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

Introduction to Varonis

April 2017

Who Am I

- Scott Walker
- Sales Engineer, Team Leader
- swalker@varonis.com
- +44 203 695 3905

Agenda

- Varonis – Who Are We?
- What is 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 do I detect it?
- Free Data Risk Assessments

About Varonis

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

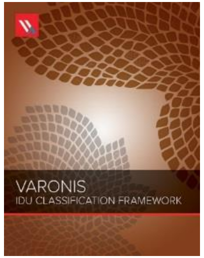
NASA

TOYOTA

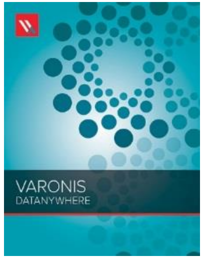
BOSTON UNIVERSITY

GDF SUEZ

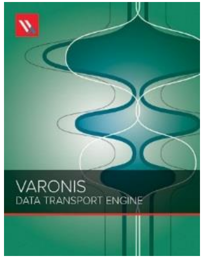
ING



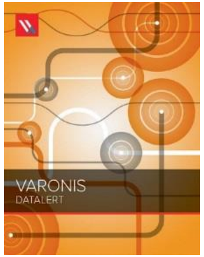
VARONIS
IDU CLASSIFICATION FRAMEWORK



VARONIS
DATANYWHERE



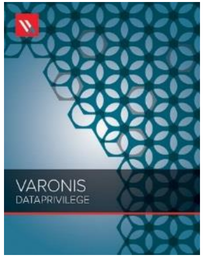
VARONIS
DATA TRANSPORT ENGINE



VARONIS
DATALERT

VARONIS
DATANSWERS

VARONIS
DATADVANTAGE for Windows



VARONIS
DATAPRIVILEGE

VARONIS

The Varonis Origin Story

- Our company's founding story is actually quite relevant to this talk.
- Our co-founders, Yaki Faitelson and Ohad Korkus, were working for NetApp on project for a client in Angola, on the western coast of Africa. The client had taken hi-resolution digital photos of the ocean floor at great expense, and stored them on their NetApp filers. And one day, they were gone. Deleted.
- The likely questions followed:
  - Who did it?
  - How did it happen?
  - Who had access to them?
  - Was it a competitor?
  - Was it an accident?
  - A hacker?
  - An insider?
- **Nobody knew**
- And so Varonis was born to give companies more visibility and protection for their high value information.

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.

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.

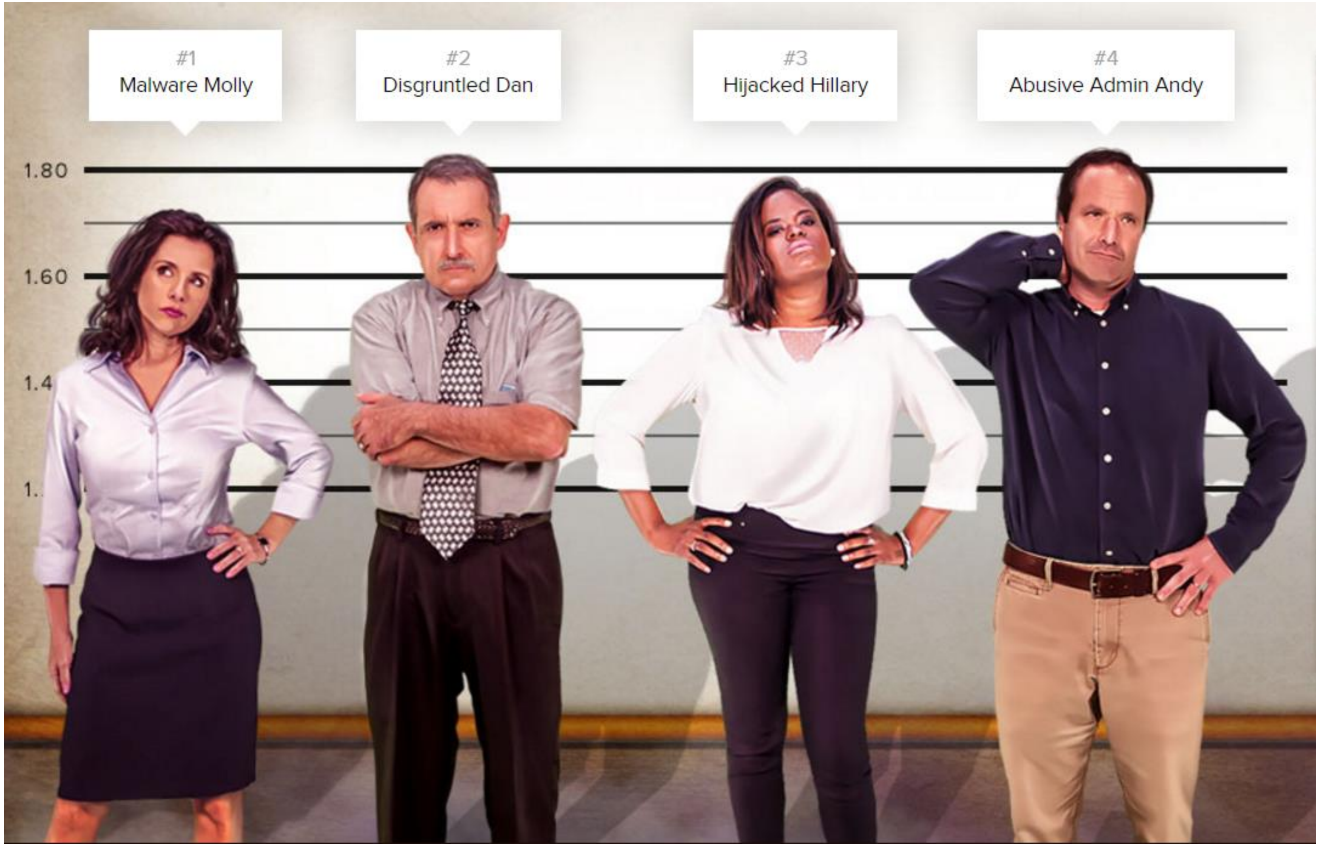
What are the new requirements?

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

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

Fundamental Unanswered Questions

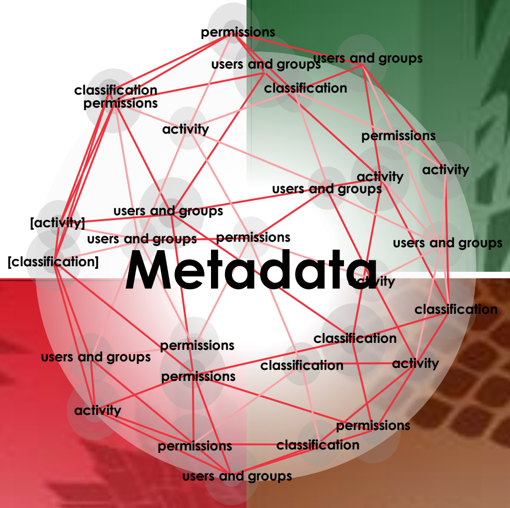
There are many questions IT and the business can't answer:

- 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?

VARONIS

Where Varonis Starts

The picture can't be displayed.



Permissions Information

knowing who can access what data

Access Activity

knowing which users do access what data, when and what they've done

Content Information

knowing which files contain sensitive and important information

Varonis Methodology

DETECT

insider threats and security threats by analysing data, account activity, and user behaviour.

PREVENT

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

SUSTAIN

a secure state by automating authorisations, migrations, and disposition.

Detect

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

The picture can't be displayed.

Classify Sensitive Information

The picture can't be displayed.

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

The picture can't be displayed.

Alert on Suspicious Activity

- Behavioural 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)

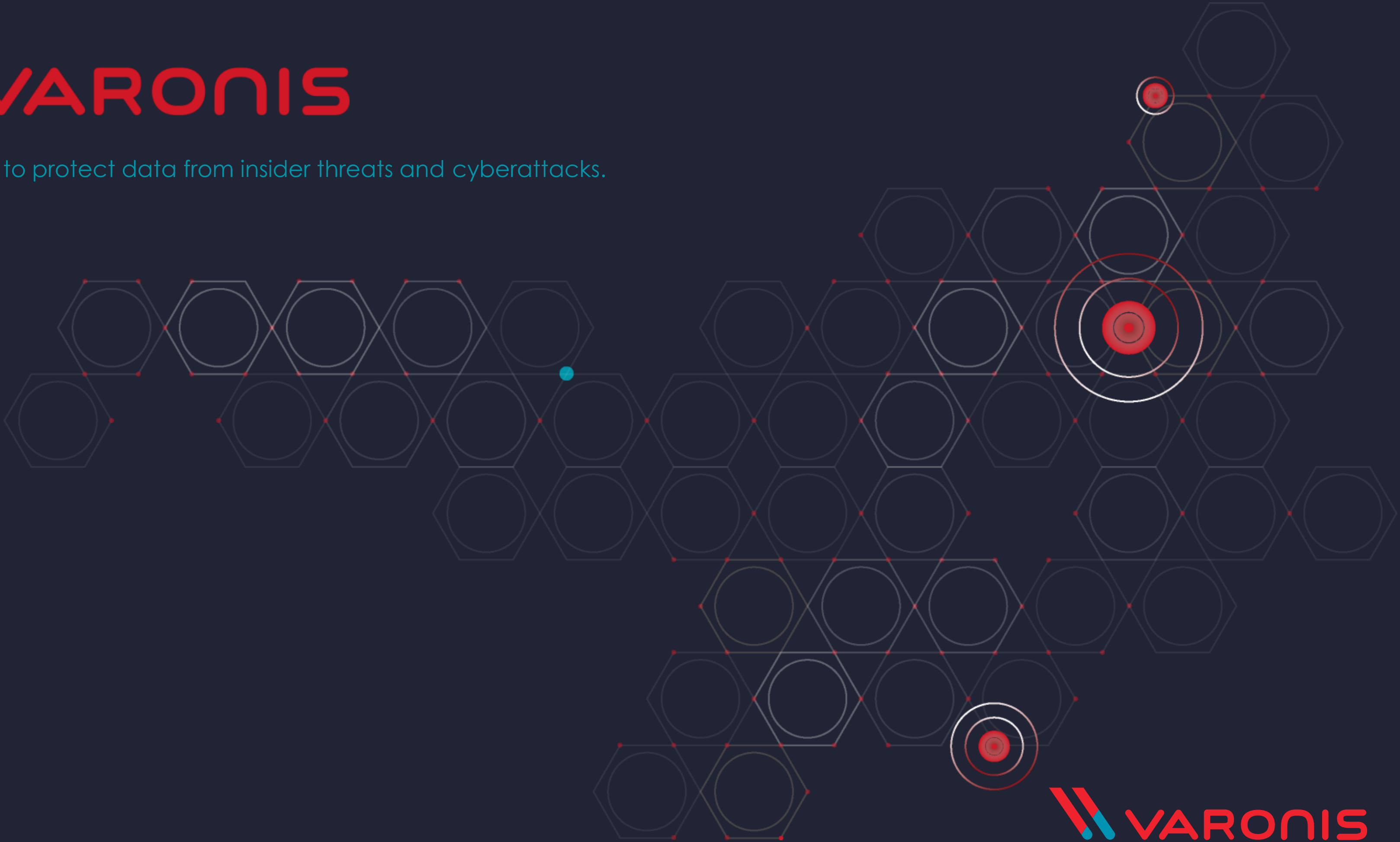
Prevent

Lockdown Sensitive Data

The picture can't be displayed.

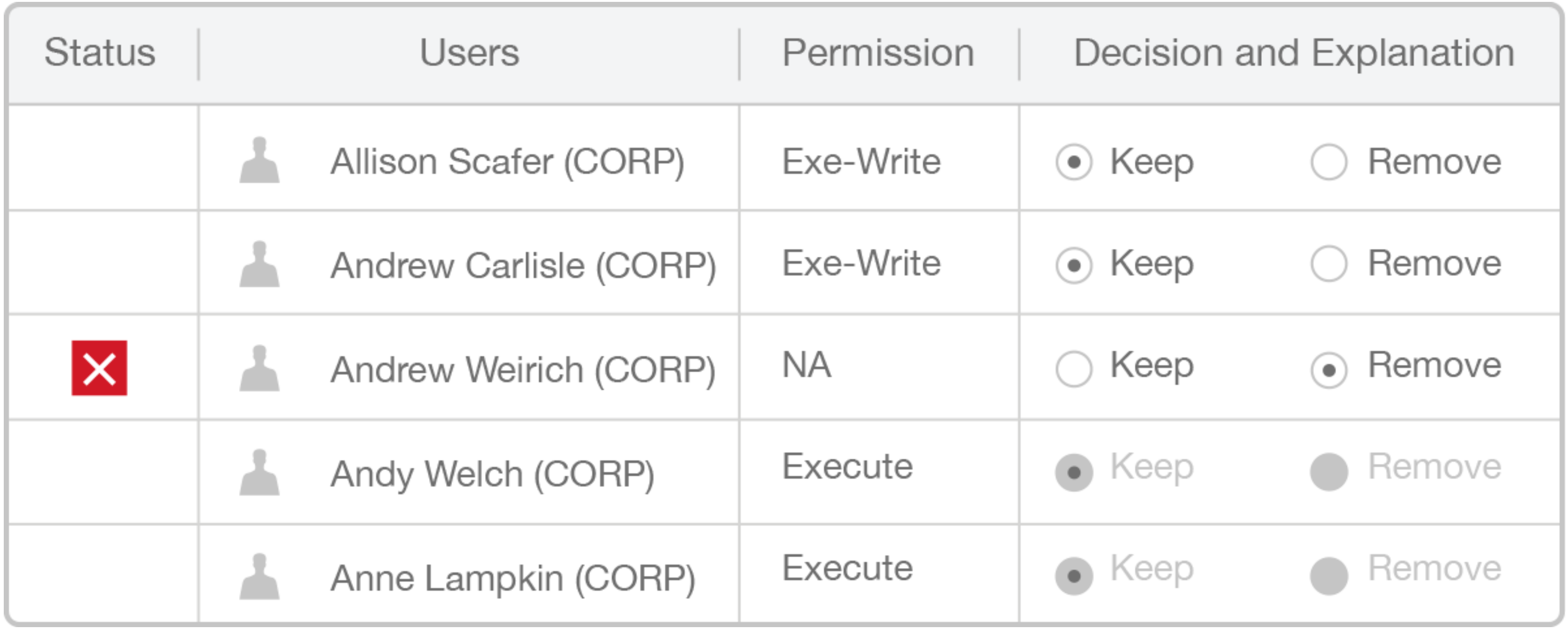
VARONIS

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



VARONIS

Eliminate Excessive Permissions



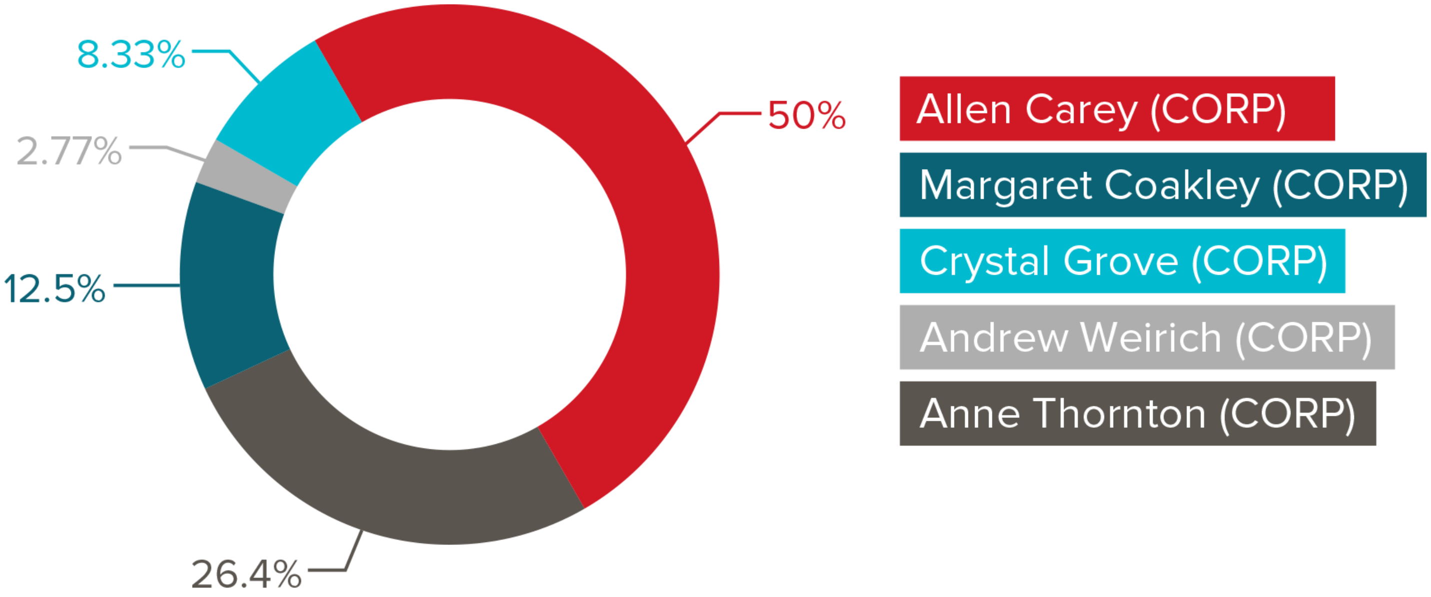
Status	Users	Permission	Decision and Explanation	
	Allison Scafer (CORP)	Exe-Write	◉ Keep	○ Remove
	Andrew Carlisle (CORP)	Exe-Write	◉ Keep	○ Remove
☒	Andrew Weirich (CORP)	NA	○ Keep	◉ Remove
	Andy Welch (CORP)	Execute	◉ Keep	● Remove
	Anne Lampkin (CORP)	Execute	◉ Keep	● Remove

Nuke Dangerous Artifacts

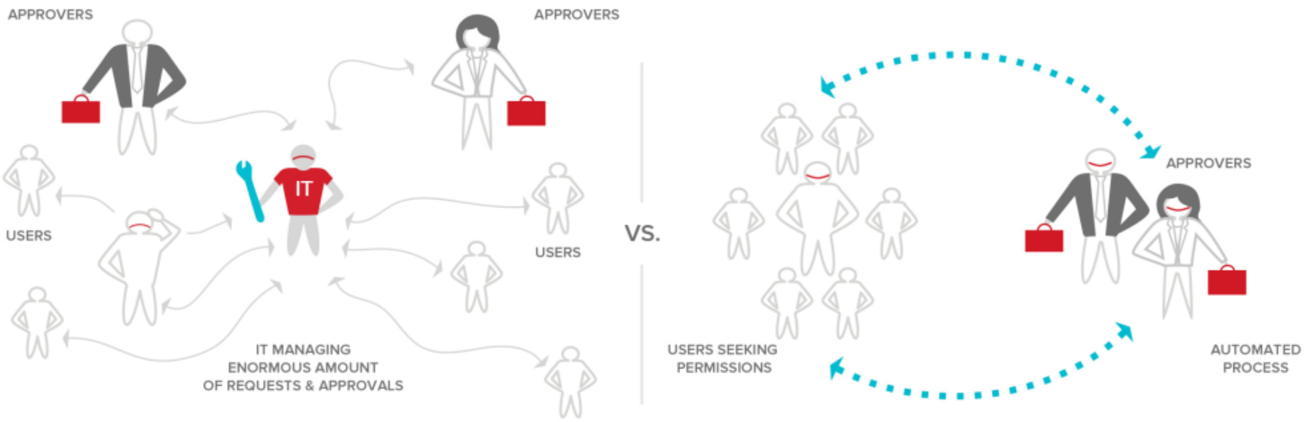
- Inactive users and groups
- Overly delegated groups
- Looped nested groups
- Broken ACLs
- Folders with unique permissions
- Stale data
- Delegated tasks in AD

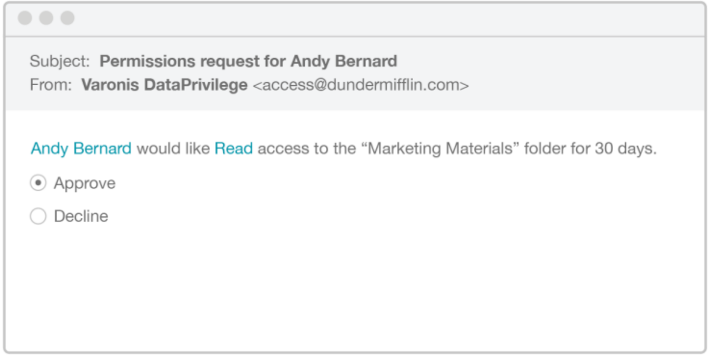
Sustain

Assign Ownership



Automate Authorization


APPROVERS
APPROVERS
IT
USERS
USERS
IT MANAGING ENORMOUS AMOUNT OF REQUESTS & APPROVALS
VS.
APPROVERS
USERS SEEKING PERMISSIONS
AUTOMATED PROCESS



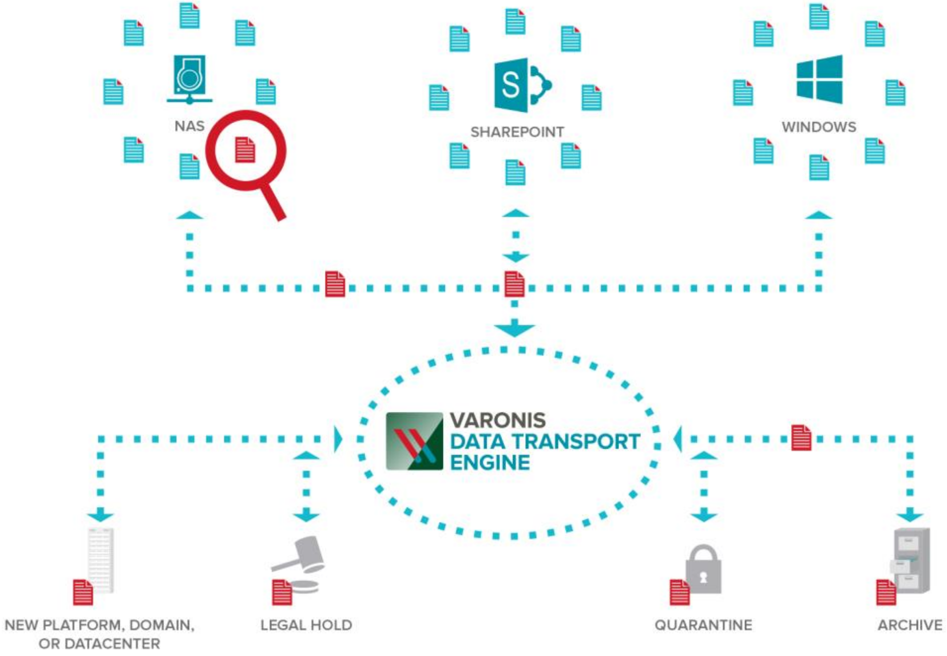
Subject: **Permissions request for Andy Bernard**
From: **Varonis DataPrivilege** <access@dundermifflin.com>

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:

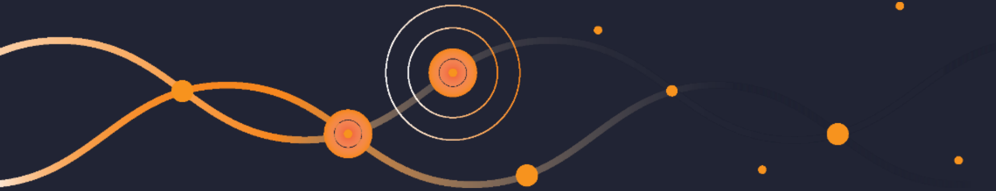
GDPR Article	What does it mean	How to address it
Article 25: Data Protection by Design and By Default	Embrace “Accountability and Privacy by Design” as a business culture.	Safely remediate access controls to Least Privilege.
Article 30: Records of Processing Activities	Implement technical and organizational 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

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.



What happens in a breach?

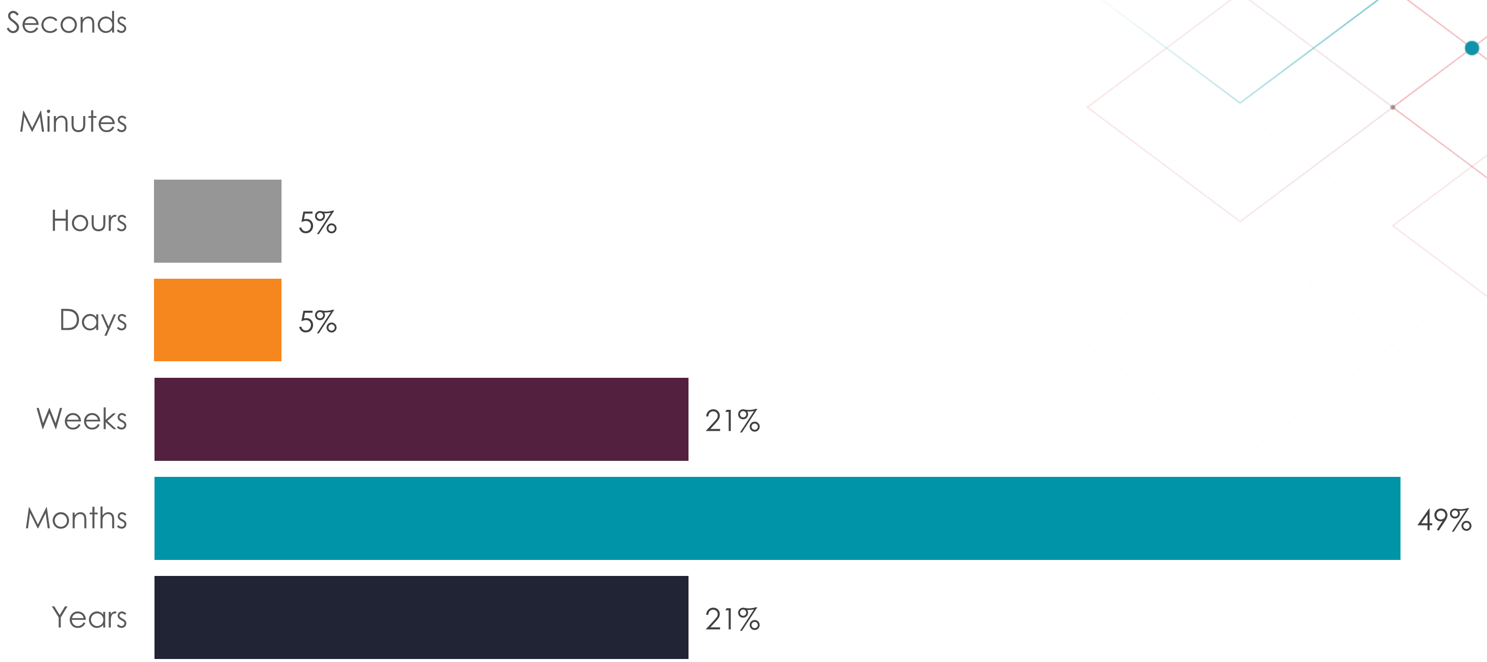
GDPR Article 33

"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.

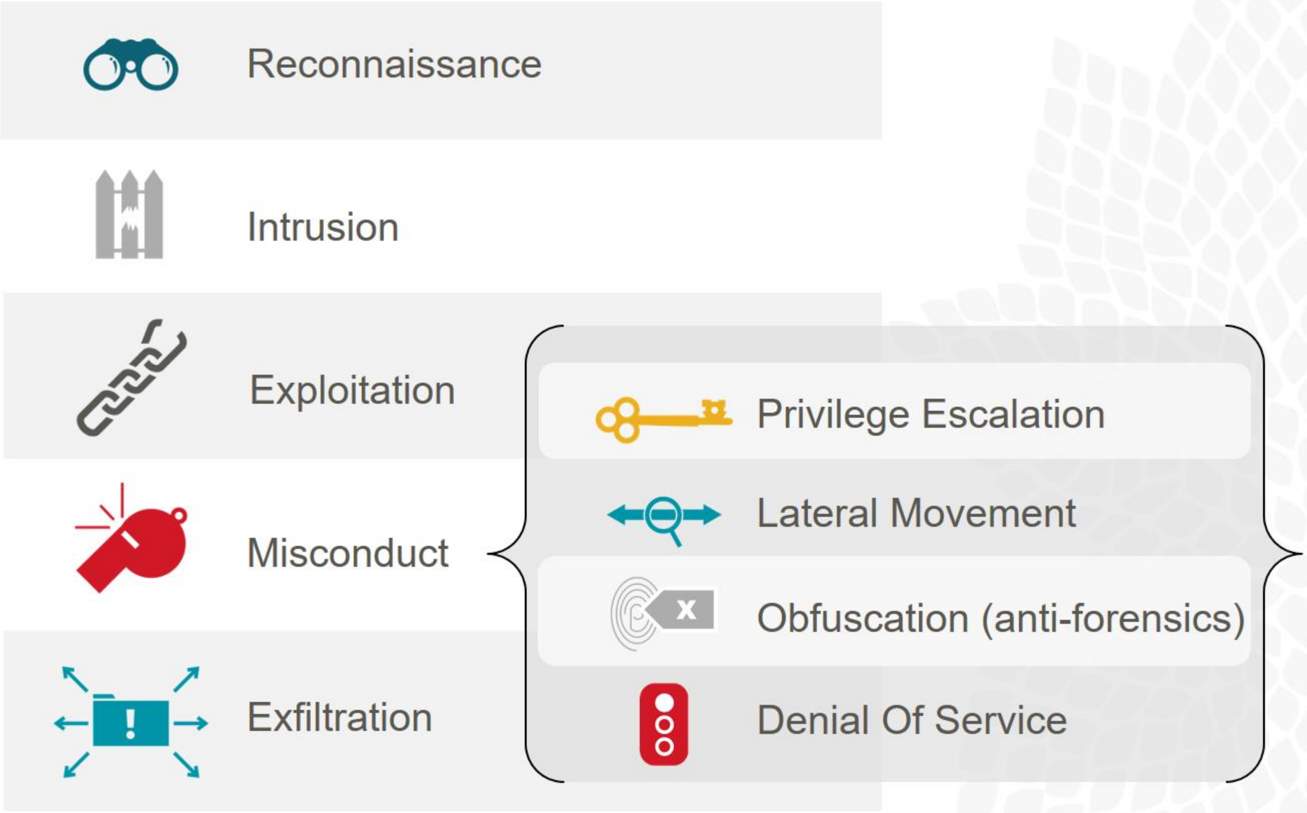
Varonis provides the ability to detect abnormal data breach activity, policy violations and real-time alert on it as it happens.

Data Breaches - Discovery Timeline



Source: Verizon 2016 Data Breach Investigations Report

Anatomy of a Breach, or “Kill Chain”



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

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.**

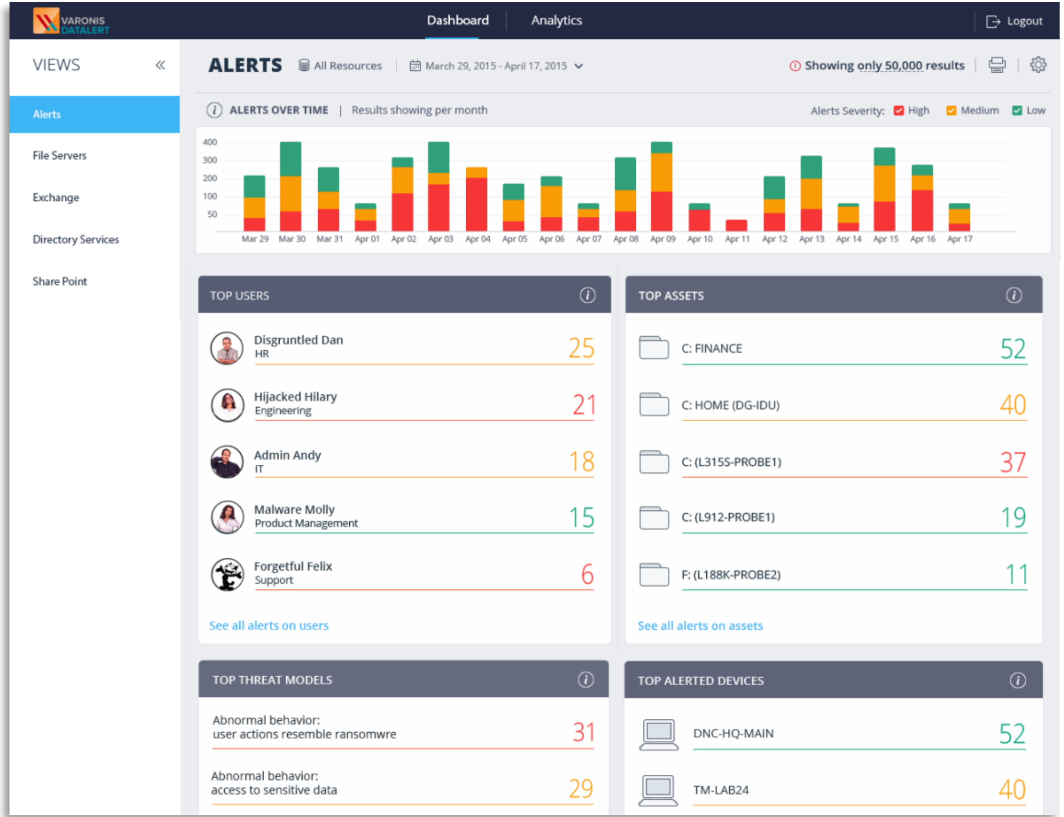
Intrusion – Wiper **malware** dropped on servers (with embedded employee credentials for execution)

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



TOP USERS

Disgruntled Dan HR	25
Hijacked Hilary Engineering	21
Admin Andy IT	18
Malware Molly Product Management	15
Forgetful Felix Support	6

See all alerts on users

TOP ASSETS

C: FINANCE	52
C: HOME (DG-IDU)	40
C: (L315S-PROBE1)	37
C: (L912-PROBE1)	19
F: (L188K-PROBE2)	11

See all alerts on assets

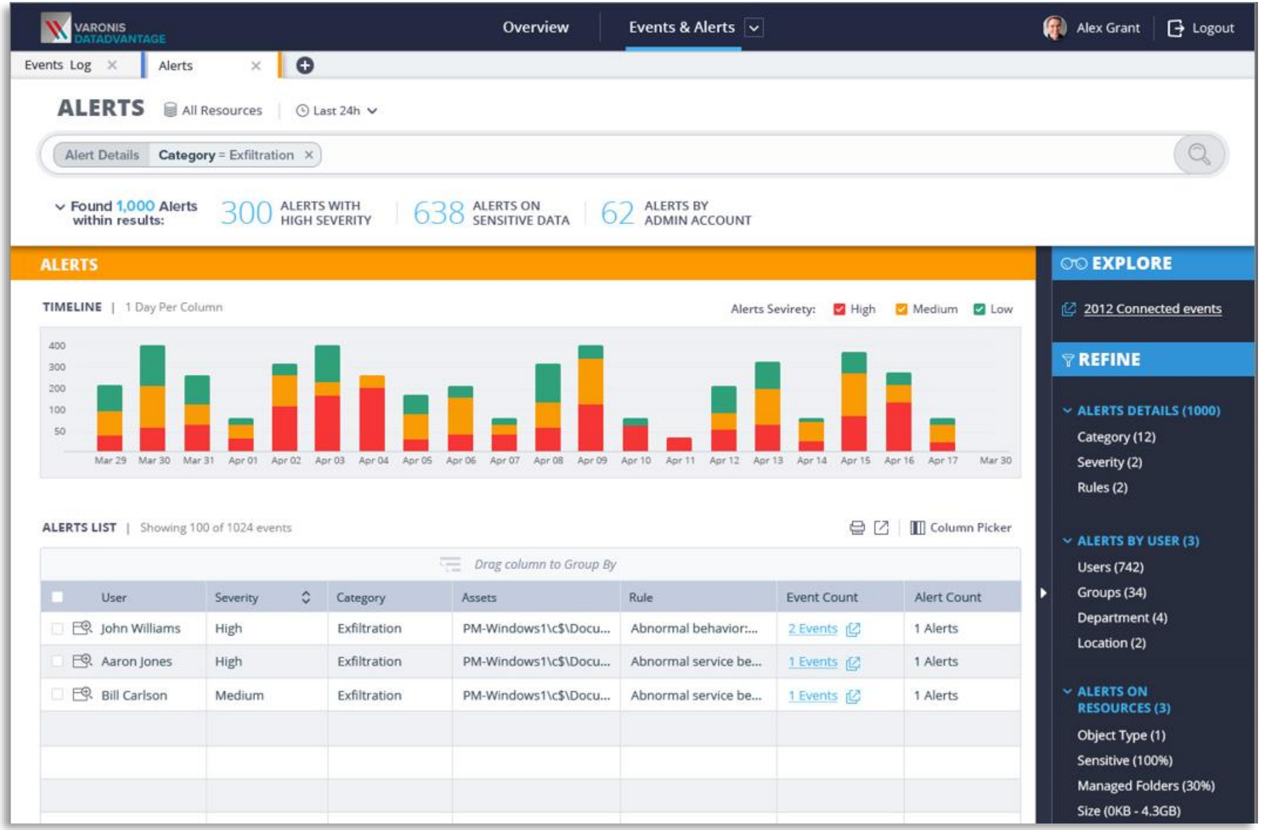
TOP THREAT MODELS

Abnormal behavior: user actions resemble ransomwre	31
Abnormal behavior: access to sensitive data	29

TOP ALERTED DEVICES

DNC-HQ-MAIN	52
TM-LAB24	40

Review Alerts



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

2012 Connected events

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

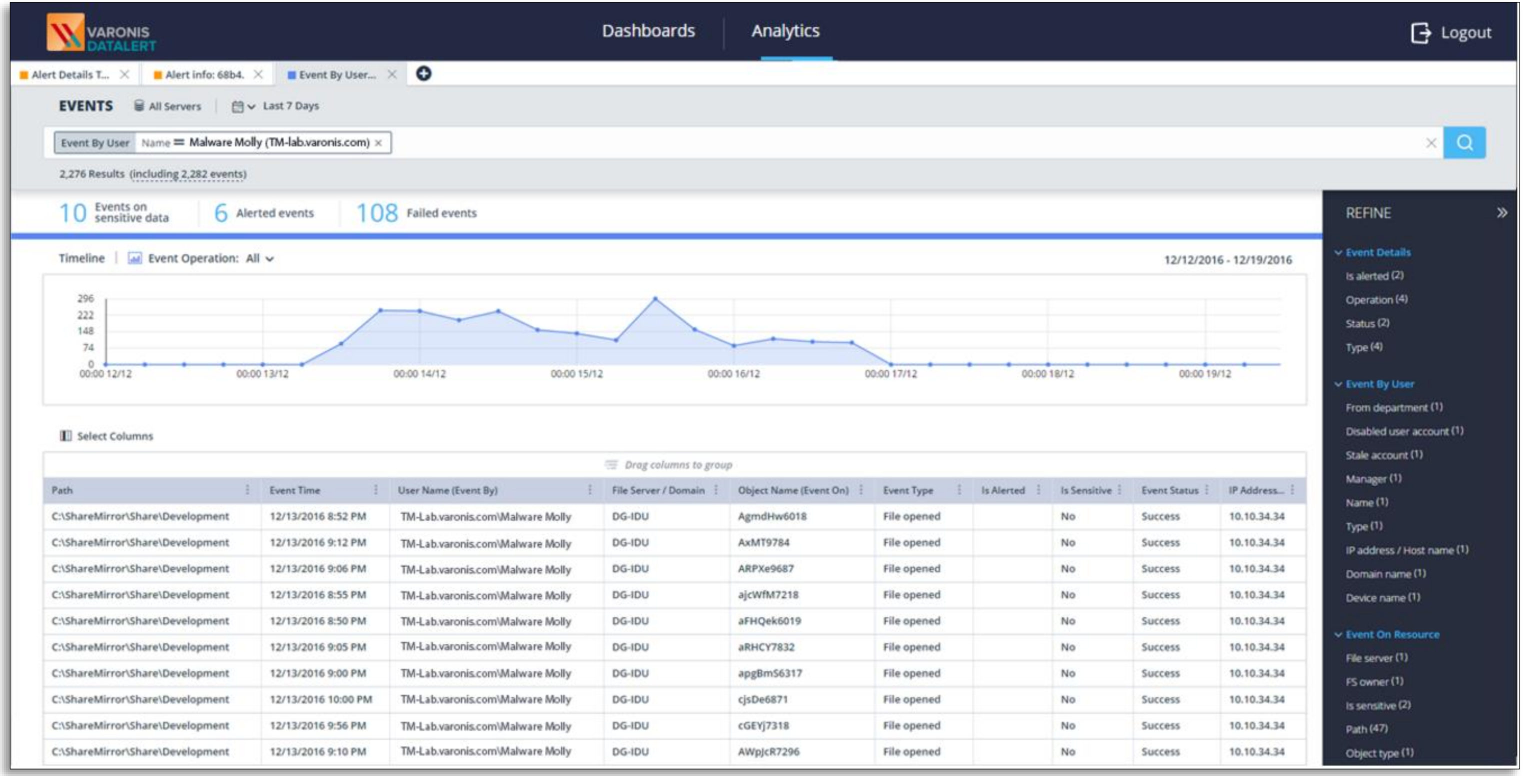
ALERTS BY USER (3)
- Users (742)
- Groups (34)
- Department (4)
- Location (2)

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

ALERTS LIST | Showing 100 of 1024 events

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

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

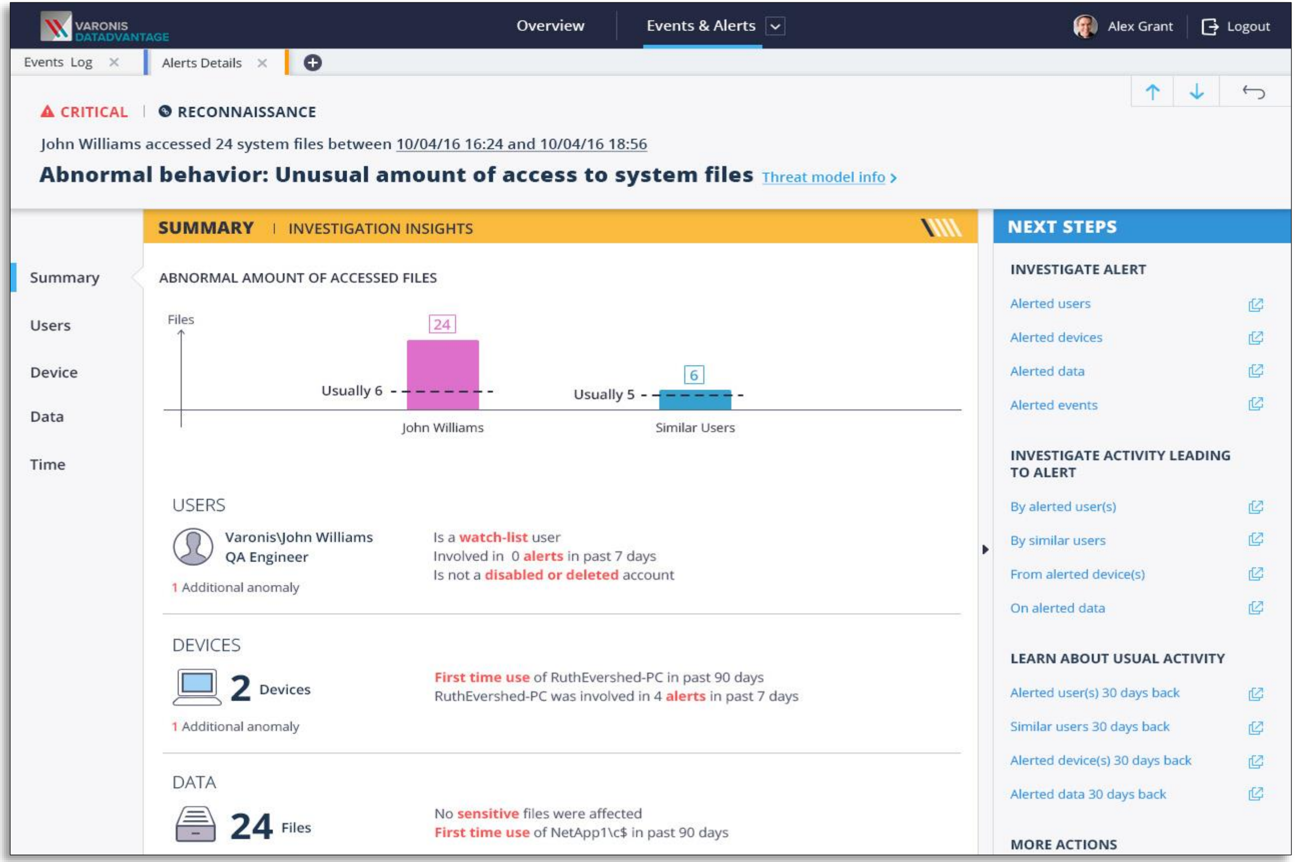
Path	Event Time	User Name (Event By)	File Server / Domain	Object Name (Event On)	Event Type	Is Alerted	Is Sensitive	Event Status	IP Address...
C:\ShareMirror\Share\Development	12/13/2016 8:52 PM	TM-Lab.varonis.com\Malware Molly	DG-IDU	AgmdHw6018	File opened		No	Success	10.10.34.34
C:\ShareMirror\Share\Development	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)

Investigate User Profiling



VARONIS DATADVANTAGE

Overview | Events & Alerts | Alex Grant | Logout

Events Log × | Alerts Details ×

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

1 Additional anomaly

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

DEVICES

2 Devices

1 Additional anomaly

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

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 LEADING 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
- Alerted data 30 days back

MORE ACTIONS

VARONIS

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

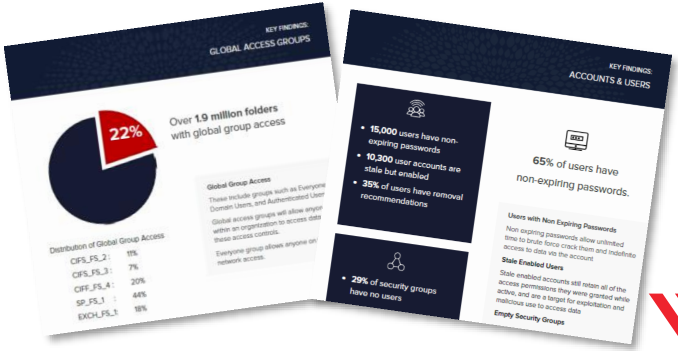
Schedule your assessment!

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.



KEY FINDINGS:
GLOBAL ACCESS GROUPS

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

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.

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%

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

Thank You

Scott Walker
Sales Engineer, Team Leader
swalker@varonis.com
+44 203 695 3905