netwrix

Top 5 Office 365 Incidents You Need Visibility Into

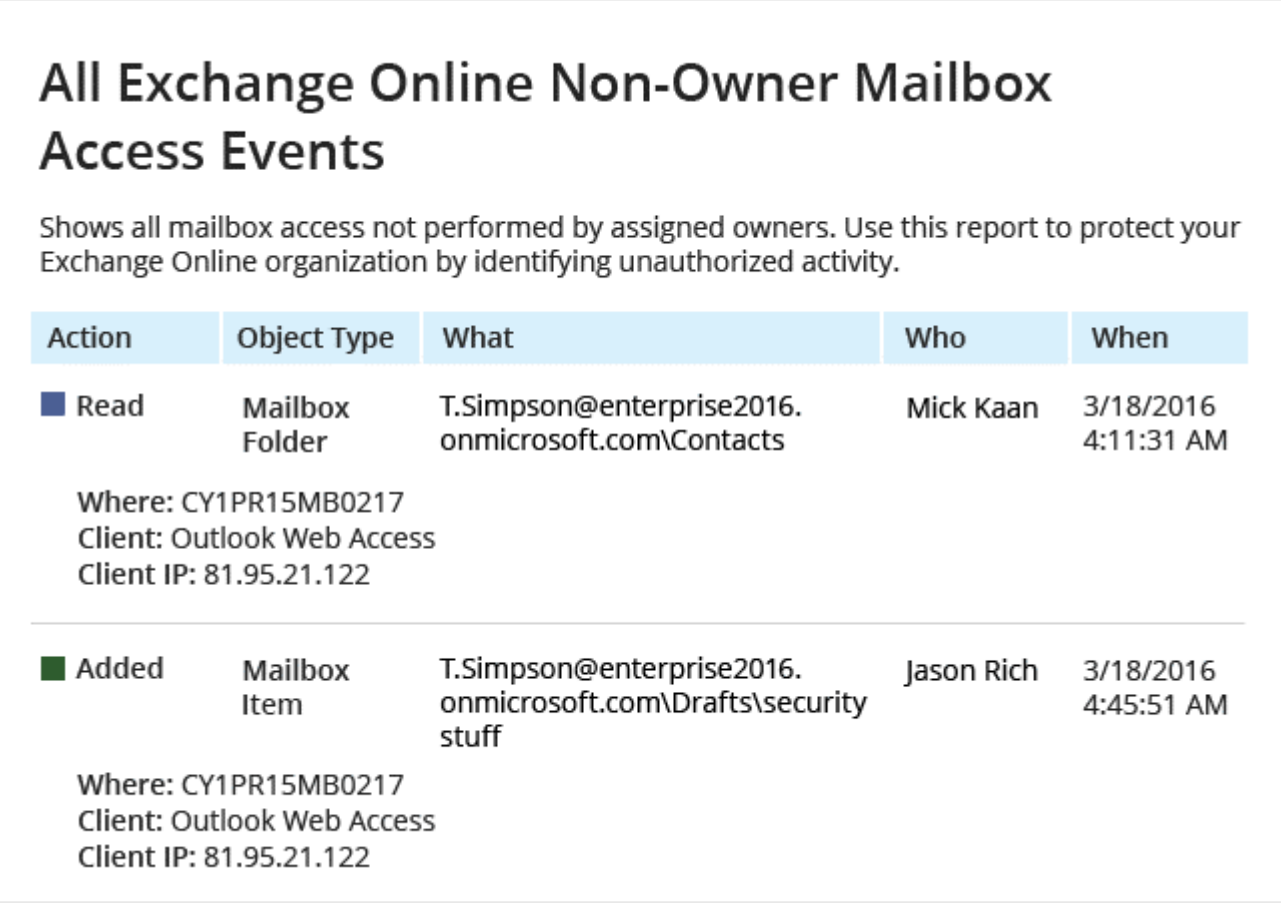
www.netwrix.com | **Toll-free**: 888-638-9749

Table of Contents

#1: Online Mailbox Access by Non-Owners

It's common for a user to be authorized to access another employees' mailbox for legitimate business reasons. Nevertheless, users granted such permissions should be monitored closely, because they can use their privileges for unsanctioned actions, such as copying or deleting messages or forwarding private information to third parties. Netwrix Auditor tracks non-owner access to any mailbox and helps answer the following questions:

- **Who** accessed another user's mailbox?
- **What operations** were performed on each mailbox?
- **When** did each action take place?
- **On which Exchange Online Server** was each action performed?



All Exchange Online Non-Owner Mailbox Access Events

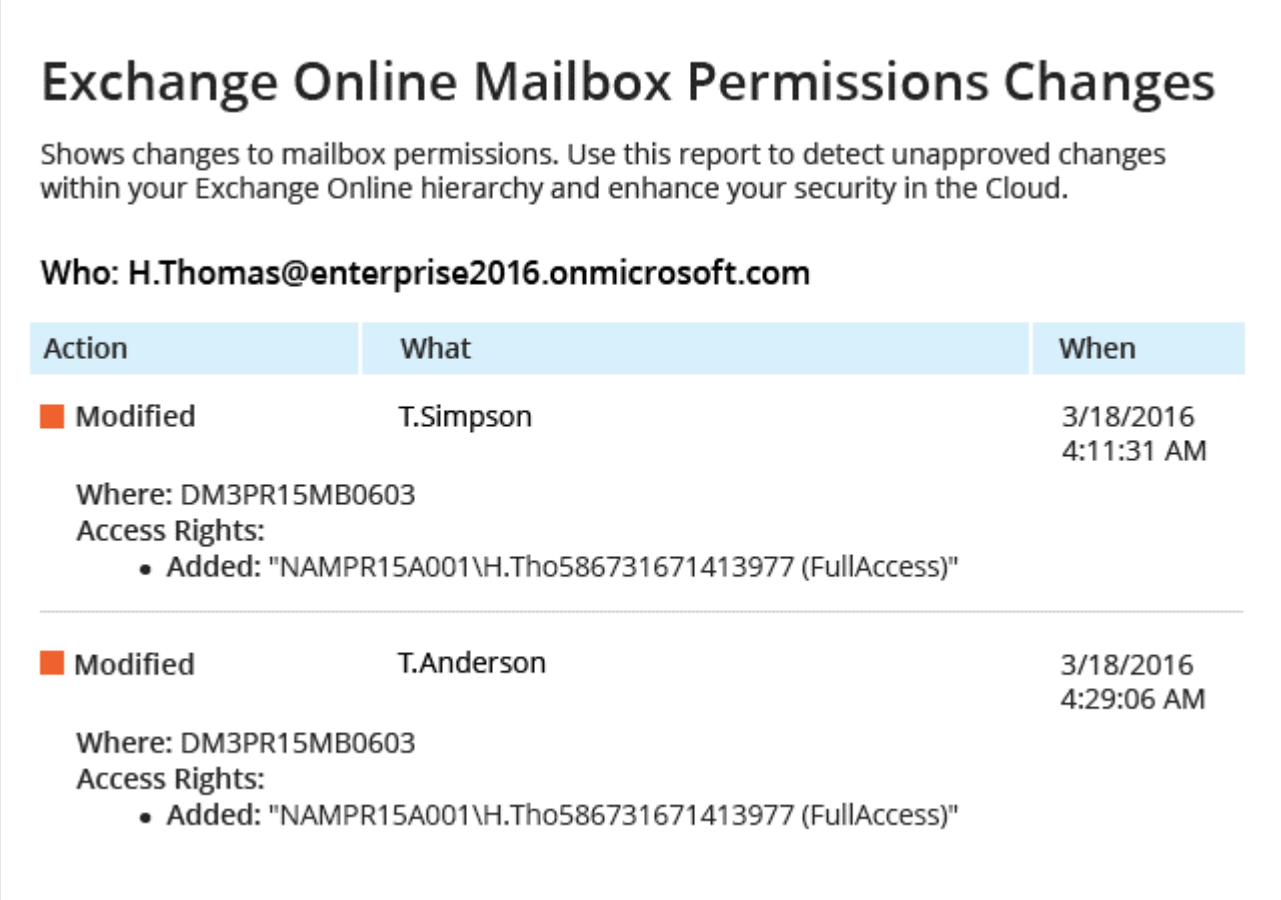
Shows all mailbox access not performed by assigned owners. Use this report to protect your Exchange Online organization by identifying unauthorized activity.

Action	Object Type	What	Who	When
Read	Mailbox Folder	T.Simpson@enterprise2016.onmicrosoft.com\Contacts	Mick Kaan	3/18/2016 4:11:31 AM
Where: CY1PR15MB0217 Client: Outlook Web Access Client IP: 81.95.21.122				
Added	Mailbox Item	T.Simpson@enterprise2016.onmicrosoft.com\Drafts\security stuff	Jason Rich	3/18/2016 4:45:51 AM
Where: CY1PR15MB0217 Client: Outlook Web Access Client IP: 81.95.21.122				

#2: Changes to Online Mailbox Permissions

In Exchange Online, a user's permissions and roles determine which actions the user can perform. Continuous monitoring of mailbox permission changes is essential to quickly spotting inappropriate assignment of access rights that could lead to security incidents. Netwrix Auditor helps you detect suspicious changes to mailbox permissions, and answers the following questions:

- **For which mailboxes** were access rights changed?
- **What permission changes** were made in each case?
- **Who** made each change?
- **On which Exchange Online Server** was each change made?
- **When** was each change made?



Exchange Online Mailbox Permissions Changes

Shows changes to mailbox permissions. Use this report to detect unapproved changes within your Exchange Online hierarchy and enhance your security in the Cloud.

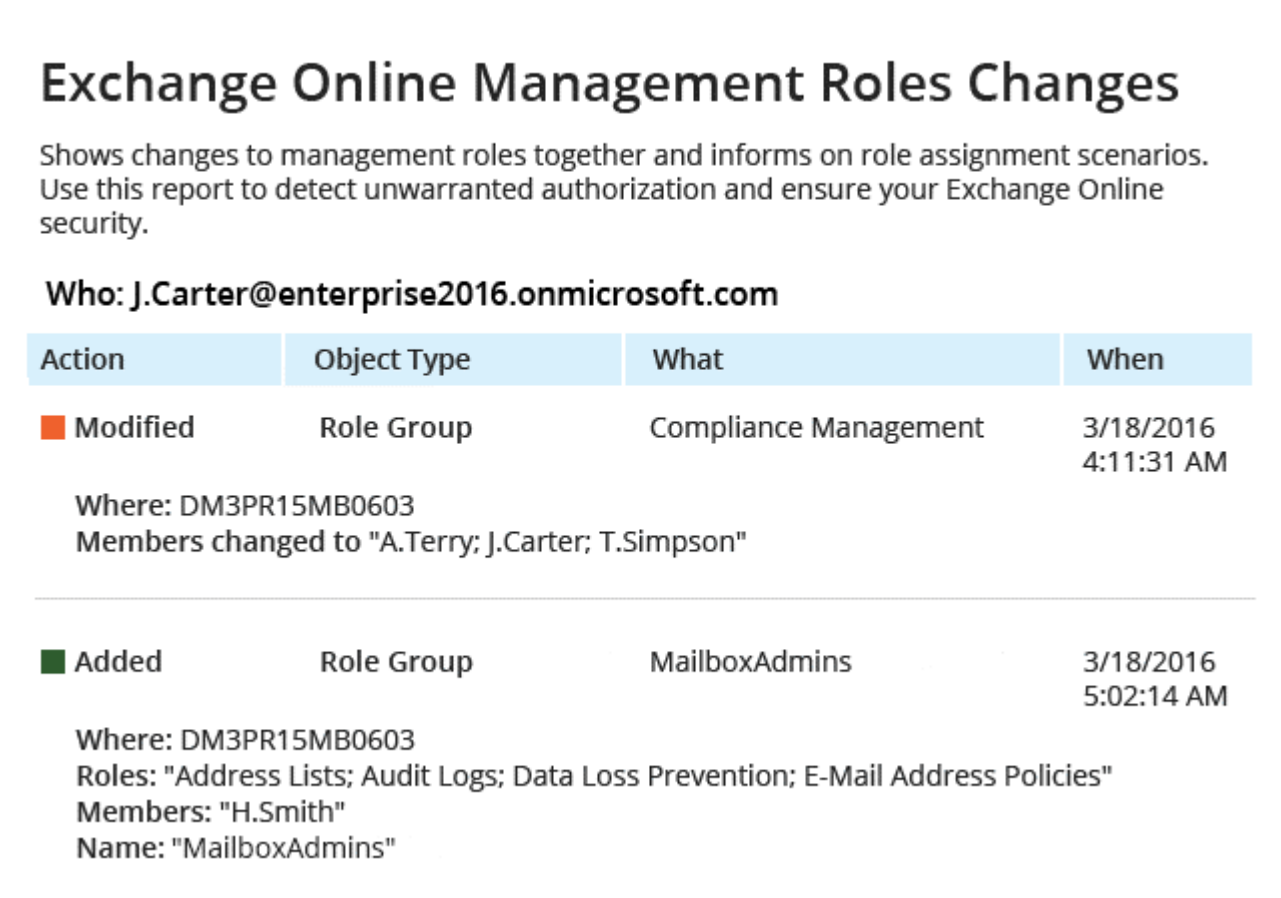
Who: H.Thomas@enterprise2016.onmicrosoft.com

Action	What	When
Modified	T.Simpson	3/18/2016 4:11:31 AM
Where: DM3PR15MB0603 Access Rights: • Added: "NAMPR15A001\H.Tho586731671413977 (FullAccess)"		
Modified	T.Anderson	3/18/2016 4:29:06 AM
Where: DM3PR15MB0603 Access Rights: • Added: "NAMPR15A001\H.Tho586731671413977 (FullAccess)"		

#3: Unwarranted Management Role Assignments

Adding a user to a management role group in Exchange Online can enable that user to delete mailbox databases, edit send/receive connectors or change mailbox permissions, any of which could put your data security at risk. Netwrix Auditor helps you detect unwarranted management role assignments by answering the following questions:

- **Which management role group** were changed?
- **Who** changed each group?
- **What change** was made to each group?
- **When** was each group changed?
- **On which Exchange Online Server** was the changed group located?



Exchange Online Management Roles Changes

Shows changes to management roles together and informs on role assignment scenarios. Use this report to detect unwarranted authorization and ensure your Exchange Online security.

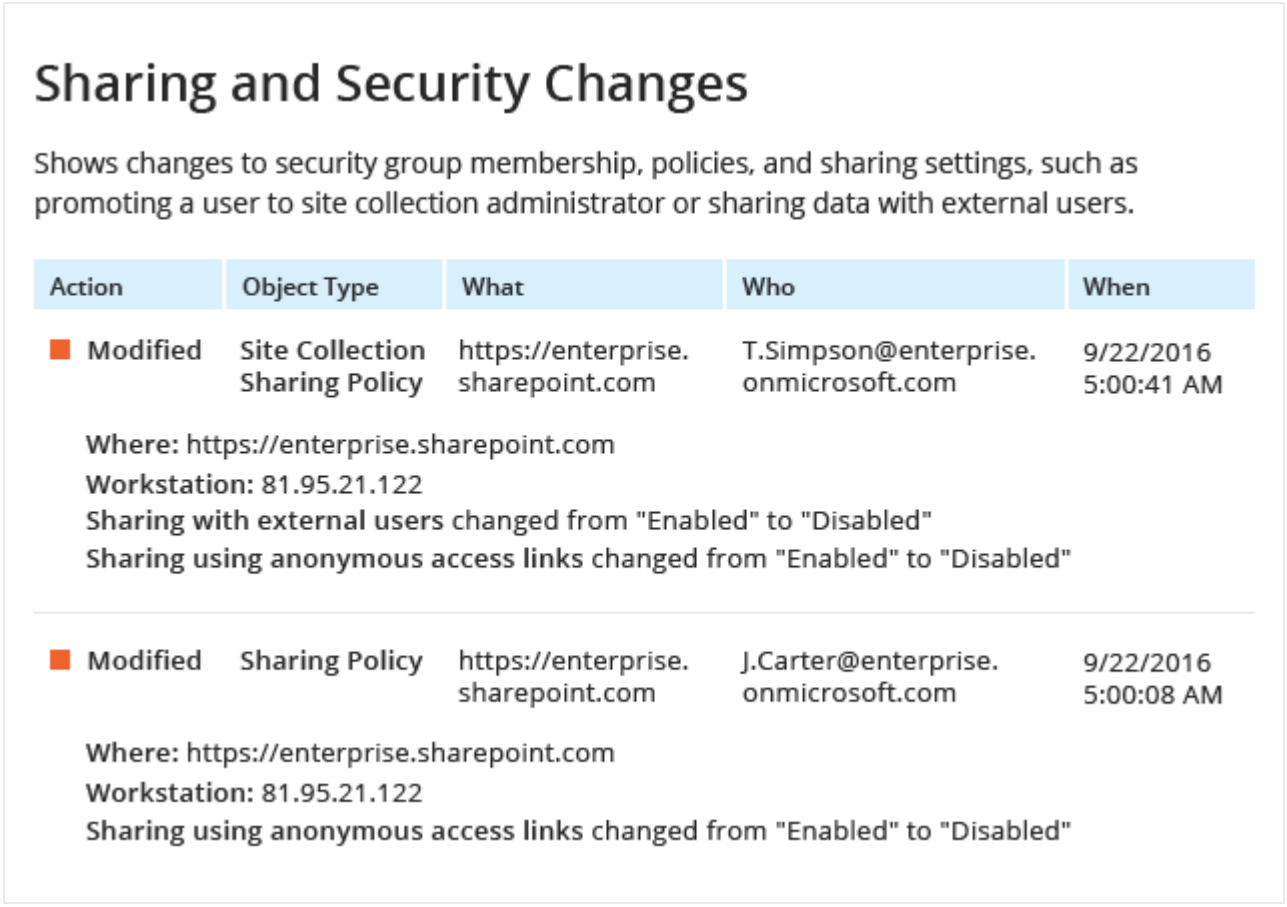
Who: J.Carter@enterprise2016.onmicrosoft.com

Action	Object Type	What	When
Modified	Role Group	Compliance Management	3/18/2016 4:11:31 AM
Where: DM3PR15MB0603 Members changed to "A.Terry; J.Carter; T.Simpson"			
Added	Role Group	MailboxAdmins	3/18/2016 5:02:14 AM
Where: DM3PR15MB0603 Roles: "Address Lists; Audit Logs; Data Loss Prevention; E-Mail Address Policies" Members: "H.Smith" Name: "MailboxAdmins"			

#4: Changes to Sharing Settings in SharePoint Online

Because the sharing settings in SharePoint Online determine how your users can collaborate with other people inside or outside your organization, it's essential to control that there are no activity bypassing these settings. Netwrix Auditor enables constant monitoring of SharePoint Online sharing settings and helps answer the following questions:

- **Which sharing settings** were changed?
- **What change** was made to each setting?
- **Who** made each change?
- **When** was each change made?
- **For which site collection** was each modification applied?



Sharing and Security Changes

Shows changes to security group membership, policies, and sharing settings, such as promoting a user to site collection administrator or sharing data with external users.

Action	Object Type	What	Who	When
Modified	Site Collection Sharing Policy	https://enterprise.sharepoint.com	T.Simpson@enterprise.onmicrosoft.com	9/22/2016 5:00:41 AM

Where: https://enterprise.sharepoint.com
Workstation: 81.95.21.122
Sharing with external users changed from "Enabled" to "Disabled"
Sharing using anonymous access links changed from "Enabled" to "Disabled"

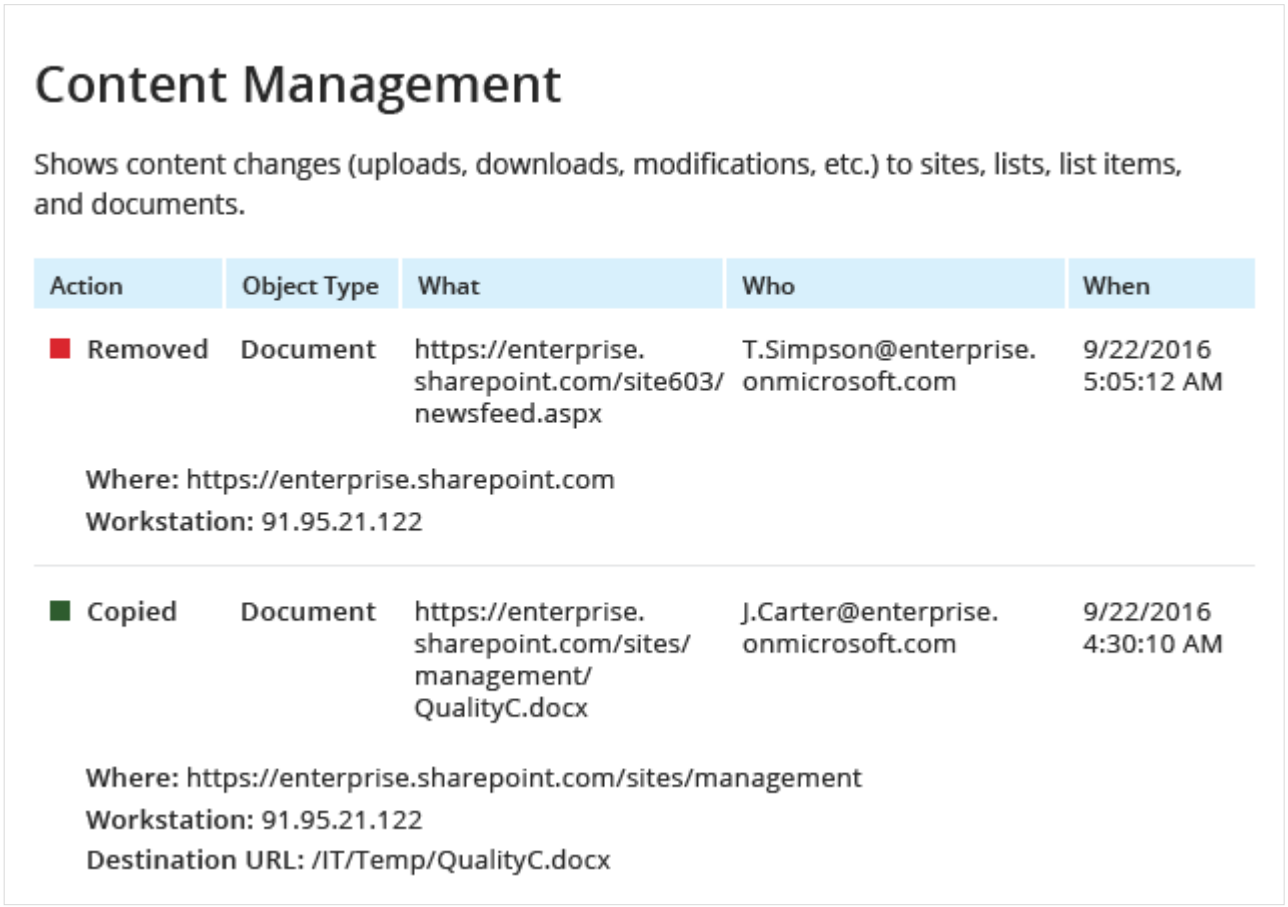
Action	Object Type	What	Who	When
Modified	Sharing Policy	https://enterprise.sharepoint.com	J.Carter@enterprise.onmicrosoft.com	9/22/2016 5:00:08 AM

Where: https://enterprise.sharepoint.com
Workstation: 81.95.21.122
Sharing using anonymous access links changed from "Enabled" to "Disabled"

#5: Content Changes in SharePoint Online

Any unauthorized content changes in your cloud SharePoint environment could be a sign of malicious activity or the result of an inappropriate permissions assignment. Timely detection and investigation of suspicious activity can help prevent the loss of important data. Netwrix Auditor shows all changes made to sites, lists, list items and documents and helps answer the following questions:

- **Were there any suspicious content changes** in your SharePoint Online?
- **Who** uploaded, copied, modified or deleted any shared items?
- **When** was each change made?
- **On which site collection** was each activity performed?



Content Management

Shows content changes (uploads, downloads, modifications, etc.) to sites, lists, list items, and documents.

Action	Object Type	What	Who	When
Removed	Document	https://enterprise.sharepoint.com/site603/newsfeed.aspx	T.Simpson@enterprise.onmicrosoft.com	9/22/2016 5:05:12 AM
Where: https://enterprise.sharepoint.com **Workstation:** 91.95.21.122				
Copied	Document	https://enterprise.sharepoint.com/sites/management/QualityC.docx	J.Carter@enterprise.onmicrosoft.com	9/22/2016 4:30:10 AM
Where: https://enterprise.sharepoint.com/sites/management **Workstation:** 91.95.21.122 **Destination URL:** /IT/Temp/QualityC.docx				

About Netwrix Auditor

Netwrix Auditor is a **visibility and governance platform** that enables control over changes, configurations and access in hybrid cloud IT environments to protect data regardless of its location. The unified platform provides security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API, Netwrix Auditor provides **endless integration, auditing and reporting capabilities** for security and compliance.

Unlike other vendors, Netwrix focuses exclusively on providing complete visibility and governance for hybrid cloud security. The sharp focus enables us to offer much more robust functionality than legacy change auditing solutions. Netwrix Auditor has been already honored with more than **100 awards** and recognized by almost **160,000 IT departments** worldwide.

Deploy Netwrix Auditor Wherever You Need It

- Free 20-Day Trial for On-Premises Deployment: netwrix.com/freetrial
- Free Virtual Appliance for Hyper-V and VMware Hypervisors: netwrix.com/go/appliance
- Free Cloud Deployment from the AWS, Azure and CenturyLink Marketplaces: netwrix.com/go/cloud

netwrix.com/social

Netwrix Corporation, 300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618, US

Toll-free: 888-638-9749

Int'l: +1 (949) 407-5125

EMEA: +44 (0) 203-318-0261