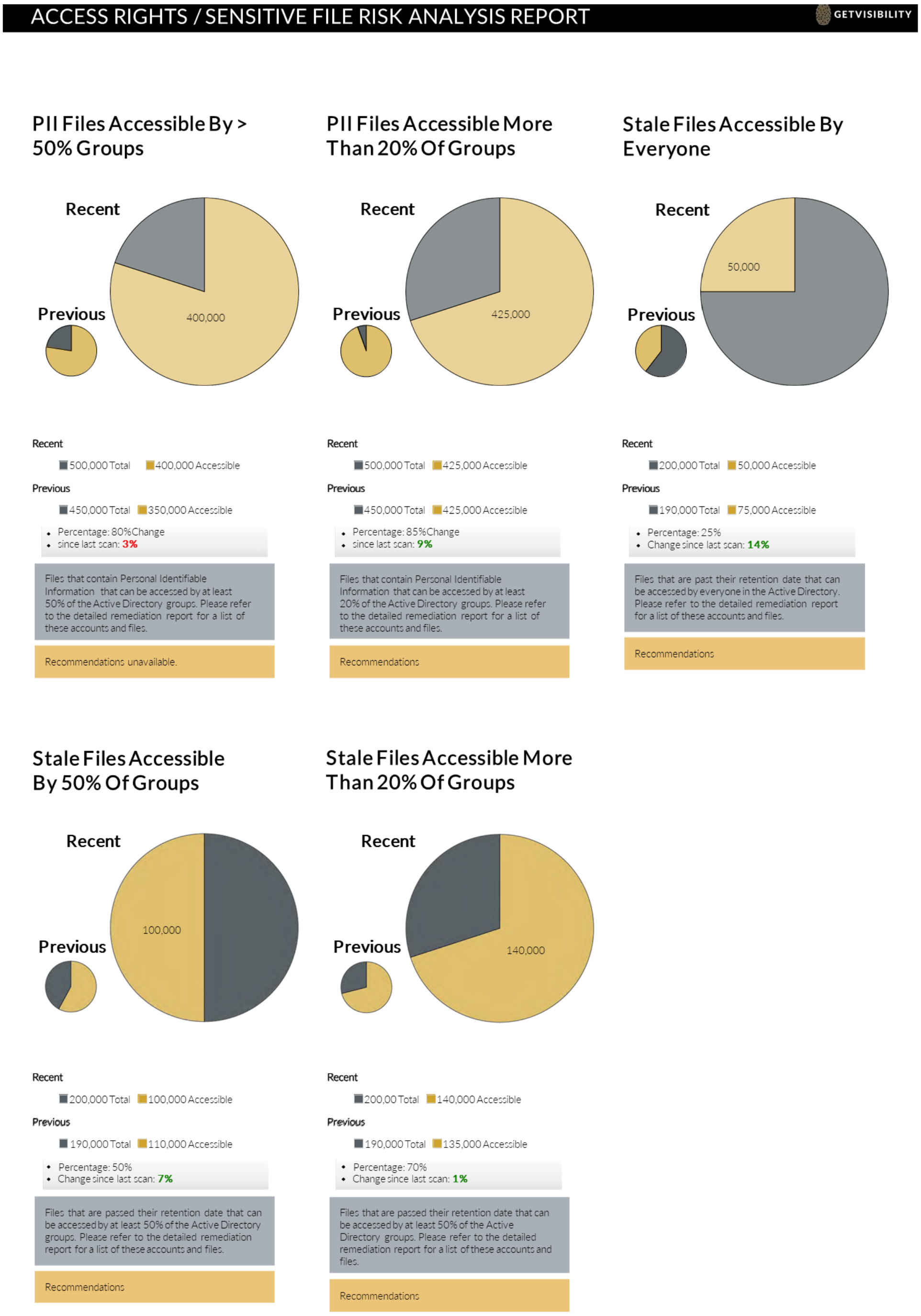
■ 450,000 Total ■ 175,000 Accessible

- Percentage: 30%
- Change since last scan: **8%**

Files that contain Personal Identifiable Information that can be accessed by everyone in the active directory and files.

Recommendations

Sample Strategic Access Report



ACCESS RIGHTS / SENSITIVE FILE RISK ANALYSIS REPORT

PII Files Accessible By > 50% Groups

Recent

■ 500,000 Total ■ 400,000 Accessible

Previous

■ 450,000 Total ■ 350,000 Accessible

- Percentage: 80%Change
- since last scan: **3%**

Files that contain Personal Identifiable Information that can be accessed by at least 50% of the Active Directory groups. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations unavailable.

PII Files Accessible More Than 20% Of Groups

Recent

■ 500,000 Total ■ 425,000 Accessible

Previous

■ 450,000 Total ■ 425,000 Accessible

- Percentage: 85%Change
- since last scan: **9%**

Files that contain Personal Identifiable Information that can be accessed by at least 20% of the Active Directory groups. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Stale Files Accessible By Everyone

Recent

■ 200,000 Total ■ 50,000 Accessible

Previous

■ 190,000 Total ■ 75,000 Accessible

- Percentage: 25%
- Change since last scan: **14%**

Files that are past their retention date that can be accessed by everyone in the Active Directory. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Stale Files Accessible By 50% Of Groups

Recent

■ 200,000 Total ■ 100,000 Accessible

Previous

■ 190,000 Total ■ 110,000 Accessible

- Percentage: 50%
- Change since last scan: **7%**

Files that are passed their retention date that can be accessed by at least 50% of the Active Directory groups. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Stale Files Accessible More Than 20% Of Groups

Recent

■ 200,00 Total ■ 140,000 Accessible

Previous

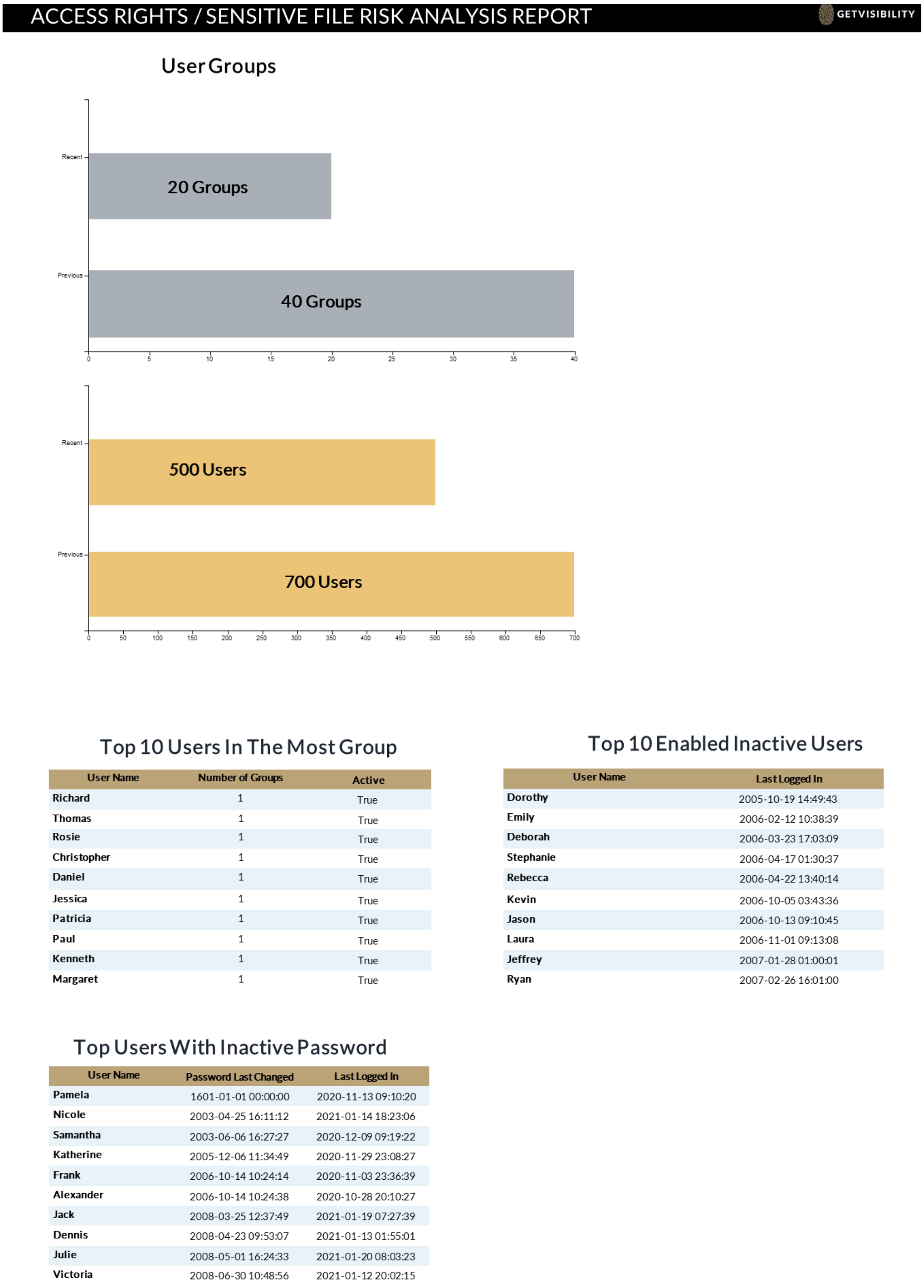
■ 190,000 Total ■ 135,000 Accessible

- Percentage: 70%
- Change since last scan: **1%**

Files that are passed their retention date that can be accessed by at least 50% of the Active Directory groups. Please refer to the detailed remediation report for a list of these accounts and files.

Recommendations

Sample Strategic Access Report



ACCESS RIGHTS / SENSITIVE FILE RISK ANALYSIS REPORT

User Groups

Top 10 Users In The Most Group

User Name	Number of Groups	Active
Richard	1	True
Thomas	1	True
Rosie	1	True
Christopher	1	True
Daniel	1	True
Jessica	1	True
Patricia	1	True
Paul	1	True
Kenneth	1	True
Margaret	1	True

Top 10 Enabled Inactive Users

User Name	Last Logged In
Dorothy	2005-10-19 14:49:43
Emily	2006-02-12 10:38:39
Deborah	2006-03-23 17:03:09
Stephanie	2006-04-17 01:30:37
Rebecca	2006-04-22 13:40:14
Kevin	2006-10-05 03:43:36
Jason	2006-10-13 09:10:45
Laura	2006-11-01 09:13:08
Jeffrey	2007-01-28 01:00:01
Ryan	2007-02-26 16:01:00

Top Users With Inactive Password

User Name	Password Last Changed	Last Logged In
Pamela	1601-01-01 00:00:00	2020-11-13 09:10:20
Nicole	2003-04-25 16:11:12	2021-01-14 18:23:06
Samantha	2003-06-06 16:27:27	2020-12-09 09:19:22
Katherine	2005-12-06 11:34:49	2020-11-29 23:08:27
Frank	2006-10-14 10:24:14	2020-11-03 23:36:39
Alexander	2006-10-14 10:24:38	2020-10-28 20:10:27
Jack	2008-03-25 12:37:49	2021-01-19 07:27:39
Dennis	2008-04-23 09:53:07	2021-01-13 01:55:01
Julie	2008-05-01 16:24:33	2021-01-20 08:03:23
Victoria	2008-06-30 10:48:56	2021-01-12 20:02:15

Tactical Reporting for Investigation and Remediation

Investigation and remediation projects often get put on hold, or struggle to receive resources and budget as they commonly require lots of manual work and interfere with daily business operations. Detailed reporting provided by Getvisibility can enable organisations to greatly reduce the drain on resources and costs involved. End users have access to detailed, actionable reports which enable efficient decision making and project rollouts. Getvisibility also integrates with a variety of remediations tools such as data loss prevention solutions, archiving, data encryption and secure deletion.

Once remediation efforts have been carried out, repeated Data Risk assessments can measure their effectiveness and drive further strategy. The following are some common remediation actions enabled by Getvisibility:

De-Duplication and ROT Data

Data Loss Prevention

Secure Deletion

Active Directory Clean Up

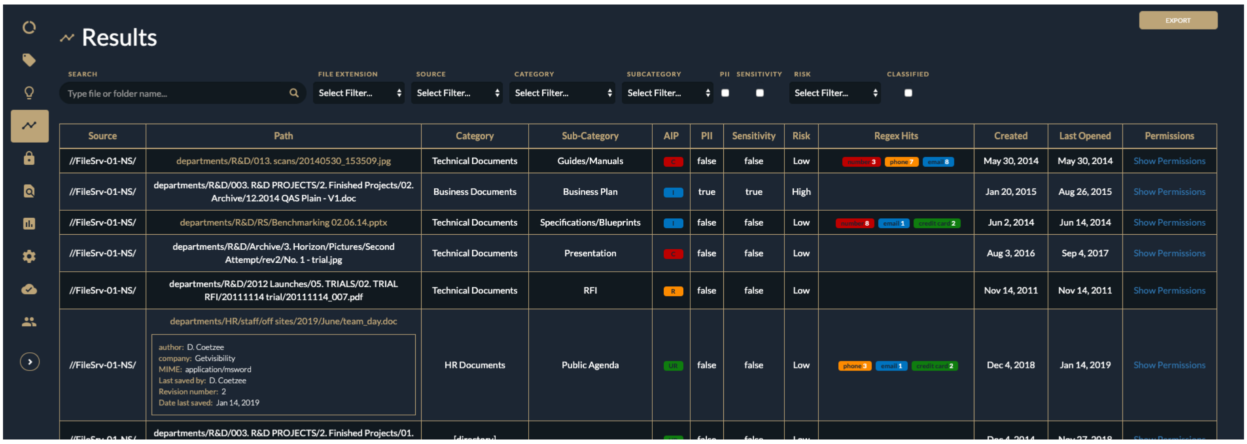
Secure Archiving

Data Encryption

Data Migration

Process and Policy Review

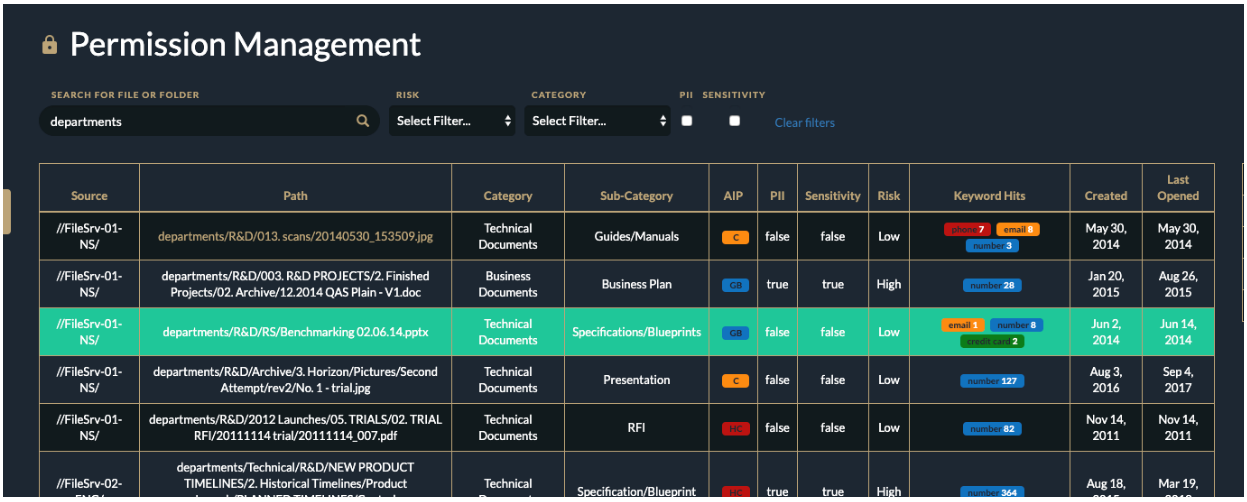
Sample Tactical Reports



Results

SEARCH: Type file or folder name... | FILE EXTENSION: Select Filter... | SOURCE: Select Filter... | CATEGORY: Select Filter... | SUBCATEGORY: Select Filter... | PII ☐ | SENSITIVITY ☐ | RISK: Select Filter... | CLASSIFIED ☐

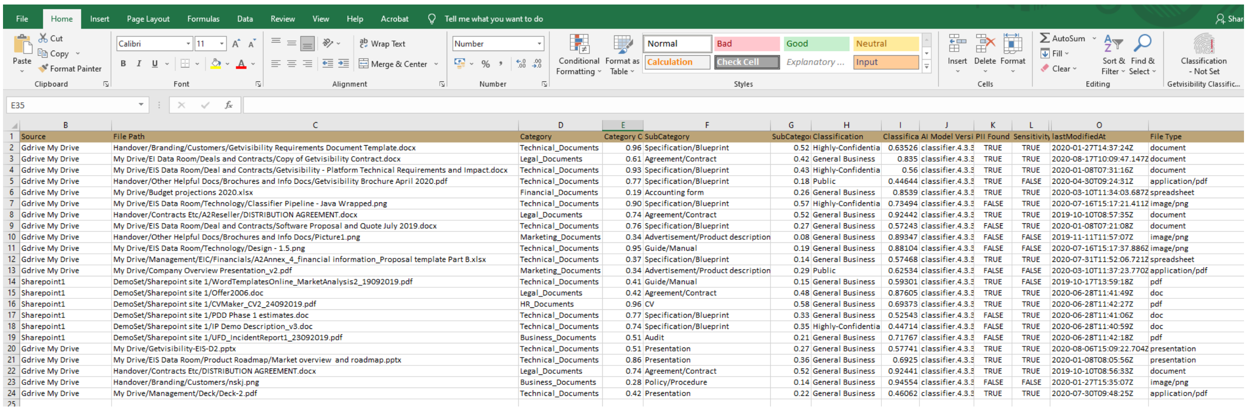
Source	Path	Category	Sub-Category	AIP	PII	Sensitivity	Risk	Regex Hits	Created	Last Opened	Permissions
//FileSrv-01-NS/	departments/R&D/013. scans/20140530_153509.jpg	Technical Documents	Guides/Manuals	C	false	false	Low	number 3 phone 7 email 8	May 30, 2014	May 30, 2014	Show Permissions
//FileSrv-01-NS/	departments/R&D/003. R&D PROJECTS/2. Finished Projects/02. Archive/12.2014 QAS Plain - V1.doc	Business Documents	Business Plan	I	true	true	High		Jan 20, 2015	Aug 26, 2015	Show Permissions
//FileSrv-01-NS/	departments/R&D/RS/Benchmarking 02.06.14.pptx	Technical Documents	Specifications/Blueprints	I	false	false	Low	number 8 email 1 credit card 2	Jun 2, 2014	Jun 14, 2014	Show Permissions
//FileSrv-01-NS/	departments/R&D/Archive/3. Horizon/Pictures/Second Attempt/rev2/No. 1 - trial.jpg	Technical Documents	Presentation	C	false	false	Low		Aug 3, 2016	Sep 4, 2017	Show Permissions
//FileSrv-01-NS/	departments/R&D/2012 Launches/05. TRIALS/02. TRIAL RFI/20111114 trial/20111114_007.pdf	Technical Documents	RFI	R	false	false	Low		Nov 14, 2011	Nov 14, 2011	Show Permissions
//FileSrv-01-NS/	departments/HR/staff/off sites/2019/June/team_day.doc author: D. Coetzee company: Getvisibility MIME: application/msword Last saved by: D. Coetzee Revision number: 2 Date last saved: Jan 14, 2019	HR Documents	Public Agenda	UR	false	false	Low	phone 3 email 1 credit card 2	Dec 4, 2018	Jan 14, 2019	Show Permissions
//FileSrv-01-NS/	departments/R&D/003. R&D PROJECTS/2. Finished Projects/01.	[directory]		UR	false	false	Low		Dec 4, 2014	Nov 27, 2018	Show Permissions



Permission Management

SEARCH FOR FILE OR FOLDER: departments | RISK: Select Filter... | CATEGORY: Select Filter... | PII ☐ | SENSITIVITY ☐ | Clear filters

Source	Path	Category	Sub-Category	AIP	PII	Sensitivity	Risk	Keyword Hits	Created	Last Opened
//FileSrv-01-NS/	departments/R&D/013. scans/20140530_153509.jpg	Technical Documents	Guides/Manuals	C	false	false	Low	phone 7 email 8 number 3	May 30, 2014	May 30, 2014
//FileSrv-01-NS/	departments/R&D/003. R&D PROJECTS/2. Finished Projects/02. Archive/12.2014 QAS Plain - V1.doc	Business Documents	Business Plan	GB	true	true	High	number 28	Jan 20, 2015	Aug 26, 2015
//FileSrv-01-NS/	departments/R&D/RS/Benchmarking 02.06.14.pptx	Technical Documents	Specifications/Blueprints	GB	false	false	Low	email 1 number 8 credit card 2	Jun 2, 2014	Jun 14, 2014
//FileSrv-01-NS/	departments/R&D/Archive/3. Horizon/Pictures/Second Attempt/rev2/No. 1 - trial.jpg	Technical Documents	Presentation	C	false	false	Low	number 127	Aug 3, 2016	Sep 4, 2017
//FileSrv-01-NS/	departments/R&D/2012 Launches/05. TRIALS/02. TRIAL RFI/20111114 trial/20111114_007.pdf	Technical Documents	RFI	HC	false	false	Low	number 82	Nov 14, 2011	Nov 14, 2011
//FileSrv-02-	departments/Technical/R&D/NEW PRODUCT TIMELINES/2. Historical Timelines/Product	Technical	Specification/Blueprint	HC	true	true	High	number 364	Aug 18,	Mar 19,



	B	C	D	E	F	G	H	I	J	K	L	O	
1	Source	File Path	Category	Category C	SubCategory	SubCategoı	Classification	Classifica	AI Model Versi	PII Found	Sensitivity	lastModifiedAt	File Type
2	Gdrive My Drive	Handover/Branding/Customers/Getvisibility Requirements Document Template.docx	Technical_Documents	0.96	Specification/Blueprint	0.52	Highly-Confidentia	0.63526	classifier.4.3.3	TRUE	TRUE	2020-01-27T14:37:24Z	document
3	Gdrive My Drive	My Drive/EI Data Room/Deals and Contracts/Copy of Getvisibility Contract.docx	Legal_Documents	0.61	Agreement/Contract	0.42	General Business	0.835	classifier.4.3.3	TRUE	TRUE	2020-08-17T10:09:47.147Z	document
4	Gdrive My Drive	My Drive/EIS Data Room/Deal and Contracts/Getvisibility - Platform Technical Requirements and Impact.docx	Technical_Documents	0.93	Specification/Blueprint	0.43	Highly-Confidentia	0.56	classifier.4.3.3	TRUE	TRUE	2020-01-08T07:31:16Z	document
5	Gdrive My Drive	Handover/Other Helpful Docs/Brochures and Info Docs/Getvisibility Brochure April 2020.pdf	Technical_Documents	0.77	Specification/Blueprint	0.18	Public	0.44644	classifier.4.3.3	TRUE	FALSE	2020-04-30T09:24:31Z	application/pdf
6	Gdrive My Drive	My Drive/Budget projections 2020.xlsx	Financial_Documents	0.19	Accounting form	0.26	General Business	0.8539	classifier.4.3.3	TRUE	TRUE	2020-03-10T11:34:03.687Z	spreadsheet
7	Gdrive My Drive	My Drive/EIS Data Room/Technology/Classifier Pipeline - Java Wrapped.png	Technical_Documents	0.90	Specification/Blueprint	0.57	Highly-Confidentia	0.73494	classifier.4.3.3	FALSE	TRUE	2020-07-16T15:17:21.411Z	image/png
8	Gdrive My Drive	Handover/Contracts Etc/A2Reseller/DISTRIBUTION AGREEMENT.docx	Legal_Documents	0.74	Agreement/Contract	0.52	General Business	0.92442	classifier.4.3.3	TRUE	TRUE	2019-10-10T08:57:35Z	document
9	Gdrive My Drive	My Drive/EIS Data Room/Deal and Contracts/Software Proposal and Quote July 2019.docx	Technical_Documents	0.76	Specification/Blueprint	0.27	General Business	0.57243	classifier.4.3.3	FALSE	TRUE	2020-01-08T07:21:08Z	document
10	Gdrive My Drive	Handover/Other Helpful Docs/Brochures and Info Docs/Picture1.png	Marketing_Documents	0.34	Advertisement/Product description	0.08	General Business	0.89347	classifier.4.3.3	FALSE	FALSE	2019-11-11T11:57:07Z	image/png
11	Gdrive My Drive	My Drive/EIS Data Room/Technology/Design - 1.5.png	Technical_Documents	0.95	Guide/Manual	0.19	General Business	0.88104	classifier.4.3.3	FALSE	FALSE	2020-07-16T15:17:37.886Z	image/png
12	Gdrive My Drive	My Drive/Management/EIC/Financials/A2Annex_4_financial information_Proposal template Part B.xlsx	Technical_Documents	0.37	Specification/Blueprint	0.14	General Business	0.57468	classifier.4.3.3	TRUE	TRUE	2020-07-31T11:52:06.721Z	spreadsheet
13	Gdrive My Drive	My Drive/Company Overview Presentation_v2.pdf	Marketing_Documents	0.34	Advertisement/Product description	0.29	Public	0.62534	classifier.4.3.3	FALSE	FALSE	2020-03-10T11:37:23.770Z	application/pdf
14	Sharepoint1	DemoSet/Sharepoint site 1/WordTemplatesOnline_MarketAnalysis2_19092019.pdf	Technical_Documents	0.41	Guide/Manual	0.15	General Business	0.59301	classifier.4.3.3	TRUE	FALSE	2019-10-17T13:59:18Z	pdf
15	Sharepoint1	DemoSet/Sharepoint site 1/Offer2006.doc	Legal_Documents	0.42	Agreement/Contract	0.48	General Business	0.87605	classifier.4.3.3	TRUE	TRUE	2020-06-28T11:41:49Z	doc
16	Sharepoint1	DemoSet/Sharepoint site 1/CVMaker_CV2_24092019.pdf	HR_Documents	0.96	CV	0.58	General Business	0.69373	classifier.4.3.3	TRUE	TRUE	2020-06-28T11:42:27Z	pdf
17	Sharepoint1	DemoSet/Sharepoint site 1/PDD Phase 1 estimates.doc	Technical_Documents	0.77	Specification/Blueprint	0.33	General Business	0.52543	classifier.4.3.3	FALSE	TRUE	2020-06-28T11:41:06Z	doc
18	Sharepoint1	DemoSet/Sharepoint site 1/IP Demo Description_v3.doc	Technical_Documents	0.74	Specification/Blueprint	0.35	Highly-Confidentia	0.44714	classifier.4.3.3	FALSE	TRUE	2020-06-28T11:40:59Z	doc
19	Sharepoint1	DemoSet/Sharepoint site 1/UFD_IncidentReport1_23092019.pdf	Business_Documents	0.51	Audit	0.21	General Business	0.71767	classifier.4.3.3	FALSE	TRUE	2020-06-28T11:42:18Z	pdf
20	Gdrive My Drive	My Drive/Getvisibility-EIS-D2.pptx	Technical_Documents	0.51	Presentation	0.27	General Business	0.57741	classifier.4.3.3	TRUE	TRUE	2020-08-06T15:09:22.704Z	presentation
21	Gdrive My Drive	My Drive/EIS Data Room/Product Roadmap/Market overview and roadmap.pptx	Technical_Documents	0.86	Presentation	0.36	General Business	0.6925	classifier.4.3.3	TRUE	TRUE	2020-01-08T08:05:56Z	presentation
22	Gdrive My Drive	Handover/Contracts Etc/DISTRIBUTION AGREEMENT.docx	Legal_Documents	0.74	Agreement/Contract	0.52	General Business	0.92441	classifier.4.3.3	TRUE	TRUE	2019-10-10T08:56:33Z	document
23	Gdrive My Drive	Handover/Branding/Customers/nskj.png	Business_Documents	0.28	Policy/Procedure	0.14	General Business	0.94554	classifier.4.3.3	FALSE	FALSE	2020-01-27T15:35:07Z	image/png
24	Gdrive My Drive	My Drive/Management/Deck/Deck-2.pdf	Technical_Documents	0.42	Presentation	0.22	General Business	0.46062	classifier.4.3.3	TRUE	TRUE	2020-07-30T09:48:25Z	application/pdf
25													

CORE FEATURE BREAKDOWN	Synergy	Synergy Pro	Enterprise Suite Synergy Pro + Focus
Email DLP on Classification	●	●	●
Live Classification of Data In Motion	●	●	●
Watermarking	●	●	●
Headers and Footers in Microsoft Office	●	●	●
One GRC Compliance Configuration	●	●	●
Customer Support Via Email, Phone or Live Chat	●	●	●
Policy Configuration	●	●	●
Windows Explorer Classification		●	●
Sharepoint		●	●
Insider Threat Monitoring		●	●
Risk Assessments		●	●
IAM		●	●
Self Service Data QA		●	●
On-Demand or Scheduled Scans			●
Data R.O.T Analysis			●
Comprehensive & User-Friendly Visualisation of Classified Data Files			●
Reporting and Remediation			●
Self Service Model Training			●
Data Risk Score Reporting	●	●	●

WEB getvisibility.com	**UNITED STATES** +1 617 861 2886	**IRELAND** +353 818 27 27 27	**GERMANY** +49 17 829 99 021
EMAIL info@getvisibility.com	**UK** +44 870 730 1090	**SWITZERLAND** +41 78 699 95 02	**APAC** +66 84 31 62785