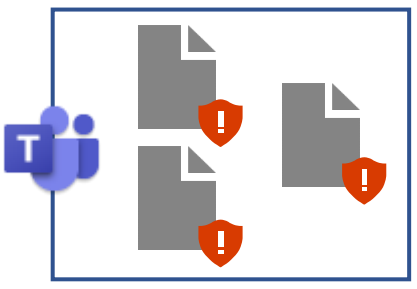
Teams with security isolation in Microsoft 365

A Microsoft Teams team with security isolation in Microsoft 365 for Enterprise combines the built-in features and security of a private team with additional access restrictions and sensitivity labels.

The result is a collaboration space for your most confidential projects with protection that travels with the files you store there.

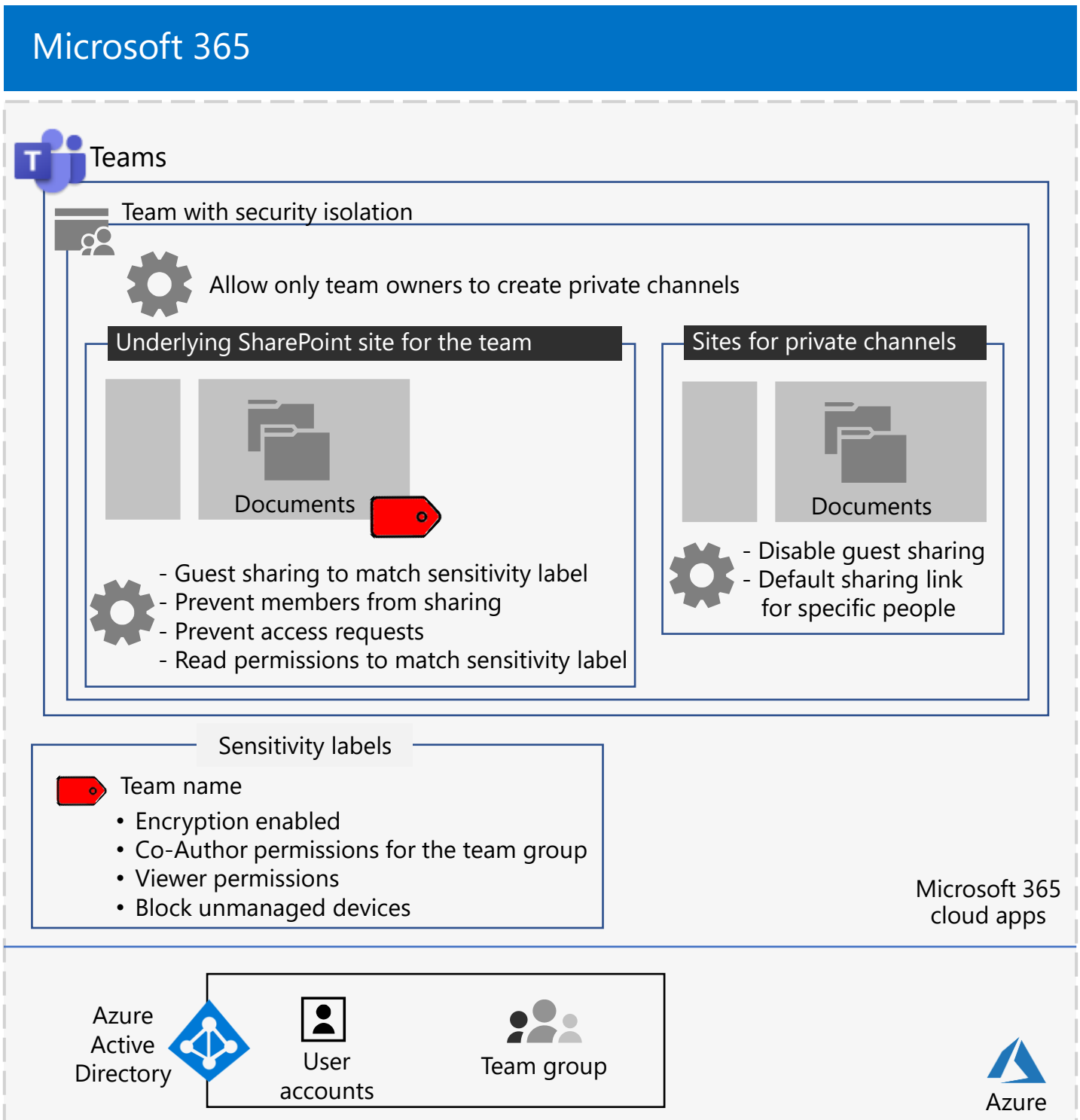


Configure

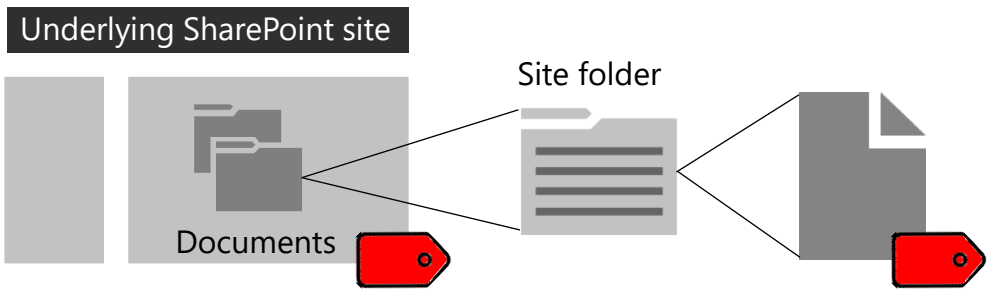
1. Create a private team.
2. Modify private channel settings for the team.
3. Create a sensitivity label.
4. Apply the sensitivity label to the team.
5. Modify settings of the underlying SharePoint site to match those in the sensitivity label.

Drive adoption

1. Train the team owners and members on how to use the team, the underlying SharePoint site, and the sensitivity label for the team.
2. Conduct periodic reviews of team and label usage.
3. Retrain team owners and members as needed.



How sensitivity labels are applied to files

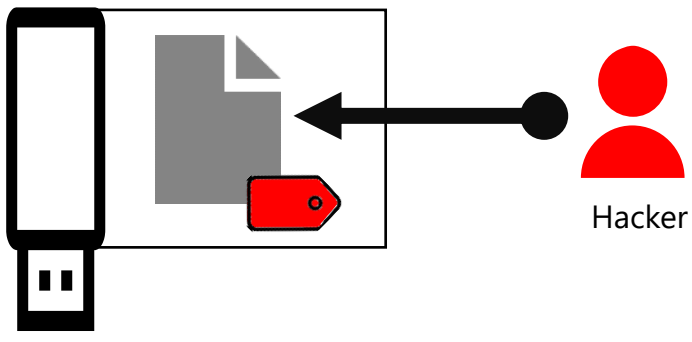


When a team member creates a file, they apply the sensitivity label with the **Sensitivity** button from the **Home** tab on the Ribbon. The applied label travels with the file.

When a file leaves the team

Contrary to their training, a team member downloads a copy of a file with the sensitivity label assigned and stores it on a thumb drive.

The thumb drive is lost and ends up with a hacker.



When the hacker tries to:

View the file contents	They can't. The file contents are encrypted.
Open the file using the file's app	The app prompts the hacker to sign in with credentials.

For detailed guidance, visit aka.ms/m365esecureteams

August 2020