

Mitigating IT Risks with Data Classification and Access Control



Tim Warner

AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim

techtrainertim.com



Microsoft
CERTIFIED
Trainer
Solutions Expert
Cloud Platform and
Infrastructure



Jeff Melnick

MANAGER OF SYSTEMS ENGINEERING,
NETWRIX

Jeff.Melnick@netwrix.com

netwrix

Overview

"Fireside chat" format

- Tim introduces a subject
- Jeff answers a related question

Jeff then presents on Netwrix

Attendee Q/A

GDPR

General Data Protection Regulation (25 May 2018)

European Union (EU)

Aims to give citizens greater control over their personal data

"Businesses here in the US might have heard of GDPR but not believe it affects them. Please explain how GDPR may indeed affect US organizations."

Question for Jeff





Data Classification

The process of organizing data into categories for its most effective and efficient use. This can be of particular importance for risk management, legal discovery, and compliance.

Microsoft File Classification Infrastructure (FCI)

Windows Server
feature

Rules for
automatically
classifying files

Classify by
location, content,
PII

Take actions:
encryption, move,
etc.

Admins can
perform manually
classification

Dynamic Access
Control (DAC)



Boldon James

A UK-based software company incorporated in February 1985, and specializing in data classification and secure messaging solutions aimed primarily at the commercial, defense, intelligence and government marketplaces.

"Some discovery/auditing software uses Boldon James keyword classification. What does Netwrix use, and why?"

Question for Jeff



"What are the risks for data classification implementation? How can a business avoid pitfalls in data classification initiatives?"

Question for Jeff





Access Control

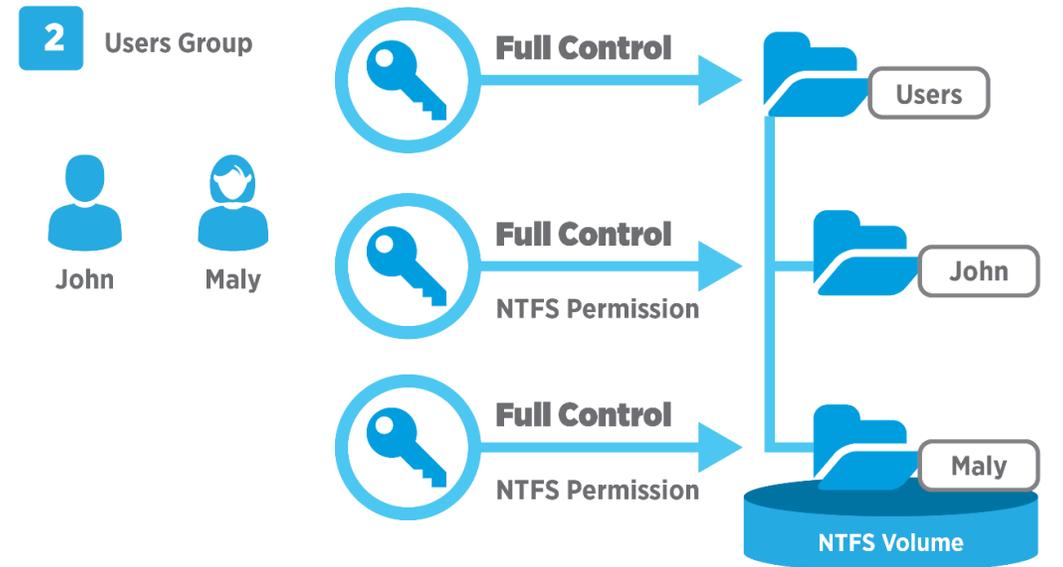
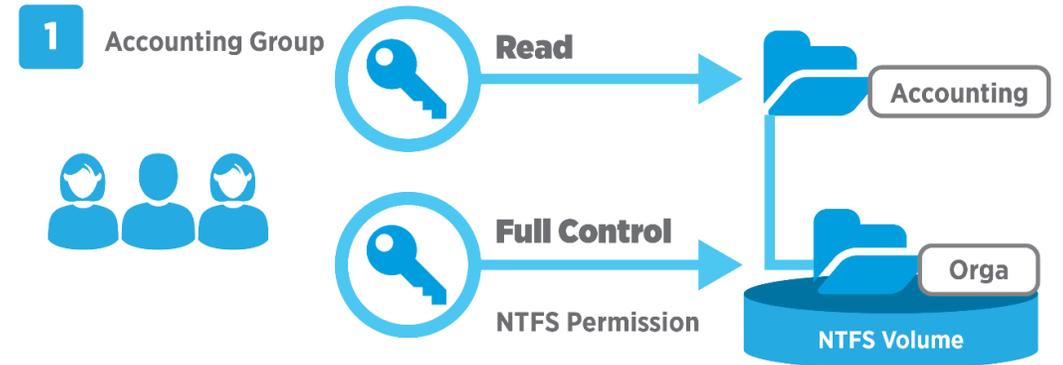
Also called *authorization*. A security technique that can be used to regulate who or what can view or use resources in a computing environment. Compare with *authentication*.

Shared Folder and NTFS Permissions

Effective permissions

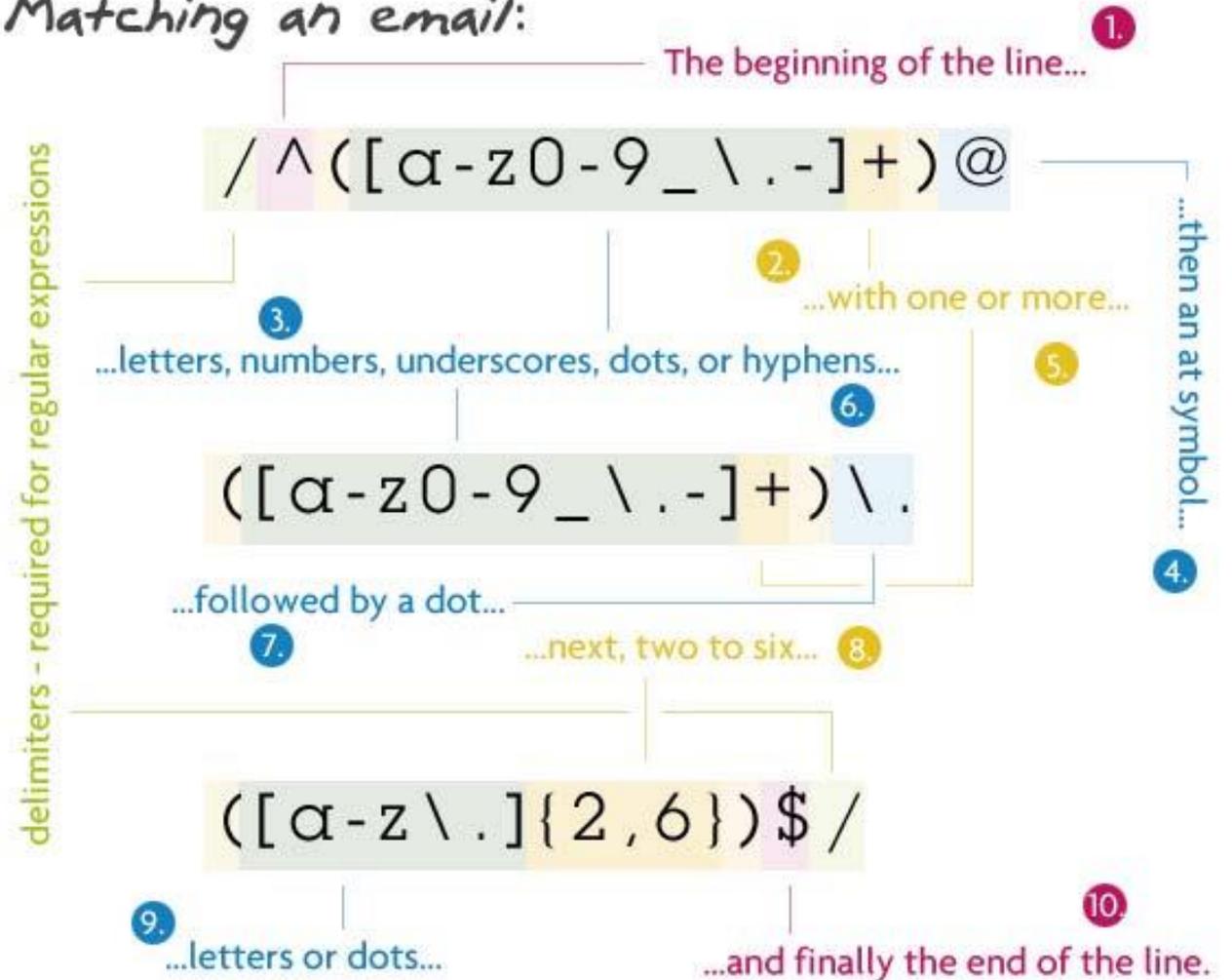
Least privilege

Inheritance



Regular Expressions (Regex)

Matching an email:



Character sequence
that defines a string
search pattern

Originated in
cognitive science

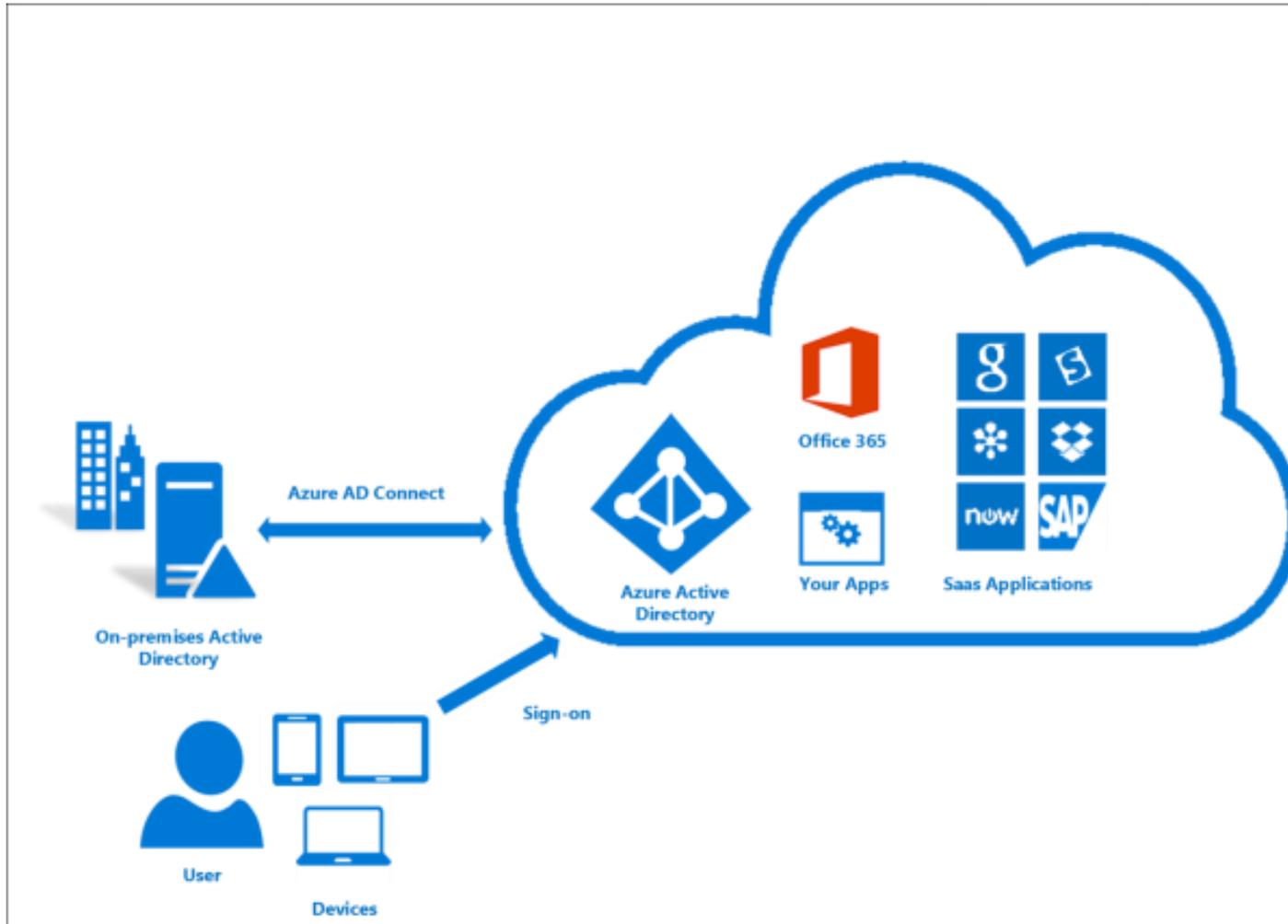
Enormously useful in
IT

"How can businesses use regexes to discover sensitive data?"

Question for Jeff



Hybrid Cloud/SaaS Infrastructure



SaaS

SSO

Cloud storage

"How can data classification work in a hybrid cloud situation; say with Dropbox, OneDrive, Amazon S3, or Azure storage?"

Question for Jeff



Real-life breach
example: Sony
Pictures Hack
(2014)

Disgruntled ex-employee

He/she was able to gain access to their personal and company-related data remotely

Results:

- Corporate public embarrassment
- PII exposure
- IP exposure
- Lost public trust
- Lost revenues

"How can Netwrix help businesses identify whether sensitive data has been breached?"

Question for Jeff

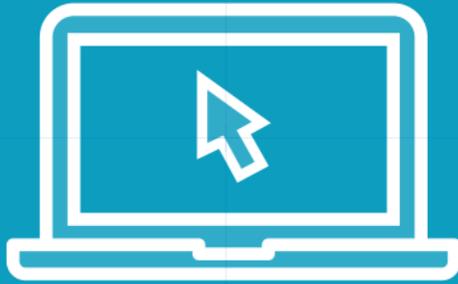


"Regarding compliance: Assuming there has been a breach, how can Netwrix help determine the breach's severity?"

Question for Jeff



Demo



Netwrix Auditor

IT Risk Assessment

IT Risk Assessment: Overview

Gives you a bird's eye view of risks in your organization. Control and mitigate your IT risks by continuously monitoring and addressing weak points in your environment, such as chaotically organized privilege structure, "shadow" user and computer accounts, and improper content on your file shares.

Total risk level for Permissions: ■ Acceptable

Risk	Level
User accounts with administrative privileges	■ Acceptable
Administrative groups	■ Acceptable
Empty security groups	■ Acceptable

Total risk level for Data: ■ Take action

Risk	Level
Shared folders accessible by Everyone	■ Take action
File names containing sensitive data	■ Take action
Potentially harmful files on file shares	■ Take action
Direct permissions on files and folders	■ Pay attention

Total risk level for Users and Computers: ■ Pay attention

Risk	Level
User accounts with Password never expires	■ Pay attention
User accounts with Password not required	■ Acceptable
Disabled computer accounts	■ Acceptable
Inactive user accounts	■ Acceptable
Inactive computer accounts	■ Acceptable

Potentially Harmful Files on File Shares

Lists files on your file shares that may be harmful or malicious, such as executables, installers, scripts, and registry keys. These files may be malware, viruses, or inappropriate distributives and should not be stored on shared resources. Use this report to detect potentially harmful files and prevent security threats.

Object Path	Owner	Creation Date
\\FS1\Shared\Accounting\Cryptolocker.msi	BUILTIN\Administrators	9/30/2017 4:32:33 AM
\\FS1\Shared\Accounting\Virus.exe	BUILTIN\Administrators	10/10/2017 5:50:34 AM
\\FS1\Shared\Finance2017\Report.docx.cmd	BUILTIN\Administrators	8/16/2017 6:59:16 AM
\\FS1\Shared\IT\installers\BitTorrent.exe	BUILTIN\Administrators	7/7/2017 9:12:23 AM
\\FS1\Shared\IT\installers\BitCoin Miner.exe	BUILTIN\Administrators	7/7/2017 6:42:08 AM
\\FS1\Shared\Managers\3xdhdnlcr.reg	BUILTIN\Administrators	7/7/2017 7:55:54 AM
\\FS1\Shared\Managers\picture.jpg.jar	BUILTIN\Administrators	7/7/2017 2:06:07 AM
\\FS1\Shared\ProductManagement\Q4plans.xlsx.bat	BUILTIN\Administrators	9/27/2017 6:37:38 AM

Alerts on Threat Patterns

Netwrix Auditor Alert

Possible ransomware activity

The alert was triggered by 150 activity records being captured within 60 seconds. The most recent of those activity records is shown below. To review the full activity trail, use the interactive search in Netwrix Auditor.

Who:	ENTERPRISE\J.Carter
Action:	Modified
Object type:	File
What:	\\fs3.enterprise.com\Documents\Contractors\payroll2017.docx
When:	4/28/2017 11:35:17 AM
Where:	fs3.enterprise.com
Workstation:	mkt025.enterprise.com
Data source:	File Servers
Monitoring plan:	Enterprise Data Visibility Plan
Details:	Size changed from "807936 bytes" to "831488 bytes"

This message was sent by Netwrix Auditor from au-srv-fin.enterprise.com.

Netwrix Auditor Alert

Possible DBA privilege abuse

Who:	ENTERPRISE\J.Smith
Action:	Removed
Object type:	Table
What:	Databases\Customers\Tables\dbo.Cardholders
When:	5/3/2017 7:19:29 AM
Where:	sql2.enterprise.com
Workstation:	mkt023.enterprise.com
Data source:	SQL Server
Monitoring plan:	Enterprise Database Visibility Plan

This message was sent by Netwrix Auditor from au-srv-fin.enterprise.com.

Behavior Anomaly Discovery

← Behavior Anomalies
Home > Behavior Anomalies

RISK SCORE TIMELINE Last 30 days

User	Risk score	Last alert time
ENTERPRISE\J.Smith	2280	10/2/2017 6:59:49 AM
ENTERPRISE\S.King	1940	09/17/2017 10:06:07 AM
ENTERPRISE\L.Fishburne	1500	10/2/2017 7:00:49 AM
ENTERPRISE\M.Lopez	800	10/2/2017 8:21:40 AM
ENTERPRISE\A.Tomlison	420	09/3/2017 7:20:10 PM
ENTERPRISE\T.Johnson	380	09/21/2017 12:10:07 AM
ENTERPRISE\J.Philips	360	09/22/2017 5:00:41 AM

[Refresh](#)

← User Profile (ENTERPRISE\J.Smith)
Home > Behavior Anomalies (ENTERPRISE\J.Smith)

RISK SCORE BY TOP FIVE ALERTS Last 30 days

1140 Non-Whitelisted Program Launched on DC
600 Creation of Potentially Harmful Files
540 Interactive Logon to DC

[Show all user activity](#)
[Show this activity record](#)

Alert time	Alert name	Risk score	Status
10/2/2017 6:59:49 AM	Creation of Potentially Harmful Files	60	Active
10/02/2017 6:30:55 AM	Non-Whitelisted Program Launched on DC	40	Active
10/2/2017 6:06:04 AM	Non-Whitelisted Program Launched on DC	40	Active
10/2/2017 6:00:10 AM	Interactive Logon to DC	30	Active

Details:
 Alert name: Creation of Potentially Harmful Files
 Risk Score: 60
 Who: ENTERPRISE\J.Smith
 Object type: File
 Action: Added
 What: \\FS1\Shared\Finance\Reports.exe
 Where: fs1.enterprise.com
 When: 10/2/2017 6:59:49 AM

Filters:
[Customize view](#)
 All filters selected
[Hide reviewed anomalies](#)

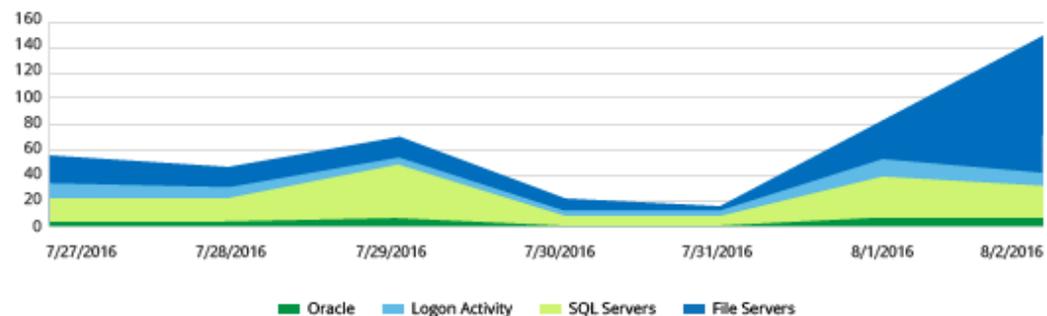
Actions:
[Mark all as reviewed](#)
[Refresh](#)

[ENTERPRISE\J.Smith](#)
Total risk score: 2280
[Show user activity](#)

User Behavior and Blind Spots Analysis

Failed Activity Trend

Shows consolidated statistics on failed actions, including failed read attempts, failed modification attempts, failed logons, etc. The report also lists the users with most failed attempts.



Date: 8/2/2016 (Attempts: 145)

Who	Attempts
ENTERPRISE\D.Harris	78
ENTERPRISE\G.Brown	7
ENTERPRISE\T.Simpson	5

Activity Outside Business Hours

Shows users who performed any actions outside their business hours. Use this report to detect suspicious user activity.

User Name	Actions
ENTERPRISE\D.Harris	663
ENTERPRISE\J.Carter	44
ENTERPRISE\T.Simpson	21
ENTERPRISE\A.Watson	15
ENTERPRISE\G.Brown	8

User Behavior and Blind Spots Analysis

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks. Track permissions assigned to accounts directly or by group membership.

Object: \\fs1\Accounting (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\N.Key	Full Control	Directly	0
ENTERPRISE\T.Simpson	Full Control	Group	0
ENTERPRISE\P.Anderson	Full Control	Group	0
ENTERPRISE\K.Miller	Write and list folder content	Directly	0
ENTERPRISE\T.Allen	Read (Execute, List folder content)	Group	0

Logons by Single User from Multiple Endpoints

Shows users who logged on from several endpoints within a short period of time. Such occurrences may indicate that the account's password was stolen or compromised. Use this report to detect suspicious user activity and prevent data breaches.

User: ENTERPRISE\J.Carter (First Attempt: 7/27/2016 2:02:26 PM)

Endpoint	Logon Attempts
172.17.6.36	2
ENTWKS0376	6

User: ENTERPRISE\D.Harris (First Attempt: 7/26/2016 5:13:16 PM)

Endpoint	Logon Attempts
WST055	12
192.168.1.1	1
ENTWKS0376	1

Data Discovery and Classification

Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

Content source	Categories	Files count
\fs1\Accounting	GDPR	1300
	PCI DSS	585
\fs1\Finance	GDPR	715
	HIPAA	250
	PCI DSS	952
\fs1\HR	GDPR	1500
	HIPAA	1085

Sensitive Files and Folders by Owner

Shows ownership of files and folders that are stored in the specified file share and contain selected categories of sensitive data. Use this report to determine the owners of particular sensitive data.

Owner: ENTERPRISE\E.Anderson

UNC path	Categories
\fs1\HR\Annual Report	PII
\fs1\HR\Compensation & Benefits	PII
\fs1\HR\Exit Interviews	PII

Owner: ENTERPRISE\J.Carter

UNC path	Categories
\fs1\HR\Training Program	PII
\fs1\HR\New Employees\Europe	GDPR

Data Discovery and Classification

Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

Content source	Categories	Files count
\fs1\Accounting	GDPR	1300
	PCI DSS	585
\fs1\Finance	GDPR	715
	HIPAA	250
	PCI DSS	952
\fs1\HR	GDPR	1500
	HIPAA	1085

Sensitive Files and Folders by Owner

Shows ownership of files and folders that are stored in the specified file share and contain selected categories of sensitive data. Use this report to determine the owners of particular sensitive data.

Owner: ENTERPRISE\E.Anderson

UNC path	Categories
\fs1\HR\Annual Report	PII
\fs1\HR\Compensation & Benefits	PII
\fs1\HR\Exit Interviews	PII

Owner: ENTERPRISE\J.Carter

UNC path	Categories
\fs1\HR\Training Program	PII
\fs1\HR\New Employees\Europe	GDPR

Interactive Search

The screenshot shows the Netwrix Interactive Search interface. At the top left, there is a back arrow and the text "Search" with a breadcrumb "Home > Search". To the right of this are five filter categories: "WHO" (person icon), "ACTION" (lightning bolt icon), "WHAT" (square and triangle icon), "WHEN" (clock icon), and "WHERE" (server rack icon). A "Tools" menu is visible in the top right corner. Below the filters is a large, empty search input field. At the bottom of the interface, there are three buttons: "Open in new window" (with an external link icon), a prominent blue "SEARCH" button, and "Advanced mode" (with a list icon). Below the buttons, the text reads: "Investigate incidents and browse your audit data" followed by "To start browsing your audit data and investigating incidents, add some filtering criteria in the Search field above."

← Search
Home > Search

WHO ACTION WHAT WHEN WHERE

Tools

Open in new window **SEARCH** Advanced mode

Investigate incidents and browse your audit data
To start browsing your audit data and investigating incidents, add some filtering criteria in the Search field above.

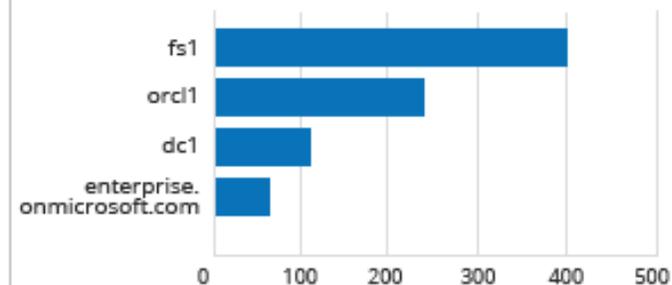
Enterprise Overview Dashboards

Enterprise Overview

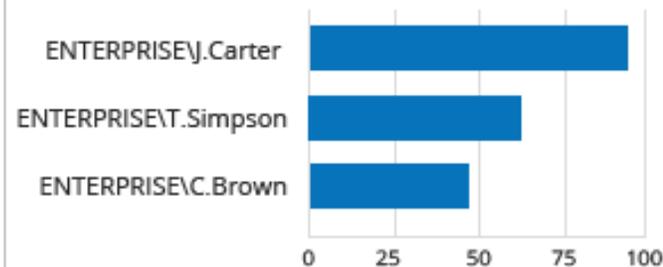
CHANGES BY DATE



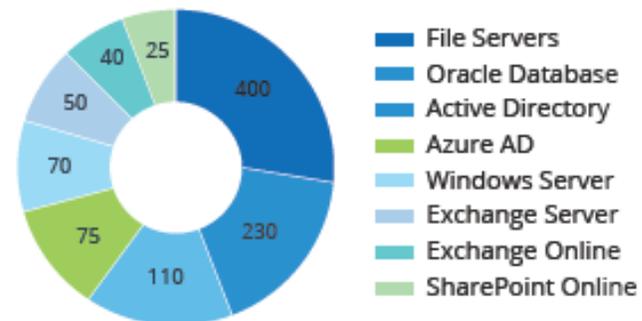
SERVERS WITH MOST CHANGES



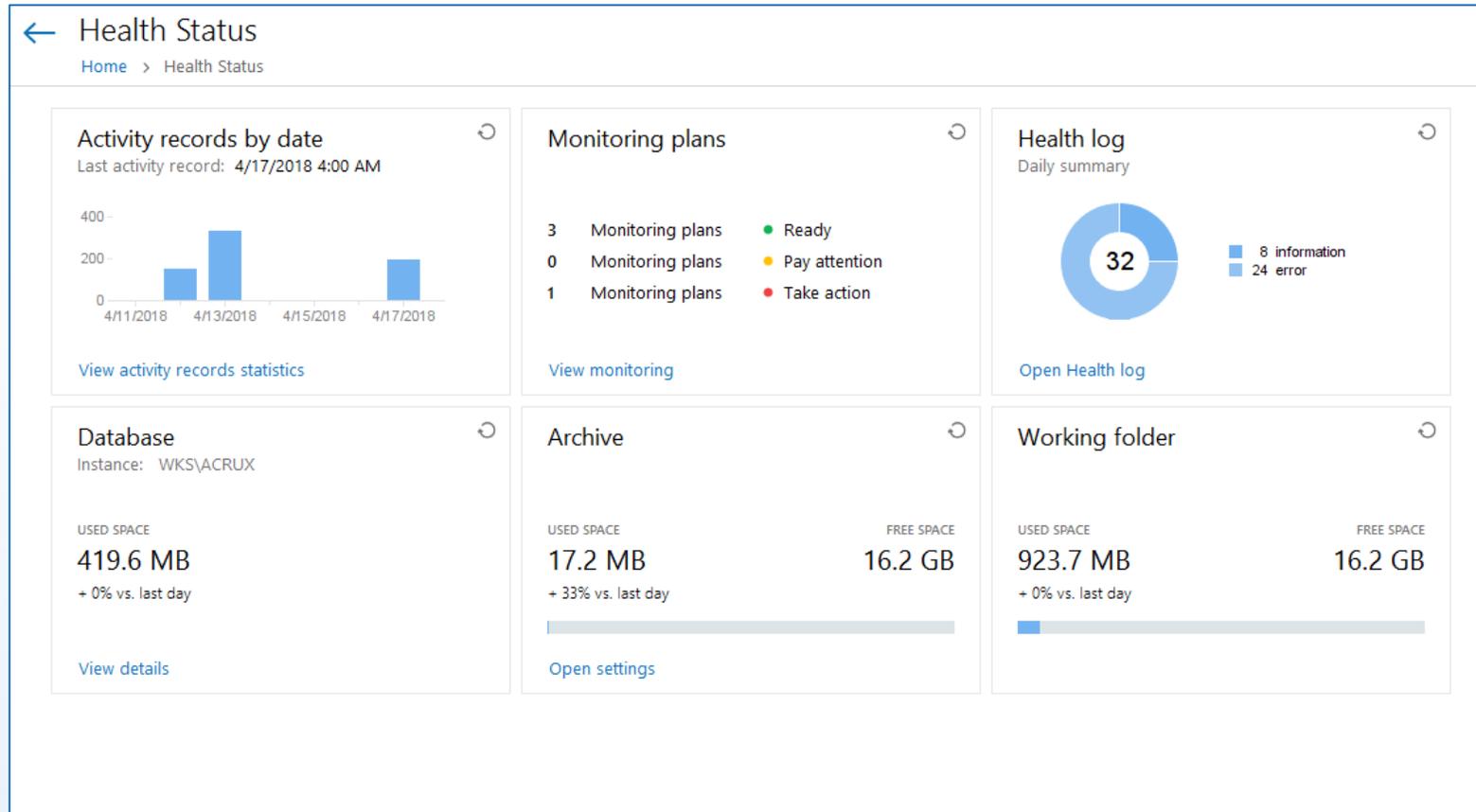
USERS WHO MADE MOST CHANGES



CHANGES BY DATA SOURCE



Health Status Dashboard



File Analysis

Potential Data Owners by Folder

Shows users who frequently access files in a given folder. Use this report to identify factual data owners and analyze usage patterns.

Folder: \\fs1\Shared\Finance
Owner: ENTERPRISE\S.Coleman

Who	Changes	Reads
ENTERPRISE\S.Coleman	88	178
ENTERPRISE\A.Dowson	43	118
ENTERPRISE\E.Swift	17	67
ENTERPRISE\E.Robinson	2	41

Duplicate Files

Shows files with the same name and size. Use this report for detecting potentially duplicate files that can be safely removed.

Object Name: Strategy2016.pptx (Size: 0.0002 MB)

Object Path	Modification Date
\\fs1\shared\Managers	11/11/2015 2:45:00 PM
\\fs1\shared\Finance	11/09/2015 10:32:11 AM

Out-of-the-box Compliance Reports

← Reports

Active Directory

- ▶ CJIS Compliance
- ▶ FERPA Compliance
- ▶ FISMA/NIST Compliance
- ▶ GDPR Compliance
- ▶ GLBA Compliance
- ▶ **HIPAA Compliance**
 - 📄 All Active Directory Changes
 - 📄 Administrative Group Members
- ▶ ISO/IEC 27001 Compliance
- ▶ NERC CIP Compliance
- ▶ PCI DSS Compliance
- ▶ SOX Compliance

Administrative Groups Membership Changes

Shows changes to members of the Domain Admins, Enterprise Admins, Schema Admins, Account Operators and other administrative groups, and affected parent groups.

Group name: \Enterprise\Users\Domain Admins

Action	Member	Who	When
■ Added	\Enterprise\Users\Jack Falcon	ENTERPRISE\R.Ferrano	8/17/2015 4:03:13 PM
Where:	dc1.enterprise.com		
■ Removed	\Enterprise\Users\John Smith	ENTERPRISE\R.Ferrano	8/17/2015 6:57:32 PM
Where:	dc1.enterprise.com		

Group name: \Enterprise\Users\Schema Admins

Action	Member	Who	When
■ Added	\Enterprise\Users\Liza Lee	ENTERPRISE\P.Jackson	8/18/2015 7:07:18 PM
Where:	dc1.enterprise.com		

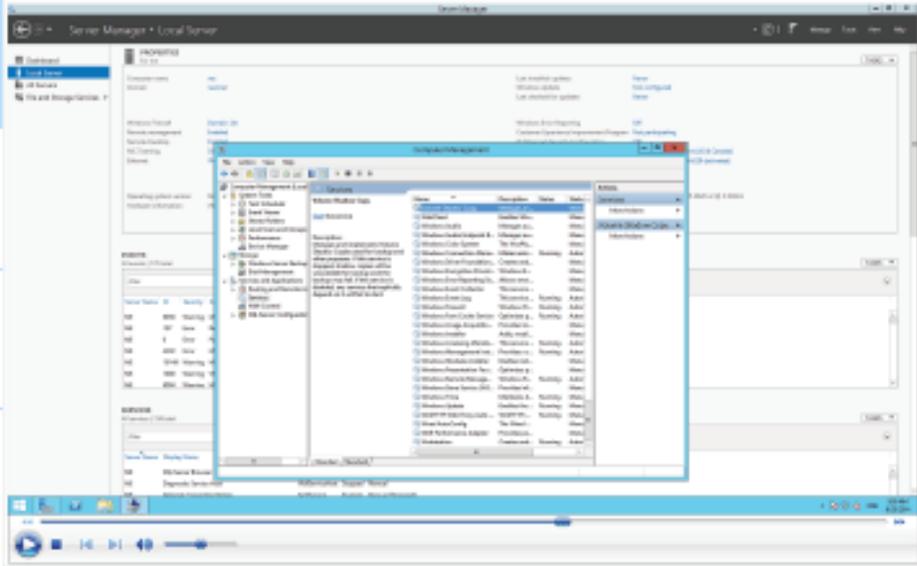
User Activity Video Recording

← Search WHO ACTION WHAT WHEN WHERE

Data source "User Activity (Video)" x

Open in new window **SEARCH** Advanced mode

Who	Object type	Action	What	Where	When
ENTERPRISE\J.Carter	Window				
Show video...					
ENTERPRISE\J.Carter	Window				
Show video...					
ENTERPRISE\J.Carter	Window				
Show video...					
ENTERPRISE\J.Carter	Window				
Show video...					



Useful links

Free 20-Day Trial: setup in your own test environment: netwrix.com/freetrial

Live One-to-One Demo: product tour with Netwrix expert: netwrix.com/livedemo

Contact Sales to obtain more information: netwrix.com/contactsales

Referral program for customers: netwrix.com/become_netwrix_referrer.html

Webinars: join our upcoming webinars and watch the recorded sessions

- netwrix.com/webinars
- netwrix.com/webinars#featured

Summary



Tim Warner



@TechTrainerTim



Pluralsight.com

Jeff Melnick



Jeff.Melnick@netwrix.com