SpinOne

A guide on protecting Office 365 from ransomware

- The impact of ransomware
- Ransomcloud: ransomware is coming to the cloud
- G Suite native ransomware protection solutions
- Best practices to prevent ransomware attacks

In addition to fully-featured Software-as-a-Service offerings such as Office 365, there are equally ominous threats to your data, both on-premises as well as in your Office 365 environment. Arguably, the most ominous threat to your data is ransomware.

In this Office 365 ransomware protection guide, we will take a look at how ransomware can affect your Office 365 environment as well as what tools are available to both protect and secure your data in Office 365 from ransomware.

SpinOne

Contents

01

WHAT IS RANSOMWARE?

SaaS Data Protection Guide

First of all, it is important to better understand what ransomware is exactly. Understanding how it works, how it can infect your environment, and how you can protect your valuable business-critical data, are key to successfully defeating it. Ransomware is a specialized type of malware that holds your data “hostage” and uses the demand for a ransom payment to return access to your data.

How is ransomware able to successfully “lock” you out of your own data?

Ransomware slyly infiltrates your own computer, assumes the identity of the user you are logged in with (with all the permissions and rights given), and encrypts all the files, folders, and other data to which you have access.

This can include all data that is stored locally, data that exists across shared network drives, and **even data that is housed in your Office 365 environment**. Below is an example of a ransom demanded by one of the popular ransomware variants known as **CrytoLocker**.

Many may underestimate the threat of ransomware on business-critical data stored in cloud environments, even discounting this threat altogether.

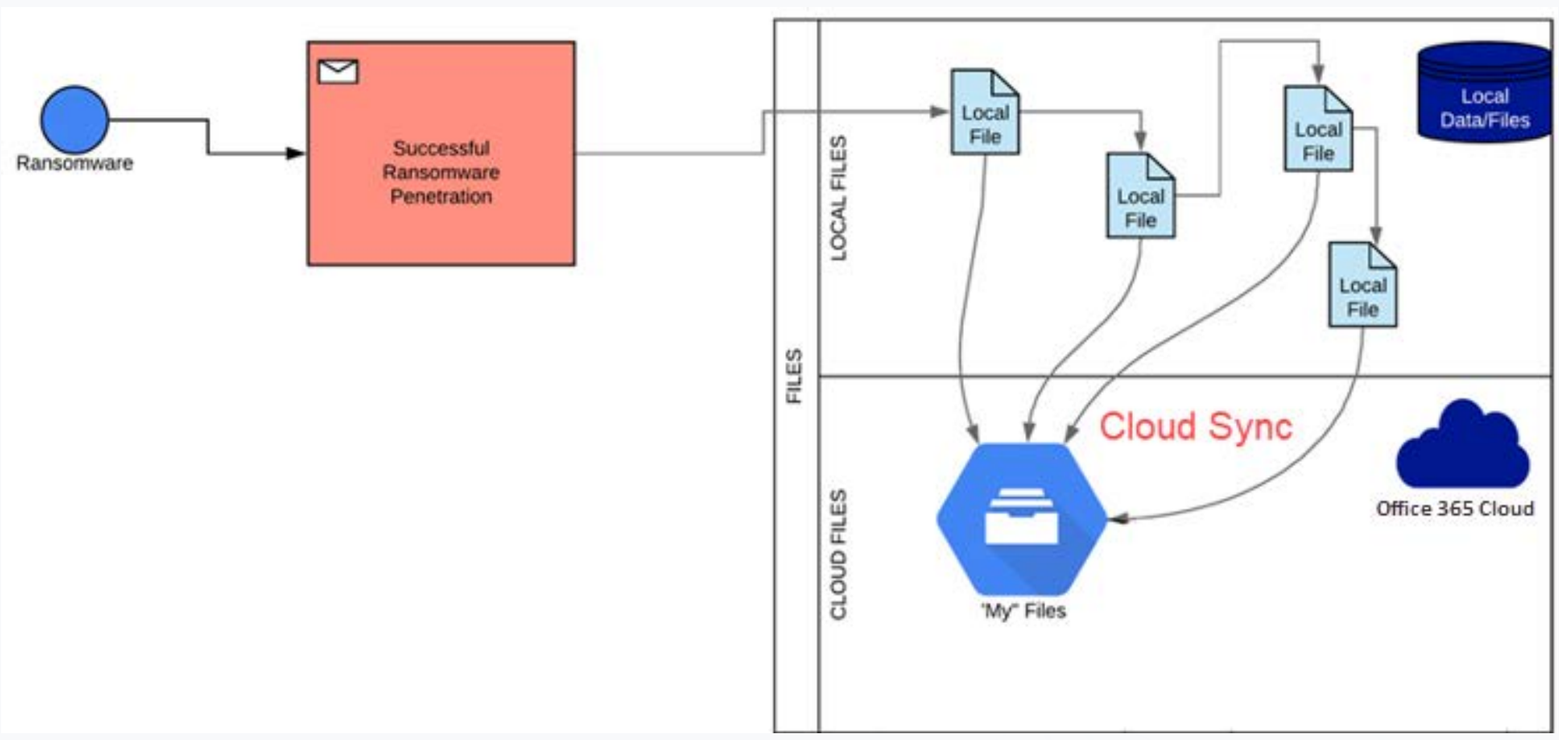
How can ransomware variants like CryptoLocker infect files that are stored in your Office 365 OneDrive for Business storage?

A tremendous threat to your cloud environment is **file synchronization**.

Most of the popular cloud SaaS offerings including Office 365 provide the ability to synchronize files stored on-premises with your Office 365 OneDrive for Business storage. This allows keeping copies of files both locally and in the cloud for collaboration purposes.

Cloud synchronization generally works based on detected file changes between on-premises and cloud copies of your data. If a file is updated, the file synchronization trigger is activated and the copy of the file in Office 365 OneDrive storage is updated with the copy stored locally. When the ransomware encrypts a locally synchronized OneDrive file, the ransomware encryption of a file is viewed as a simple “change” in the file and is synchronized.

Thinking about ransomware, from a security and business continuity perspective, this is extremely dangerous. Since OneDrive for Business storage can be shared across many users for collaboration purposes, it provides an extremely enticing target for ransomware. A single end-user who is infected with ransomware can inadvertently synchronize ransomware encrypted files to the cloud resulting in file access disruption for all users attached to shared OneDrive storage.



Synchronizing on-premises files with OneDrive can propagate ransomware infections

Aside from OneDrive file storage targeted by ransomware, there is another dangerous target in your Office 365 environment that can cause major business-continuity issues. That target is your Office 365 **email**.

RANSOMCLOUD

The emerging cloud security threat

Another ransomware variant that can wreak havoc on your Office 365 environment does not affect OneDrive storage but rather your Office 365 email. This type of ransomware attack has been named “Ransomcloud” by “black hat” turned “white hat” hacker, Kevin Mitnick who exposed this threat to the masses.

Ransomcloud has been demonstrated to do what no other ransomware variant before it could. It can successfully encrypt an Office 365 user email inbox so that all emails are encrypted in real-time after infection occurs. Alarmingly, all the end-user has to do to fall victim is click a simple “permissions allow request” to a fictitious email attachment posing as a legitimate Microsoft service.

Email in most organizations is the primary communication platform. Ransomware that denies access to your organization’s email resources can certainly result in major challenges to your business-continuity.

04

HOW OFFICE 365 PROTECTS FROM RANSOMWARE

SaaS Data Protection Guide

Does Microsoft protect you from ransomware?

Not entirely as we will see. However, there are native tools available in your Office 365 environment that can reduce the threat of ransomware and remediate its effects to some degree. Let's take a look at the following native built-in tools to protect and secure your Office 365 environment from ransomware:

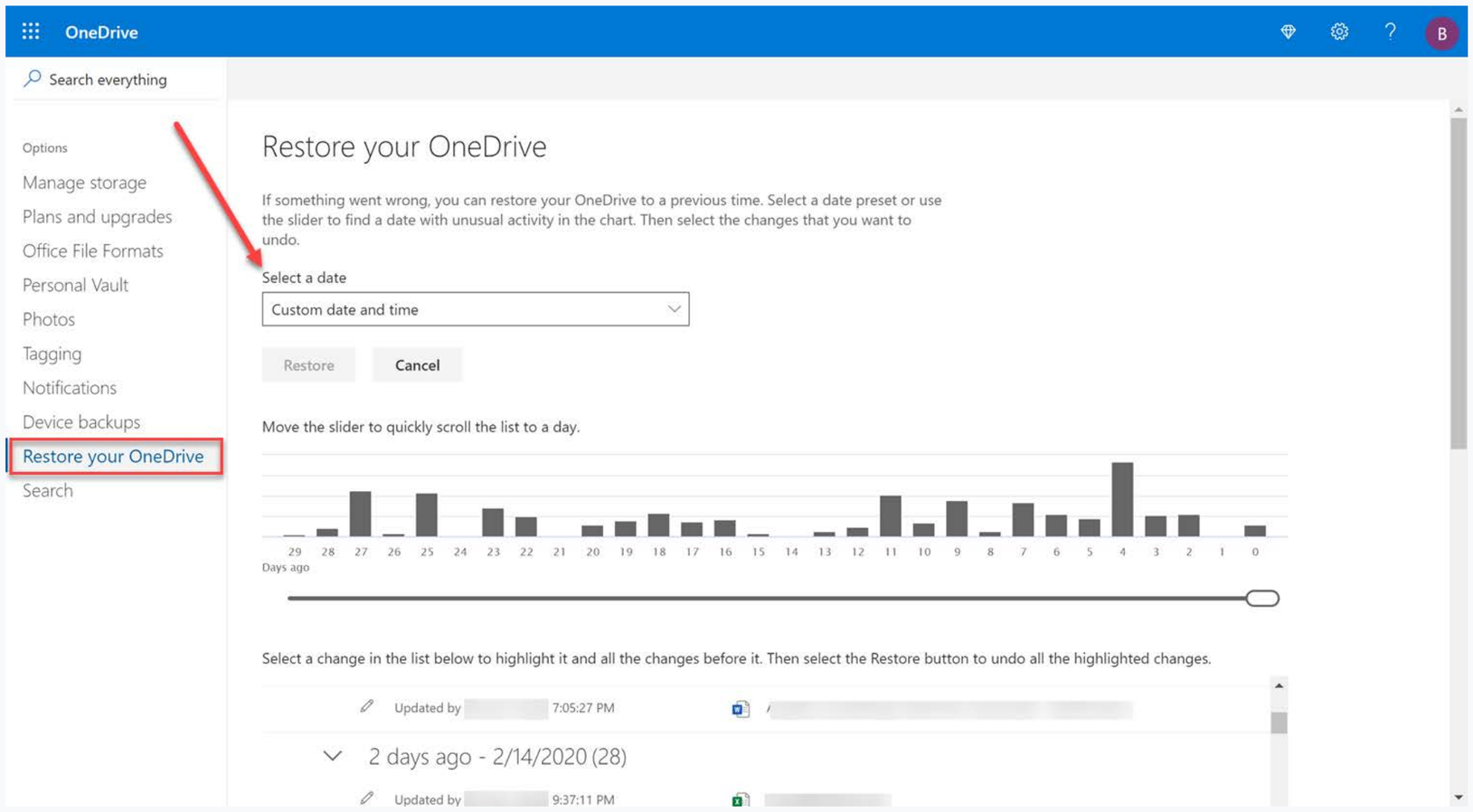
1. Files restore
2. Ransomware detection and recovery

How do each of these mechanisms protect you from data loss? Are they enough?

Files Restore

Microsoft has included a new feature called **files restore** in both OneDrive for Business and Personal editions. Files restore is a new feature in OneDrive that allows you to recover an entire OneDrive to a previous point in time within the **last 30 days**. This feature can recover files that have been deleted as the result of a mass file delete operation, corruption, accidental unintended file saves, ransomware, or any other catastrophic event.

The **Restore your OneDrive** option is found under account options for OneDrive. The interface for using files restore is fairly simple and intuitive. You can either choose a recovery date by using the Select a data dropdown menu, or you can use the slider found underneath the



Using the Files Restore to recover files in OneDrive

The files restore capability in OneDrive is a great new feature to help recover your data from corruption as a result of a ransomware attack. Even though the files restore is a great start to native functionality that can help protect your data, it has limitations to be aware of.

As mentioned above, the files restore operation can only restore files within a window of 30 days. There may be cases where data corruption or file damage may fall outside of this window of time. Think about a case where a business-critical spreadsheet is only accessed on a monthly basis. What if damage to the spreadsheet is only discovered outside of the files restore 30-day time period?

Additionally, the files restore operation is a **manual** process. There is no automated workflow initiated to automatically recover data affected by a ransomware attack. It is dependent upon the Office 365 administrator to initiate this process. When hours or even minutes count to your business, manual processes can lead to extended disruption to business continuity.

Lastly, at this time, the files restore operation only covers OneDrive and SharePoint files. Office 365 email is currently not protected by the files restore functionality to allow rolling an email inbox back to a previous point in time or granularly recovering specific emails. This means there is currently no protection using files restore for a “Ransomcloud” attack.

Ransomware detection & recovery

Microsoft has also introduced a service that works in tandem with the files restore functionality called **ransomware detection & recovery**. This new capability allows Office 365 to now detect ransomware attacks proactively and help facilitate restoring OneDrive to a point in time prior to a ransomware attack.

If a ransomware attack is detected, Office 365 sends an alert via email, mobile, or desktop notification. In the notification, a link is included to the files restore dashboard with the recovery point in time automatically selected to revert files to a known good state. The process guides you through restoring files to a healthy state, prior to the ransomware attack.

Mobile notification from Office 365 of a ransomware attack (Image courtesy of Microsoft)

The new ransomware detection & recovery capability found in Office 365 is a welcomed new Office 365 feature that helps to speed along the process of manually restoring files using the files restore feature. However, the process to recover data relies on human intervention and using the manual steps required to roll back to a recovery point using files restore.

NATIVE TOOLS ARE NOT ENOUGH

Weaknesses of Native Office 365 Ransomware Tools

While the files restore tool and ransomware detection & recovery functionality are great steps in the right direction for protecting your Office 365 environment from ransomware using native tools, they may not be enough. There are currently gaps in the services covered, the recovery window, and the process to recover your data using these native capabilities:

1. You aren't able to recover individual files from earlier recovery points while maintaining the files that were added later. In other words, you can't recover files selectively. After clicking restore to a specific date, files added later the recovery point will be deleted.
2. The possibility of recovery is only for the next 30 days until today. If the attack occured more than a month ago and you discovered the attack later than a month ago, you won't be able to roll back the changes and restore your OneDrive.
3. Data recovery doesn't occur automatically. User intervention is always required.

Bolstering Office 365 data protection and security with a capable third-party solution that provides automated protection, recovery, and security features is a must.

How to Protect Office 365 from Ransomware

There are additional best practices and recommendations per Microsoft that can help protect your Office 365 environment from the threat of ransomware. These include:

07

OFFICE 365 SECURITY BEST PRACTICES

SaaS Data Protection Guide

How to Protect Office 365 from Ransomware

There are additional best practices and recommendations per Microsoft that can help protect your Office 365 environment from the threat of ransomware. These include:

- **Using an anti-malware solution** – Effective security often starts with a multi-layered approach. Protecting end-user devices from malware is a necessary part of your overall security posture. This includes automatic scans, periodic file scans, automatic download of signature updates, alerting, cleaning, and other operations for end-user clients.
- **Exchange Online Protection (EOP) filtering and customizations –** Exchange Online Protection (EOP) is on by default in Office 365. Customizations can be made by each company for filtering specific email content or to block custom patterns for various content. Along with the real-time and automatic response provided by EOP, the customizations can provide great protection against ransomware.
- **Prevent dangerous files through email –** Microsoft allows you to protect your business against ransomware even further by preventing potentially dangerous files altogether. These include Javascript, batch, and executables from being opened in Outlook. Learn how to configure this here.
- **Using Advanced Threat Protection (ATP) –** Office 365 ATP is an optional service that is provided in some plans or included in higher tiers of Office 365. It is a filtering service that provides additional protection against specific types of malware, including ransomware. Utilizing a feature called safe attachments, it can provide much better protection against zero-day ransomware (new ransomware for which there his no known signature or pattern).
- **Use SharePoint Online and OneDrive for Business recycle bins –** Included versioning with SharePoint and OneDrive for Business does not protect against ransomware that copies, encrypts, and then deletes the original files. In this case, the SharePoint Online and OneDrive for Business recycle bins can restore files that are up to 90 days old. If under 30 days, the files restore feature can also be used.

08

BEST-IN-CLASS RANSOMWARE PROTECTION

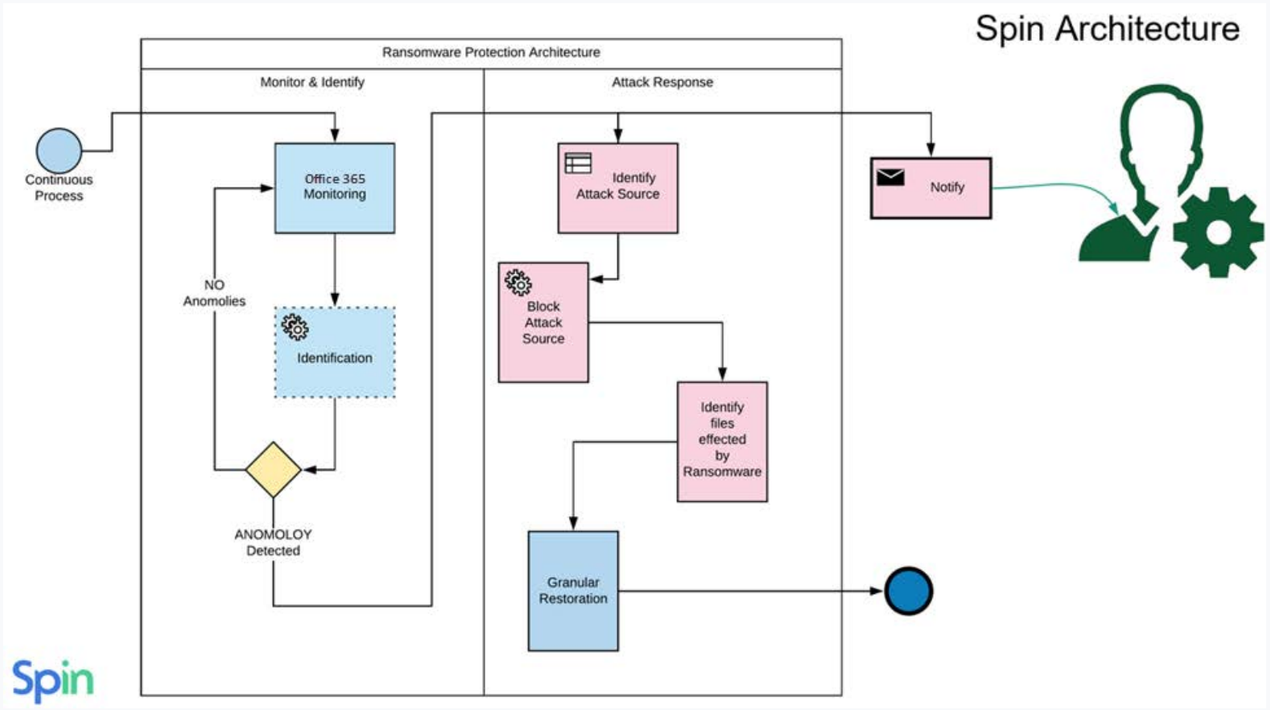
SaaS Data Protection Guide

SpinSecurity

When the very livelihood of your business is at stake (your business-critical data), you need to use the best solution available to safeguard your data from attack by ransomware. **SpinSecurity** from **SpinOne** is a “best-in-class” solution that provides the tools and capabilities needed to safeguard your data from the dangers of ransomware.
SpinSecurity is a modern API-driven CASB solution that makes use of machine learning to provide automated intelligence to fight today’s security threats such as ransomware. It does this by using a powerful two-fold ransomware protection architecture that can detect and remediate **99%** of all ransomware infections.

Ransomware Protection by SpinOne includes the following **four stages**:

- **Detect** – Machine learning algorithms monitor Office 365 for any anomalies that indicate a ransomware attack.
- **Stop** – SpinSecurity provides a quick and effective attack response. The attack source is identified and stopped immediately by blocking the ransomware process.
- **Remediate** - Once the attack is identified and stopped, any files affected by the ransomware attack are identified.
- **Recover** - SpinSecurity automatically restores the files that have been identified as affected by the ransomware attack. Office 365 administrators are notified of the attack and the automatic recovery.



SpinOne provides automated ransomware protection and remediation

SpinOne's two-fold, automated ransomware protection is unique among its competitors. Not only does SpinOne backup your business-critical data, it proactively monitors and secures your data against the very threats that often require data recovery such as ransomware.

SpinOne

ABOUT SPINONE

SpinOne is a multi-tenant platform created by Spin Technology and designed to simplify the complexity of cloud data security. As an all-in-one platform, SpinOne combines three solutions that make business data bulletproof from the security breach and insider threats: SpinSecurity, SpinAudit, and SpinBackup.

SpinOne is trusted by over 1,500 organizations worldwide including HubSpot, Vopak, IBT Industrial Solutions. We have more than 1,200,000 business users in more than 100 countries.

Try SpinOne Free →

Spin Technology Inc

2100 Geng Rd Suite 210

Palo Alto, CA 94303, USA

USA and Canada Toll Free:

+1-888-883-2993
(9am to 5pm PST)

EU, CIS and Asia:

+48-22-602-2440
(7am to 4pm GMT)