

# **SysAdmin** **Magazine** netwrix

## **Let's Talk Security**



May 2016

# Contents

**3** **Introducing Netwrix Auditor 8.0. What's New?**  
by Michael Fimin

**6** **What You Need to Know About Cloud Security Breaches**  
by Alex Vovk

**8** **5 Initiatives to Enhance Security Awareness in Organization**  
by Richard Muniz

**12** **Exchange Best Practices: How to Detect Who Accessed Another User's Mailbox**  
by Danny Murphy

**14** **Tech Guide: Group Policy for Password Monitoring**  
by Matt Hopton

**17** **Free Tool of the Month: Effective Permissions Reporting Tool**

Introducing Netwrix Auditor 8.0

# Detect Data Security Threats — on Premises and in the Cloud

NEW

## Netwrix Auditor for Office 365



Strengthens the security of data in the cloud by auditing all changes to security settings and non-owner mailbox access in Microsoft Exchange Online.

NEW

## Netwrix Auditor for NetApp



Enables you to detect insider threats and prevent breaches of unstructured data in all the latest versions of Data ONTAP, including 8.3.2.

NEW

## Netwrix Auditor for EMC



Solidifies threat resilience with complete visibility into changes and data access in EMC Isilon, VNX and VNXe.

ENHANCED

## Netwrix Auditor for Windows File Servers



Now provides security analytics about effective permissions for unstructured data by correlating both NTFS and share-level permissions.

ENHANCED

## Netwrix Auditor for SharePoint



Enables you to establish audit controls and prevent unstructured data exfiltration by providing visibility into data access.

[Lean More](#)

---

# FAQ: What's New in Netwrix Auditor 8.0?



**by Michael Fimin**  
Netwrix Co-founder and CEO

Netwrix has introduced its major release of **Netwrix Auditor 8.0**. New Netwrix Auditor provides complete visibility into hybrid cloud IT infrastructures to protect corporate data at rest regardless of its location.

The new version of company's leading IT auditing platform simplifies detection of security threats and enables organizations to gain rigorous control over critical data across all levels of IT environment, including hybrid cloud and storage appliances



---

**Q:** Are you planning to support EMC Isilon?

**A:** Great news, we are introducing a new application for EMC storage auditing. Netwrix Auditor for EMC delivers visibility into changes and data access for EMC Isilon, as well as VNX and VNXe.

**Q:** Will this version support NetApp?

**A:** The answer is yes. Another new application Netwrix Auditor for NetApp supports all the latest versions of Data OnTAP, including 8.3.1. and 8.3.2. All this is available as a part of Netwrix Auditor 8.0 starting from April 12, 2016.

**Q:** When API would be available?

**A:** Along with other features, Netwrix Auditor 8.0 offers its customers **RESTful API** to enable endless integration with any existing on-premises or cloud-based application. The release date is April 12, 2016.

**Q:** Will this version work with other services or applications?

**A:** *There was a number of questions about: Dropbox, Citrix ShareFile, AirWatch, MobileIron, SharePoint Online, Linux/Unix, etc.*

These systems are not yet supported by Netwrix Auditor out of the box. However, Netwrix API is available to all customers starting on April 12. What does this mean for you:

You can start building your integrations with any systems you may need. We consider releasing an API-based add-on for the most requested systems, so stay tuned! We consider to continue adding fully functional support for new systems in the future releases.

Do you need to audit something we don't support yet? Please keep the feedback coming, tell us in the comments below.

**Q:** I heard last time about integration with Splunk. I believe this is available in 8.0. Can you confirm?

**A:** Yes, Netwrix Auditor 8.0 continues to support integration with Splunk. This functionality will allow you to bring more context into your Splunk data and [slash your SIEM costs](#).

**Learn More:**  
**Netwrix Auditor 8.0.**



---

# What You Need to Know About Cloud Storage Security Breaches



**by Alex Vovk**  
Netwrix Co-founder and CEO

As more and more companies join Netflix, Pinterest, and Apple in moving to the cloud, hackers – and a healthy dose of user error – are making these large sources of sensitive information more sensitive to breach.

Recent breaches affecting Dropbox and Google Drive show that this new generation of storage solutions have yet to meet their match of security tools to counter the growing threats to cloud storage.



---

Are you confident that your organization's cloud storage is secure? If not, read on.

### **Why Is Cloud Storage At Risk?**

Cloud storage is uniquely susceptible to security breach because of the significant amount of noise generated by today's cloud storage solutions. It's also difficult to maintain an awareness of overall security when individual links or uploaded items can have a variety of shared settings, sometimes with public access or inclusion in public search results.

With so many users having access to one pile of data, it becomes difficult to focus on tangible methods of prevention and detection of new threats — and IT pros are feeling the stress.

The solution to [cloud storage security](#) is not fortifying the walls of your existing network; after all, the purpose of cloud storage in many situations is to provide access to data to teams that need it, often virtually or across the globe. Instead, it comes down to a new approach to preventative action.

### **Guaranteeing Cloud Storage Security for Your Organization**

Want to bring more attention to securing your company's sensitive data? Here are three things you can do to improve your ability to keep your cloud storage secure from hackers and user error:

#### **Don't assume cloud storage is the same as on-site storage**

When you shift your organization's storage to the cloud, new rules apply. Sharing settings, network

reliability, and server reliability are all factors that can shift according to user settings and circumstances.

#### **Build or purchase your storage solution with security in mind**

Have security baked in from the start rather than treating it as an add-on to an already existing storage solution. Newer platform approaches have built-in API-based services that can be embedded into the app rather than something added after the fact.

#### **Intelligent security tools can help you**

Intelligent security tools scale to your data and cloud configuration. Furthermore, you can deploy contextual security around your data, your users, and their respective storage needs, recording and monitoring that data without burdening your busy IT team. [Click here](#) to get a sense of which solution might be best for your organization.

The new generation of cloud storage brings with it attractive capabilities that draw in bigger and bigger companies over time. However, this generation has yet to uncover the best and most secure methods for maintaining tight control over who has access to the data. Use these tips to make sure that your company's cloud storage remains secure.

**Read More:**  
[Breaches related articles](#)

---

# 5 Initiatives to Enhance **Security Awareness** in Organization



**by Richard Muniz**

Deployment Engineer.

Some time ago there was a big discussion on Spiceworks about FedEx data leakage. Roughly 5 GBs of data was going from it daily to an IP address in Bulgaria. Since a third-party actually owned the system, they were somewhat limited in what they could do and was wondering what to do next.



Most of the advice posted in the Spiceworks post tread dealt with how to determine what was going out. In this blog we'll try to think in terms of having things in place to guard against the day when we suspect something is going on.



---

## 1. Look at your risks

Determine what data you need to monitor and watch. What information has personal data in it, and what do you absolutely need to keep things running (user and email accounts and such)? Identifying this will help drive that 20 cent word “Mitigation” which we define as taking the worst thing that can happen and either eliminate the possibility of it occurring or minimizing the impact. You may also want to know about certain events happened such as deletion or copying of files. Set up you’re auditing program, or set scheduled tasks on the file server to notify you when certain events occur.

*Part of the mitigation process might include configuring NTFS permission to deny anonymous access to certain files and to ensure only authorized individuals are hitting it.*

## 2. Consider at least two scenarios

Your plan should have a couple of scenarios, everything from just one machine doing weird stuff to Denial of Service Attacks. Part of what you need to consider is laws in relation to data breeches. Part of the headache here is finding out governmental laws, and understanding how they apply to your particular case. Most will at a minimum include written notification and credit counseling.

## 3. Have a decision matrix

Several of the crucial decision you need to have mapped out is what to when a breach in discovered. Some the events you need to have mapped out are:

What to do when the breach is discovered. Is it still happening? And then what do you do? Do you drop the Internet connection (creating a Denial of Service event on yourself and possibly tipping the cyber-crook that you’re on to them), or do just let it keep going. When do you call for additional help, and when do you call in Law Enforcement?

---

## 4. Who you going to call?

Obviously you're going to want a Computer Forensic expert to help sift through all the files and etc. to determine what happened. There are several things you want to look for when it comes to an expert however:

- Experience: Has this individual or company ever done this before?
- Court: Is the investigator an expert witness. In short, are the credentials such that the court can recognizer has recognized them as an expert in the field
- Training: The investigator should hold several certifications in the field, and should be current as far as training is concerned. Things change fast in IT, and they need to keep up.
- Professional Association: What are they a member of?

## 5. Handle information

Part of your planning needs to include who key individuals are that need notification. One person that often not thought of is whoever handles Public Relations. While it's doubtful that we in IT will be the party handling that, whoever does needs to know what information to put out, through what conduits, and most of all, not to give information they don't know (for example, a reported asks "Who many people are impacted by the breech"? If the Public Relations Officer doesn't know, their response should be something like, "We don't have an exact number yet. Out forensic investigators are determining that and as soon as we have numbers, we'll let you know") or speculate. The best advice here is stick to the facts you have rather than look stupid later.

**Read More:**  
[Security related articles](#)

# Free Training Academy for IT Pros

Free training materials designed to help IT Pros gain visibility into their hybrid-cloud IT environments for security and compliance

How-to's  
Exam Study Guides  
Research



Visit Academy

---

# Exchange Best Practices:

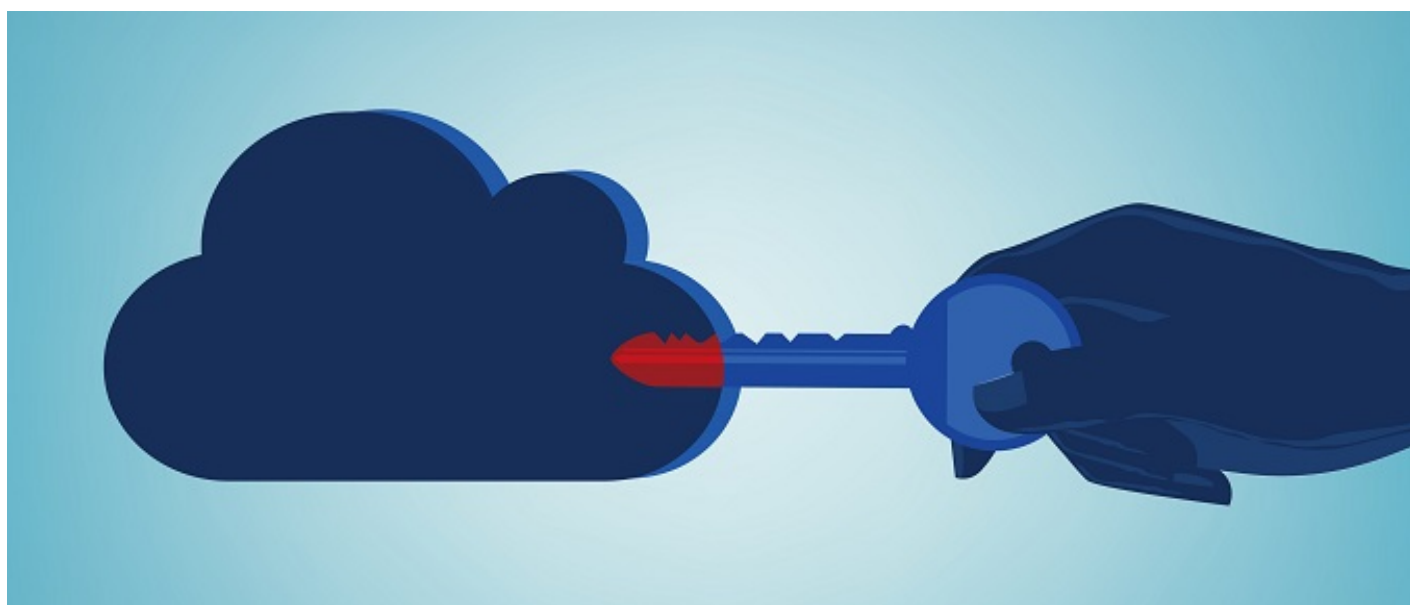
## How to Detect Who Accessed Another User's Mailbox



**by Danny Murphy**

Systems administrator and IT evangelist

Using shared mailboxes in Office 365 can facilitate communication in team projects. However, giving multiple users access permissions for the same mailbox increases the risk of security incidents and leaks of sensitive data. Non-owners with access rights can, unintentionally or maliciously, forward a message, move an e-mail with sensitive content to another location, or — even worse — delete something important from an Exchange Online shared mailbox.



1. Open PowerShell -> Run the following command to connect with Exchange Online instance and enter your credentials in the pop-up window:

```
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic
-AllowRedirection
Import-PSSession $Session
```

2. To enable mailbox auditing run:

- **For a single mailbox:**

```
Set-Mailbox -Identity "TestUser" -AuditEnabled $true
```

- **For all mailboxes:**

```
$UserMailboxes = Get-mailbox -Filter {(RecipientTypeDetails -eq 'UserMailbox')}
$UserMailboxes | ForEach {Set-Mailbox $_.Identity -AuditEnabled $true}
```

- **To check what mailboxes have auditing enabled run:**

```
Get-Mailbox | FL Name,AuditEnabled
```

3. Open Exchange Administration Center -> Navigate to “Compliance Management” Auditing.

4. Click “Run a non-owner mailbox access report”. You will get the report on non-owner access to all mailboxes with enabled auditing over the past two weeks.

5. To view non-owner access to a specific mailbox Click on a mailbox to view all non-owner access events with the details.

Time:	2/29/2016 11:29 AM
Performed by:	Harry Thompson
Signed in as:	User with delegate access
Operation:	Move
Subject:	Cash 2015
Source:	Inbox\Production
Destination:	Deleted Items
Status:	Succeeded

Time:	2/29/2016 11:29 AM
Performed by:	Harry Thompson
Signed in as:	User with delegate access
Operation:	Hard-delete
Subject:	Cash 2015
Source:	Inbox
Status:	Succeeded

**Read More:**  
**How-tos for IT Pros**



---

# Tech Guide: Group Policy for Password Monitoring



**by Matt Hopton**

Network Manager

As an administrator, you have to ensure that your network is secure. A big part of that includes deciding on a password strategy for user accounts and administrator accounts. You can educate your users on best practices for password creation but you can also enable policies that force users to adhere to the best practices. In addition, you can monitor your network for password changes and account lockouts.



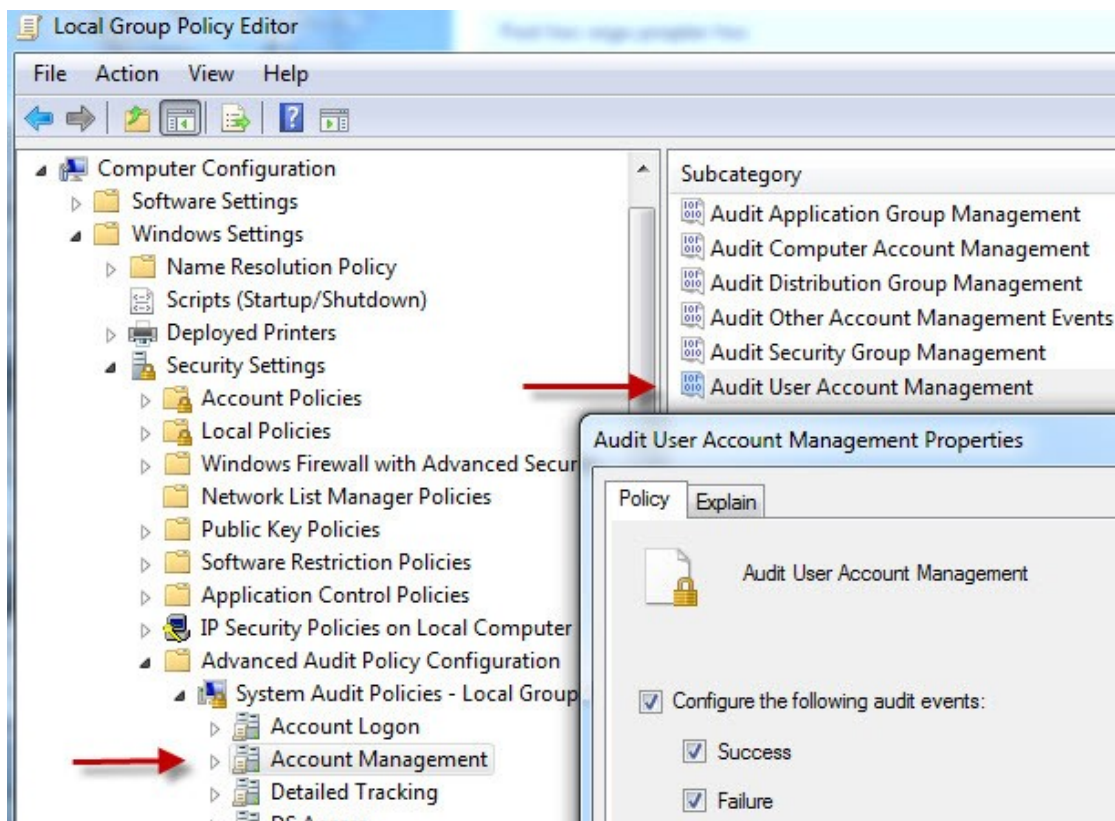
## Educating Users

- Require the use of strong passwords. Below is the definition of a **Strong password as defined by Windows**:
  - a. Password is at least eight characters long.
  - b. Does not contain your user name, real name, or company name.
  - c. Does not contain a complete word.
  - d. Is significantly different from previous passwords.
  - e. Contains characters from each of the following four categories: Define a Minimum password length policy setting so that passwords must consist of at least a specified number of characters. Long passwords—seven or more characters—are usually stronger than short ones. With this policy setting, users cannot use blank passwords, and they have to create passwords that are a certain number of characters long.
- You always hear that passwords should never be written down. In some cases, a password may be too complex to memorize. If that is that case, be sure to store the paper in a secure place and destroy it when it is no longer needed.
- Never share passwords.
- A different password should be used for all user accounts.
- If a password is believed to have been compromised, it should be changed immediately.
- If there is an option for an application to remember the password, the user should choose never.
- Do not allow previous passwords to be used.
- Require users to change their passwords on a regular basis. Depending on your organization, a good rule of thumb is for users to change passwords every 90 days and administrators to change their passwords every 30 days.
- Define a minimum password age to prevent users from repeatedly changing their passwords to bypass the enforce password history policy.

## Group Policy to Monitor Password Changes

The Group Policy that you need to enable to monitor password changes is the User Account Management Audit Policy. This policy setting allows you to [audit changes to user accounts](#) to include when a user account is created, changed, deleted; renamed, disabled, enabled, locked out, or unlocked. It also monitors when a user account's password is set or changed.

You can get to this setting by going to Computer Configuration | Windows Settings | Security Settings | Advanced Audit Policy Configuration | Account Management | User Account Management. (see figure 1)



After enabling the Success and Failure of the Audit User Account Management, you can look for the events 4273 and 4274 in the Security log of the Event Viewer. Event 4273 indicates an attempt was made to change an account's password and Event 4274 indicates an attempt was made to reset an account's password. (see figure 2)

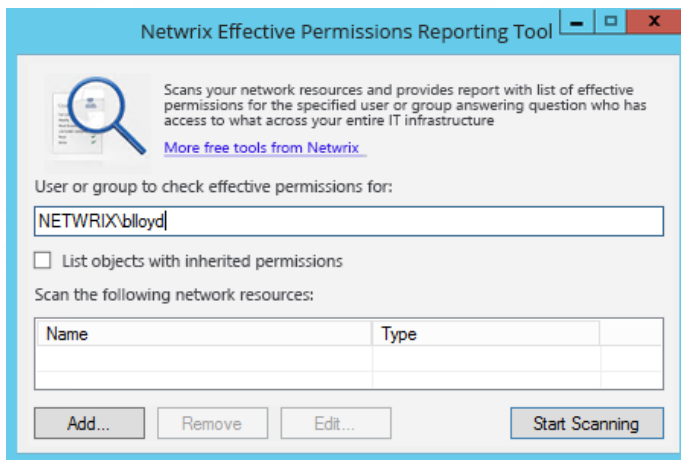


# Free Tool of the Month

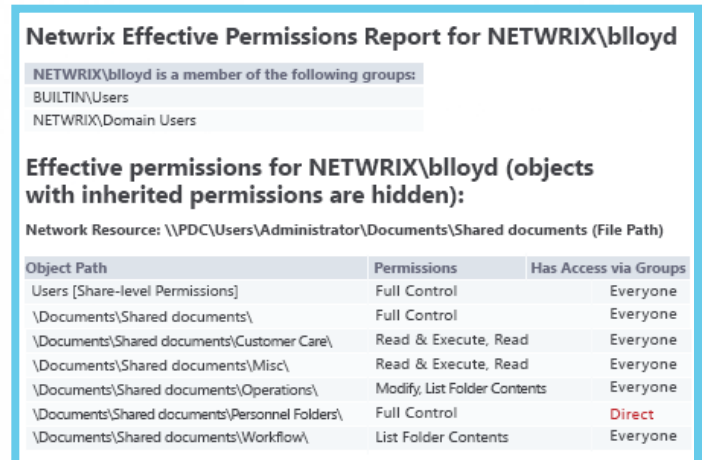
## Effective Permissions Reporting Tool

Free **Effective Permissions Reporting** Tool helps you make sure that employees' permissions correspond to their roles in your organization by showing who has permissions to what in Active Directory and File Shares.

### Tool in Action



Check any user or group you want for validation of their effective permissions



Get an easy-to-read report showing effective permissions and group memberships for specific user or group

Get Freeware



# Next Steps:

**Try:** auditing software to ensure your network security  
[netwrix.com/go/auditor](http://netwrix.com/go/auditor)

**Learn:** 70-410 Exam Study Guide  
[netwrix.com/go/study\\_guide](http://netwrix.com/go/study_guide)

**Watch:** educational webinars with IT experts  
[netwrix.com/go/webinars](http://netwrix.com/go/webinars)

[netwrix.com](http://netwrix.com) | Follow us



**Corporate Headquarters:** 8001  
Irvine Center Drive, Suite 1100  
Irvine, CA 92618

**Phone:** 1-949-407-5125  
**Toll-free:** 888-638-9749  
**EMEA:** +44 (0) 203-318-02

**netwrix**

Copyright © Netwrix Corporation. All rights reserved. Netwrix is trademark of Netwrix Corporation and/or one or more of its subsidiaries and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are the property of their respective owners.