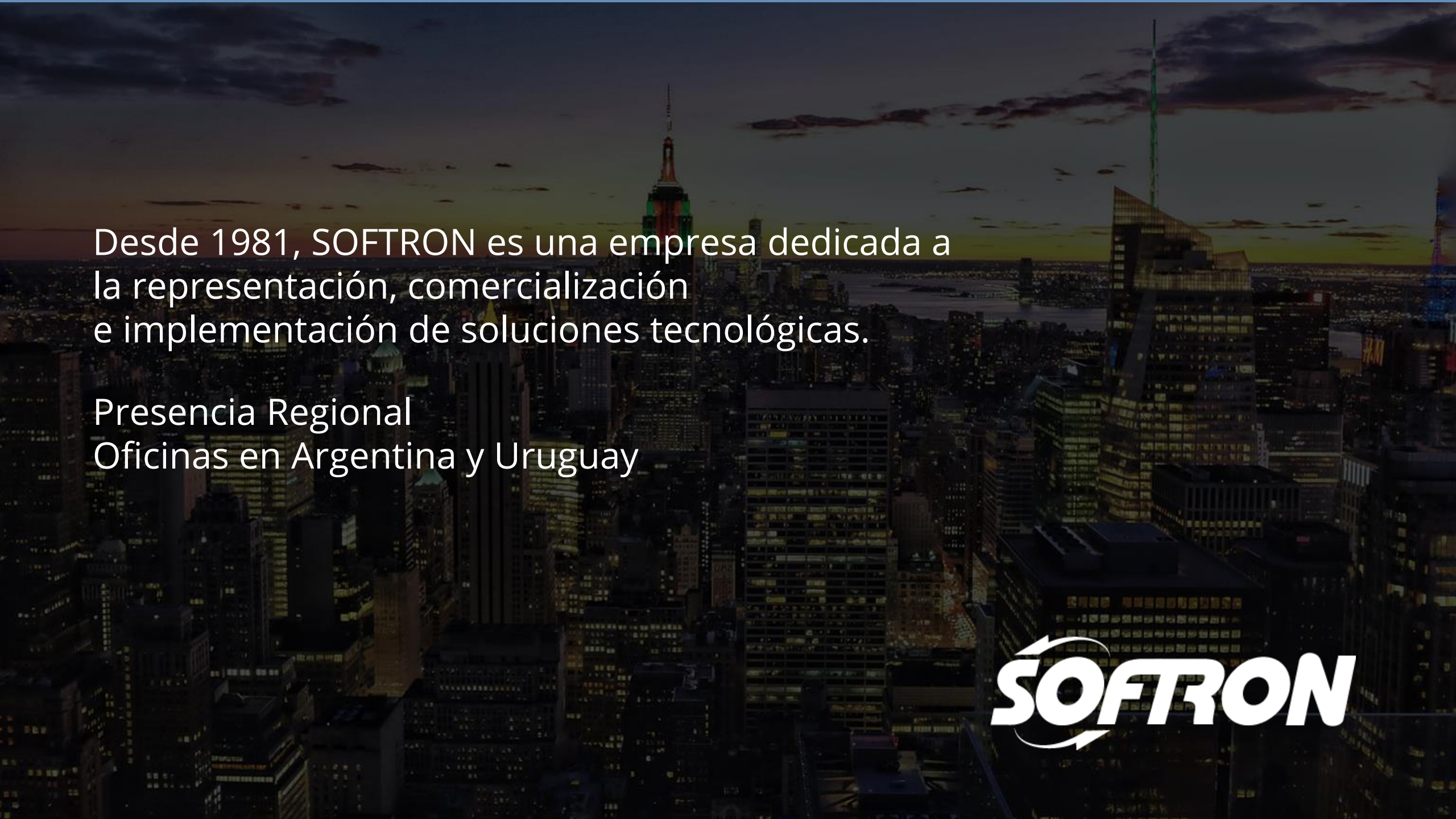
Cómo minimizar los riesgos en torno a los datos confidenciales con Netwrix y Softron

Nicolás López
Softron

Kenny Hernandez
Netwrix


Desde 1981, SOFTRON es una empresa dedicada a
la representación, comercialización
e implementación de soluciones tecnológicas.
Presencia Regional
Oficinas en Argentina y Uruguay
SOFTRON

netwrix

Fundada: 2006

Oficinas centrales: Irvine, California

Clientes Globales: más de 11,000

Reconocimiento:

- 7 años entre las compañías de software de EEUU con más rápido crecimiento
- Más de 150 premios de la industria
- Softron trabaja con Netwrix desde 2016

Finanzas

Credit Suisse · Standard Chartered · Allianz · Santander · First Insurance Company of Hawaii · LPL Financial

Salud y Farmacéutica

Texas Children's Hospital · R1 · Boston Medical Center · Pfizer · Yale NewHaven Health Greenwich Hospital · DaVita Medical Group · CHRISTUS Health

Educación

Columbia University · UCSF University of California San Francisco · FSCJ Florida State College at Jacksonville · american career college · UT Health Science Center · ACU Australian Catholic University

Servicios

Blackboard · Hilton · BCG · AT&T · DHL · Insight · EY · pwc

Gobierno

Ministry of Defence · Maine · DC.gov · BNA

Industria y Tecnología

Hyundai · Mitsubishi · Airbus · SICK Sensor Intelligence. · Honda · Electrolux · eset · thyssenkrupp

¿Por qué estamos hoy aquí?

$2.56 millones de dólares es el costo total promedio de una filtración de datos.*

Los datos confidenciales crecen sin control y están en riesgo.

Los usuarios tienen acceso a más datos confidenciales de lo que necesitan.

Las filtraciones de datos tardan demasiado en identificarse y contenerse, lo que amplifica el daño.

Las herramientas de seguridad en silos dejan huecos y reducen la eficiencia.

*Fuente: Cost of a Data Breach Report 2021

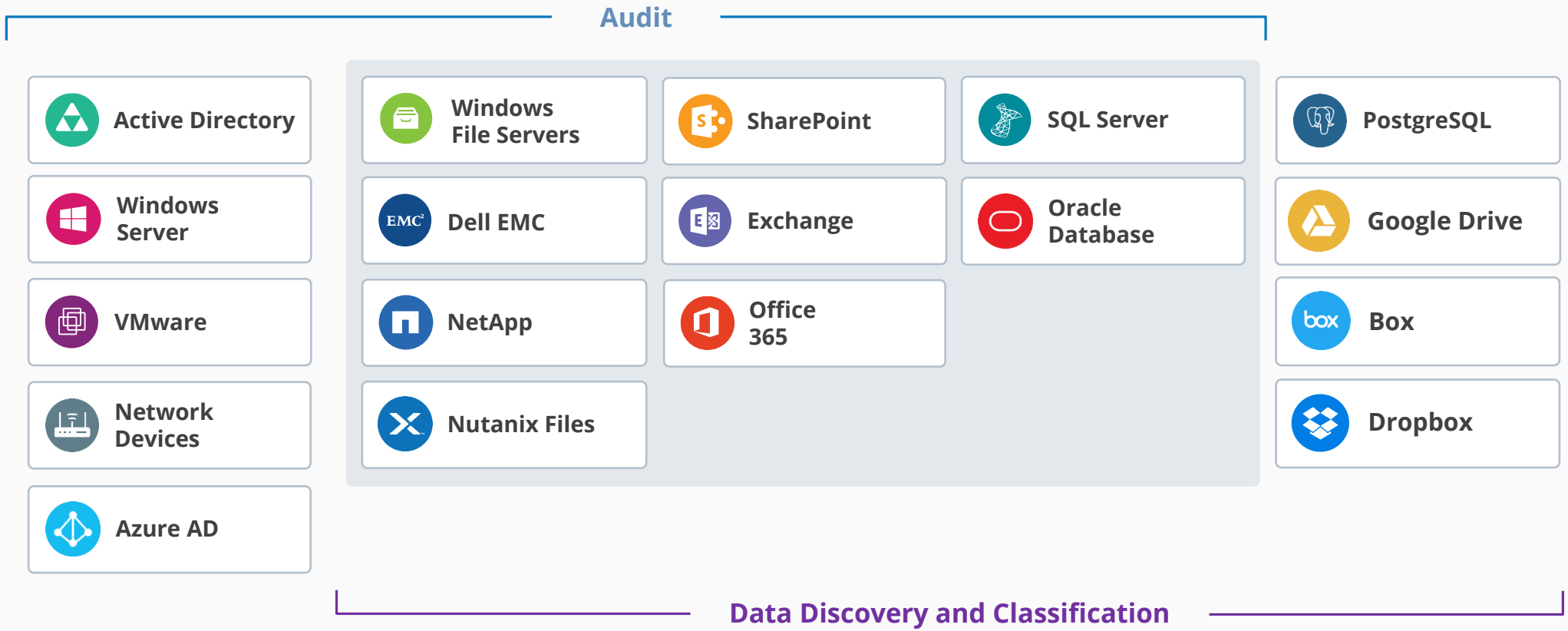
¿Cuáles son sus procesos de Gobierno de Acceso a los Datos?

PREVENIR		REMEDIAR		
IDENTIFICAR	**PROTEGER**	**DETECTAR**	**RESPONDER**	**RECUPERAR**
¿Qué información es sensible? ¿Dónde está? ¿Está en riesgo? ¿Quién tiene acceso a esa información?	¿Quién debe tener acceso a los datos confidenciales? ¿Cómo mantener los derechos de acceso al mínimo requerido? ¿Cómo minimizar el daño del ransomware y otros ataques?	¿Quién está accediendo a los datos confidenciales? ¿Qué tan rápido podemos detectar actividad inusual en torno a datos confidenciales?	¿Qué tan rápido puede responder a un incidente? ¿Podemos determinar cómo se desarrolló? ¿Sabemos si hay que reportar una filtración?	¿Qué datos debemos recuperar? ¿Cómo podría haberse prevenido o bloqueado el incidente en sus primeras etapas?

Ciclo completo de Gobierno de Acceso a los Datos

PREVENIR		REMEDIAR		
IDENTIFICAR	**PROTEGER**	**DETECTAR**	**RESPONDER**	**RECUPERAR**
Identifique los datos sensibles, sus propietarios y quién tiene acceso. Detecte los riesgos a su alrededor, como el acceso abierto.	Remedie los permisos excesivos. Realice revisiones periódicas del acceso de los usuarios para hacer cumplir el principio de privilegio mínimo.	Detecte actividades sospechosas en torno a los datos, como accesos inusuales o intentos de elevación de privilegios.	Responda a las amenazas en torno a los datos confidenciales más rápido. Investigue el incidente para formular la mejor respuesta.	Cree un plan de recuperación e incorpore las lecciones aprendidas.

“Navaja Suiza” para visibilidad en toda su infraestructura



Demostración

netwrix

SOFTRON

Netwrix Data Classification 5.5.2.4

Sources | Taxonomies | Workflows | Config | Users | Reports | Dashboard | Help

Term Management | Graph | Rollback | User Edits | Bulk Updates | Taxonomy Settings | Global Settings | Help

Financial Records

- Financial Records
  - ABA routing number (0)
  - IBAN (0)
  - IP Address (5)
  - Payrolls (4)
  - SWIFT (2)
  - US bank account number (0)

Dashboard

[NFR] Softron | VAP | VAP\Administrator

© 2020 Netwrix Corporation

netwrix

Netwrix Data Classification 5.5.2.4

Sources | Taxonomies | Workflows | Config | Users | Reports | Dashboard | Help

General | Box | Dropbox | Exchange Mailbox | File | Google Drive | SharePoint

Sources

Sources > VAP Shared Folders

Delete | Re-Collect | Re-Index | Re-Classify | Pause | Resume | Remove From Group | Add

Page Url	Status	Discovery Only	Build Index	Documents	Size
\\vapi\Accounting	Error	—	✓	49	-
\\vapi\Clients	Error	—	✓	22	-
\\vapi\Public	Error	—	✓	55	-

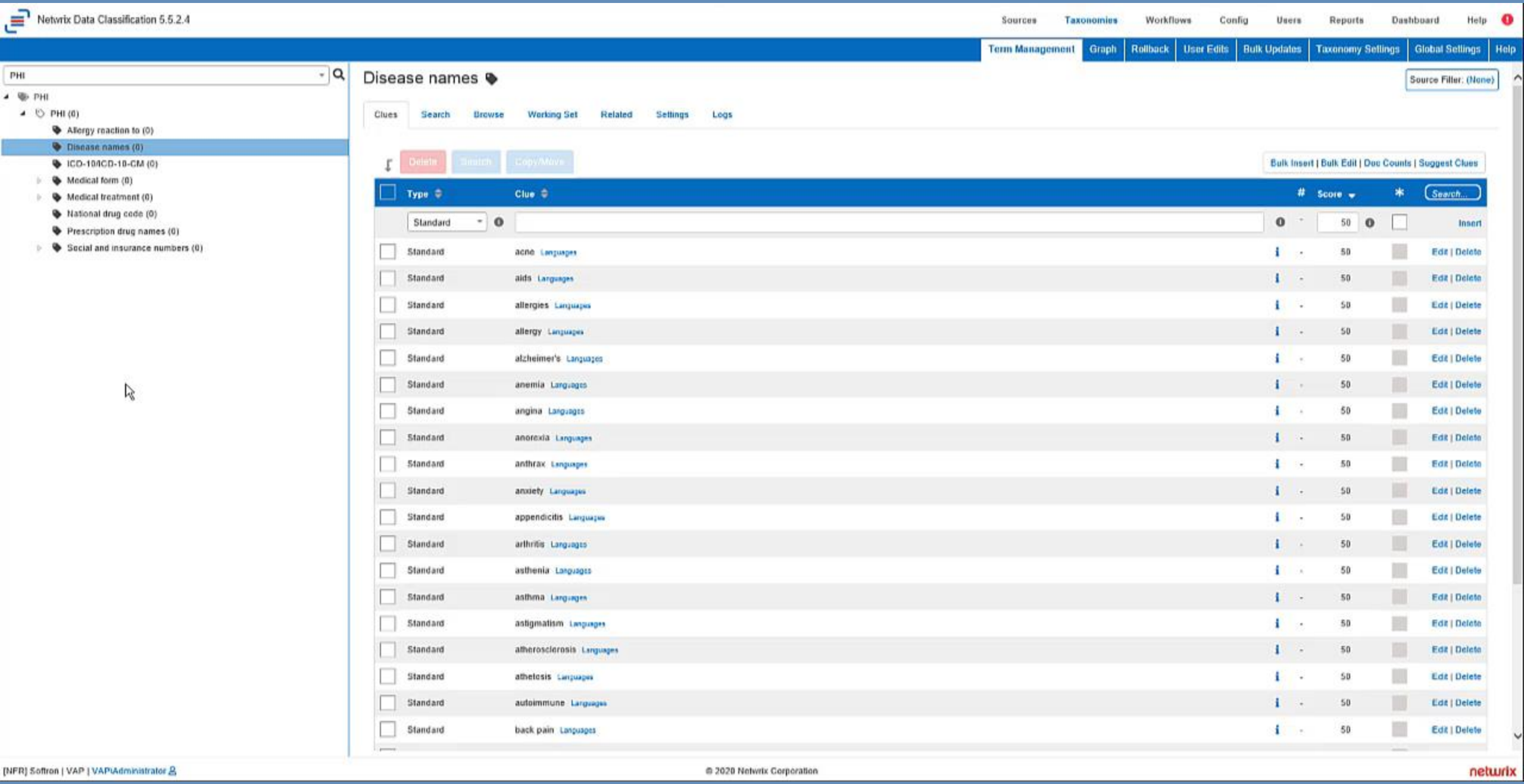
Search...

Copy | CSV | XLSX | Showing 3 record(s) | Page Size: 10 | 25 | 50 | 100 | 200

http://localhost/conceptQS/SourcesGrid/Page/2555

© 2020 Netwrix Corporation

netwrix


Netwrix Data Classification 5.5.2.4
Sources
Taxonomies
Workflows
Config
Users
Reports
Dashboard
Help
Term Management
Graph
Rollback
User Edits
Bulk Updates
Taxonomy Settings
Global Settings
Help
PHI
PHI
PHI (0)
Allergy reaction to (0)
Disease names (0)
ICD-10/CD-10-CM (0)
Medical form (0)
Medical treatment (0)
National drug code (0)
Prescription drug names (0)
Social and insurance numbers (0)
Disease names
Source Filter: (None)
Clues
Search
Browse
Working Set
Related
Settings
Logs
Delete
Switch
Copy/Move
Bulk Insert | Bulk Edit | Doc Counts | Suggest Clues
Type
Clue
#
Score
Search...
Standard
50
Insert
Standard acne Languages 50 Edit | Delete
Standard aids Languages 50 Edit | Delete
Standard allergies Languages 50 Edit | Delete
Standard allergy Languages 50 Edit | Delete
Standard alzheimer's Languages 50 Edit | Delete
Standard anemia Languages 50 Edit | Delete
Standard angina Languages 50 Edit | Delete
Standard anorexia Languages 50 Edit | Delete
Standard anthrax Languages 50 Edit | Delete
Standard anxiety Languages 50 Edit | Delete
Standard appendicitis Languages 50 Edit | Delete
Standard arthritis Languages 50 Edit | Delete
Standard asthenia Languages 50 Edit | Delete
Standard asthma Languages 50 Edit | Delete
Standard astigmatism Languages 50 Edit | Delete
Standard atherosclerosis Languages 50 Edit | Delete
Standard athetosis Languages 50 Edit | Delete
Standard autoimmune Languages 50 Edit | Delete
Standard back pain Languages 50 Edit | Delete
[NFR] Softron | VAP | VAP\Administrator
© 2020 Netwrix Corporation
netwrix

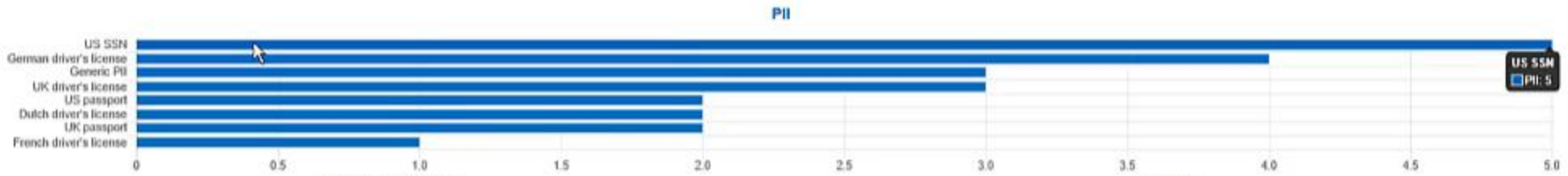
Netwrix Data Classification 5.5.2.4

Sources | Taxonomies | Workflows | Config | Users | Reports | Dashboard | Help

Term Management | Graph | Rollback | User Edits | Bulk Updates | Taxonomy Settings | Global Settings | Help

PII

- PII
  - Australia (0 of 0)
  - Austria (0 of 0)
  - Belgium (0 of 0)
  - Brazil (0 of 0)
  - Bulgaria (0 of 0)
  - Canada (0 of 0)
  - Croatia (0 of 0)
  - Cyprus (0 of 0)
  - Czech Republic and Slovakia (0 of 0)
  - Denmark (0 of 0)
  - Estonia (0 of 0)
  - Finland (0 of 0)
  - France (0 of 2)
  - Generic PII (3 of 3)
  - Germany (0 of 5)
  - Greece (0 of 0)
  - Hong Kong (0 of 0)
  - Hungary (0 of 0)
  - Iceland (0 of 0)
  - India (0 of 0)
  - Ireland (0 of 0)
  - Italy (0 of 0)
  - Latvia (0 of 0)
  - Lithuania (0 of 0)
  - Luxembourg (0 of 0)
  - Malta (0 of 0)
  - Netherlands (0 of 2)
  - Norway (0 of 0)
  - Poland (0 of 0)
  - Portugal (0 of 0)
  - Romania (0 of 0)
  - Russia (0 of 0)
  - Singapore (0 of 0)
  - Slovenia (0 of 0)
  - South Africa (0 of 0)
  - Spain (0 of 0)
  - Sweden (0 of 0)
  - United Kingdom (0 of 6)
  - USA (0 of 7)



[NFR] Softron | VAP | VAP\Administrator

© 2020 Netwrix Corporation

netwrix

Reports

Home › Reports

Enter your search

- User Behavior and Blind Spot Analysis
- Active Directory
  - Active Directory Changes
  - Active Directory — State-in-Time
  - Group Policy Changes
  - Group Policy — State-in-Time
  - Logon Activity
- Azure AD
- Exchange
- Exchange Online
- File Servers
- Oracle Database
- SharePoint
- SharePoint Online
- SQL Server
- VMware
- Windows Server
- Data Discovery and Classification
  - Activity Related to Sensitive Files and Folders
  - File and Folder Categories by Object
  - Most Accessible Sensitive Files and Folders
  - Overexposed Files and Folders
  - Sensitive File and Folder Permissions Details
  - Sensitive Files and Folders by Owner
  - Sensitive Files Count by Source
- Compliance
- Custom

Data Discovery and Classification

Summary:

Contains a set of reports that help to detect sensitive data. Use this reports for security investigations related to unauthorized access and when planning data protection measures.
Note: For these reports to function properly, the "Data discovery and classification feature" must be enabled.

Netwrix Auditor 9.96

Visibility Platform for User Behavior Analysis and Risk Mitigation

Help Center

New Netwrix Auditor 10.0 is here.

Released on 09/14/2021. Learn more...

Quick Start

- New Active Directory Plan
- New Windows File Servers Plan
- New Windows Server Plan
- New SQL Server Plan
- New Exchange Plan
- New Exchange Online Plan
- New Azure AD Plan
- All data sources

Intelligence

- Search
- Reports
- Behavior anomalies
- Risk assessment
- Enterprise overview
- Failed activity trend
- User account status changes
- Activity outside business hours
- Logons by single user from multiple endpoints
- Administrative group and role changes
- AD or Group Policy modifications by administrator

Configuration

- Monitoring Plans
- Alerts
- Subscriptions
- Compliance mappings
- Live news (9)
- Settings
- Health status

Enterprise Overview

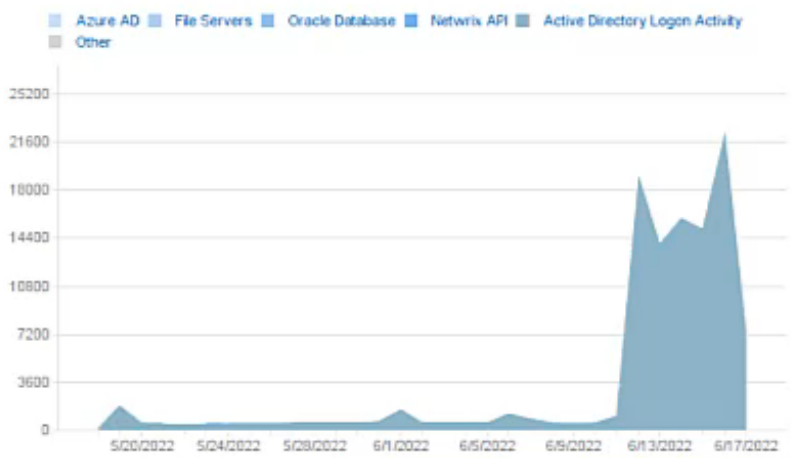
Home > Enterprise Overview

Filters | Not set

Top: 5 Timeframe: Last 30 days

CHANGES BY DATE

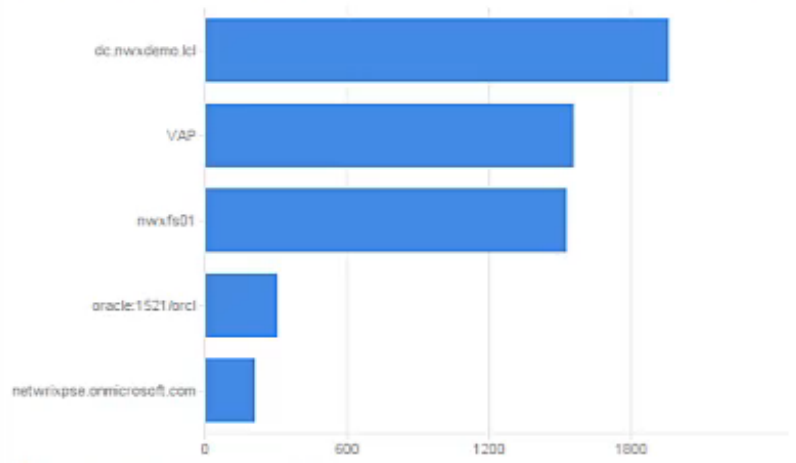
FAILED ACTIVITY TREND



DATA ACCESS TREND

WHERE MOST CHANGES WERE MADE

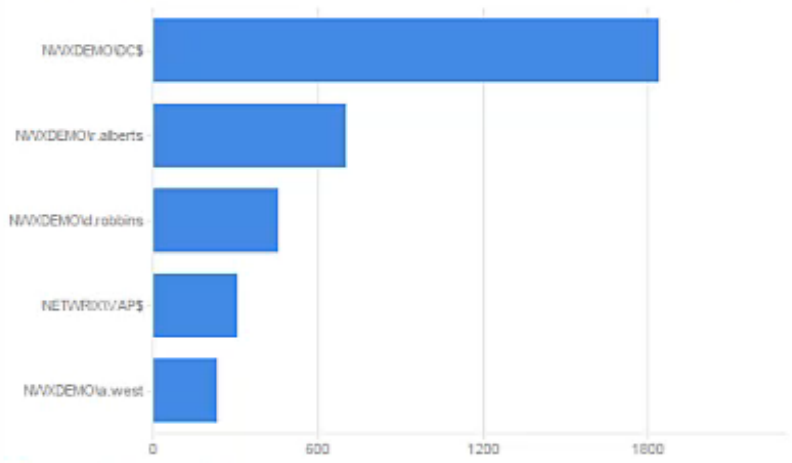
Top: 5



Some data was not displayed. View details

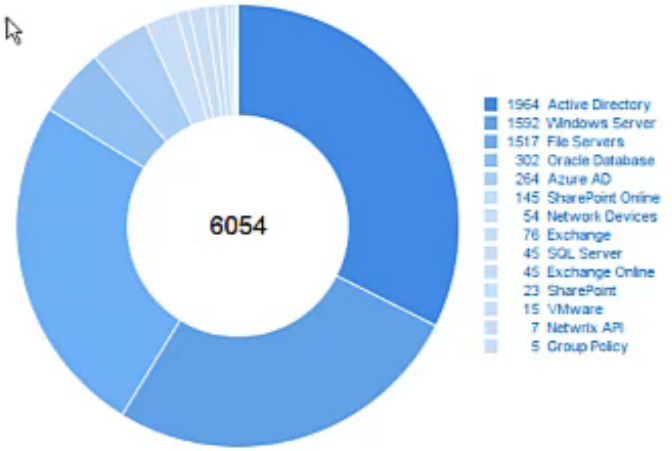
WHO MADE MOST CHANGES

Top: 5



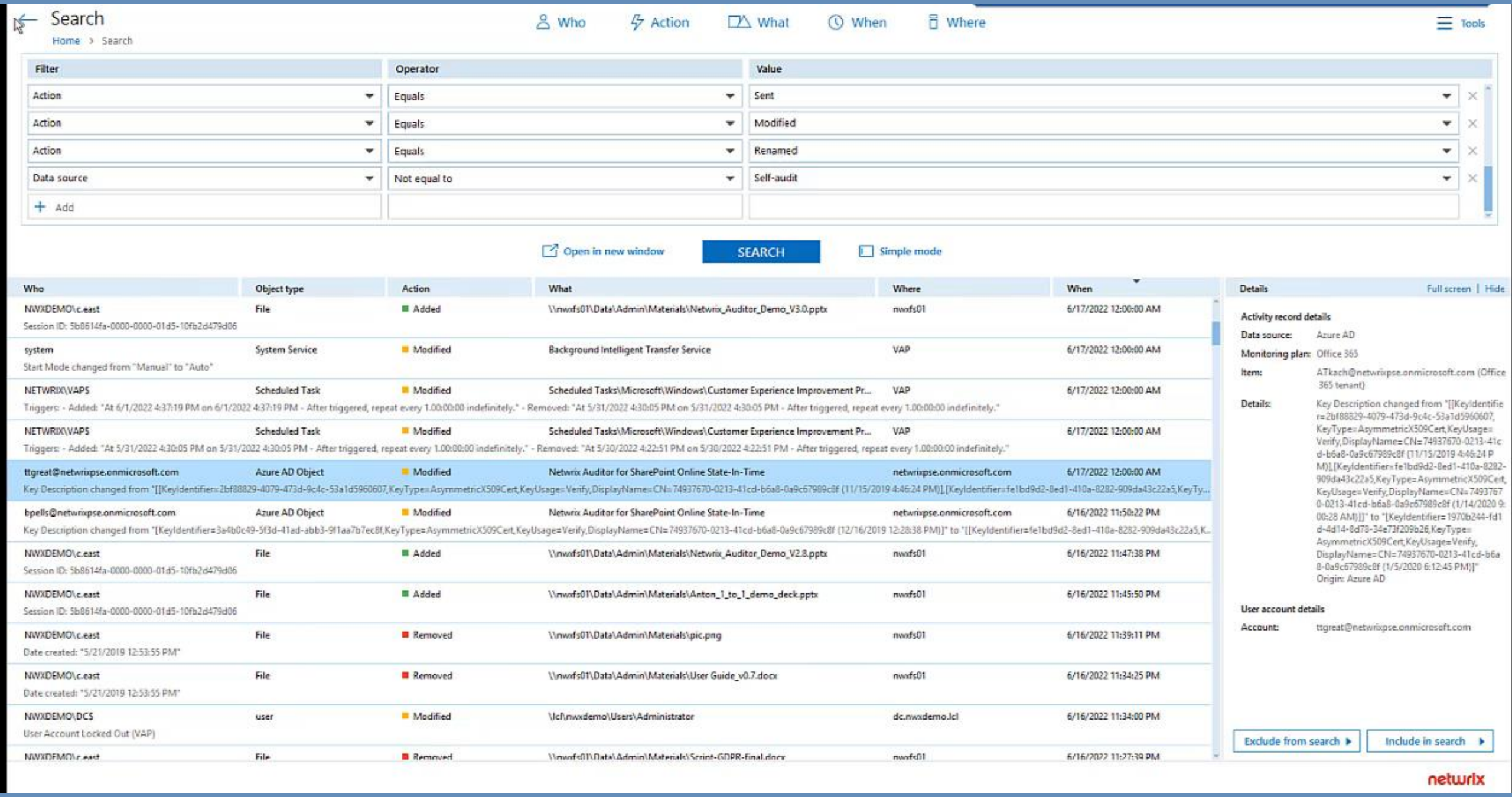
Some data was not displayed. View details

CHANGES BY DATA SOURCE



Subscribe Export

netwrix


Search
Home > Search
Who
Action
What
When
Where
Tools
Filter
Operator
Value
Action
Equals
Sent
Action
Equals
Modified
Action
Equals
Renamed
Data source
Not equal to
Self-audit
Add
Open in new window
SEARCH
Simple mode
Who
Object type
Action
What
Where
When
NWXDEMO\c.east
File
Added
\\nwxfs01\Data\Admin\Materials\Netwrix_Auditor_Demo_V3.0.pptx
nwxfs01
6/17/2022 12:00:00 AM
Session ID: 5b8614fa-0000-0000-01d5-10fb2d479d06
system
System Service
Modified
Background Intelligent Transfer Service
VAP
6/17/2022 12:00:00 AM
Start Mode changed from "Manual" to "Auto"
NETWRIX\VAP$
Scheduled Task
Modified
Scheduled Tasks\Microsoft\Windows\Customer Experience Improvement Pr...
VAP
6/17/2022 12:00:00 AM
Triggers: - Added: "At 6/1/2022 4:37:19 PM on 6/1/2022 4:37:19 PM - After triggered, repeat every 1.00:00:00 indefinitely." - Removed: "At 5/31/2022 4:30:05 PM on 5/31/2022 4:30:05 PM - After triggered, repeat every 1.00:00:00 indefinitely."
NETWRIX\VAP$
Scheduled Task
Modified
Scheduled Tasks\Microsoft\Windows\Customer Experience Improvement Pr...
VAP
6/17/2022 12:00:00 AM
Triggers: - Added: "At 5/31/2022 4:30:05 PM on 5/31/2022 4:30:05 PM - After triggered, repeat every 1.00:00:00 indefinitely." - Removed: "At 5/30/2022 4:22:51 PM on 5/30/2022 4:22:51 PM - After triggered, repeat every 1.00:00:00 indefinitely."
ttgreat@netwrixpse.onmicrosoft.com
Azure AD Object
Modified
Netwrix Auditor for SharePoint Online State-In-Time
netwrixpse.onmicrosoft.com
6/17/2022 12:00:00 AM
Key Description changed from "[[KeyIdentifier=2bf88829-4079-473d-9c4c-53a1d5960607,KeyType=AsymmetricX509Cert,KeyUsage=Verify,DisplayName=CN=74937670-0213-41cd-b6a8-0a9c67989c8f (11/15/2019 4:46:24 PM)],[KeyIdentifier=fe1bd9d2-8ed1-410a-8282-909da43c22a5,KeyTy...
bpells@netwrixpse.onmicrosoft.com
Azure AD Object
Modified
Netwrix Auditor for SharePoint Online State-In-Time
netwrixpse.onmicrosoft.com
6/16/2022 11:50:22 PM
Key Description changed from "[KeyIdentifier=3a4b0c49-5f3d-41ad-abb3-9f1aa7b7ec8f,KeyType=AsymmetricX509Cert,KeyUsage=Verify,DisplayName=CN=74937670-0213-41cd-b6a8-0a9c67989c8f (12/16/2019 12:28:38 PM)]" to "[[KeyIdentifier=fe1bd9d2-8ed1-410a-8282-909da43c22a5,K...
NWXDEMO\c.east
File
Added
\\nwxfs01\Data\Admin\Materials\Netwrix_Auditor_Demo_V2.8.pptx
nwxfs01
6/16/2022 11:47:38 PM
Session ID: 5b8614fa-0000-0000-01d5-10fb2d479d06
NWXDEMO\c.east
File
Added
\\nwxfs01\Data\Admin\Materials\Anton_1_to_1_demo_deck.pptx
nwxfs01
6/16/2022 11:45:50 PM
Session ID: 5b8614fa-0000-0000-01d5-10fb2d479d06
NWXDEMO\c.east
File
Removed
\\nwxfs01\Data\Admin\Materials\pic.png
nwxfs01
6/16/2022 11:39:11 PM
Date created: "5/21/2019 12:53:55 PM"
NWXDEMO\c.east
File
Removed
\\nwxfs01\Data\Admin\Materials\User Guide_v0.7.docx
nwxfs01
6/16/2022 11:34:25 PM
Date created: "5/21/2019 12:53:55 PM"
NWXDEMO\DC$
user
Modified
\lcl\nwxdemo\Users\Administrator
dc.nwxdemo.lcl
6/16/2022 11:34:00 PM
User Account Locked Out (VAP)
Details
Full screen | Hide
Activity record details
Data source: Azure AD
Monitoring plan: Office 365
Item: ATkach@netwrixpse.onmicrosoft.com (Office 365 tenant)
Details: Key Description changed from "[[KeyIdentifier=2bf88829-4079-473d-9c4c-53a1d5960607, KeyType=AsymmetricX509Cert,KeyUsage=Verify,DisplayName=CN=74937670-0213-41cd-b6a8-0a9c67989c8f (11/15/2019 4:46:24 PM)],[KeyIdentifier=fe1bd9d2-8ed1-410a-8282-909da43c22a5,KeyType=AsymmetricX509Cert, KeyUsage=Verify,DisplayName=CN=74937670-0213-41cd-b6a8-0a9c67989c8f (1/14/2020 9:00:28 AM)]]" to "[KeyIdentifier=1970b244-fd1d-4d14-8d78-34e73f209b26,KeyType=AsymmetricX509Cert,KeyUsage=Verify, DisplayName=CN=74937670-0213-41cd-b6a8-0a9c67989c8f (1/5/2020 6:12:45 PM)]" Origin: Azure AD
User account details
Account: ttgreat@netwrixpse.onmicrosoft.com
Exclude from search
Include in search
netwrix

Risk Assessment Overview

Home › Risk Assessment Overview

Type to filter risks

Filters | Not set

Help Center

Risk name	Current value	Risk level
Users and Computers		
User accounts with "Password never expires"	No data	
User accounts with "Password not required"	No data	
Disabled computer accounts	No data	
Inactive user accounts	No data	
Inactive computer accounts	No data	
Servers with Guest account enabled	0% (0 of 1)	Low (0%)
Servers that have local user accounts with "Password never expires"	100% (1 of 1)	High (0% - 100%)
Permissions		
User accounts with administrative permissions	No data	
Administrative groups	No data	
Administrative group membership sprawl	100% (1 of 1)	High (0% - 100%)
Empty security groups	No data	
Site collections with the "Get a link" feature enabled	No data	
Sites with the "Anonymous access" feature enabled	No data	
Site collections with broken inheritance	No data	
Data		
Files and folders accessible by Everyone	100% (189 of 189)	High (5% - 100%)
File and folder names containing sensitive data	26	High (20 - unlimited)
Potentially harmful files on file shares	0	Low (0)
Direct permissions on files and folders	100% (189 of 189)	High (40% - 100%)
Documents and list items accessible by Everyone and Authenticated Users	No data	
Infrastructure		
Servers with inappropriate operating systems	0% (0 of 1)	Low (0%)
Servers with under-governed Windows Update configurations	100% (1 of 1)	High (75% - 100%)
Servers with unauthorized antivirus software	100% (1 of 1)	High (0% - 100%)

Details

Files and folders accessible by Everyone

Files and folders shared with "Everyone" security group / Overall number of shared files and folders (%).

Use this metric and underlying report to detect whether your files and folders can be accessed by Everyone.

Last update time: 6/17/2022 3:07 AM

Risk threshold values:

Low:	0% - 1%
Medium:	1% - 5%
High:	5% - 100%

Actions

Modify thresholds

View Report

Subscribe | Export

netwrix

Member Added to Privileged Group

Home › All Alerts › Member Added to Privileged Group

- General
- Recipients
- Filters
- Thresholds
- Risk Score
- Response Action

Take action when alert occurs

Off

Run: D:\Integrations\Netwrix_Auditor_Integration_Add_on_for_Slack\Netwrix.Integrations.Client.exe

With parameters: slack

Working directory:

Options: Write data to CSV file Limit row count in a file to: 10

Credentials: By default Netwrix Auditor uses the LocalSystem account to run the executable file.

Use custom credentials

User name:

Password:

Command line preview:

D:\Integrations\Netwrix_Auditor_Integration_Add_on_for_Slack\Netwrix.Integrations.Client.exe slack {AlertId} {RecordId}

Test run

Note: {AlertId} - unique alert item identifier,
{RecordId} - unique activity record identifier.

Save & Close | Save | Discard

netwrix

¿Por qué Netwrix?

Ciclo completo

Cierre la brecha entre los controles de seguridad de sus datos y facilite todas las funciones clave de la seguridad de TI: identificar, proteger, detectar, responder y recuperar.

Gartner peerinsights™

"Provee gran valor para una inversión razonable"

★★★★★

Clasificación precisa

Obtenga resultados de clasificación de datos mucho más precisos que los que ofrecen otras herramientas y clasifique tipos de datos específicos para su empresa.

Cobertura más amplia

Controle el acceso a sus datos confidenciales estructurados y no estructurados, independientemente de dónde residan.

Ecosistema de integraciones

Maximice el valor de las inversiones anteriores integrando las soluciones de Netwrix con sus herramientas actuales de TI, seguridad y gestión de riesgos.

Soporte de primera clase

Haga que sus problemas sean resueltos definitivamente por nuestro equipo de atención al cliente receptivo y experto.

¡Netwrix ha crecido! Aquí está la descripción de los productos para ayudarlo con la seguridad y la administración de TI.

Netwrix Auditor

Identifique riesgos de TI, detecte actividades sospechosas e investigue incidentes de seguridad

Netwrix StealthAUDIT

Identifique y reduzca sus riesgos relacionados con datos confidenciales

Netwrix Data Classification

Descubra y clasifique datos confidenciales, regulados y de misión crítica

Netwrix StealthDEFEND

Detecte ataques avanzados en tiempo real

Netwrix Password Policy Enforcer

Mejore la seguridad con políticas de contraseña seguras

Netwrix Password Reset

Identifique riesgos de TI, detecte actividades sospechosas e investigue incidentes de seguridad

Netwrix StealthINTERCEPT

Impida cambios y accesos maliciosos

Netwrix StealthRECOVER

Recupérese de cambios y eliminaciones no deseados en Active Directory

Netwrix Change Tracker

- Alternativa a Tripwire
- File Integrity Monitoring
- Certificado CIS & STIG Hardening
- Gestión de vulnerabilidades

Netwrix PolicyPak

- Cumpla con los controles NIST and CMMC
- Elimine los permisos de Administrador Local, elevación de permisos y baypass de UAC
- Prevenga malware
- Simplifique la gestión de Windows 10 / Group Policy / VDI

Netwrix SbPAM

- 3rd Generation PAM
- Zero Trust
- BYOV


Preguntas y
Respuestas
netwrix
SOFTRON