netwrix

Keeping Tabs on the Top 5 Critical Changes in Exchange Online with Netwrix Auditor

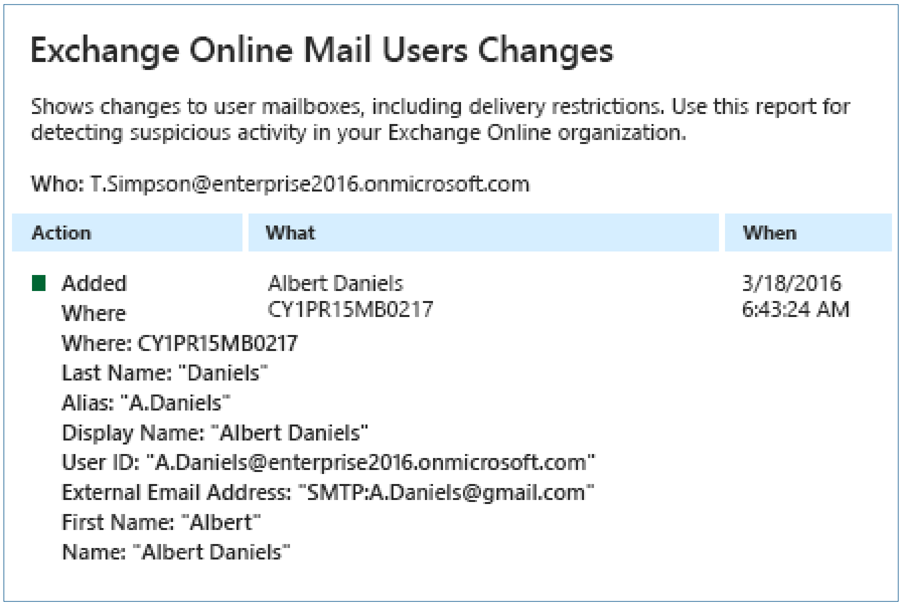
www.netwrix.com | **Toll-free**: 888.638.9749

Table of Contents

#1: Mailbox Changes

If a user mailbox is improperly modified or deleted, the user may lose access to it. And unauthorized creation of a mailbox can be a sign that a malefactor is trying to get access to your cloud-hosted Exchange Server to perform phishing or spam attacks.
Netwrix Auditor tracks all mailbox changes and helps answer the following questions:

- Who made mailbox changes?
- Which mailboxes were changed?
- What changes were made to each mailbox?
- When was the mailbox changed?
- In which Exchange Online Server was the changed mailbox located?



Exchange Online Mail Users Changes

Shows changes to user mailboxes, including delivery restrictions. Use this report for detecting suspicious activity in your Exchange Online organization.

Who: T.Simpson@enterprise2016.onmicrosoft.com

Action	What	When
🟩 Added Where	Albert Daniels CY1PR15MB0217	3/18/2016 6:43:24 AM

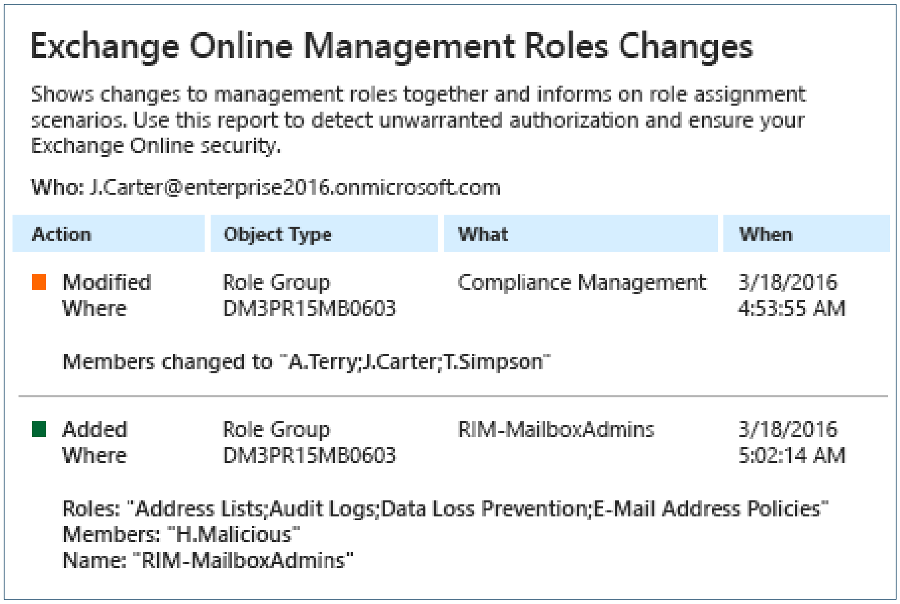
Where: CY1PR15MB0217
Last Name: "Daniels"
Alias: "A.Daniels"
Display Name: "Albert Daniels"
User ID: "A.Daniels@enterprise2016.onmicrosoft.com"
External Email Address: "SMTP:A.Daniels@gmail.com"
First Name: "Albert"
Name: "Albert Daniels"

#2: Changes to Exchange Role Groups

Adding a user to a management role group on a cloud-hosted Exchange Server gives that user full control over that server. The user can delete mailbox databases, edit send/receive connectors and change mailbox permissions — any of which can lead to a security breach.

Netwrix Auditor tracks all changes to Exchange Online role groups and helps answer the following questions:

- Who changed an Exchange Online role group?
- Which groups were changed?
- Who was added to or removed from each group?
- How was the Exchange Online role group changed?
- In which Exchange Online Server was the changed group located?
- When was the group changed?



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.

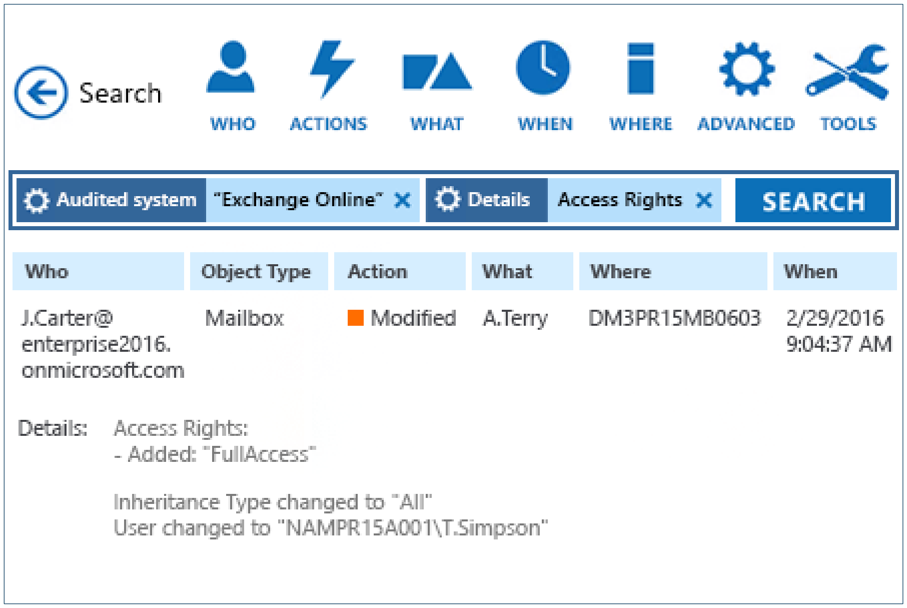
Who: J.Carter@enterprise2016.onmicrosoft.com

Action	Object Type	What	When
🟧 Modified Where	Role Group DM3PR15MB0603	Compliance Management	3/18/2016 4:53:55 AM
Members changed to "A.Terry;J.Carter;T.Simpson"			
🟩 Added Where	Role Group DM3PR15MB0603	RIM-MailboxAdmins	3/18/2016 5:02:14 AM
Roles: "Address Lists;Audit Logs;Data Loss Prevention;E-Mail Address Policies" Members: "H.Malicious" Name: "RIM-MailboxAdmins"			

#3: Changes to Mailbox Permissions

Anyone who has mailbox permissions can delete emails, forward them to another recipient, change mailbox content and more. All of these actions can go unnoticed by the mailbox owner and IT staff unless continuous monitoring of mailbox permission changes is in place.
Netwrix Auditor tracks all changes to mailbox permissions and helps answer the following questions:

- Who made changes to mailbox permissions?
- Which mailboxes were affected?
- In which Exchange Online Server was each change made?
- When was each change to mailbox permissions made?
- What changes were made?



Audited system "Exchange Online" ✕ Details Access Rights ✕

Who	Object Type	Action	What	Where	When
J.Carter@ enterprise2016. onmicrosoft.com	Mailbox	🟧 Modified	A.Terry	DM3PR15MB0603	2/29/2016 9:04:37 AM

Details: Access Rights:
- Added: "FullAccess"

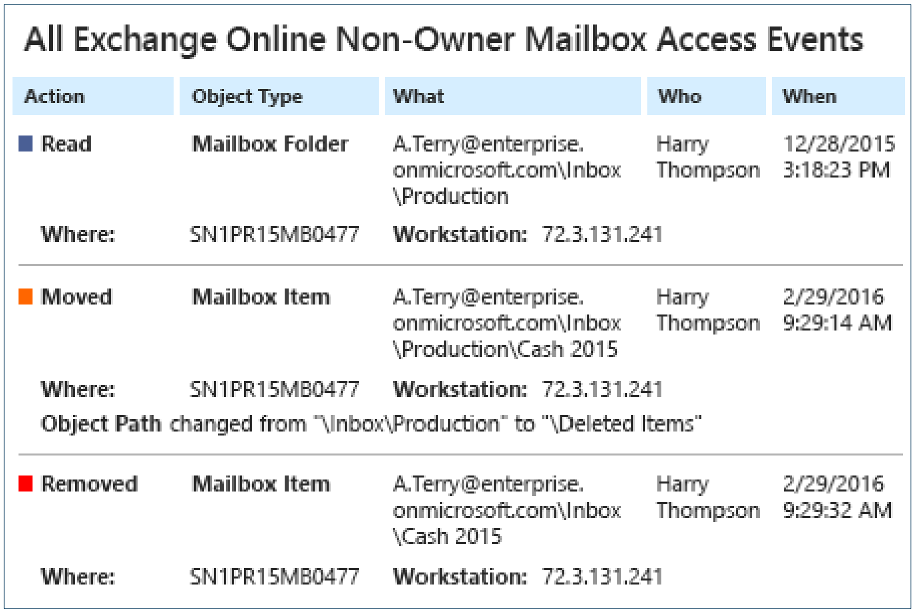
Inheritance Type changed to "All"
User changed to "NAMPR15A001\T.Simpson"

#4: Mailbox Access and Content Changes Performed by Non-Owners

Non-owners with permissions to access other users' mailboxes can misuse sensitive data, for example, by reading, copying or forwarding it. Without continuous monitoring of non-owner mailbox access events in Exchange Online, IT admins cannot maintain security and prevent leakage of sensitive data in the cloud.

Netwrix Auditor tracks non-owner mailbox access and helps answer the following questions:

- Who accessed a mailbox?
- Which mailbox was accessed?
- What operations were performed to a mailbox?
- In which Exchange Online Server was the mailbox accessed?
- When was the mailbox accessed?



All Exchange Online Non-Owner Mailbox Access Events

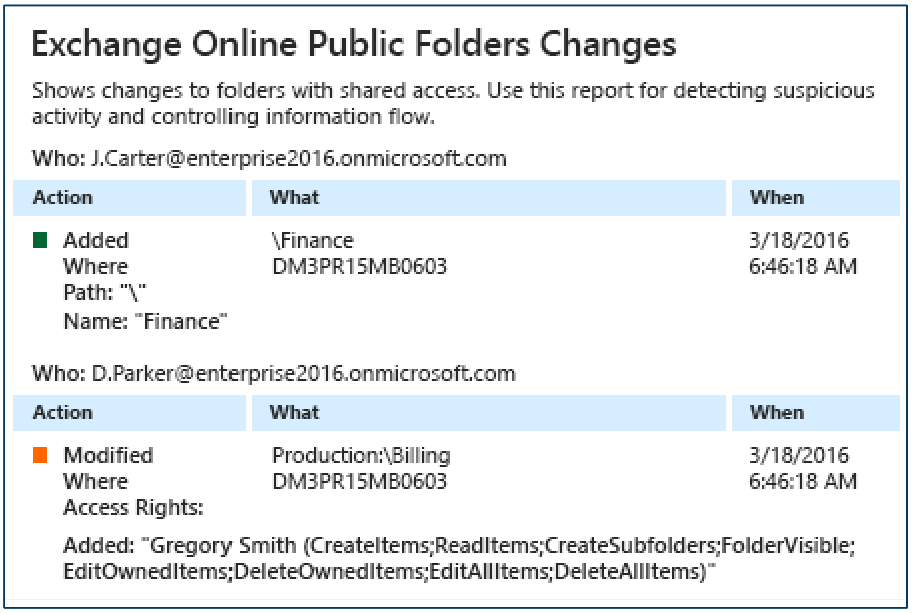
Action	Object Type	What	Who	When
🟦 Read	Mailbox Folder	A.Terry@enterprise.onmicrosoft.com\Inbox\Production	Harry Thompson	12/28/2015 3:18:23 PM
Where:	SN1PR15MB0477	Workstation: 72.3.131.241		
🟧 Moved	Mailbox Item	A.Terry@enterprise.onmicrosoft.com\Inbox\Production\Cash 2015	Harry Thompson	2/29/2016 9:29:14 AM
Where:	SN1PR15MB0477	Workstation: 72.3.131.241		
Object Path changed from "\Inbox\Production" to "\Deleted Items"				
🟥 Removed	Mailbox Item	A.Terry@enterprise.onmicrosoft.com\Inbox\Cash 2015	Harry Thompson	2/29/2016 9:29:32 AM
Where:	SN1PR15MB0477	Workstation: 72.3.131.241		

#5: Changes to Public Folders

An unauthorized user who gets access to a public folder can read and change its content, delete or relocate the folder, or perform other actions, depending on the specific permissions obtained. Such misuse of permissions can lead to data losses and leaks.

Netwrix Auditor tracks all changes to public folders and helps answer the following questions:

- Who changed any public folder?
- Which public folders were changed?
- What was changed in each public folder?
- In which Exchange Online Server was each public folder changed?
- When was each public folder changed?



Exchange Online Public Folders Changes

Shows changes to folders with shared access. Use this report for detecting suspicious activity and controlling information flow.

Who: J.Carter@enterprise2016.onmicrosoft.com

Action	What	When
🟩 Added Where Path: "\" Name: "Finance"	\Finance DM3PR15MB0603	3/18/2016 6:46:18 AM

Who: D.Parker@enterprise2016.onmicrosoft.com

Action	What	When
🟧 Modified Where Access Rights:	Production:\Billing DM3PR15MB0603	3/18/2016 6:46:18 AM

Added: "Gregory Smith (CreateItems;ReadItems;CreateSubfolders;FolderVisible; EditOwnedItems;DeleteOwnedItems;EditAllItems;DeleteAllItems)"

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 at rest regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs. Netwrix Auditor helps organizations detect data security threats on premises and in the cloud, pass compliance audits with less effort and expense, and increase the productivity of security and operations teams.

Netwrix Auditor enables auditing of the broadest variety of IT systems, including Active Directory, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, SQL Server, VMware and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises and cloud-based IT systems in a unified way. More than 230,000 IT pros worldwide rely on Netwrix Auditor to secure IT infrastructure, prove compliance and increase operational efficiency. The product has earned over 90 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

Download Free Trial: www.netwrix.com/auditor.html

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

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-318-0261