TABLE 1-2 B2B collaboration versus AAD B2C

	B2B collaboration	AAD B2C
Scenario	Provides access to external users while allowing them to bring their own identities. Access can be given to Microsoft applications or your applications (SaaS apps, custom-developed apps, and so on), which are protected by your organization's AAD tenant.	Allows external consumers and customers to access your published application, which could be a SaaS application or a custom developed application. This application cannot be a Microsoft 365 application like Teams, SharePoint, Office, and so on.
Type of Users	Business partners from various organizations, like suppliers, partners, or vendors. These organization may or may not have AAD.	End customers or consumers of products and services.
User Directory and Management	B2B users are onboarded or invited as guest users and appear as guest users in the organization's AAD in which the organization's employee identities are managed. These external user identities can be managed similarly to employee identities.	These users are managed in an AAD B2C directory that is separate from the organization's AAD and any other partner's AAD.
Identity providers supported	Work accounts, school accounts, email addresses, identities from SAML or WS-Fed based identity providers, and social identity providers like Google and Facebook.	Local application accounts (any email address, user name, or phone number), AAD, various supported social identities and consumer identities.
Single sign-on (SSO) Support	Supported for all applications that are to AAD. These could be Microsoft 365 applications, applications running on-premises, or other SaaS applications.	Supported only for the application registered in AAD B2C. This application cannot be a Microsoft 365 application.

AAD is a cloud-native identity solution. But in real-world implementations, large enterprises will likely continue to run at least some of their workloads on-premises—for example, for compliance purposes, because they still rely on some legacy systems, and so on. Such a hybrid environment calls for hybrid identity management. In this scenario, users should be able to use the same identity to access workloads in the cloud or on-premises.

Azure AD Connect

Azure AD Connect helps organizations sync their on-premises Active Directory to AAD. It requires the deployment of an Azure AD Connect application in an on-premises environment. This enables users to employ the same identity and password to access applications and workloads on-premises or in Azure Cloud.

Depending on the configured Azure AD Connect synchronization options for sign-in, authentication can take place in the cloud or on-premises. The three available authentication methods are as follows:

- **Password hash synchronization (PHS)** When this sign-in option is configured for Azure AD Connect synchronization, a hash of the password is synchronized in AAD. As a result, AAD can authenticate users in the cloud itself without any dependencies. Users can use the same password as the on-premises password.
- **Pass-through authentication (PTA)** This sign-in option also allows users to use the same password to authenticate and access applications or workloads on-premises or