GETVISIBILITY

GETVISIBILITY DATA RISK SCORE REPORT

getvisibility.com

GETVISIBILITY

Getvisibility
01/09/21
Overall Risk Report

Data Risk Score 9

This score represents the overall risk an organisation’s sensitive & regulated (critical) data, users, software, and policies present to the occurrence of a data breach. After scanning and assessing the selected file servers and user access, this overall score represents an aggregation of data risk across the organisation.

Data Risk Scores per Share

The individual scores that affected the data risk score for each share are also shown.

Key Data Risk Scores for: User_Documentation

9

Data Risk Score

- 9 Critical Files accessible to Inactive Users
- 8 Critical Files
- 8 Duplicate Critical Files

Key Data Risk Scores for: HR

8

Data Risk Score

- 8 Critical Files
- 8 Critical Stale Files
- 7 Outdated Paswords

Key Data Risk Scores for: Comp_01

9

Data Risk Score

- 9 Critical Files accessible to Inactive Users
- 8 Duplicate Critical Files
- 8 Critical Files

Key Data Risk Scores for Share_5

7

Data Risk Score

- 7 Outdated Passwords
- 7 Duplicate Critical Files
- 6 Enabled Inactive Users

Key Data Risk Scores for XD-120

6

Data Risk Score

- 7 Outdated Passwords
- 6 Enabled Inactive Users
- 6 Critical Files

Key Data Risk Scores for Processes

7

Data Risk Score

- 8 Critical Files
- 7 Outdated Passwords
- 6 Critical Stale Files

Key Data Risk Scores for Finance

9

Data Risk Score

- 9 Critical Files accessible to Inactive Users
- 8 Duplicate Critical Files
- 8 Critical Files

Key Data Risk Scores for IT

7

Data Risk Score

- 7 Outdated Passwords
- 7 Duplicate Critical Files
- 6 Enabled Inactive Users

Content Risk Score 8

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.

Critical Files

- 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

- 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

- 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

- 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

- 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

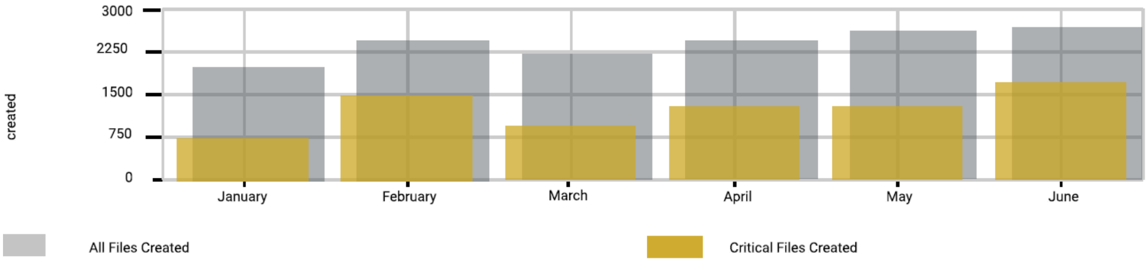
Critical Files available to Inactive Users

- 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

Dynamic Risk Score 6

This score charts the creation of sensitive and regulsted files over time. While their creation is not a risk in itself, the rates that they are created may be indicitive of policy or security issues

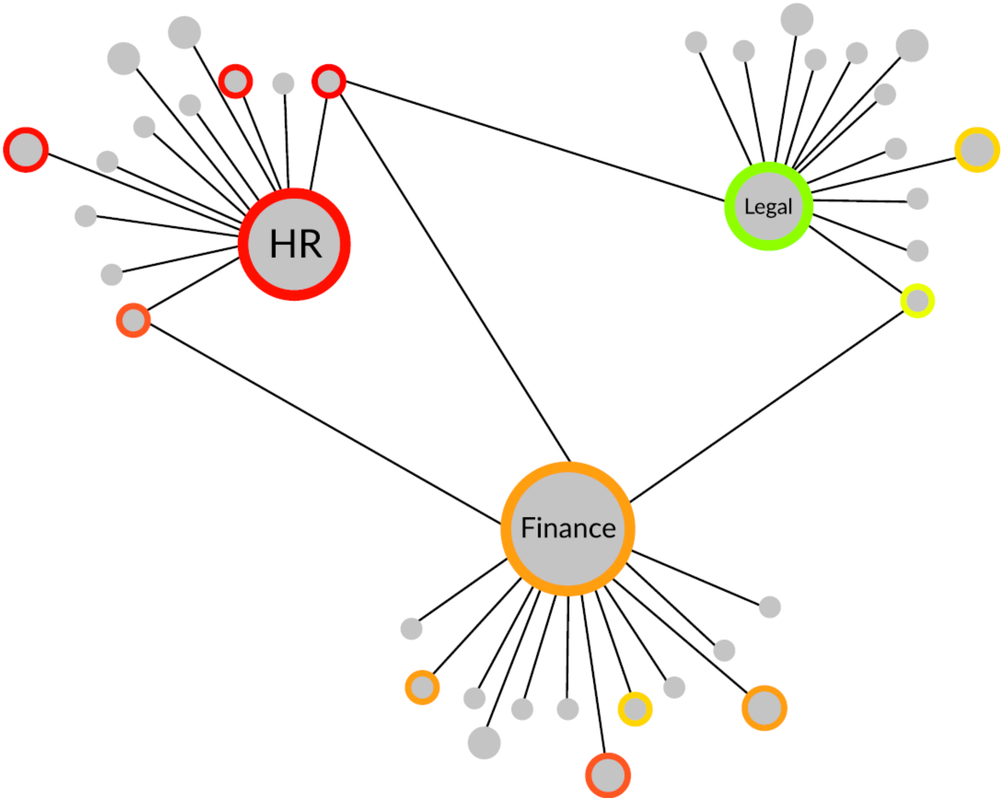
All & critical files created in the last 6 months



Classified as Confidential by Getvisibility © 2021

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 7



Devices with the most critical data

Critical Files	Device ID
6,457	HR_03
6,325	HR_46
6,267	HR_25
5,234	FIN_05
4,756	FIN_62
3,895	FIN_35

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

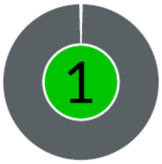
The coloured nodes indicate that a high percentage of sensitive & regulated files are stored in the device.

Edges represent access rights. They are not weighted.

This score assesses the file access permissions of the users on the network and the vulnerability that these permission settings represent to the critical data on the file share scanned.
A list of permission changes and additional remediation steps are available in the more detailed reports.

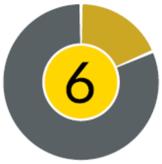
Access Risk Score 7

Critical Files in Everyone Group



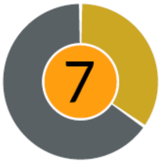
- The Everyone Group (EG) includes all users in the network
- 47 critical files
- 0 accessible to EG
- 0% of critical files can be accessed by EG

Enabled Inactive Users



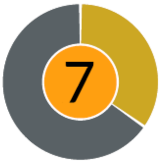
- Inactive uers still retain privileges
- 123 enabled users have been inactive for 100 days or more
- 19% of users are enabled inactive users

Critical Files available to Inactive Users



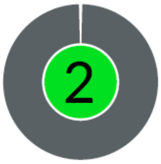
- Inactive Users (UI) are those that have not logged-in in more than 90 days
- 234 files accessible to inactive users
- 124 critical files accessible to inactive users
- 0% of S&R files can be accessed by Inactive groups

Outdated Passwords



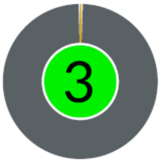
- Passwords that are not changed frequently
- 199 users have outdated passwords
- 35% of passwords have not been changed in more than 100 days

Highly-accessible Critical Files



- 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

Domain Administrators



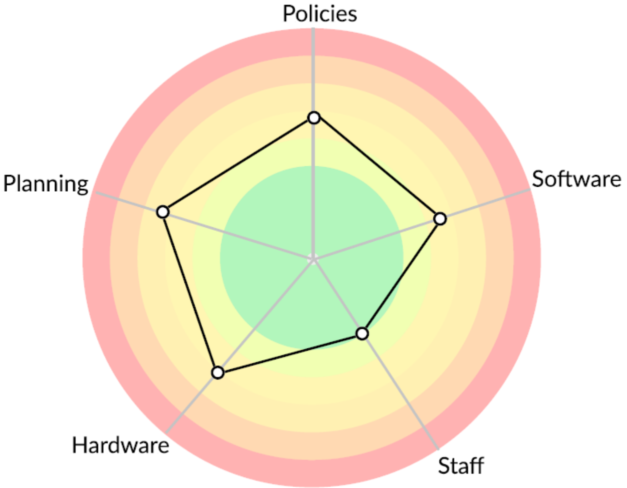
- Domain administrators are not Active Directory administrators but may have the same privilages
- 10 users have Domain Administrator privileges
- 0.18% of Active Directory accounts are Domain Administrators

GETVISIBILITY

Getvisibility
01/09/21
Overall Risk Report

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.

Scan Statistics

Statistic	Value
File Found	681,354
Shares Found	17
Shares Assessed for Data Risk	8
Total Data Size	12.68TB
Mean File Size	24MB
Median File Size	287KB
Total Users	1,098
Number of AD Groups	235
Most Numerous File Category	Technical Documents
Most Numerous File Subcategory	Configuration

Detailed Scores Table

Score	E	Computational	Users	IT	4D-110	Process Sciences
Critical Files	7.87	8.28	8.13	5.39	5.82	7.54
Duplicate Critical Files	7.76	5.23	7.23	7.35	2.43	2.78
Critical Stale Files	7.09	8.10	6.26	5.34	2.38	5.86
Critical Files in Everypone Group	8.28	1.23	1.23	1.23	1.23	1.23
Critical files accessible to Inactive Users	8.71	-	8.65	1.23	-	-
Highly Accessible Critical Files	2.94	2.84	3.84	3.84	1.94	1.84
Domain Administrators	2.52	2.52	2.52	2.52	2.52	2.52
Outdated Passwords	6.82	6.82	6.82	6.82	6.82	6.82
Enabled Inactive Users	5.23	5.03	5.75	5.25	5.95	5.95

Information based on disclosed file server(s) scanned.

The preceding information and analysis was compiled using Getvisibility's Data Risk Model Version 1.0.0

Information based on disclosed file server(s) scanned.
Classified using Getvisibility's generic machine learning model.
Modifications based on customer specific data are not included, but can be added during future engagments.

The preceding information and analysis was compiled using Getvisibility's Data Risk Model Version 1.0.0.

GETVISIBILITY
DATA RISK
ASSESSMENT