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

Varonis and GDPR

February 2017

Who Am I

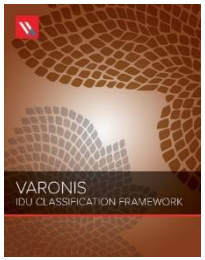
- Matt Lock
- Director of Sales Engineers, UK
- mlock@varonis.com +447795153900
- blog.varonis.com

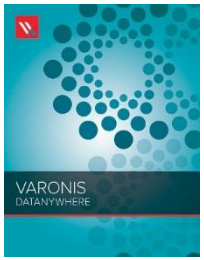
Agenda

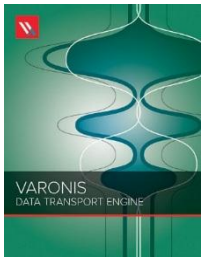
- Varonis – Who Are We?
- What is the GDPR? Why do we need it?
- Varonis – What do we do?
  - **Detect**
  - **Prevent**
  - **Sustain**
- GDPR – How to Get There
- What happens in a breach? How to I detect it?
- Q&A

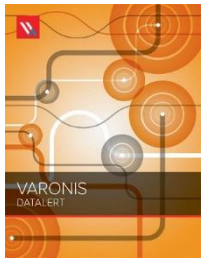
About Varonis

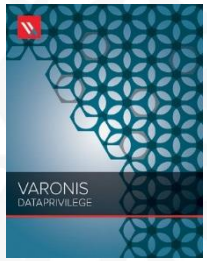
- Started operations in 2005
- ~5,000 Customers
  (as of June 2016)
- We protect your most critical
  data from the insider threat





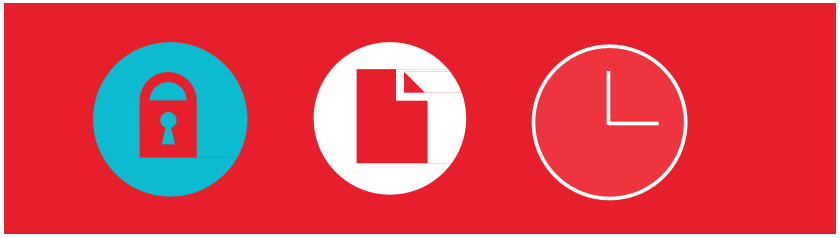






The Varonis Origin Story

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.

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

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 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.

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.

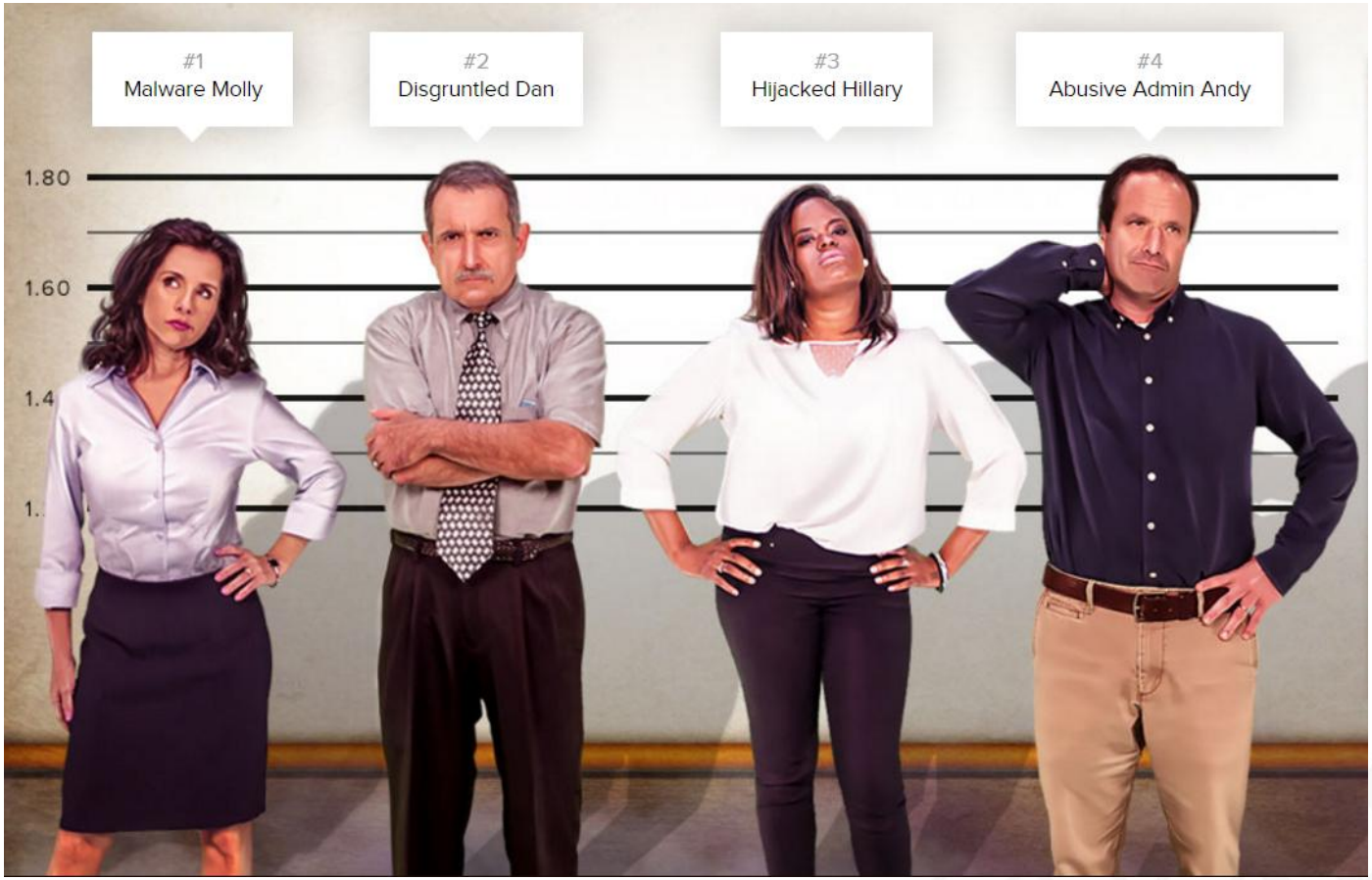
A lesser fine of up to 2% of global revenue can be issued if company records are not in order or a supervising authority and data subjects are not notified after a breach. This makes breach notification oversights a serious and expensive offense.

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, and who should be accessing it — will now become even more critical.

The Usual Suspects

Why do we have this regulation? Its all their fault



The impact of insider threats

- **3.8** insider attacks per organization per year (on average)
- **45%** of organizations can't tell if they've suffered an insider breach
- **34%** estimate the cost of an insider breach to be **> $1 million**
- **Reputational damage** is immeasurable
- CEOs and CISO are **losing their jobs** due to breaches

SANS Crowd Research Partners

VARONIS

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?

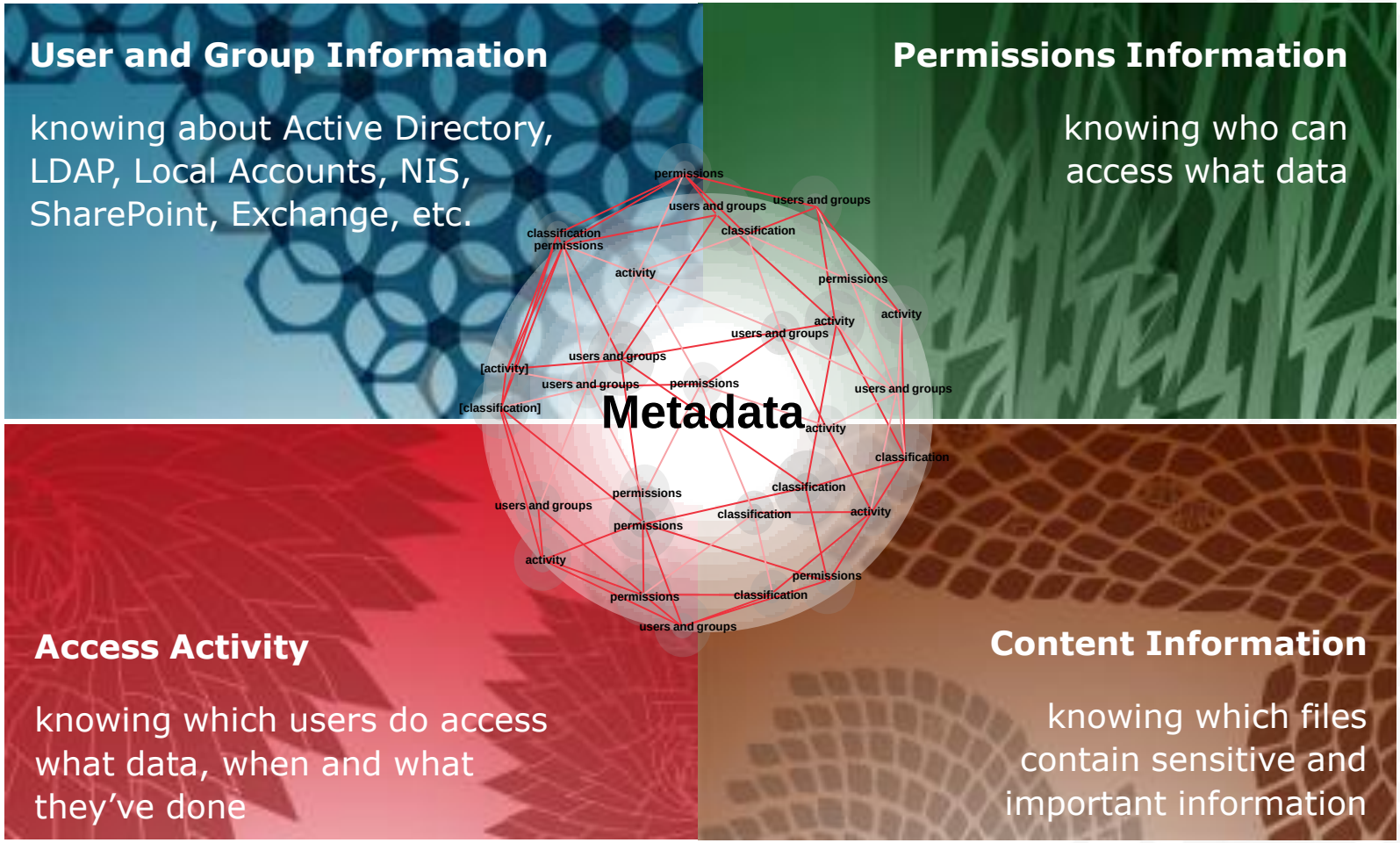
Which files contain critical information?

Which data is exposed to too many people?

Who owns data and how do I get them involved?

What data isn't being used?

Where Varonis Starts



Management and Protection Methodology

DETECT

Enable auditing

Baseline user behavior

Inventory sensitive data

PREVENT

Lock down sensitive information

Remove dangerous artifacts

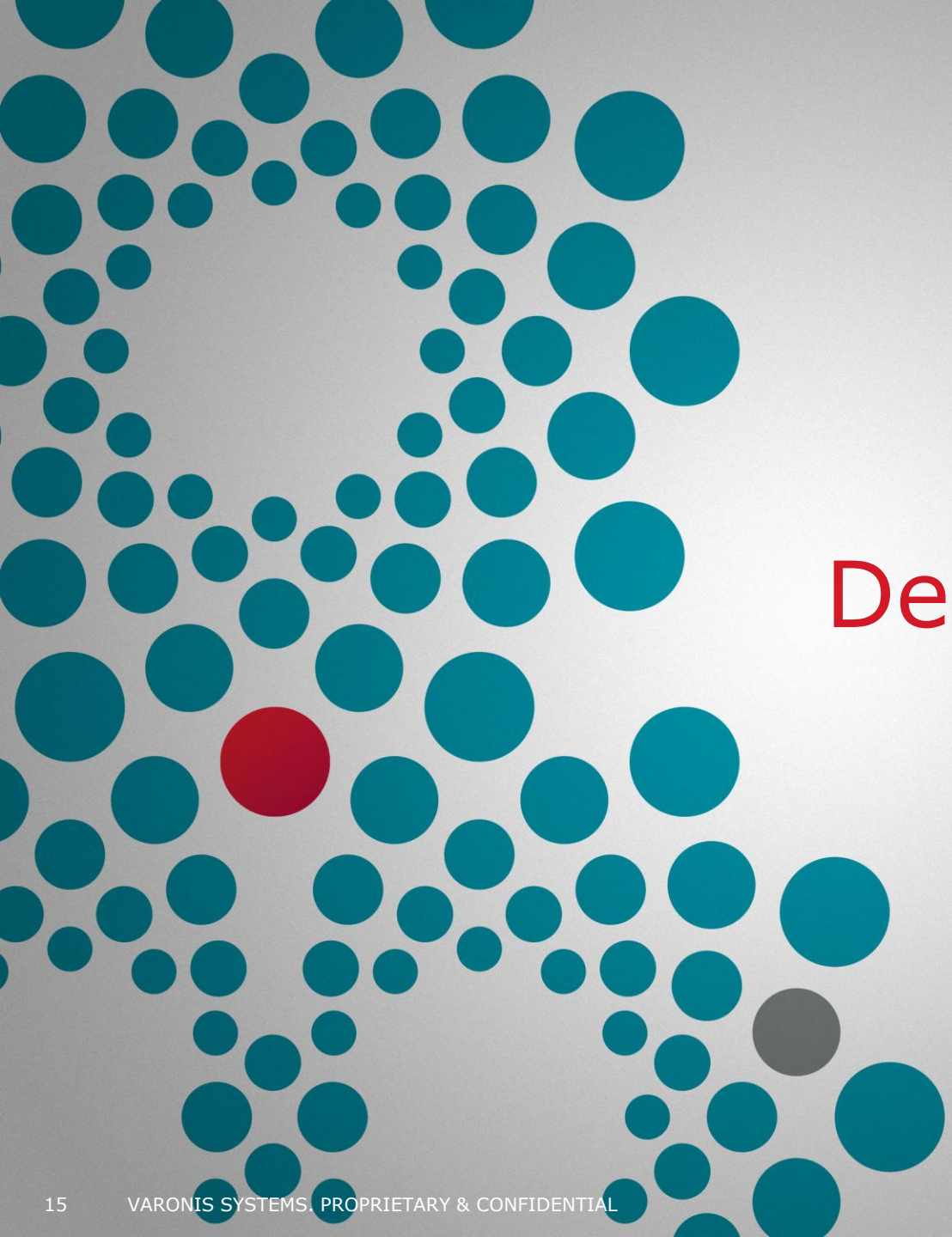
Simplify permissions

SUSTAIN

Automate cleanup tasks

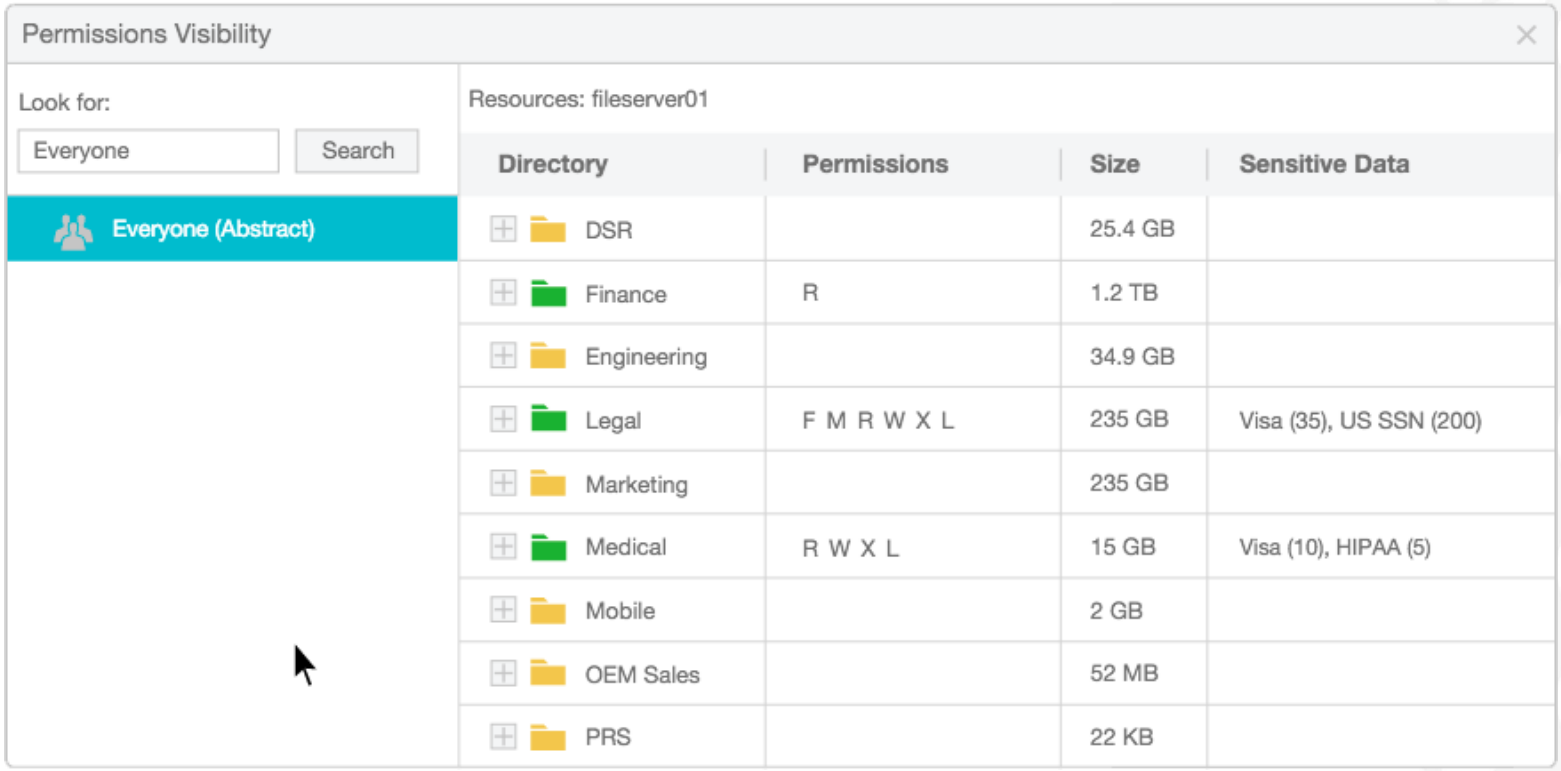
Automate authorization

Automate entitlement reviews

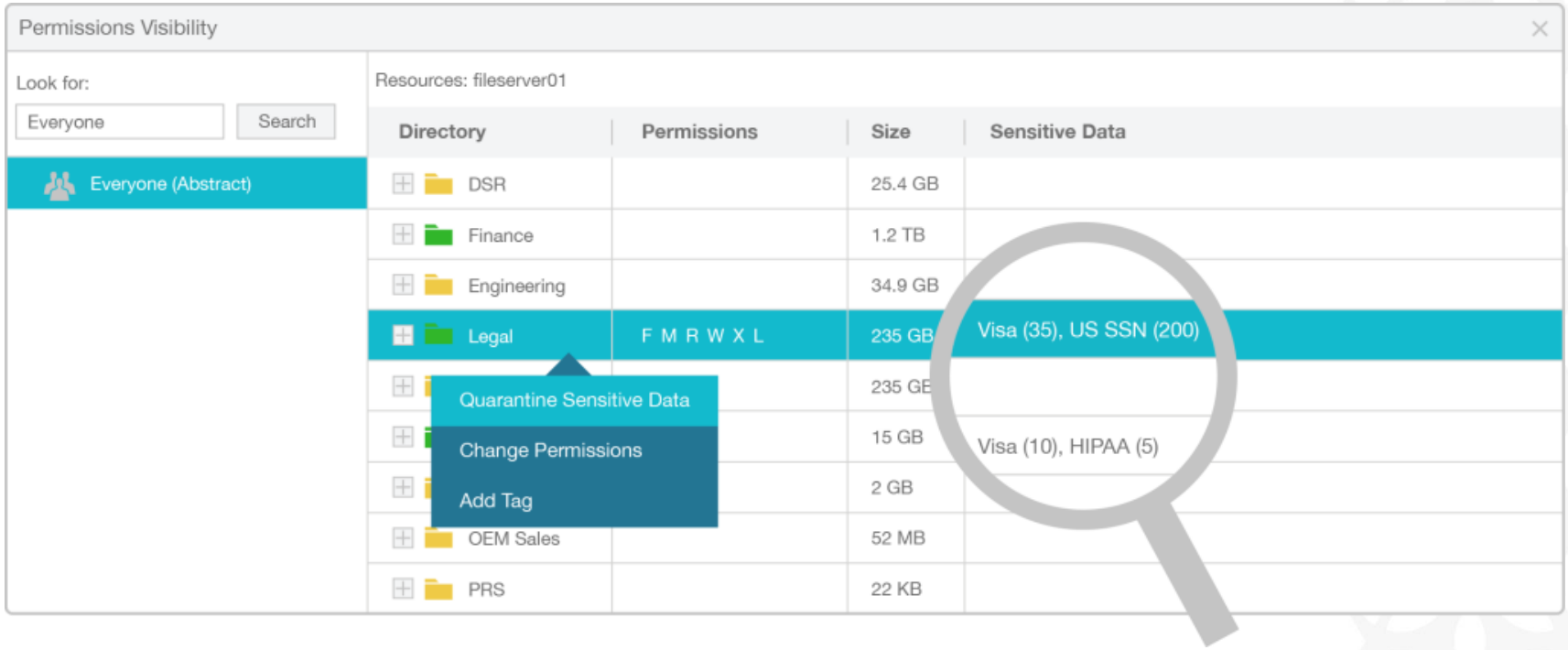


Detect

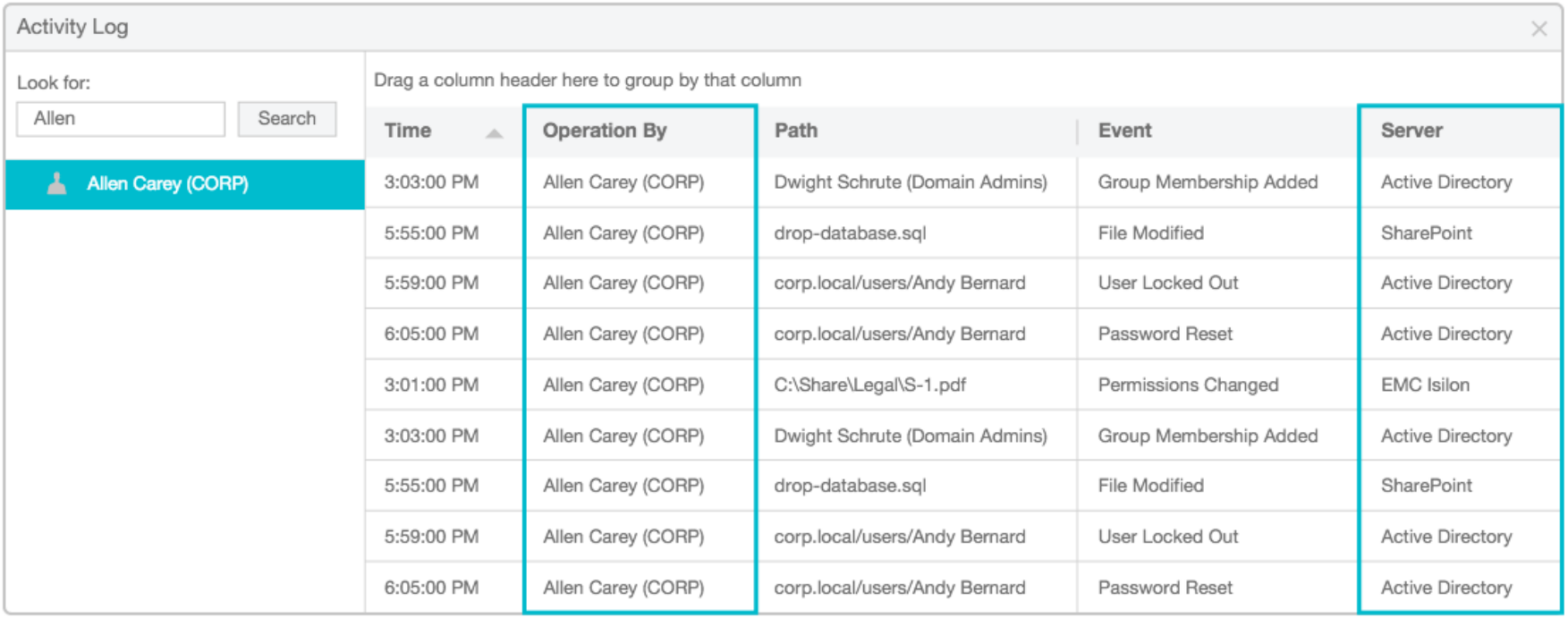
Map Your Environment (that's what hackers do!)



Classify Sensitive Information



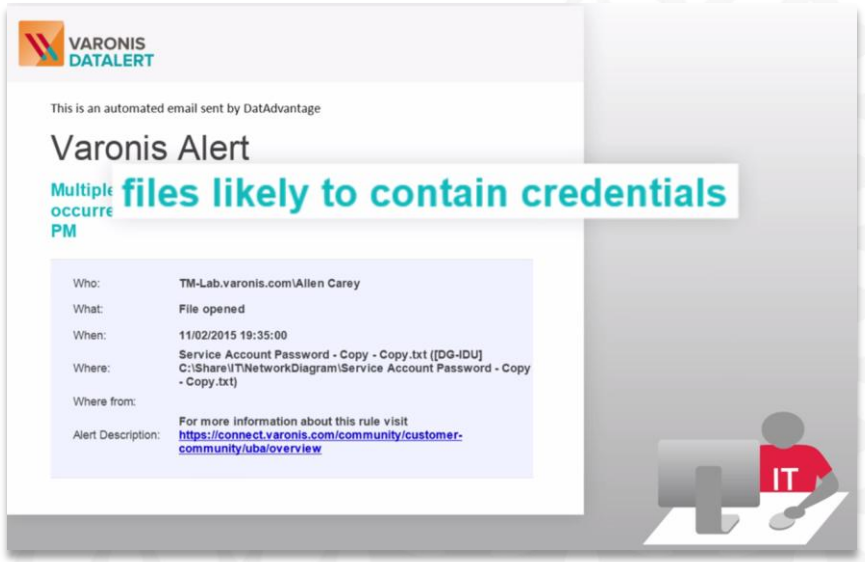
Enable Auditing (files, emails, AD, etc.)



Time	Operation By	Path	Event	Server
3:03:00 PM	Allen Carey (CORP)	Dwight Schrute (Domain Admins)	Group Membership Added	Active Directory
5:55:00 PM	Allen Carey (CORP)	drop-database.sql	File Modified	SharePoint
5:59:00 PM	Allen Carey (CORP)	corp.local/users/Andy Bernard	User Locked Out	Active Directory
6:05:00 PM	Allen Carey (CORP)	corp.local/users/Andy Bernard	Password Reset	Active Directory
3:01:00 PM	Allen Carey (CORP)	C:\Share\Legal\S-1.pdf	Permissions Changed	EMC Isilon
3:03:00 PM	Allen Carey (CORP)	Dwight Schrute (Domain Admins)	Group Membership Added	Active Directory
5:55:00 PM	Allen Carey (CORP)	drop-database.sql	File Modified	SharePoint
5:59:00 PM	Allen Carey (CORP)	corp.local/users/Andy Bernard	User Locked Out	Active Directory
6:05:00 PM	Allen Carey (CORP)	corp.local/users/Andy Bernard	Password Reset	Active Directory

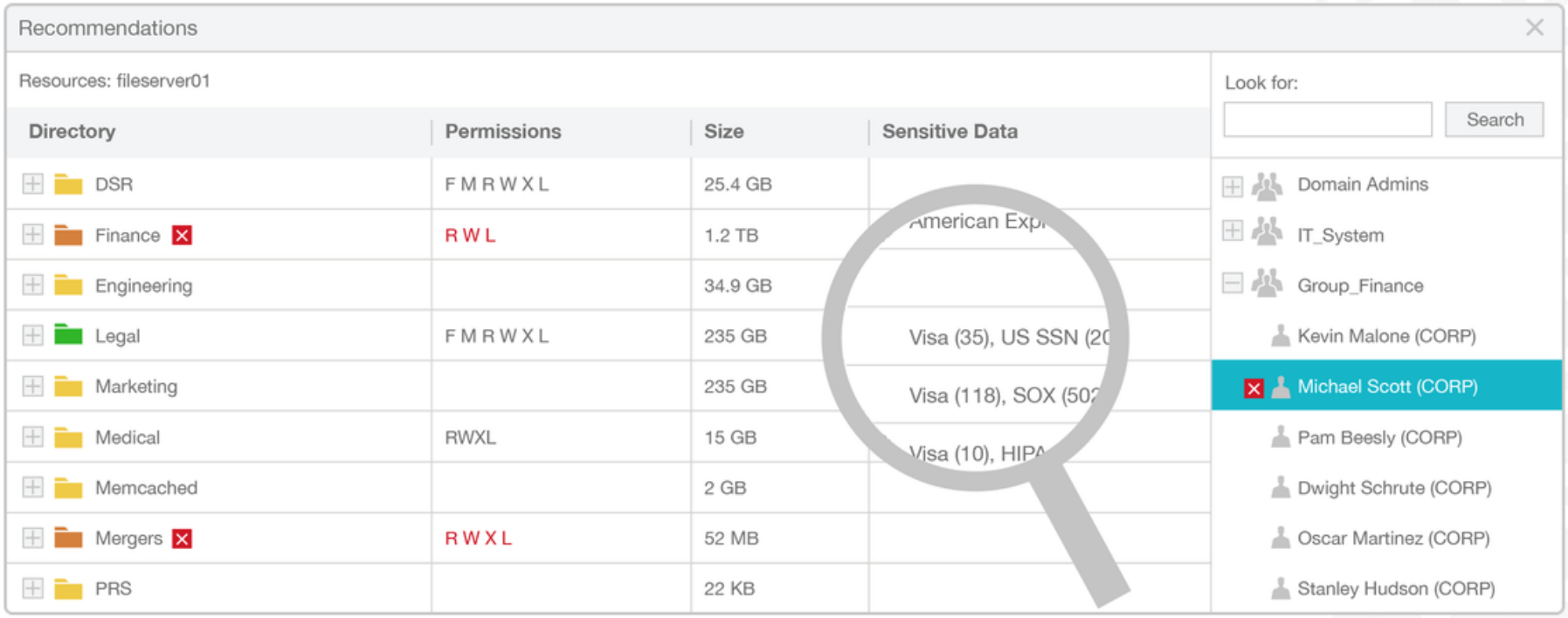
Alert on Suspicious Activity

- Behavioral activity spikes (email, files, access denied)
- Access to data not typical for a user (or service account)
- Multiple open events on files likely to contain credentials
- Abnormal access to sensitive data
- Abnormal access to stale data
- Critical GPO modified
- Privilege escalation (user added to Domain Admins)

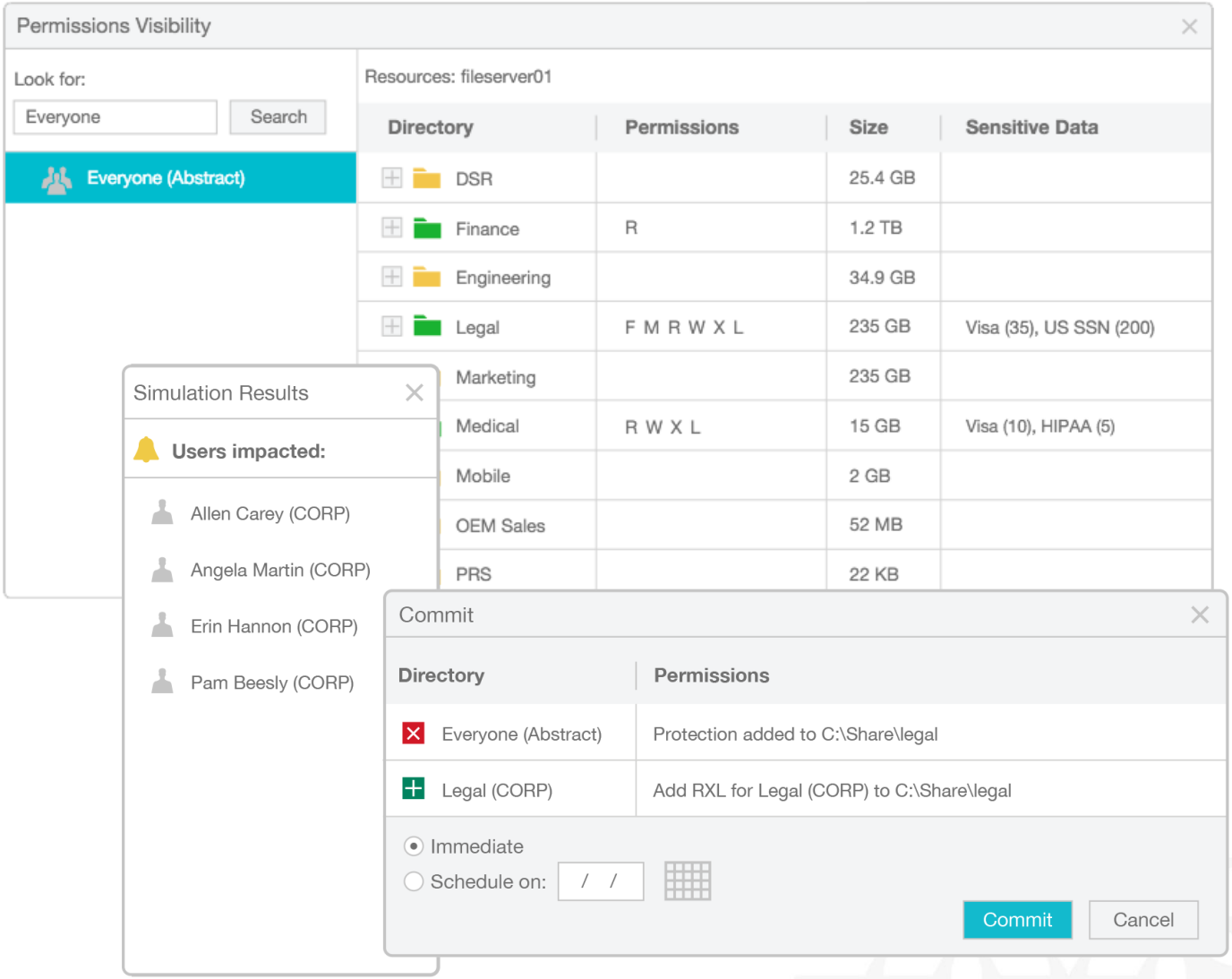


Prevent

Lockdown Sensitive Data



Eliminate Global Access



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

Eliminate Excessive Permissions

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

VARONIS

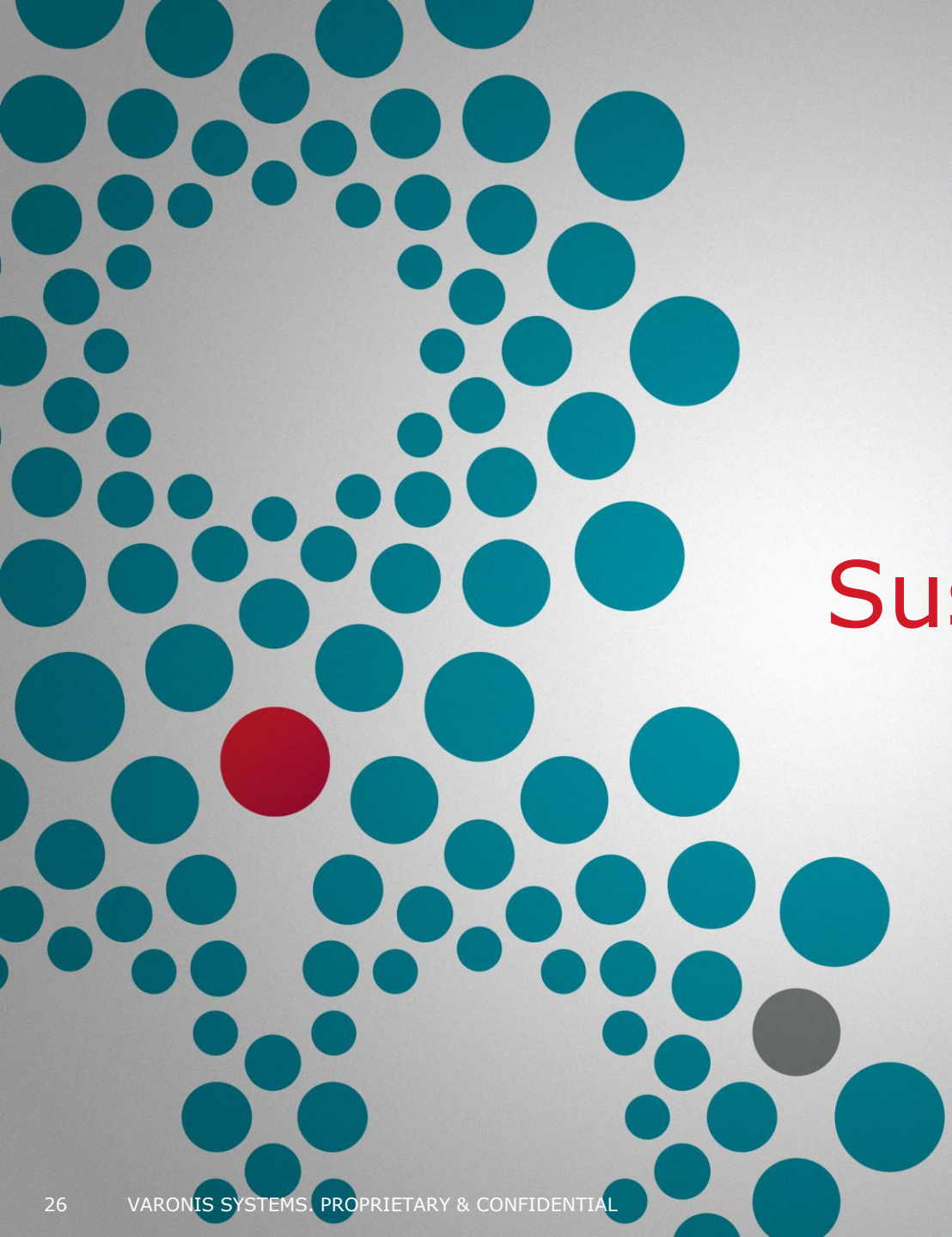
Nuke Dangerous Artifacts

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

Automation Engine

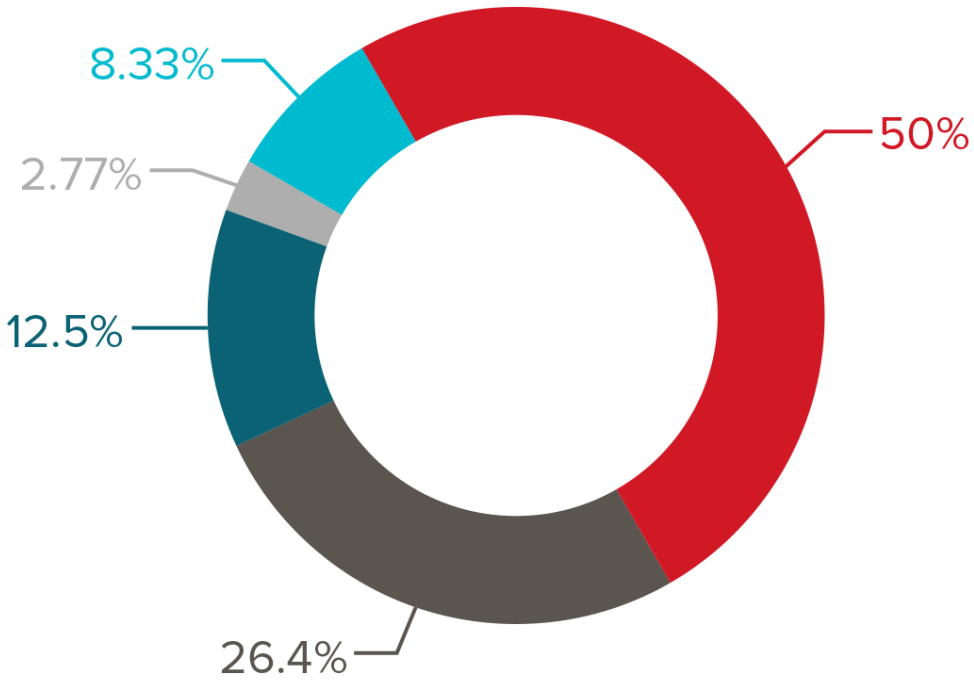
- Reduce risk non-disruptively by revoking excessive access permissions - Automatically
- Automatically repair and maintain file systems
- Detect and repair hidden security vulnerabilities like broken ACLs and Global Access to sensitive data.
- Comply with audit requirements without costly and laborious manual remediation projects.

*"The AE essentially allows us to remediate the broken and global access contradiction to **PbD** efficiently, accurately and without impacting the business."*



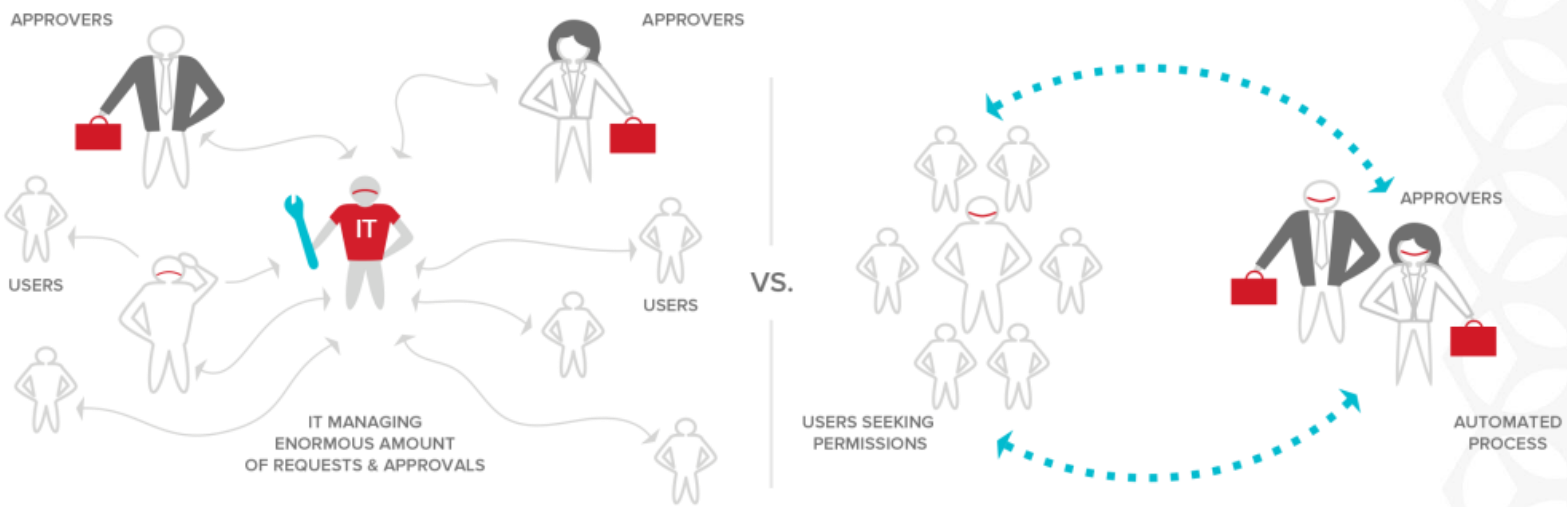
Sustain

Assign Ownership



- Allen Carey (CORP)
- Margaret Coakley (CORP)
- Crystal Grove (CORP)
- Andrew Weirich (CORP)
- Anne Thornton (CORP)

Automate Authorization

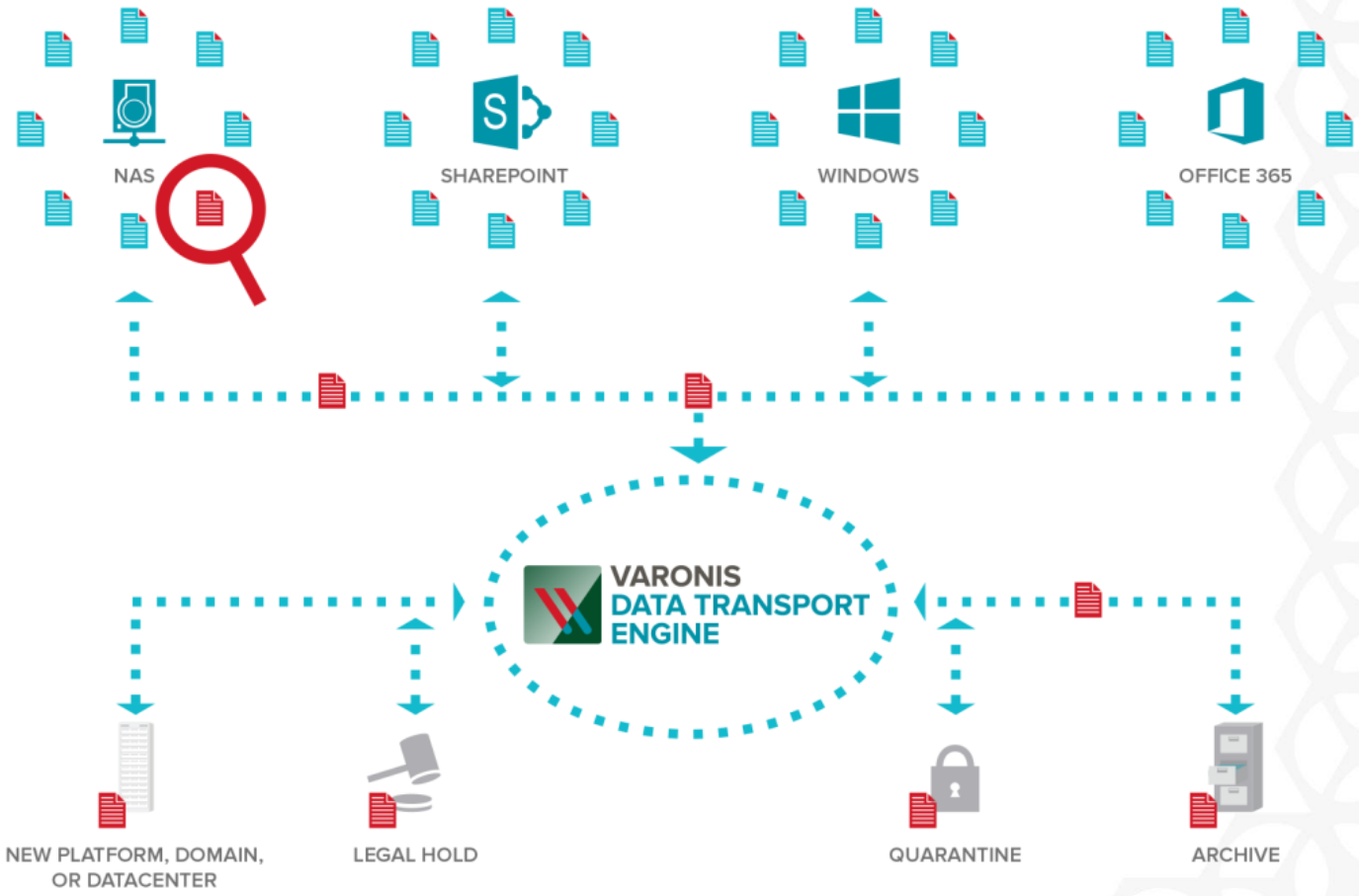


Subject: **Permissions request for Andy Bernard**
From: **Varonis DataPrivilege** <access@dundermifflin.com>

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

- (•) Approve
- ( ) Decline

Automate archiving and data migrations



General Data Protection Regulation

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.

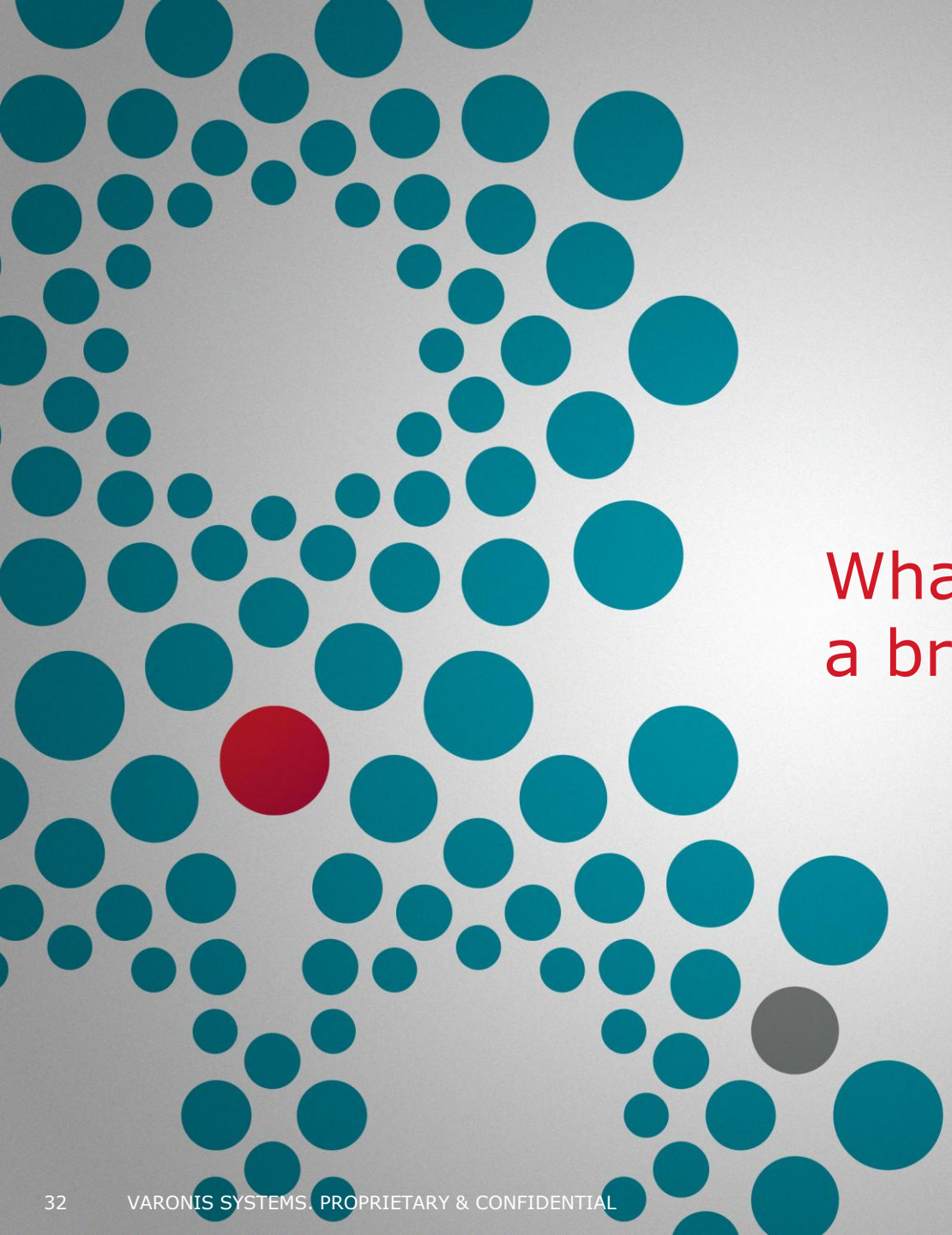
VARONIS

General Data Protection Regulation

How to Get There…cont.

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



What happens in a breach?

GDPR Article 33

“Notification of personal data breach to the supervisory authority within 72 hours”

Organisations are concerned they do not have the capability to meet this Article, particularly around access to data.

Varonis provides the ability to detect abnormal data breach activity, policy violations and real-time alert on it as it happens.

Anatomy of a Breach, or “Kill Chain”

Reconnaissance

Intrusion

Exploitation

Misconduct

Exfiltration

Privilege Escalation

Lateral Movement

Obfuscation (anti-forensics)

Denial Of Service

Example: Sony Breach – At a Glance

What data was exposed?

- **47,000** social security numbers
- Financial records and payroll information
- Personal data and addresses, visa and passport numbers, tax records
- Over **30,000** confidential business documents
- Embarrassing and incriminating C-level **email correspondence**
- **Private keys** to Sony's servers

How much did it cost?

- **$15,000,000** in cleanup
- **$35,000,000** for the fiscal year

VARONIS

Example: the Sony Breach Kill Chain

Reconnaissance – Attackers gained access with **stolen credentials** obtained with **phishing emails**, then downloaded tools to **map the environment.**

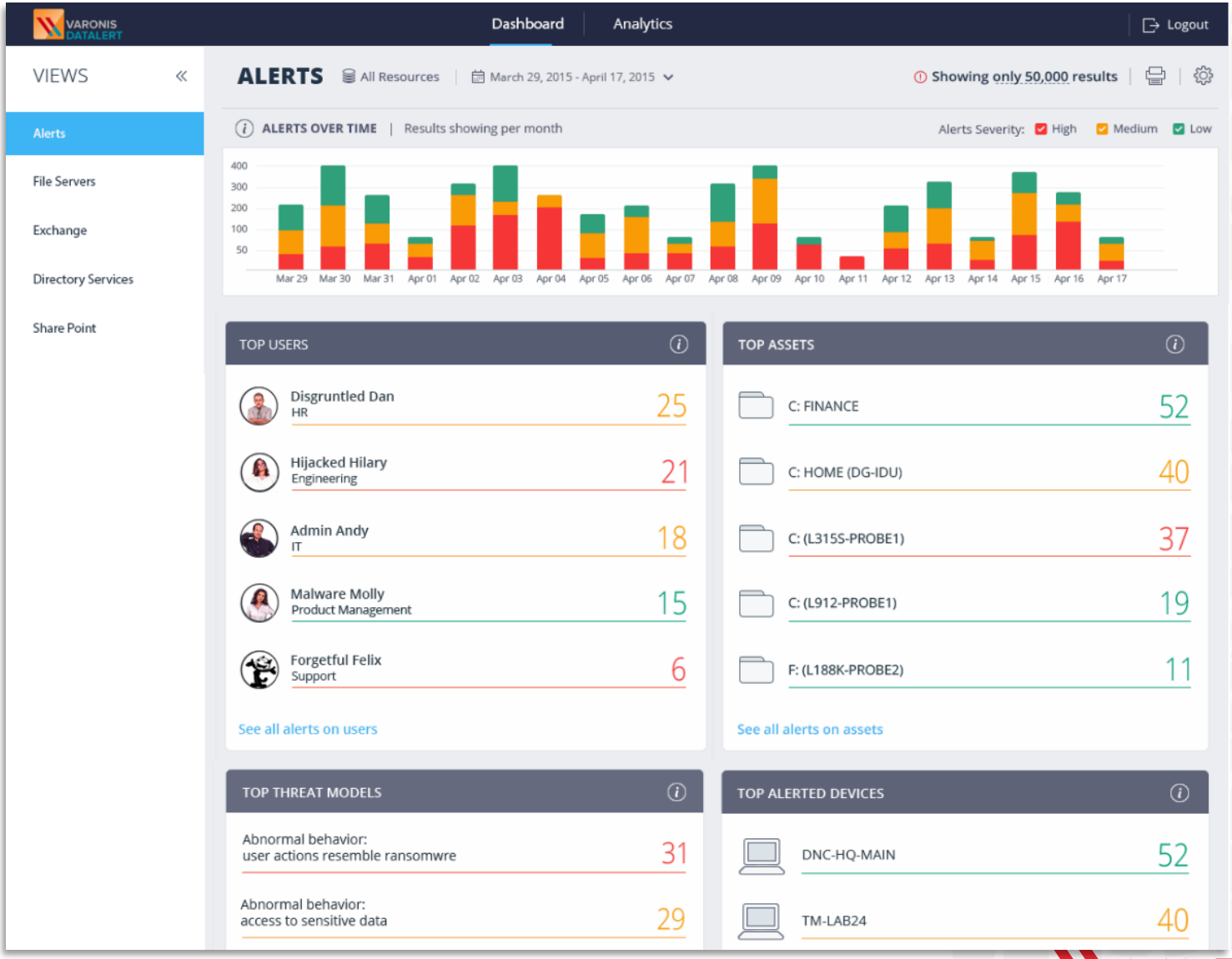
Intrusion – Wiper **malware** dropped on servers (with embedded employee credentials for execution)

Lateral movement – Attackers **located passwords** so they could continue to **expand or elevate rights**. They later released **usernames and passwords** for everything from internal systems to corporate Twitter accounts.

Privilege escalation – The attackers discovered treasure troves of **plain-text passwords** which gave them even more access to everything they needed to own the organization, including **certificates and RSA token information.**

Data exfiltration – **Hundreds of GB of sensitive data was released,** containing everything from **PII information** to **confidential business documents** including **budgets** and **upcoming projects**, to embarrassing **emails** between executives.

Alert to insider and cyber threat activity



VARONIS DATADVANTAGE | Overview | Events & Alerts | Alex Grant | Logout

Events Log | Alerts

ALERTS

All Resources | Last 24h

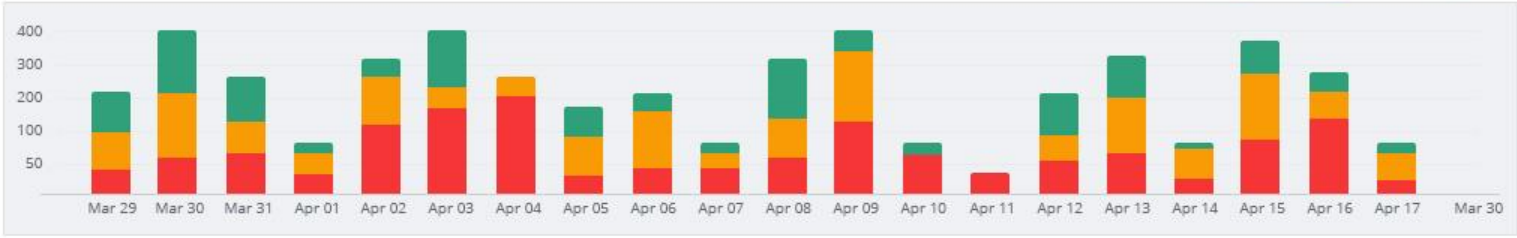
Alert Details | **Category** = Exfiltration

Found 1,000 Alerts within results: 300 ALERTS WITH HIGH SEVERITY | 638 ALERTS ON SENSITIVE DATA | 62 ALERTS BY ADMIN ACCOUNT

ALERTS

TIMELINE | 1 Day Per Column

Alerts Sevirety: High Medium Low



ALERTS LIST | Showing 100 of 1024 events

Column Picker

Drag column to Group By

User	Severity	Category	Assets	Rule	Event Count	Alert Count
John Williams	High	Exfiltration	PM-Windows1\c$\Docu...	Abnormal behavior:...	2 Events	1 Alerts
Aaron Jones	High	Exfiltration	PM-Windows1\c$\Docu...	Abnormal service be...	1 Events	1 Alerts
Bill Carlson	Medium	Exfiltration	PM-Windows1\c$\Docu...	Abnormal service be...	1 Events	1 Alerts

EXPLORE

2012 Connected events

REFINE

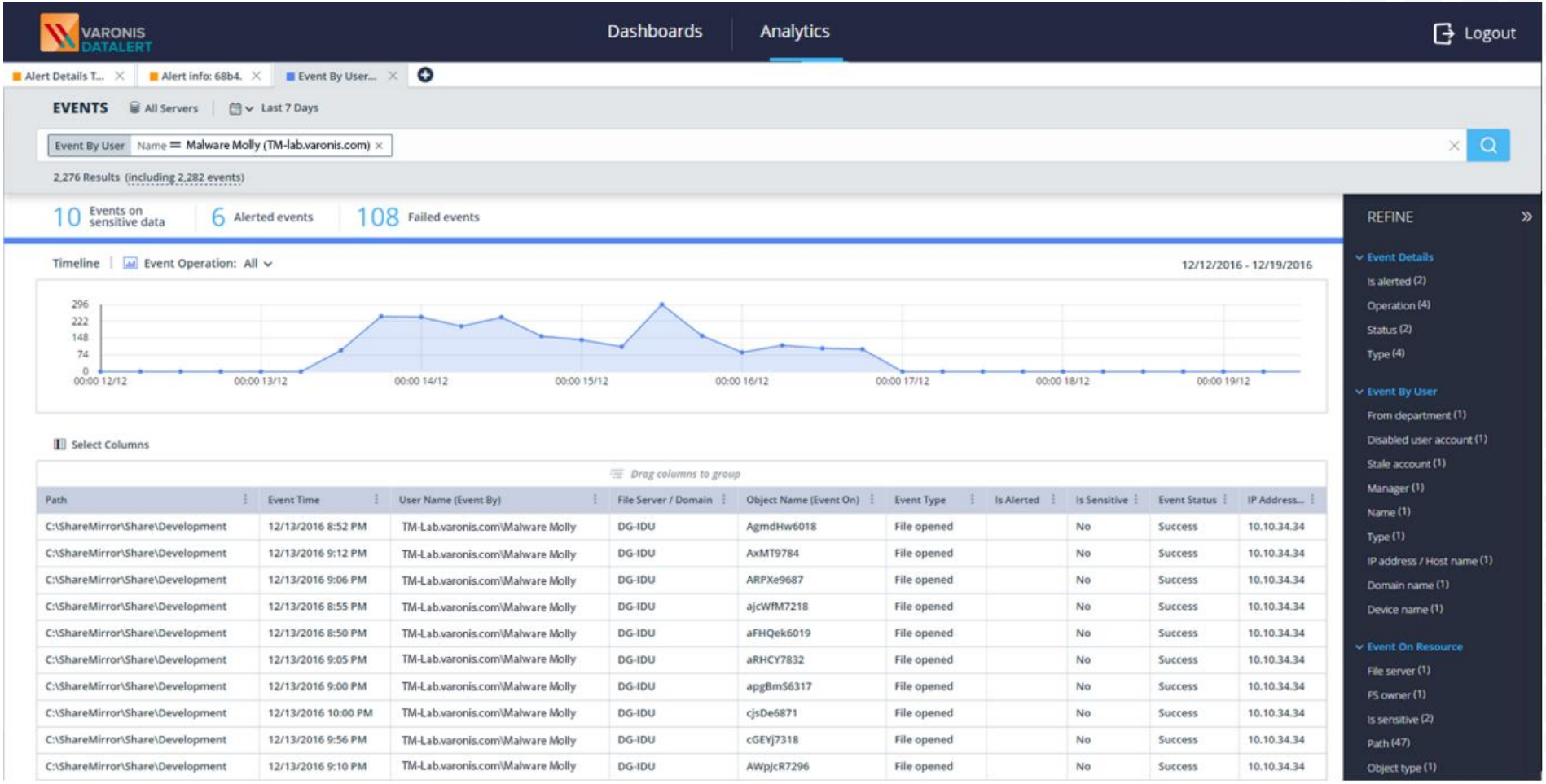
ALERTS DETAILS (1000)
- Category (12)
- Severity (2)
- Rules (2)

ALERTS BY USER (3)
- Users (742)
- Groups (34)
- Department (4)
- Location (2)

ALERTS ON RESOURCES (3)
- Object Type (1)
- Sensitive (100%)
- Managed Folders (30%)
- Size (0KB - 4.3GB)

Review Alerts

Investigate with hi-fidelity audit logs



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

CRITICAL | RECONNAISSANCE

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
Users
Device
Data
Time

SUMMARY | INVESTIGATION INSIGHTS

ABNORMAL AMOUNT OF ACCESSED FILES

USERS

Varonis\John Williams
QA Engineer

Is a **watch-list** user
Involved in 0 **alerts** in past 7 days
Is not a **disabled or deleted** account

1 Additional anomaly

DEVICES

2 Devices

First time use of RuthEvershed-PC in past 90 days
RuthEvershed-PC was involved in 4 **alerts** in past 7 days

1 Additional anomaly

DATA

24 Files

No **sensitive** files were affected
First time use of NetApp1\c$ in past 90 days

NEXT STEPS

INVESTIGATE ALERT

Alerted users
Alerted devices
Alerted data
Alerted events

INVESTIGATE ACTIVITY LEADIN TO ALERT

By alerted user(s)
By similar users
From alerted device(s)
On alerted data

LEARN ABOUT USUAL ACTIVITY

Alerted user(s) 30 days back
Similar users 30 days back
Alerted device(s) 30 days back
[illegible] days back

MORE ACTIONS

Investigate

Free Data Risk Assessment

Get your **free** GDPR **Readiness** Assessment

Our team will do all the heavy-lifting for you: setup, configuration, and analysis with concrete steps to improve your General Data Protection Regulation compliance.

YOUR DEDICATED ENGINEER WILL HELP YOU:

- Identify in-scope GDPR data
- Find and revoke excessive access to personal information
- Audit user activity and detect risky behaviour / ransomware
- Identify and prioritize gaps in GDPR compliance

Schedule your assessment!

Get in Touch:

UK: +0-800-756-9784 **US:** +1-877-292-8767 **INTL:** +1-646-706-7336

info.varonis.com/gdpr-risk-assessment

About Varonis

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Through an innovative software platform, Varonis allows organizations to analyse, secure, manage, and migrate their volumes of unstructured data. Varonis specializes in file and email systems that store valuable spreadsheets, word processing documents, presentations, audio and video files, emails, and text. This rapidly growing data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. IT and business personnel deploy Varonis software for a variety of use cases, including data security, governance and compliance, user behaviour analytics, archiving, search, and file synchronization and sharing.

Take aways from today

- What are the steps your organisation is going to take to address GDPR?
- How will you evidence that all GDPR data is accounted for and governed?
- How will you detect and prevent a data breach or provide full forensics?
- How will you mitigate data breach risk from open access with limited resources or understanding of your data?
- How can the business or auditors measure the success of our efforts?

Thank you

Matt Lock
mlock@varonis.com
+44 7795 153 900