VARONIS

Our mission is to protect data from insider threats and cyberattacks.

Detect, Secure & Govern your GDPR data

General
Data
Protection
Regulation

Agenda

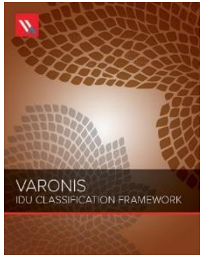
- Varonis – Who Are We?
- What is GDPR? Why do we need it?
- Varonis – What do we do?
  - Detect
  - Prevent
  - Sustain
- GDPR Readiness – How to get there
- Q&A

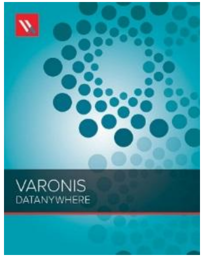
About Varonis

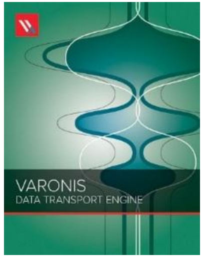
- Started operations in 2005
- 6,000+ Customers
- Our mission is to protect your sensitive information from threats, automate time-consuming tasks, and extract valuable insights from your data.

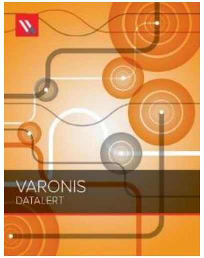
NASA TOYOTA BOSTON UNIVERSITY

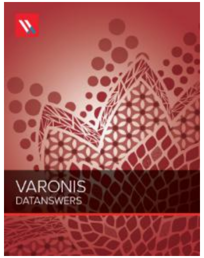
GDF SUEZ ING


VARONIS
IDU CLASSIFICATION FRAMEWORK

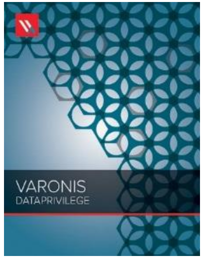

VARONIS
DATANYWHERE


VARONIS
DATA TRANSPORT ENGINE


VARONIS
DATALERT


VARONIS
DATANSWERS

VARONIS
DATADVANTAGE for Windows


VARONIS
DATAPRIVILEGE

What is the GDPR? Why do we need it?

GDPR concisely summarized by Wikipedia:

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU.

GDPR addresses many of the shortcomings in Data Protection Directive (DPD):

- Adding requirements for documenting IT procedures
- Performing risk assessments under certain conditions
- Notifying the consumer and authorities when there is a breach
- Strengthening rules for data minimization.

EU GDPR covers personal data (PII):

Think names, addresses, phone numbers, account numbers, and more recently email and IP addresses.

What are the new requirements?

Privacy by Design

Privacy by Design (PbD) has always played a part in EU data regulations. But with the new law, its principles of minimizing data collection and retention and gaining consent from consumers when processing data are more explicitly formalised.

Data
Risk
Assessment

Data Protection Impact Assessments (DPIA)

When certain data associated with subjects is to be processed, companies will have to first analyse the risks to their privacy.

Right to Erasure and To Be Forgotten

There's been a long standing requirement in the DPD allowing consumers to request that their data be deleted. The GDPR **extends** this right to include data published on the web.

VARONIS

What are the new requirements?

Extraterritoriality

The new principle of extraterritoriality in the GDPR says that even if a company doesn't have a physical presence in the EU but collects data about EU data subjects, for example, through a web site—then all the requirements of GDPR are in effect. In other words, the new law will extend outside the EU.

Breach Notification

A new requirement not in the existing DPD is that companies will **have** to notify data authorities within 72 hours after a breach of personal data has been discovered. Data subjects will also have to be notified but only if the data poses a "high risk to their rights and freedoms".

Fines

The GDPR has a tiered penalty structure that will take a large bite out of offender's funds. More serious infringements can merit a fine of up to 4% of a company's global revenue.

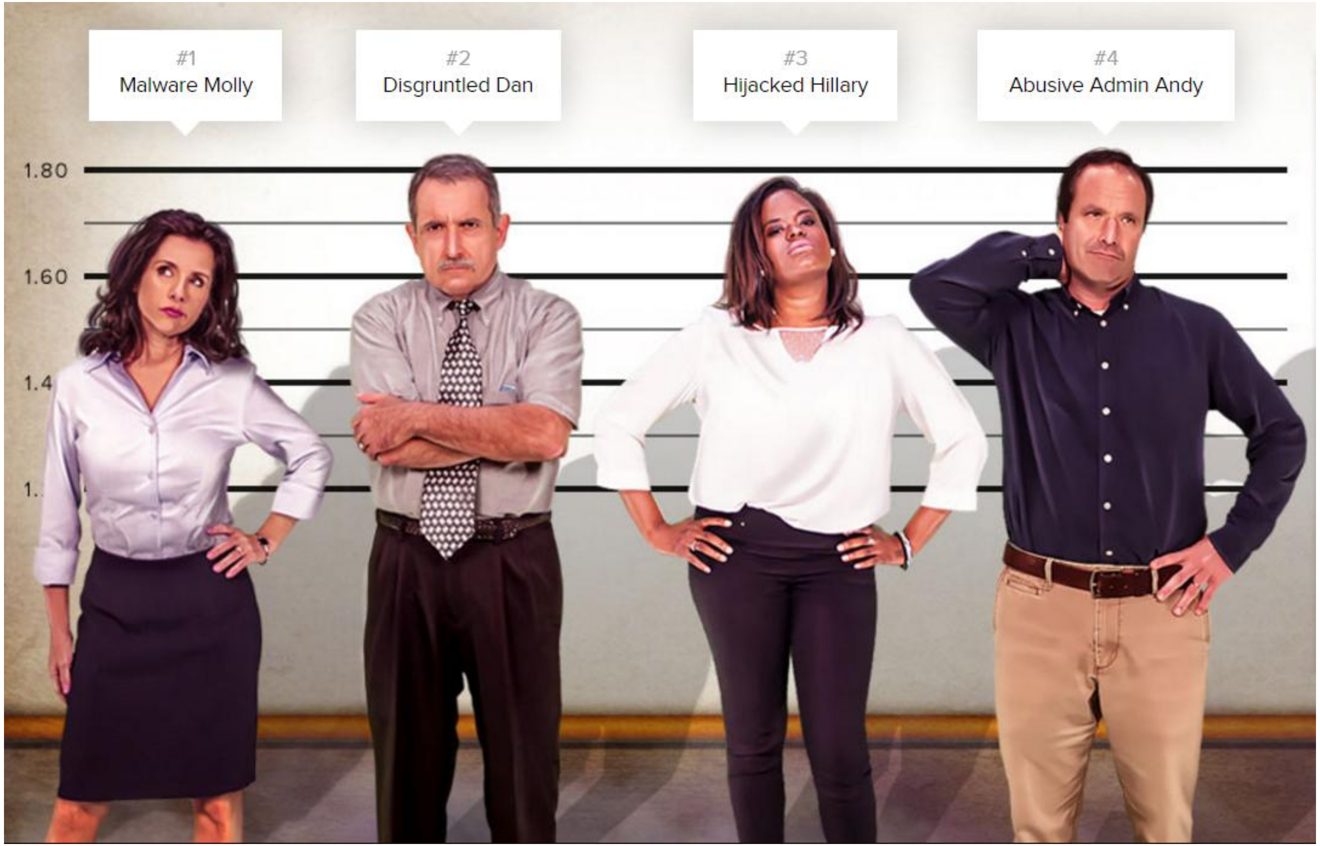
What are the new requirements?

Overall, the message for companies that fall under the GDPR is that awareness of your data —

- where is sensitive data stored
- who’s accessing it
- who should be accessing it

— will now become even more critical.

The Usual Suspects



Why do we have this regulation?

Its all their fault

Rebuilding Trust

Adopting a new way forward

What Businesses haven’t been doing

Privacy by Design

Accountability by Design

Incident Response Plan

PbD is only as good as those you trust with access

Monitor

Baseline

Alert

VARONIS How We Do It

General Data Protection Regulation

DETECT

PREVENT

SUSTAIN

Fundamental Unanswered Questions

There are many questions IT and the business can't answer:

- Who has access to files, folders, mailboxes?
- Who is accessing, modifying, moving, deleting files and email?
- Which files contain critical information?
- Which data is exposed to too many people?
- Who owns data and how do I get them involved?
- What data isn't being used?

User and Group information

Permission Information

Access Activity

Content Information

Management and Protection Methodology

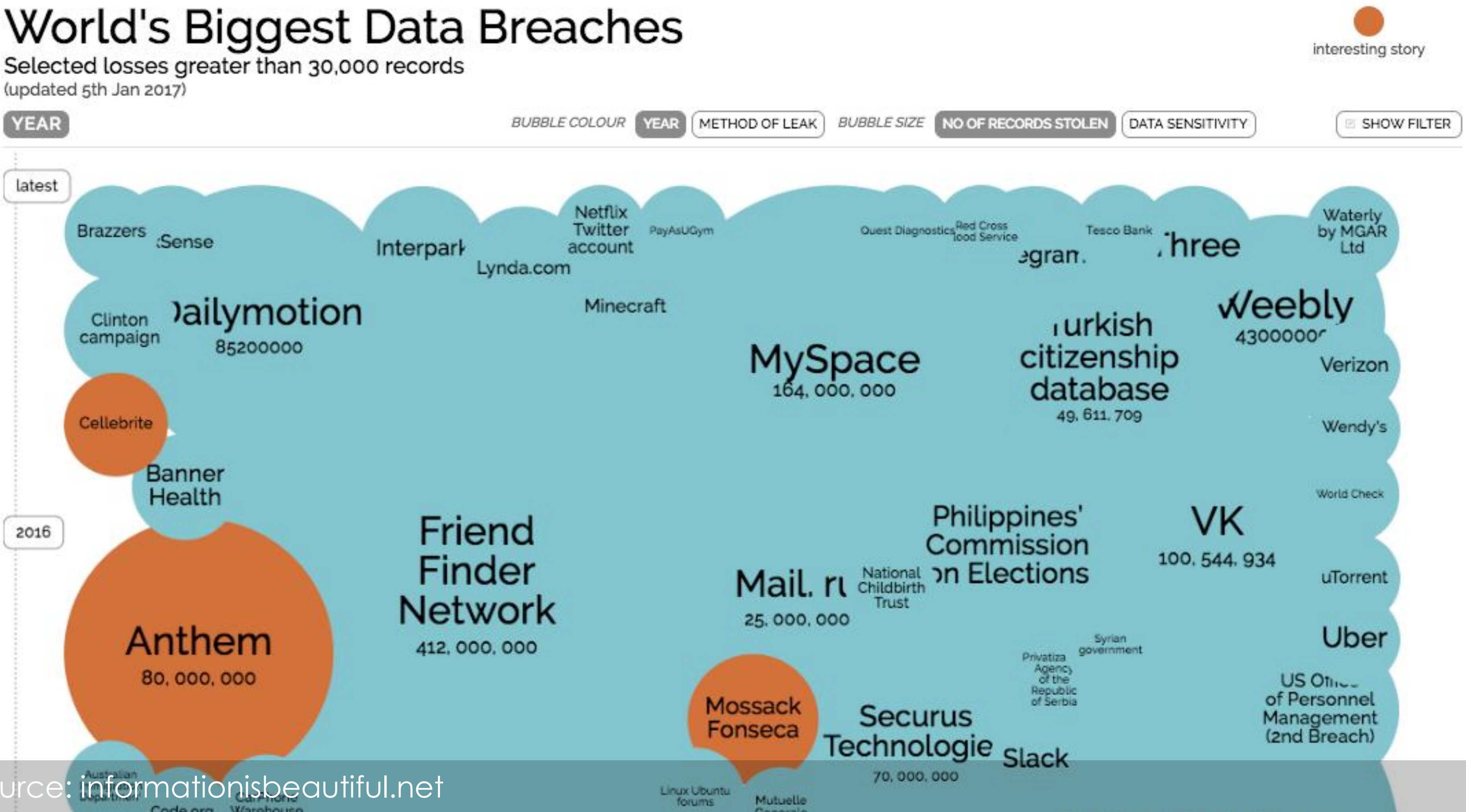
DETECT
insider threats and security threats by analyzing data, account activity, and user behavior.

PREVENT
disaster by locking down sensitive and stale data, reducing broad access, and simplifying permissions.

SUSTAIN
a secure state by automating authorizations, migrations, and disposition.

Detect

Incident Response Plan



World's Biggest Data Breaches

Selected losses greater than 30,000 records

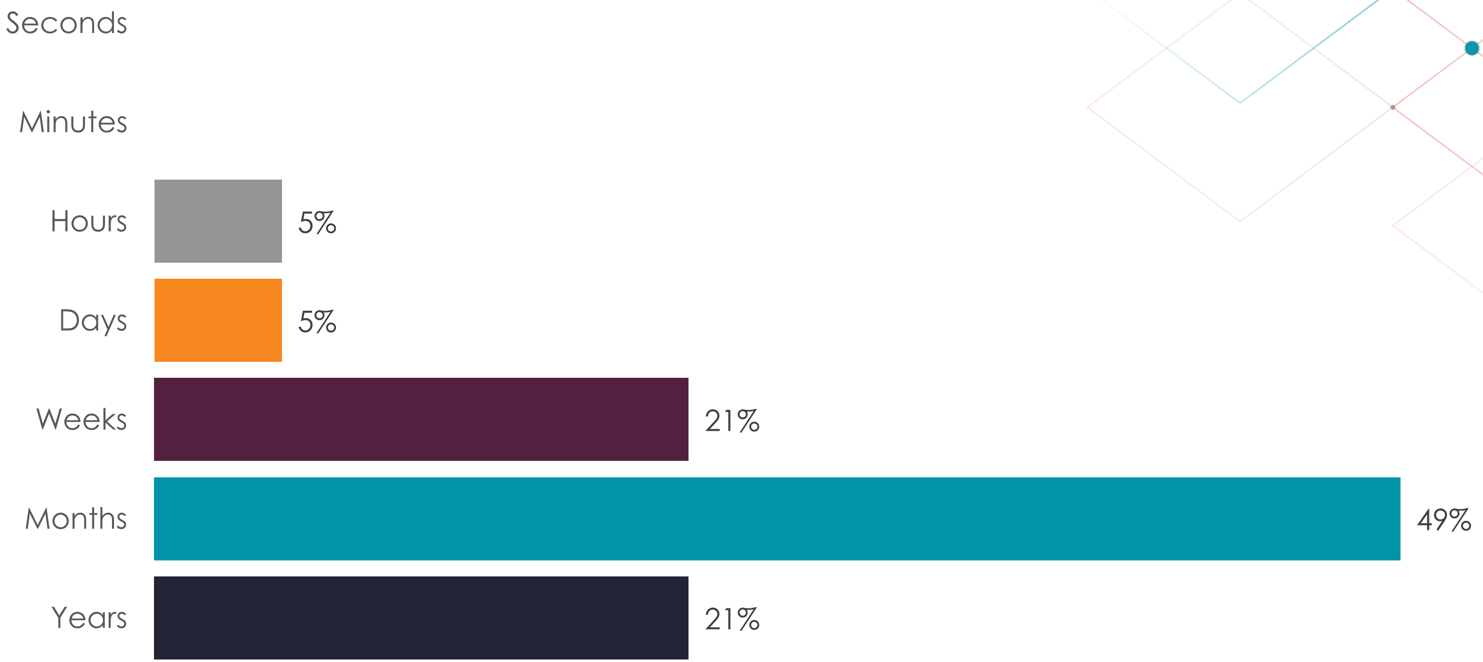
(updated 5th Jan 2017)

BUBBLE COLOUR: YEAR

BUBBLE SIZE: NO OF RECORDS STOLEN

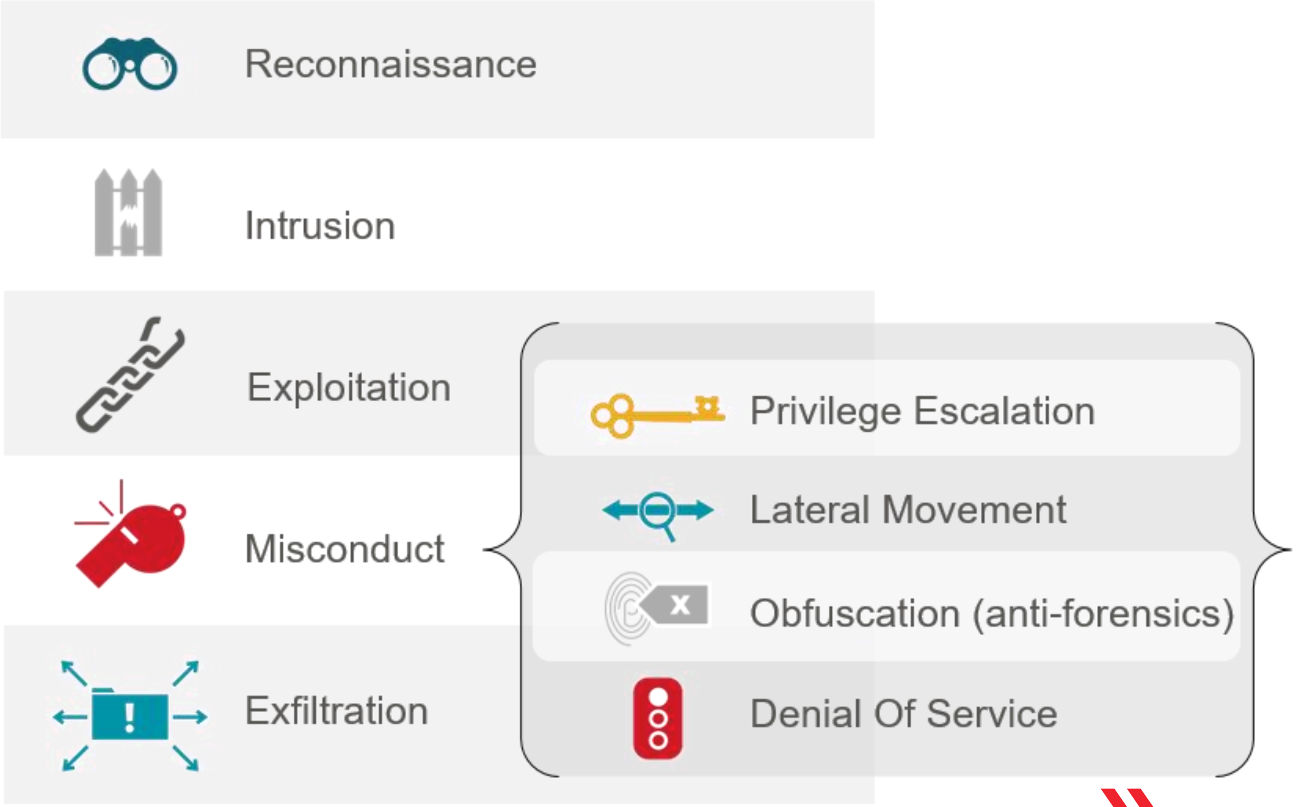
Source: informationisbeautiful.net

Discovery Timeline for Data Breaches



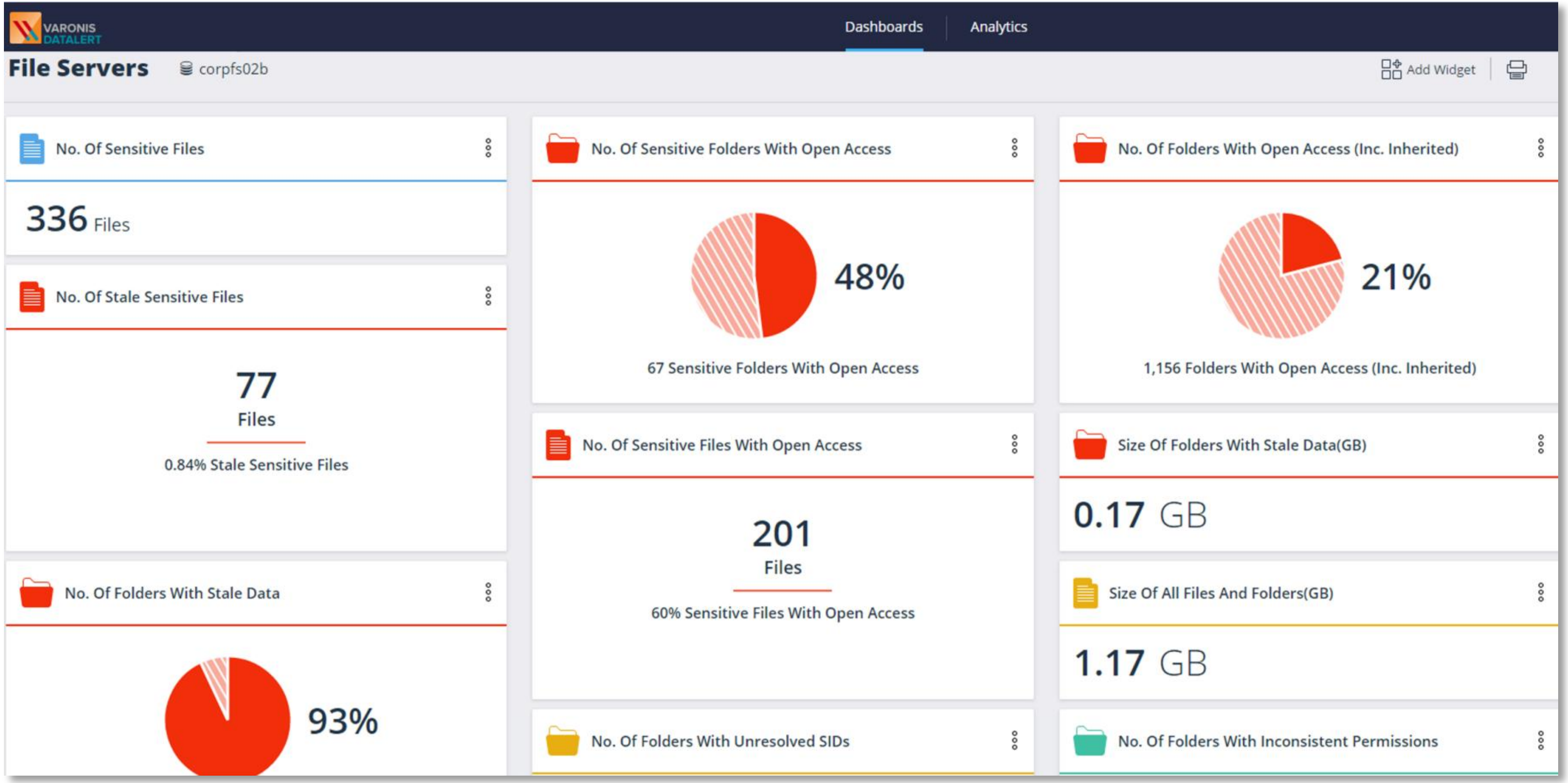
Source: Verizon 2016 Data Breach Investigations Report

Anatomy of a Breach, or “Kill Chain”



- Reconnaissance
- Intrusion
- Exploitation
  - Privilege Escalation
  - Lateral Movement
  - Obfuscation (anti-forensics)
  - Denial Of Service
- Misconduct
- Exfiltration

Conduct a Full Map Your Environment (that’s what hackers do!)



File Servers corpfs02b

No. Of Sensitive Files

336 Files

No. Of Stale Sensitive Files

77 Files

0.84% Stale Sensitive Files

No. Of Folders With Stale Data

93%

No. Of Sensitive Folders With Open Access

48%

67 Sensitive Folders With Open Access

No. Of Sensitive Files With Open Access

201 Files

60% Sensitive Files With Open Access

No. Of Folders With Unresolved SIDs

No. Of Folders With Open Access (Inc. Inherited)

21%

1,156 Folders With Open Access (Inc. Inherited)

Size Of Folders With Stale Data(GB)

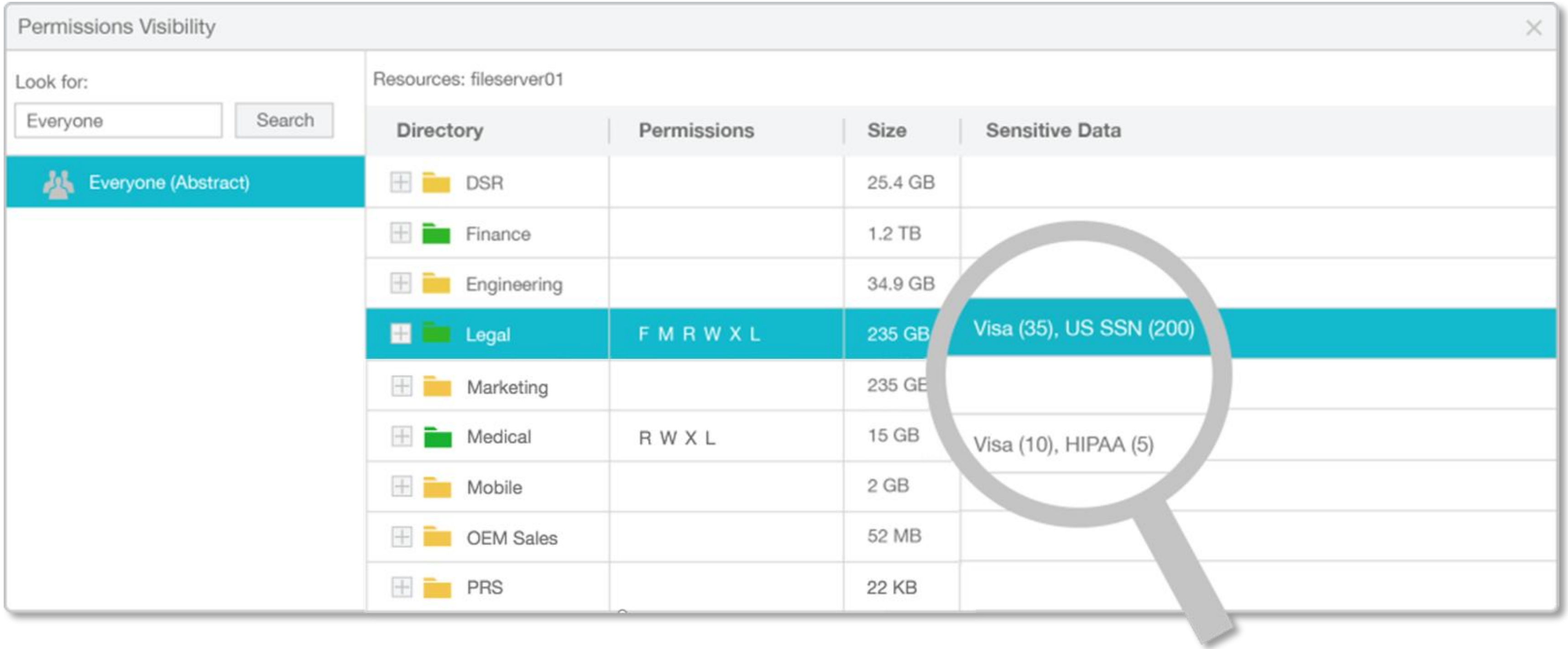
0.17 GB

Size Of All Files And Folders(GB)

1.17 GB

No. Of Folders With Inconsistent Permissions

Understand Where Sensitive Information Resides



Permissions Visibility

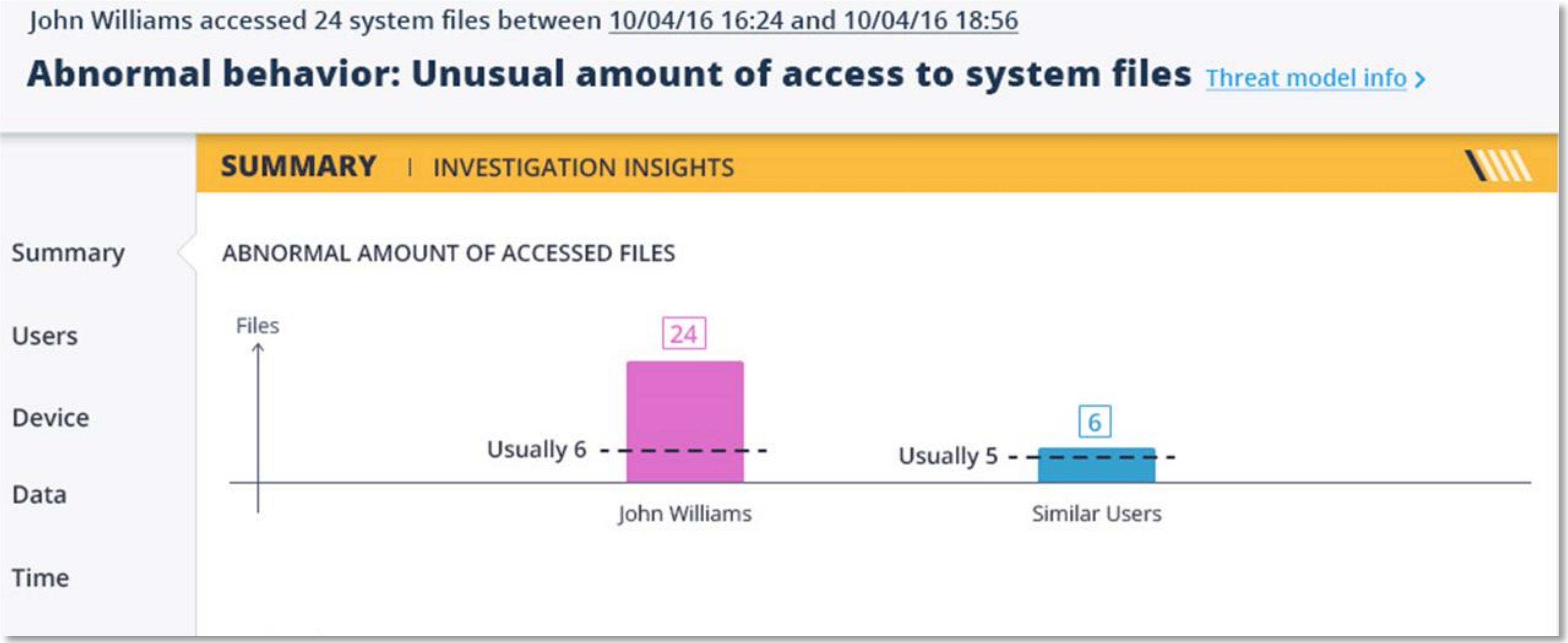
Look for: Everyone

Everyone (Abstract)

Resources: fileserver01

Directory	Permissions	Size	Sensitive Data
DSR		25.4 GB	
Finance		1.2 TB	
Engineering		34.9 GB	
Legal	F M R W X L	235 GB	Visa (35), US SSN (200)
Marketing		235 GB	
Medical	R W X L	15 GB	Visa (10), HIPAA (5)
Mobile		2 GB	
OEM Sales		52 MB	
PRS		22 KB	

Normalise User Behaviour and their Data Access Patterns



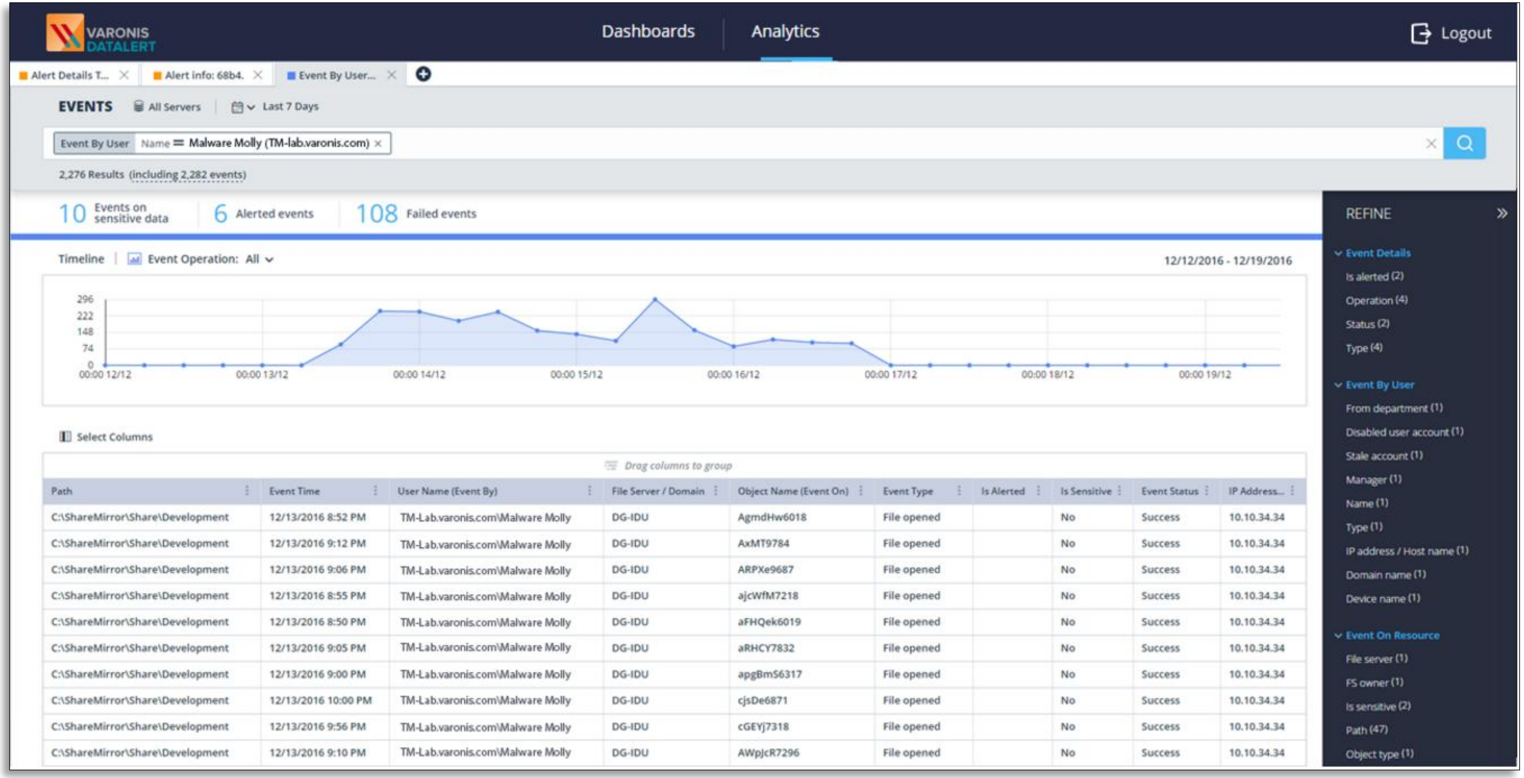
John Williams accessed 24 system files between 10/04/16 16:24 and 10/04/16 18:56

Abnormal behavior: Unusual amount of access to system files Threat model info ›

SUMMARY | INVESTIGATION INSIGHTS

ABNORMAL AMOUNT OF ACCESSED FILES

Investigate with hi-fidelity audit logs



Event By User Name = Malware Molly (TM-lab.varonis.com)

2,276 Results (including 2,282 events)

10 Events on sensitive data

6 Alerted events

108 Failed events

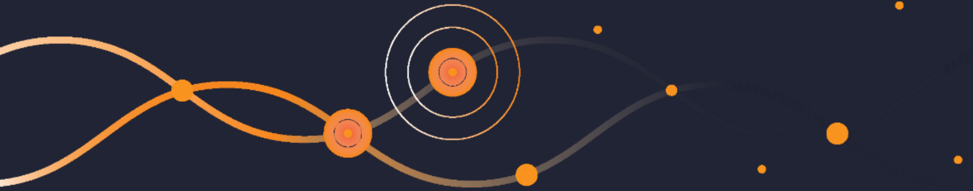
12/12/2016 - 12/19/2016

Path	Event Time	User Name (Event By)	File Server / Domain	Object Name (Event On)	Event Type	Is Alerted	Is Sensitive	Event Status	IP Address...
C:\ShareMirror\Share\Development	12/13/2016 8:52 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	AgmdHw6018	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 9:12 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	AxMT9784	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 9:06 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	ARPXe9687	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 8:55 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	ajcWfM7218	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 8:50 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	aFHQek6019	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 9:05 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	aRHCY7832	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 9:00 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	apgBmS6317	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 10:00 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	cjsDe6871	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 9:56 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	cGEYj7318	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	12/13/2016 9:10 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	AWpJcR7296	File opened		No	Success	10.10.34.34

Event Details
- Is alerted (2)
- Operation (4)
- Status (2)
- Type (4)

Event By User
- From department (1)
- Disabled user account (1)
- Stale account (1)
- Manager (1)
- Name (1)
- Type (1)
- IP address / Host name (1)
- Domain name (1)
- Device name (1)

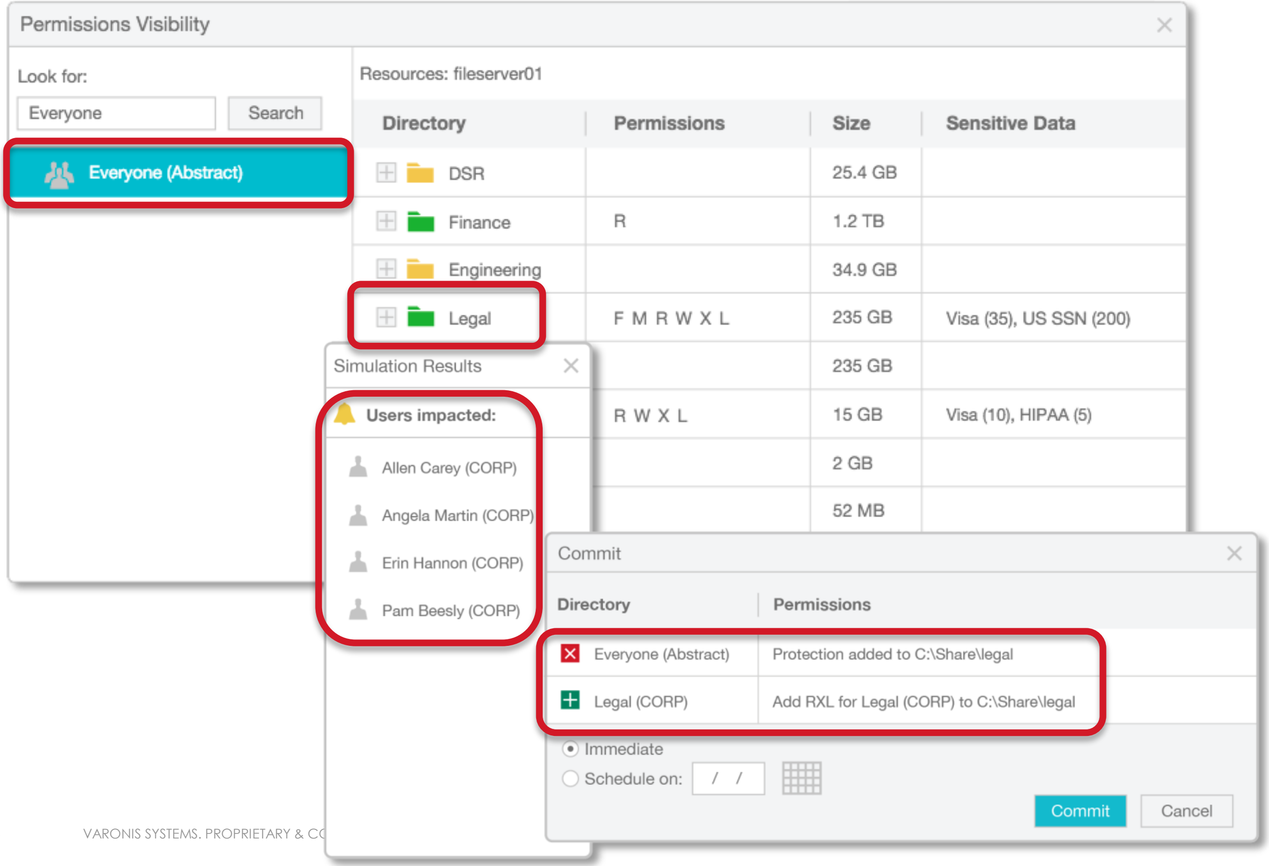
Event On Resource
- File server (1)
- FS owner (1)
- Is sensitive (2)
- Path (47)
- Object type (1)



Prevent

Privacy by Design

Remove Everyone Access



Permissions Visibility

Look for: Everyone

Everyone (Abstract)

Resources: fileserver01

Directory	Permissions	Size	Sensitive Data
DSR		25.4 GB	
Finance	R	1.2 TB	
Engineering		34.9 GB	
Legal	F M R W X L	235 GB	Visa (35), US SSN (200)
		235 GB	
	R W X L	15 GB	Visa (10), HIPAA (5)
		2 GB	
		52 MB	

Simulation Results

Users impacted:

- Allen Carey (CORP)
- Angela Martin (CORP)
- Erin Hannon (CORP)
- Pam Beesly (CORP)

Commit

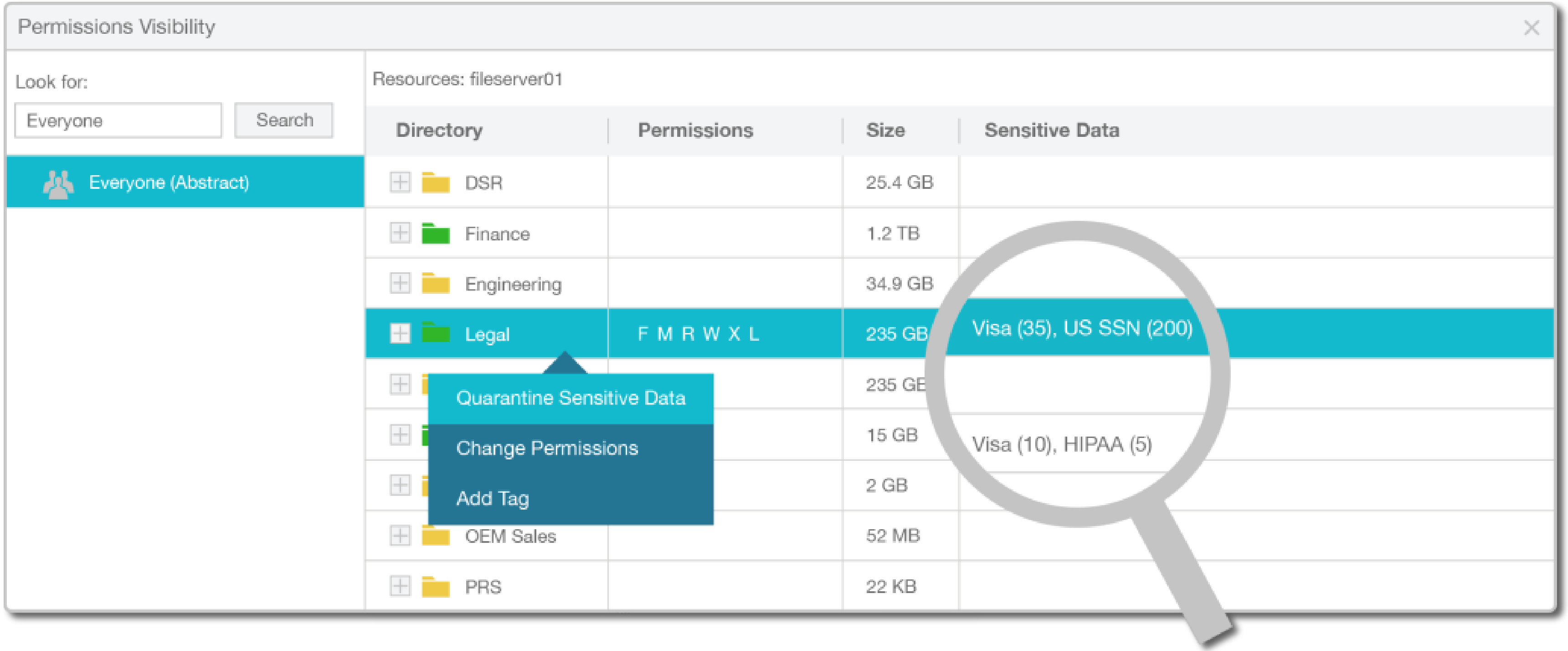
Directory	Permissions
☒ Everyone (Abstract)	Protection added to C:\Share\legal
⊞ Legal (CORP)	Add RXL for Legal (CORP) to C:\Share\legal

● Immediate

○ Schedule on: / /

Warning!
Erin Hannon will lose access to data she's been using!

De-risk through data discovery & deletion



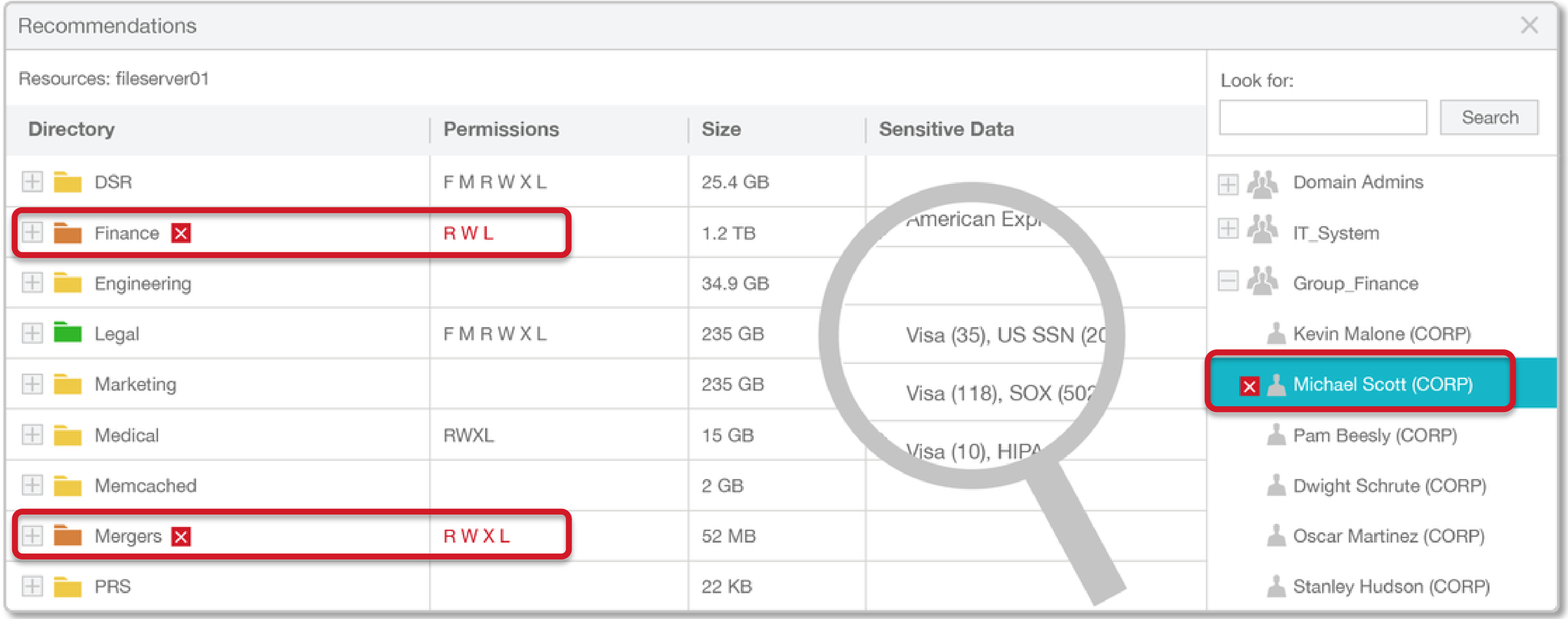
Look for: Everyone

Everyone (Abstract)

Resources: fileserver01

Directory	Permissions	Size	Sensitive Data
DSR		25.4 GB	
Finance		1.2 TB	
Engineering		34.9 GB	
Legal	F M R W X L	235 GB	Visa (35), US SSN (200)
		235 GB	
		15 GB	Visa (10), HIPAA (5)
		2 GB	
OEM Sales		52 MB	
PRS		22 KB	

Remove Excessive Access



Recommendations

Resources: fileserver01

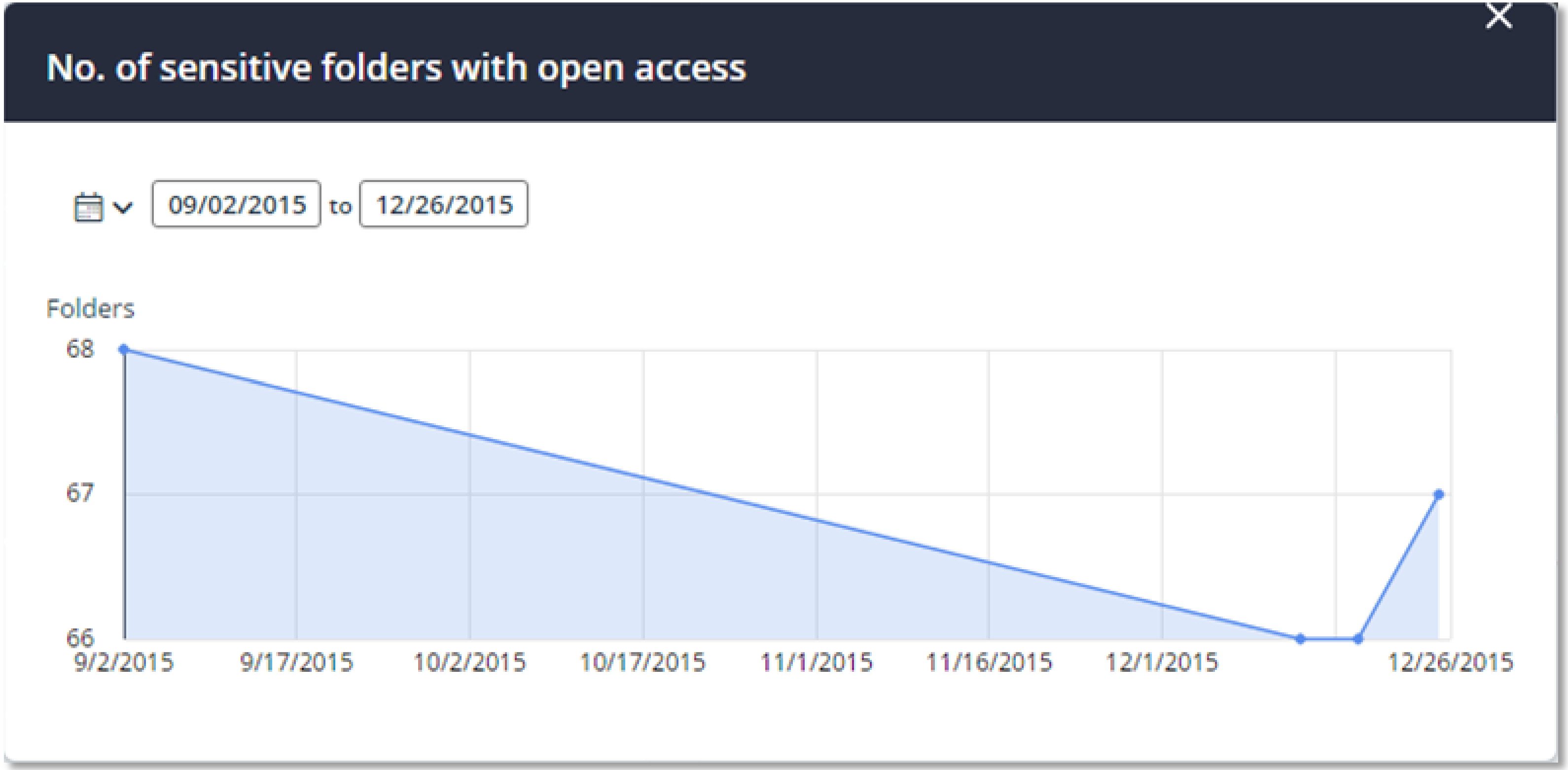
Directory	Permissions	Size	Sensitive Data
DSR	F M R W X L	25.4 GB	
Finance ☒	R W L	1.2 TB	American Exp
Engineering		34.9 GB	
Legal	F M R W X L	235 GB	Visa (35), US SSN (2(
Marketing		235 GB	Visa (118), SOX (50
Medical	RWXL	15 GB	Visa (10), HIPA
Memcached		2 GB	
Mergers ☒	R W X L	52 MB	
PRS		22 KB	

Look for:

Search

- Domain Admins
- IT_System
- Group_Finance
  - Kevin Malone (CORP)
  - ☒ Michael Scott (CORP)
  - Pam Beesly (CORP)
  - Dwight Schrute (CORP)
  - Oscar Martinez (CORP)
  - Stanley Hudson (CORP)

Evidence Success



No. of sensitive folders with open access

09/02/2015 to 12/26/2015

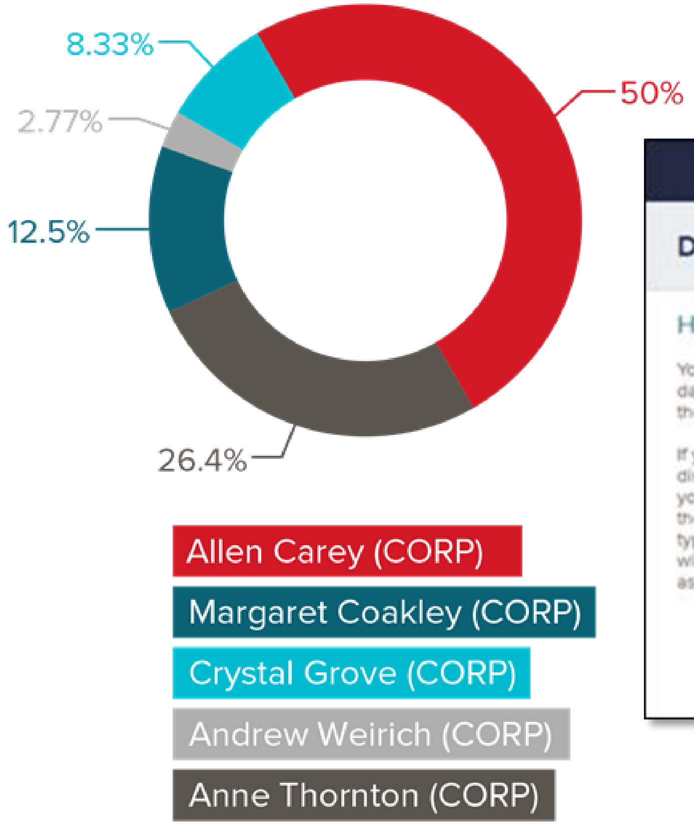
Address other Risk Vectors

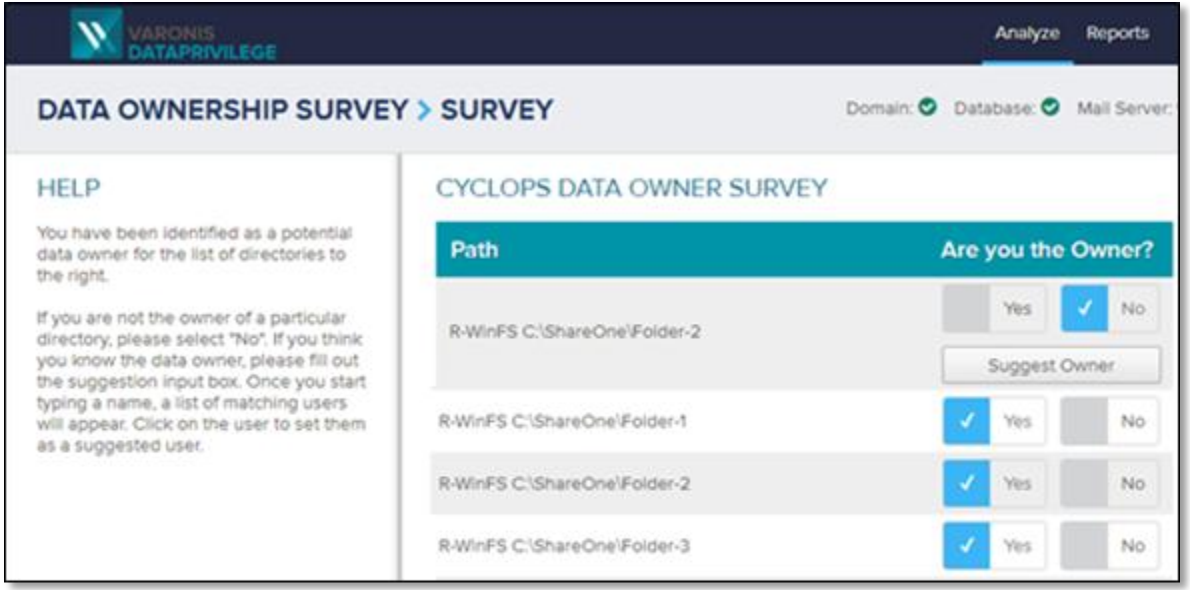
- Inactive users and groups
- Overly delegated groups
- Looped nested groups
- Broken ACLs
- Folders with unique permissions
- Stale data
- Delegated tasks in AD

Sustain

Accountability by design

Find and Assign Data Owners





DATA OWNERSHIP SURVEY > SURVEY

Domain: ✓ Database: ✓ Mail Server:

HELP

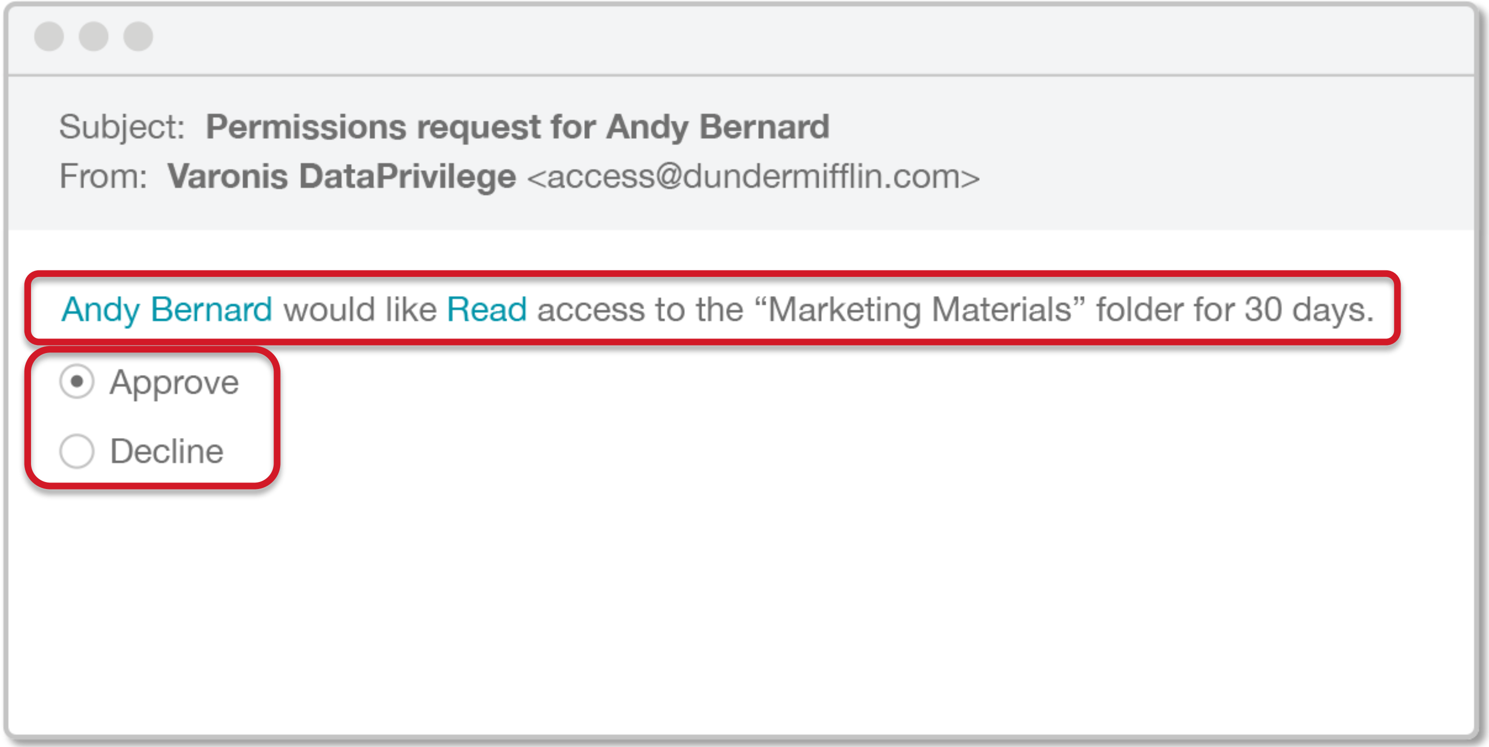
You have been identified as a potential data owner for the list of directories to the right.

If you are not the owner of a particular directory, please select "No". If you think you know the data owner, please fill out the suggestion input box. Once you start typing a name, a list of matching users will appear. Click on the user to set them as a suggested user.

CYCLOPS DATA OWNER SURVEY

Path	Are you the Owner?
R-WinFS C:\ShareOne\Folder-2	□ Yes ☑ No Suggest Owner
R-WinFS C:\ShareOne\Folder-1	☑ Yes □ No
R-WinFS C:\ShareOne\Folder-2	☑ Yes □ No
R-WinFS C:\ShareOne\Folder-3	☑ Yes □ No

Automate Authorisation



Subject: **Permissions request for Andy Bernard**

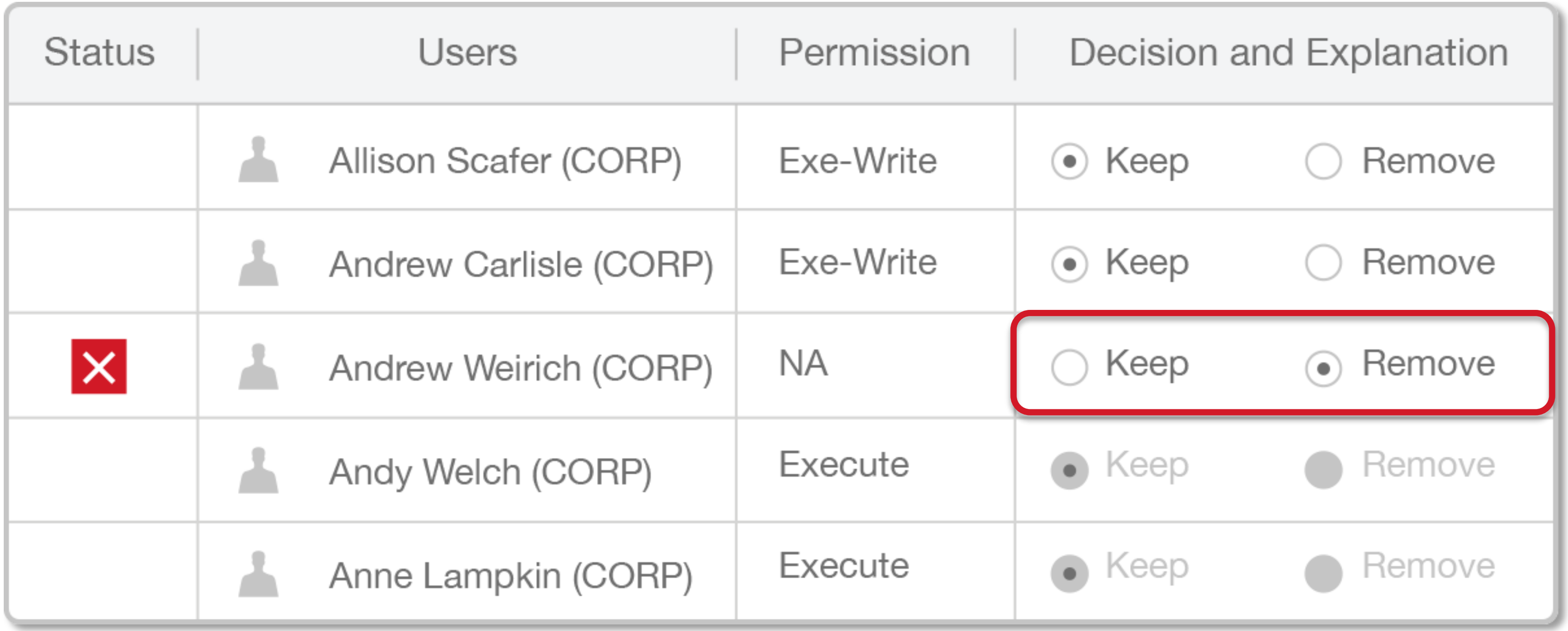
From: **Varonis DataPrivilege** <access@dundermifflin.com>

Andy Bernard would like Read access to the "Marketing Materials" folder for 30 days.

● Approve

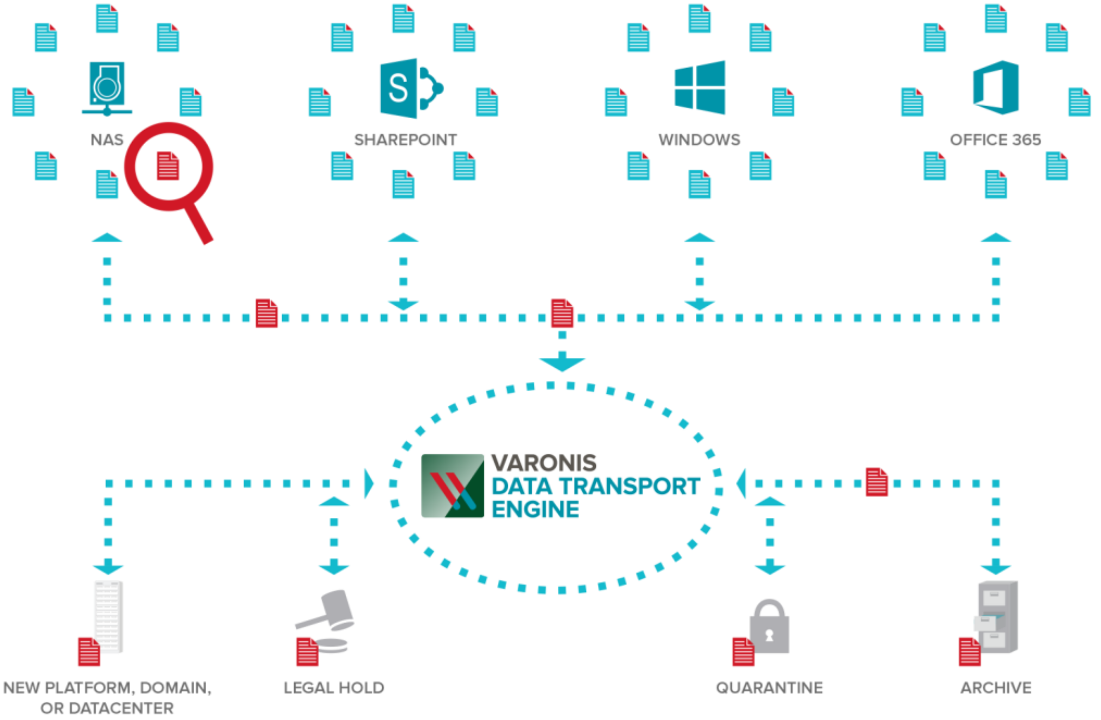
○ Decline

Sustain Privacy by Design

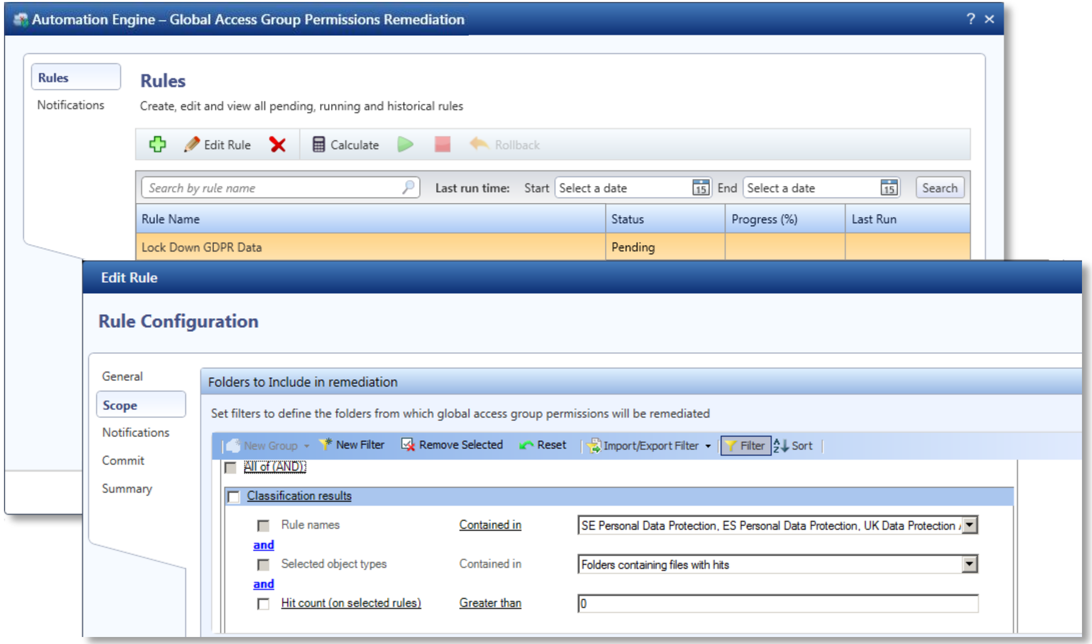


Status	Users	Permission	Decision and Explanation
	Allison Scafer (CORP)	Exe-Write	● Keep ○ Remove
	Andrew Carlisle (CORP)	Exe-Write	● Keep ○ Remove
☒	Andrew Weirich (CORP)	NA	○ Keep ● Remove
	Andy Welch (CORP)	Execute	● Keep ○ Remove
	Anne Lampkin (CORP)	Execute	● Keep ○ Remove

Automate Defensible Deletion and Migrations



Never see everyone access again



Automation Engine – Global Access Group Permissions Remediation

Rules

Create, edit and view all pending, running and historical rules

Rule Name	Status	Progress (%)	Last Run
Lock Down GDPR Data	Pending		

Edit Rule

Rule Configuration

Folders to Include in remediation

Set filters to define the folders from which global access group permissions will be remediated

□ All of (AND)

□ Classification results

□ Rule names — Contained in — SE Personal Data Protection, ES Personal Data Protection, UK Data Protection

and

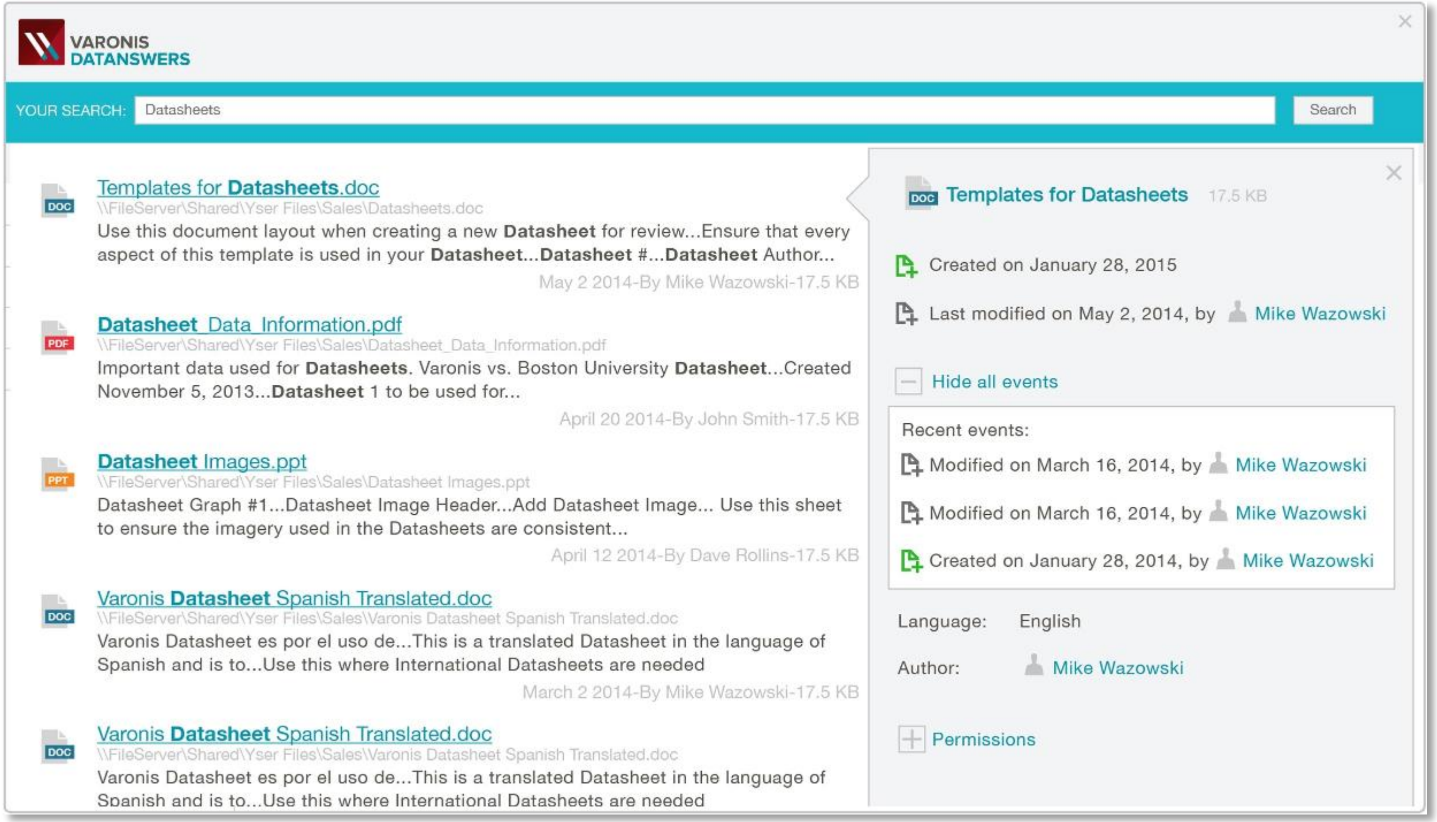
□ Selected object types — Contained in — Folders containing files with hits

and

□ Hit count (on selected rules) — Greater than — 0

> “The Automation Engine allowed us to remediate the contradiction to PbD that global access presents. It was efficient, accurate and didn’t impact the business.”

Respond to Subject Access Requests



VARONIS DATANSWERS

YOUR SEARCH: Datasheets Search

Templates for **Datasheets**.doc
\\FileServer\Shared\Yser Files\Sales\Datasheets.doc
Use this document layout when creating a new **Datasheet** for review...Ensure that every aspect of this template is used in your **Datasheet**...**Datasheet** #...**Datasheet** Author...
May 2 2014-By Mike Wazowski-17.5 KB

Datasheet_Data_Information.pdf
\\FileServer\Shared\Yser Files\Sales\Datasheet_Data_Information.pdf
Important data used for **Datasheets**. Varonis vs. Boston University **Datasheet**...Created November 5, 2013...**Datasheet** 1 to be used for...
April 20 2014-By John Smith-17.5 KB

Datasheet Images.ppt
\\FileServer\Shared\Yser Files\Sales\Datasheet Images.ppt
Datasheet Graph #1...Datasheet Image Header...Add Datasheet Image... Use this sheet to ensure the imagery used in the Datasheets are consistent...
April 12 2014-By Dave Rollins-17.5 KB

Varonis **Datasheet** Spanish Translated.doc
\\FileServer\Shared\Yser Files\Sales\Varonis Datasheet Spanish Translated.doc
Varonis Datasheet es por el uso de...This is a translated Datasheet in the language of Spanish and is to...Use this where International Datasheets are needed
March 2 2014-By Mike Wazowski-17.5 KB

Varonis **Datasheet** Spanish Translated.doc
\\FileServer\Shared\Yser Files\Sales\Varonis Datasheet Spanish Translated.doc
Varonis Datasheet es por el uso de...This is a translated Datasheet in the language of Spanish and is to...Use this where International Datasheets are needed

Templates for Datasheets 17.5 KB

Created on January 28, 2015

Last modified on May 2, 2014, by Mike Wazowski

Hide all events

Recent events:

Modified on March 16, 2014, by Mike Wazowski

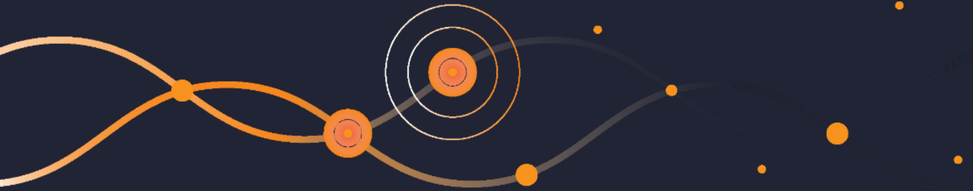
Modified on March 16, 2014, by Mike Wazowski

Created on January 28, 2014, by Mike Wazowski

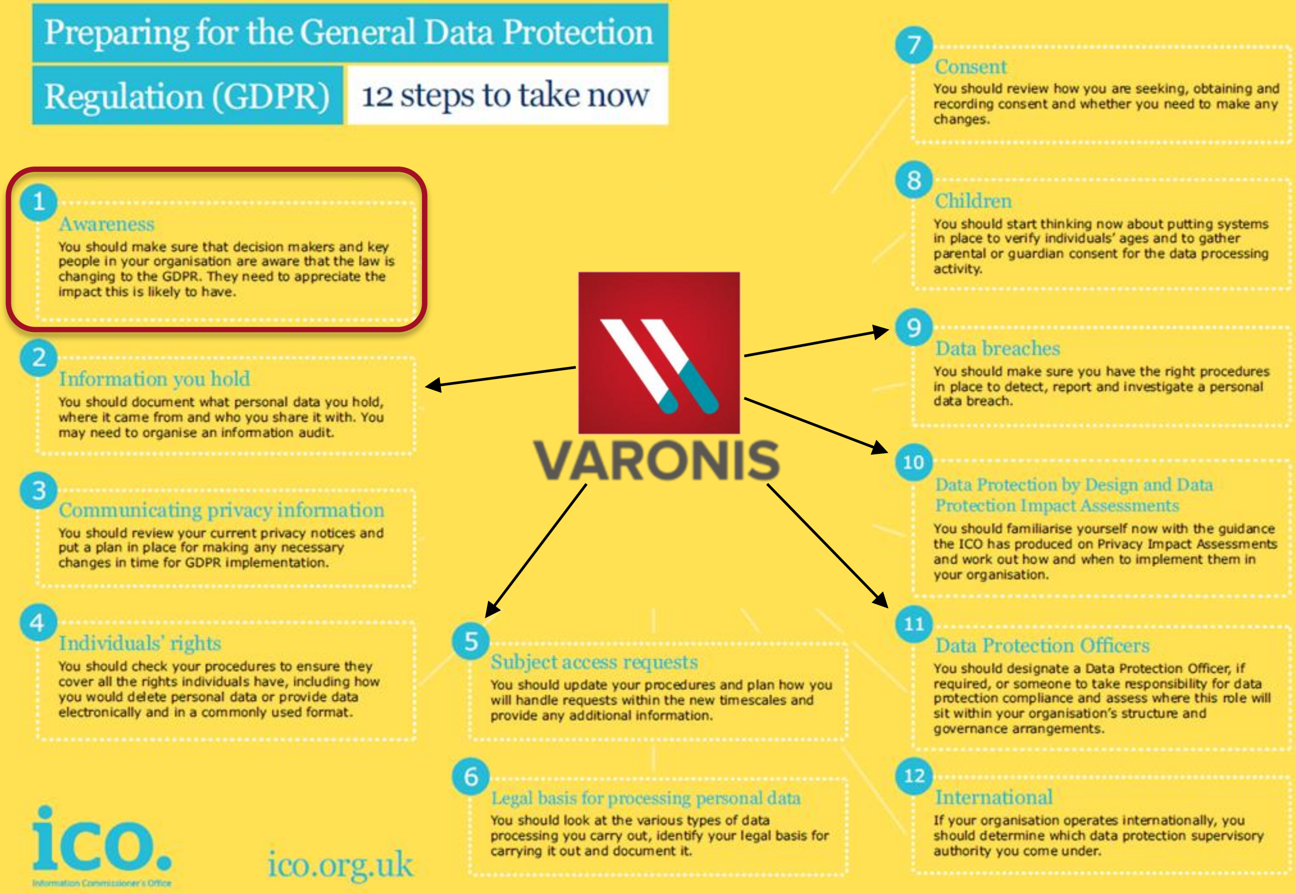
Language: English

Author: Mike Wazowski

Permissions



What do others say about preparing for GDPR?



Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 **Awareness**
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 **Information you hold**
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 **Communicating privacy information**
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 **Individuals' rights**
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 **Subject access requests**
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 **Legal basis for processing personal data**
You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 **Consent**
You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 **Children**
You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 **Data breaches**
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 **Data Protection by Design and Data Protection Impact Assessments**
You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 **Data Protection Officers**
You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 **International**
If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

How to Get There

- Let’s break down some of the challenges in the new GDPR and how to address them:

GDPR Article	What does it mean	How to address it
Article 25: Data Protection by Design and By Default	Embrace “Accountability and Privacy by Design” as a business culture.	Safely remediate access controls to Least Privilege.
Article 30: Records of Processing Activities	Implement technical and organizational measures to properly process personal data.	- Create asset register of sensitive files - Understand who has access - Know who is accessing it - Know when data can and should be deleted.
Article 17: Right to Erasure and “to be forgotten”	Be able to discover and target specific data and automate removal.	Find it, flag it, remove it.

General
Data
Protection
Regulation

How to Get There

GDPR Article	What does it mean	How to address it
Article 32: Security of Processing	- Ensure least privilege access - Implement accountability via Data Owners - Provide reports that show policies and processes are in place and are successful.	Automate and impose Least Privilege through Entitlement Reviews and proactively enforced ethical walls.
Article 33: Notification of personal data breach to the supervisory authority	- Prevent and alert on data breach activity - Ensure an Incidence Response Plan is in place.	Detect abnormal data breach activity, policy violations and real-time alert on it as it happens.
Article 35: Data Protection Impact Assessment	- Quantify data protection risk profiles.	Conduct regular quantified data risk assessments.

VARONIS

Get your **free**
Data Risk Assessment

KEY FINDINGS:
GLOBAL ACCESS GROUPS

Over **1.9 million folders** with global group access

Distribution of Global Group Access

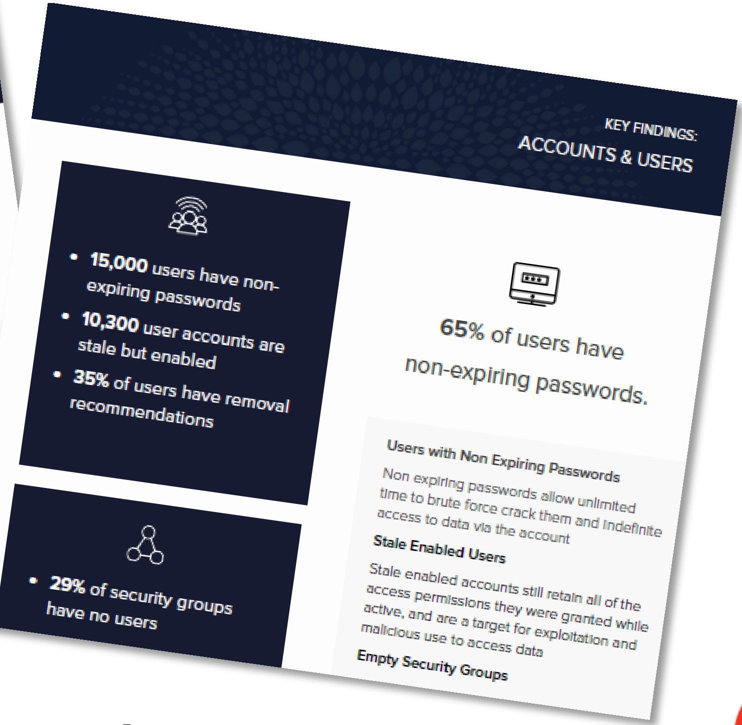
CIFS_FS_2 :	11%
CIFS_FS_3 :	7%
CIFF_FS_4 :	20%
SP_FS_1 :	44%
EXCH_FS_1:	18%

Global Group Access

These include groups such as Everyone Domain Users, and Authenticated User

Global access groups will allow anyon within an organization to access data these access controls.

Everyone group allows anyone on network access.



KEY FINDINGS:
ACCOUNTS & USERS

- **15,000** users have non-expiring passwords
- **10,300** user accounts are stale but enabled
- **35%** of users have removal recommendations

- **29%** of security groups have no users

65% of users have non-expiring passwords.

Users with Non Expiring Passwords

Non expiring passwords allow unlimited time to brute force crack them and indefinite access to data via the account

Stale Enabled Users

Stale enabled accounts still retain all of the access permissions they were granted while active, and are a target for exploitation and malicious use to access data

Empty Security Groups

Inform your GDPR Strategy Today

BYTES
SECURITY PARTNERSHIPS

VARONIS

We know where our sensitive data lives

Only the right people have access

Cyber threats are detected and stopped

Sustain a secure state without manual effort

Thank you

Thank You

Leon Turner – Senior SE, Strategic Accounts
lturner@varonis.com
07584 677637