ManageEngine
RecoveryManager Plus

Regulatory compliance with customizable retention policies

Introduction

Due to regulatory compliance policies or internal policies, organizations may be required to store data in their Exchange Online and other Office 365 services for a fixed amount of time, and violating these regulations can be costly.

It's crucial that organizations find a way to comply with all retention policies to ensure they don't incur severe financial penalties, and also to retain the trust of their customers.

Can I do this with native tools?

Microsoft allows administrators to define retention policies, also called litigation holds, which can be used to ensure regulatory compliance. When applied to mailboxes, retention policies ensure that no content can be deleted from them. Retention policies can be applied to entire mailboxes, or just specific items that fit certain criteria such as emails to and from a particular email address, emails with particular phrases or words, etc.

In short, native tools can be used to achieve regulatory compliance, but there are a couple of limitations when you rely on them.

What are the limitations of retention policies?

1. Increased mailbox sizes and potentially higher costs for storage

Any retention policy can be turned off by the administrator at any time, and any item can be removed from mailboxes after the policy has been switched off. If your administrators turn rogue, or if your privileged accounts' credentials are compromised, the retention policy can be paused until all items have been purged from your mailboxes.

To combat this, Microsoft provides a feature called **retention lock or preservation lock** that ensures no one, including administrators, can turn the retention policies off or make them less restrictive. However, retention locks allow administrators to widen the scope of a retention policy by adding locations or extending its duration. Retention lock prevents people with malicious intentions from undoing the retention policy.

The downside of a retention lock is that this change can never be undone. A restrictive and wide retention lock can quickly result in your allotted storage space being filled up, and you might be forced to buy additional storage space from Microsoft.

Depending on the size of your organization and the volume of data that passes through your mailboxes on a daily basis, you could end up spending quite a bit on storing all your data.

2. Inability to recover from ransomware attacks

Almost all ransomware attacks have targeted files in computers and other storage devices, and owing to large-scale attacks like WannaCry and Petya, most organizations are aware of the kind of damage ransomware can cause. However, most don't know that in 2018, a white hat hacker developed a ransomcloud strain that can encrypt Office 365 emails in real time.

Ransomware can encrypt all emails and other items in your mailboxes even if a litigation hold is applied. The presence of a litigation hold does not mean you can restore a mailbox to a previous point-in-time, and Microsoft has explicitly mentioned that mailbox point-in-time recovery is not in its scope.

Overcoming the native tool's limitations

The easiest way to overcome the native tool's limitation is by deploying a third-party Office 365 backup solution like RecoveryManager Plus.

With RecoveryManager Plus, you can:

1. **Customize retention policies to comply with regulations**

   Create retention policies for your Office 365 backups, and automatically discard backups when the retention limit is reached. All data in your mailboxes, even the deleted data in first-stage and second-stage Recycle Bins, is backed up.

2. **Store all backups locally**

   All backup data is stored within your premises in your existing data centers. Having all the data in your mailboxes backed up allows you to delete items from your mailboxes, so you don't have to worry about running out of mailbox storage.

3 Ability to recover from ransomware attacks

In case of ransomware attacks, you can delete all the encrypted mailbox data and restore the mailbox data from the backups.