

Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams

- 03/19/2019

To view the contributors for this article access the link below

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

In this article

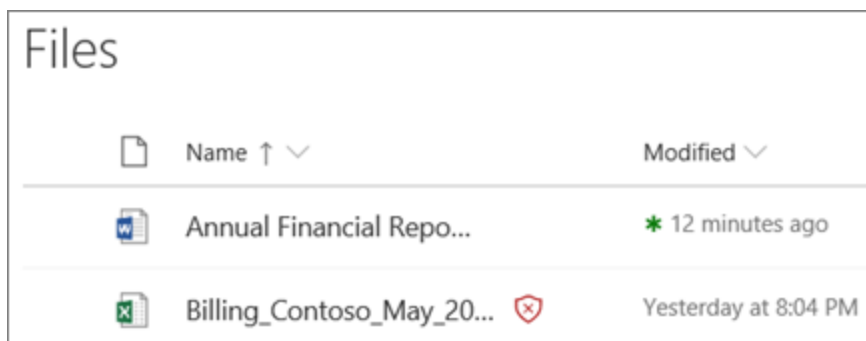
1. [Overview of Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams](#)
2. [How it works](#)
3. [Keep these points in mind](#)
4. [Quarantine in ATP for SharePoint Online, OneDrive for Business, and Microsoft Teams](#)
5. [Next steps](#)

Overview of Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams




People regularly share files and collaborate using SharePoint, OneDrive, and Microsoft Teams. With [Office 365 Advanced Threat Protection](#) (ATP), your organization can collaborate in a safer manner. ATP helps detect and block files that are identified as malicious in team sites and document libraries.

How it works

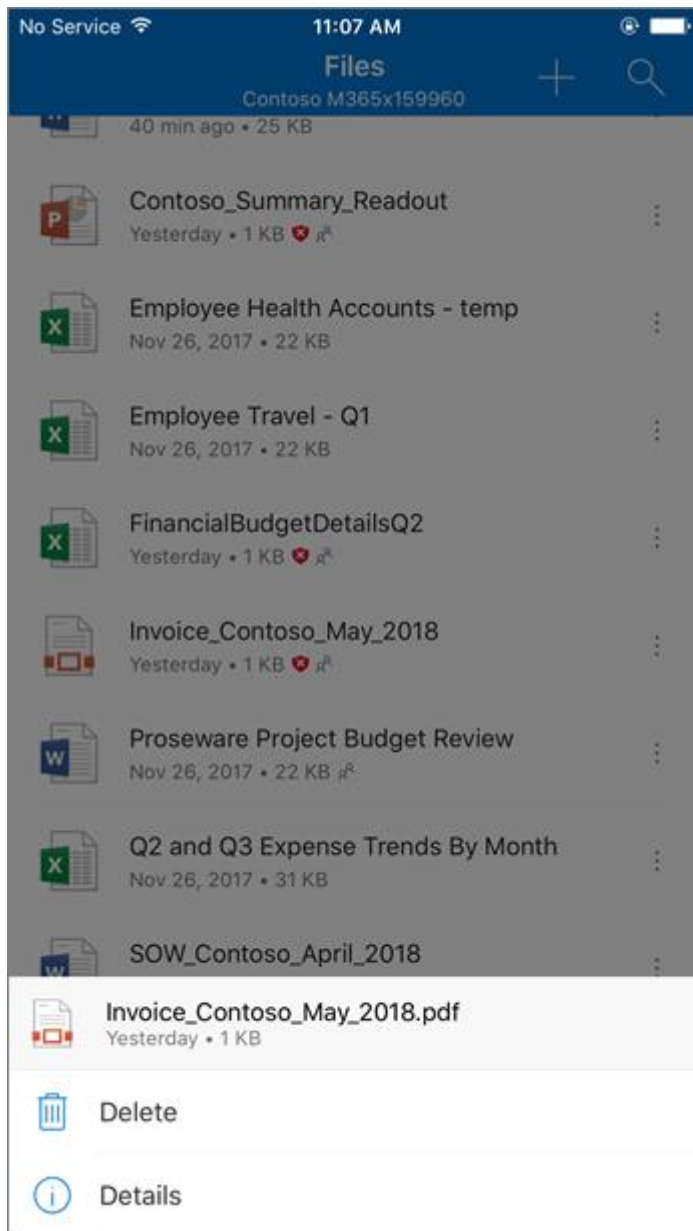
When a file in SharePoint Online, OneDrive for Business, and Microsoft Teams has been identified as malicious, ATP directly integrates with the file stores to lock that file. The following image shows an example of a malicious file detected in a library.



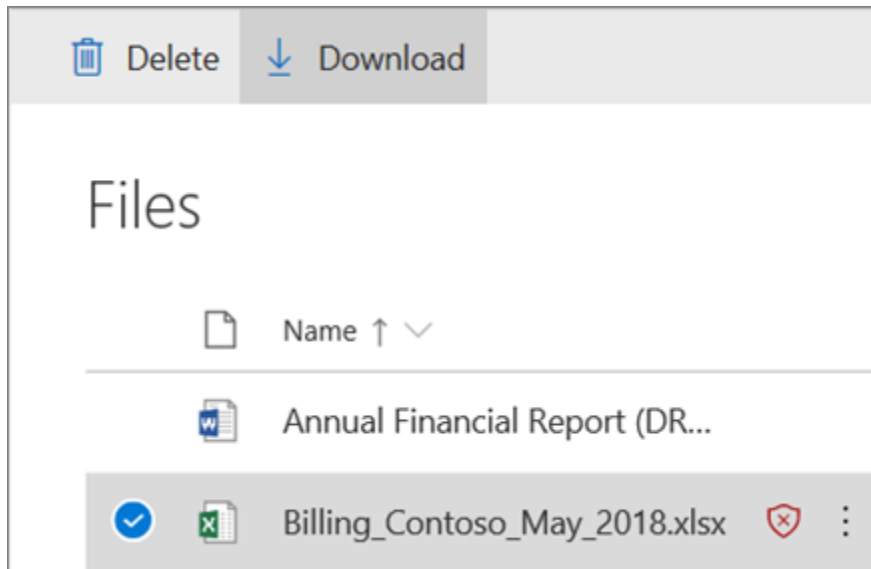
The screenshot shows a file library interface with the following details:

Files	
Name ↑ ↓	Modified ↓
 Annual Financial Repo...	* 12 minutes ago
 Billing_Contoso_May_20... 	Yesterday at 8:04 PM

Although the blocked file is still listed in the document library and web, mobile, or desktop applications, the blocked file cannot be opened, copied, moved, or shared. People can, however, delete a blocked file. Here's an example of what that looks like on a user's mobile device:



Depending on how Office 365 is configured, people might or might not have the ability to download a blocked file. Here's what downloading a blocked file looks like on a user's mobile device:



To learn more, see [Turn on Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams](#).

Keep these points in mind

- ATP will not scan every single file in SharePoint Online, OneDrive for Business, or Microsoft Teams. This is by design. Files are scanned asynchronously, through a process that uses sharing and guest activity events along with smart heuristics and threat signals to identify malicious files.
- Make sure your SharePoint sites are configured to use the [Modern experience](#). When a file is identified as malicious and blocked, people can see that this has occurred in the Modern experience, but not the Classic view. ATP protection applies whether the Modern experience or the Classic view is used; however, visual indicators that a file is blocked are present only in the Modern experience.
- Files that are identified as malicious in SharePoint Online, OneDrive for Business, or Microsoft Teams will show up in [reports for Office 365 Advanced Threat Protection](#) and in [Explorer \(and real-time detections\)](#).
- ATP is part of your organization's overall threat protection strategy, which includes anti-spam and anti-malware protection, as well as Safe Links and Safe Attachments. To learn more, see [Protect against threats in Office 365](#).
- A SharePoint Online administrator can determine whether to enable people to download files that are detected as malicious. **This is done by running the Set-SPOTenant PowerShell cmdlet using a DisallowInfectedFileDownload parameter** (see [Turn on Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams](#)).

Quarantine in ATP for SharePoint Online, OneDrive for Business, and Microsoft Teams

Beginning in late May 2018, [quarantine](#) capabilities in the Security & Compliance Center are being extended to ATP for SharePoint Online, OneDrive for Business, and Microsoft Teams.

When a file in SharePoint Online, OneDrive for Business, or Microsoft Teams is identified as malicious, in addition to ATP blocking the file from being opened or shared, that file is included in a list of quarantined items. (In the Security & Compliance Center, go to **Threat management** > **Review** > **Quarantine** and filter for **Content**.)

If you're part of your organization's Office 365 security team and have the necessary [permissions assigned in the Office 365 Security & Compliance Center](#), you can download, release, report, and delete files that are detected as malicious by ATP from quarantine.

- **Releasing and reporting** a file removes the ATP block on the file in the respective team site or document library for SharePoint, OneDrive, or Microsoft Teams. Users are then able to open, share, and download the file. And, when the **Send report to Microsoft** option is selected, the file is reported as a false positive to Microsoft.
- **Deleting a file** removes the file from quarantine; however, the file is still blocked from being opened or shared. The file must also be deleted in its respective document library or team site (SharePoint Online, OneDrive for Business, or Microsoft Teams).
- **Downloading a file** enables you to download and analyze the file for any false positives.