

UPDATE>

Directions

on Microsoft

 US CLOUD

issue

JUNE 2021

www.DirectionsOnMicrosoft.com

INDEPENDENT IT PLANNING INFORMATION & ADVISORY SERVICE

3

Managing Apps in Teams

- Teams apps extend the functionality of Teams with information and content from Microsoft and third-party services.
- Organizations can use Teams apps to bring task-relevant information into the places already being used for communication and collaboration.
- The Teams admin center provides capabilities to manage and monitor apps within an organization to ensure security and promote their use.

13

Microsoft Defender for Endpoint Platform Support

- Microsoft Defender for Endpoint now offers centrally managed threat monitoring for Macs and PCs.
- Microsoft Defender for Endpoint is available for iOS, iPadOS, and Android, but the available features are very limited.
- Most Microsoft Defender for Endpoint capabilities are still exclusive to Windows.

20

Consolidating Azure Deployments During M&A

- Azure deployments under different Azure Active Directory tenancies resulting from mergers and acquisitions should be consolidated under a single tenancy.
- The difficulties and risks of consolidation may be best handled with the assistance of an external consulting partner.

32

Licensing Microsoft Defender for Endpoint on Servers

- Microsoft Defender for Endpoint offers endpoint security for servers, with potential savings for existing Microsoft 365 E5 customers.
- Organizations will need to compare costs over time, as one licensing avenue is more flexible but far more expensive.
- Licensing rights for Microsoft Defender for Endpoint on Linux-based servers are not as liberal as for Windows Server.

UPDATE is a monthly digest of the latest *Directions on Microsoft* roadmaps, product reports, and licensing guides to keep you informed about changes at Microsoft that could impact your project plans and purchase decisions.

3 Business Applications & Services

12 Operating Systems & Hardware

13 Systems Management & Security

20 Application Platform

32 Licensing & Support



Download
This Issue

UPDATE

June 2021

Business Applications & Services

Business application software and online services for enterprises, including Office, Exchange, SharePoint, Skype for Business, Office 365, and Dynamics.

ANALYST: Joshua Trupin (joshuat@directionsonmicrosoft.com)

Managing Apps in Teams	3
App Management in the Teams Admin Center	3
Teams Apps Offer Extension and Integration	4
eDiscovery Evolves to Improve Investigations	6
Comparing Core and Advanced eDiscovery	7
Turning Off Self-Service Power Platform Purchases	8
Power Platform Improves Governance and Administration Controls	10
Operator Connect Will Expand Availability of Teams Calling	11
Skype for Business Server 2019 Adds Modern Control Panel	12

Operating Systems & Hardware

Operating systems, infrastructure as a service, and Microsoft-branded hardware, including Windows, Windows Server, Azure infrastructure services and software, and Surface devices.

ANALYST: Michael Cherry (mikech@directionsonmicrosoft.com)

More Time Between Edge Updates	12
--------------------------------------	----

Systems Management & Security

Software and online services for computer systems management and IT security, including System Center, Intune, and identity management.

ANALYST: Wes Miller (wmiller@directionsonmicrosoft.com)

Microsoft Defender for Endpoint Platform Support	13
Microsoft Defender for Endpoint Features by Platform	13
XDR, Microsoft 365 Defender, and Azure Defender	14
Microsoft Defender for Endpoint Platform Support Scorecard	15
Microsoft Defender for Endpoint Suite Licensing	15
Azure Defender Can Secure a Range of Azure Services	16
Family of Azure Defender Services	17
Azure Defender for Servers Features	18

Application Platform

Software, tools, APIs, runtime systems, and online services for software developers, including SQL Server, Visual Studio, the .NET Framework, and Azure platform as a service.

ANALYST: Rob Sanfilippo (robsa@directionsonmicrosoft.com)

Consolidating Azure Deployments During M&A	20
SQL Server Database Options in Azure & On-Premises	22
SQL Server Database Offerings Comparison	23
Cognitive Services Simplifies Machine Learning Deployments	26
Alternatives to Cognitive Services	27
Azure IoT Services	28
Understanding Azure IoT Hub and Azure Event Hubs	28
IoT Protocols	29
Azure IoT Solution Architecture	30
Previews of Java Distributions Available	31
Nuance Communications Acquired by Microsoft	31
DAPR Can Simplify Creation and Management of Microservices	32
Azure Synapse Pathway Simplifies Data Warehouse Migration	32

Licensing & Support

Product and subscription packaging, licensing, and pricing; programs for volume licensing, ISVs, and outsourcing; license compliance and use rights; product support.

ANALYST: Rob Horwitz (robth@directionsonmicrosoft.com)

Licensing Microsoft Defender for Endpoint on Servers	32
Comparing Microsoft Defender for Endpoint Server Licensing Options	33
Power BI Premium Introduces Per-User Licensing	34
A Licensing Overview of Power BI Back-End Platforms	35

Directions on Microsoft

1410 Market Street, Suite 200
Kirkland, WA 98033 USA
Tel. +1 425.739.4669
Fax +1 425.739.0339
Email info@DirectionsOnMicrosoft.com
www.DirectionsOnMicrosoft.com

CEO & Research Chair	Robert Horwitz
President	Jeff Parker
Managing Vice President	Rob Helm
Lead Analysts	Barry Briggs, Michael Cherry, Jim Gaynor, Wes Miller, Rob Sanfilippo, Andrew Snodgrass, Joshua Trupin
Copy Editors	Paula Thurman, Marie La Fond
Design	K. Brian Neel
Operations	Mona Wolf

Managing Apps in Teams

By Jim Gaynor

- Teams apps extend the functionality of Teams with information and content from Microsoft and third-party services.
- Organizations can use Teams apps to bring task-relevant information into the places already being used for communication and collaboration.
- The Teams admin center provides capabilities to manage and monitor apps within an organization to ensure security and promote their use.

Teams is a Microsoft 365 service for organizations that offers group-based collaboration spaces with persistent chat, voice and video meetings, integrated access to several Microsoft 365 services, and connections to many third-party services. The service is promoted as a platform by Microsoft, with Teams apps used to customize Teams within an organization and to encourage greater use of the service. Organizations could find apps useful to bring information from other business applications and services directly into the Teams spaces where users are already collaborating. Customers who want to extend Teams functionality in their organization need to understand how to manage apps in order to effectively promote their use.

What Are Teams Apps?

Apps are extensions to Teams that allow information and content from other services to be brought into team channels or made directly available to Teams users. Apps can make it easier for users to access and share information, or allow a team to collaborate on shared data without leaving the Teams client application. Users can select apps from an app catalog within the Teams client, which displays apps allowed by their organization and can also include custom in-house apps added by administrators.

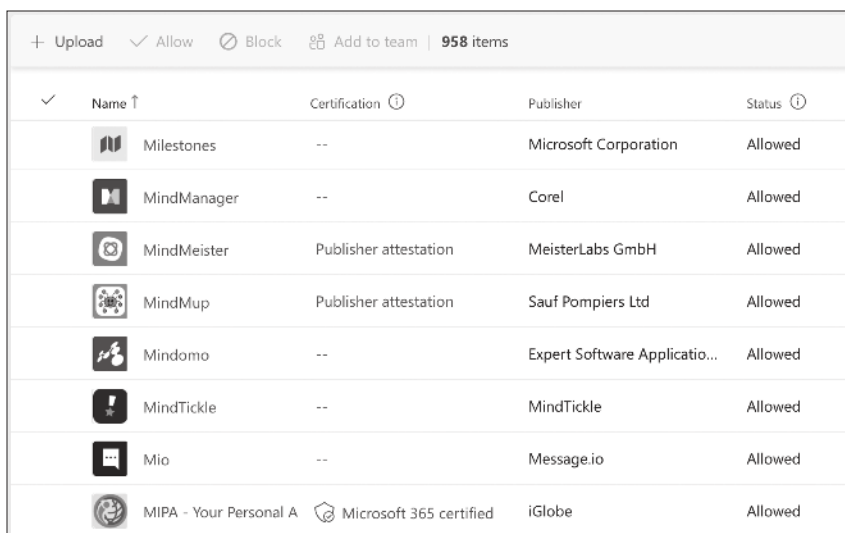
Depending on their purpose, Teams apps can be installed for a specific user or added to a chat or team channel for use by all members. Teams apps can surface the user interface in several places within the Teams client application, including channels, meetings, or even as custom interfaces to other services. (For details, see the sidebar “Teams Apps Offer Extension and Integration” on page 4.)

For management purposes, apps are also separated into first-party, third-party, and custom apps:

First-party apps are Microsoft-written apps for use with Teams. First-party apps encompass several features that are often considered or marketed as a part of Teams: Lists, SharePoint, Praise, and Shifts are all first-party apps. Others might require additional licensing, like apps for Project for the Web or Dynamics 365. First-party apps are governed by the Microsoft Online Subscription Agreement.

Third-party apps are written by vendors other than Microsoft and can provide integration with services from other providers. For example, an app from a help-desk service provider might allow Teams users to view and collaborate on help-desk tickets from within Teams. Third-party apps are not covered by the Microsoft Online Subscription Agreement and may require accounts with or subscriptions to a third-

App Management in the Teams Admin Center



✓	Name ↑	Certification ⓘ	Publisher	Status ⓘ
	Milestones	--	Microsoft Corporation	Allowed
	MindManager	--	Corel	Allowed
	MindMeister	Publisher attestation	MeisterLabs GmbH	Allowed
	MindMup	Publisher attestation	Sauf Pompier Ltd	Allowed
	Mindomo	--	Expert Software Applicatio...	Allowed
	MindTickle	--	MindTickle	Allowed
	Mio	--	Message.io	Allowed
	MIPA - Your Personal A	Microsoft 365 certified	iGlobe	Allowed

This screen shot shows the main “Manage Apps” interface within the Teams admin center.

This pane controls organization-wide settings for Teams apps and can also be used to add an app to a team. All apps that are potentially available are listed, with a customizable selection of columns that display information about the app. Columns available include Name, Certification, Publisher, Publishing Status, Status, Licenses, Custom app, Permissions, Categories, and Version.

The list also contains any custom apps that have been submitted by developers within the organization for inclusion in the organization's Teams app store. Apps can be sorted by column or searched for by name. Once an app is selected from the list, an administrator can view more details about the app, allow or block the app for the entire organization, or add it to a specific team (for apps that provide functionality within a team context). While not visible in this screen shot, this pane is also where administrators can set organization-wide settings to allow or block all third-party or custom apps.

party service to use. Organizations are responsible for reviewing the terms, conditions, permissions, and privacy statements of third-party apps.

Custom apps are written in-house for an organization's internal use. Like third-party apps, custom apps require appropriate licensing or subscriptions for any services they rely on.

Controlling App Availability

Users add apps from the Teams App Store, which is available in the Teams desktop or Web client. By default, team owners are the only users who can add apps for use within a team.

Administrators can control which Teams apps are available in their organization's app store. This can be done for an

entire organization and for specific users.

If allowed by Teams administrators, a developer can upload a custom app for their personal use (called sideloading) or to share with a team without submitting it to the organization's Teams app catalog.

Managing Apps for Organizational Settings

The Manage Apps pane in the Teams admin center allows categories of apps or individual apps to be allowed or blocked for an entire organization. Admins can also view information about individual apps, including the category, certification, permissions required, any available settings, and what plans might be offered for that app within Teams. (See the illustration "App Management in the Teams Admin Center" on page 3.) Additional app information, including security, compliance, and data privacy details, and a list of teams the app has been added to, is planned for late 2021.

Organization-wide app settings can be used to allow (the default) or block the entire categories of third-party apps or custom apps. First-party apps cannot be blocked by category. Administrators can also select individual apps and allow or block them for the entire organization.

Most organizations will want to leave categories of apps allowed for the organization, and instead either block only specific apps organization-wide or use permission policies to block categories of apps for lists of users.

Permission Policies for Users and Groups

Administrators can define app permission policies in the Teams Admin center. Policies assigned to a user block or allow apps for that user and provide the options to allow or block apps based on their category (first-party, third-party, or custom apps).

A Global app permission policy applies to all users and can be set with defaults for the entire organization.

Custom permission policies can be assigned to users in the Teams admin center or using PowerShell commands. PowerShell is recommended for bulk operations on large numbers of users. Group-based assignment of app permission policies is not currently supported but is part of the Teams roadmap for 2021.

Administrators should carefully review how app permission policies interact with organization-wide settings in the "Manage Apps" pane. For example, blocking a category of apps (such as third-party apps) will block it for all users, regardless of the app permission policies applied to those users.

Teams Apps Offer Extension and Integration

Teams apps expose their functionality in different places within the Teams client, depending on their intended capabilities and how users are meant to use them. All Teams apps provide at least one, and often several, of these ways to interact, sometimes referred to as the "context" of the app. These contexts include the following:

Tabs

Tabs are one of the most common ways for an app to provide information. They are visible as part of a team channel or chat and are intended to provide common resources for all members. Tabs can be added to the top of the channel or chat and provide a view, usually simplified, into the app content. Common uses include documents or file libraries, project dashboards, SharePoint sites, or Web content.

Personal View

Teams apps that provide user-specific information or a customized interface offer what is called a personal view. Teams apps with this functionality usually have their own icons that are displayed along the left navigation bar of the main Teams client window. These icons can be pinned to the navigation bar and reordered for easy access, and some can be "popped out" into their own window. "Shifts," a time and schedule management app for first-line workers, is an example of a Teams app that provides a personal view.

Connectors

Connectors are used by Teams apps to bring information directly into a channel on an automated basis. These can include alerts, project status, information from services like Twitter or Yammer, support tickets, or other information. Connectors work within a Teams channel and are added and configured from the channel management menu.

Bots

Bots are a Teams app capability that provides a digital agent that can respond to user requests submitted through a chat, channel, or search with natural language commands. For example, a bot could accept orders, make reservations, search for information, and look up product prices or sales figures. Interacting with bots in Teams is usually done by @mentioning the bot in a chat or channel, the same way a user might @mention another user to get their attention.

Messages

Some Teams apps provide content that can be directly inserted into messages in a chat or channel, such as weather reports, approval requests, task status, or polls. Message functionality is found as icons in the conversation or message interface and is called by members of chat or channel as part of their messages.

Meetings

The most recent context added for Teams apps is within meetings. Teams apps that provide meetings functionality are visible in a pane on the right side of the meeting window, using the same pane that shows meeting chat, attendee lists, and other information relevant to the meeting. They provide a way to get to information quickly without switching away from the meeting window, such as editing a list of tasks that are under discussion.



Deploying Apps to Teams and Users

Teams administrators might need to push apps to teams or ensure that users have specific apps available to them for their tasks. For example, a retail worker might need to have the Shifts app available to manage their work schedule, or a member of the sales team might need a contact management app. Admins can use the Teams admin center to deploy apps directly to teams or users.

Add Apps to Teams Using Manage Apps

Team owners can add apps with a team context (such as tabs, bots, and connectors) to their teams using the Teams desktop or Web application.

Administrators can add apps to a team using the Manage Apps pane in the Teams admin center. Only one app can be added at a time and to only one team at a time. Adding an app to a team does not grant all team users access to the app; users must have access to the app using organization-wide settings or app permission policies, described earlier, to interact with an app added to a team.

Assign Apps to Users with App Setup Policies

App setup policies allow administrators to install Teams apps for specific users and to control how apps are displayed in the Teams client: for example, a policy can permit users to pin app icons in the Teams client navigation bar or mandate a specific list of app icons in a specific order.

Similar to app permission policies, app setup policies include a default Global policy that is assigned to all users. Also, a predefined FirstLineWorker app permission defines a smaller set of pinned apps, including the Shifts app for work schedule management, and disables user pinning.

Custom app setup policies can be assigned to users in the Teams admin center or using PowerShell commands. PowerShell is recommended when managing large numbers of users. Group-based as-

signment of app setup policies is not currently supported but is part of the Teams roadmap for 2021.

Monitoring App Usage

The Analytics and Reports pane, available from the Teams admin center, can generate several kinds of usage reports on Teams activity. Organizations can use the Apps usage report to determine which Teams apps are being actively used, monitor adoption trends, and ensure that users are not making use of apps that are not part of organizational standards.

Notably, the Apps usage report can be run manually to return usage data for the last 7, 30, or 90 days. It displays a chart of overall app usage over time for first-party, third-party, and custom apps. A downloadable report in CSV format includes details of all Teams apps used over that period, including the number of active users and active teams using the app.

Recommendations

By default, all Teams apps are allowed, including first-party, third-party, and custom apps. However, the default Global app setup policy prevents users from uploading their own custom apps. Organizations should examine these defaults to determine what is most appropriate for their users.

For most organizations, organization-wide settings to block applications (assigned in the “App Management” pane) should be used sparingly, as they cannot be changed using app permission policies. Instead, administrators should use the Global app permission and app setup policies to set organization-wide defaults and use individual policies for exceptions. For example, organizations might want to block custom applications using the Global app permission policy, then use a custom app permission policy to allow in-house developers and testers to use custom applications, and apply a similar custom app setup policy to allow developers and testers to sideload apps for testing.

Custom applications in particular should be closely monitored for security purposes. Organizations should consider modifying the Global app permission policy for custom apps to allow only specific in-house apps and block all others.

Lastly, app setup policies can be used to ensure users have easy access to apps they need for their work and can be used to encourage adoption of apps that are organizational standards by ensuring they appear in the Teams navigation bar.

Roadmap

Several enhancements for Teams app management are planned for 2021, including the following:

- Visibility of security, compliance, and data privacy details for apps, which could aid in security and compliance reviews
- When viewing an app’s details, the teams using that app will be listed
- Support for assignment of app permission and app setup policies to Azure Active Directory groups, which will ease assignment of Team policies
- Availability of app management and app permission policies in Government Community Cloud (GCC)
- App customization, including colors, logo, and branding, for apps that support the capability.

Resources

The roadmap for Teams is summarized in the *Microsoft 365 Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/teams>.

Teams app management is documented at <https://docs.microsoft.com/Microsoft-Teams/manage-apps>.

Policy assignment and precedence is detailed at <https://docs.microsoft.com/microsoftteams/assign-policies>.

App setup policies for Teams are documented at <https://docs.microsoft.com/microsoftteams/teams-app-setup-policies>. ➤

eDiscovery Evolves to Improve Investigations

By Michael Cherry

- Advanced eDiscovery, designed for enterprises, provides end-to-end investigations across geographies.
- Organizations may find the features a compelling reason to deploy Microsoft 365 E5 licenses and eliminate third-party tools.
- License enforcement for the Advanced eDiscovery components might be tightening.
- Organizations using eDiscovery must monitor changes to its components to ensure a change does not negatively impact an ongoing investigation.

Key updates to Microsoft 365 eDiscovery components and tighter license enforcement could influence an organization to deploy Microsoft 365 E5 licenses (or a compliance sub-suite) to all users. Electronic Discovery (eDiscovery) is the process of collecting data stored in computer systems by specific users, which are referred to as data custodians, as part of an investigation. An open eDiscovery case can run for a long time, so organizations must monitor changes to Microsoft 365 eDiscovery features. The retirement of existing components and the introduction of new components require diligence to protect ongoing investigations.

eDiscovery

Generally, an organization begins an eDiscovery process to investigate an internal incident, such as a claim of harassment, or an external event, such as litigation or a regulatory enforcement action. Because an organization can store substantial amounts of data in Microsoft 365 services such as Exchange and SharePoint Online, the Microsoft 365 hosted service includes an eDiscovery feature with two levels of components:

- Core eDiscovery, included with Microsoft 365 E3 licenses, has components that enable administrators to create cases, and to identify, hold, and export user data
- Advanced eDiscovery, included with Microsoft 365 E5 licenses, adds components that enable administrators to better focus an investigation to truly relevant data.

An organization not using Advanced eDiscovery components will likely need to further process the data exported by Core eDiscovery manually or with a third-party eDiscovery tool. eDiscovery investigations typically follow a workflow defined by the electronic discovery reference model (EDRM), which is a conceptual view of the iterative discovery process. (For an illustration of the EDRM, and how Core and Advanced eDiscovery components align with the model, see “Comparing Core and Advanced eDiscovery” on page 7.)

Core eDiscovery Components

eDiscovery Managers use Core eDiscovery components to create a case (a logical construct for managing an investigation) for each investigation and to find and preserve (hold) data related to the investigation. An eDiscovery Manager, which is a Microsoft 365 role-based security principal, can view and manage the Core eDiscovery case(s) they create. A higher-level principal, the eDiscovery Administrator(s), can perform all case management tasks, view all cases, manage any case, and access and export data for any case.

Once a case is created, the eDiscovery Manager can use Core eDiscovery to hold or preserve user data stored in Microsoft 365 features including Exchange mailboxes, SharePoint sites, and OneDrive accounts, as well as the mailboxes and sites associated with Microsoft Teams and Office 365 Groups. This held data can be indexed, searched, and exported for manual or additional automated review using a third-party eDiscovery tool. But such data likely includes many nonrelevant documents and messages, duplicate documents or messages, and unthreaded messages. This unfiltered data increases the risk of turning over confidential or private data about the organization or its personnel that is not related or required to complete an investigation.

Core eDiscovery Workflow

The basic workflow with the Core eDiscovery components includes:

- Creating a case
- Placing holds on the data of people of interest to the investigation
- Searching and indexing data with the built-in Core eDiscovery components
- Exporting and downloading search results for manual review and further processing with a third-party tool.

Core eDiscovery Licensing

Generally, licensing for Core eDiscovery requires the correct organizational subscriptions (the right to assign licenses for

a Microsoft 365 tenancy) and the correct Per-User licenses for users in that tenancy. Therefore, to use Core eDiscovery, an organization must have a Microsoft 365 E3 or Office 365 E3 subscription or higher.

Microsoft calls users whose data will be held and processed by Core eDiscovery “data custodians.” Each such user must be assigned the following licenses associated with the organization’s subscription:

- A Microsoft 365 E3 or Office 365 E3 license or higher (typically the case); or
- An Office 365 E1 license with an Exchange Online Plan 2 or Exchange Online Archiving add-on license, and
- An Office 365 E1 license with a SharePoint Online Plan 2 or OneDrive for Business Plan 2 add-on license.

Frontline workers accessing Microsoft 365 services under a Microsoft 365 F3 or Office 365 F3 license who are involved in an eDiscovery case may need to be upgraded to an E3 license if their data will be put on hold and queried.

Most organizations doing significant numbers of investigations, or investigations with significant risk to the organization, will likely need to use Core eDiscovery to start the investigation and get data in Microsoft 365 data stores held and preserved. Generally, organizations relying on Core eDiscovery, included in Office 365 E3 and Microsoft 365 E3 suites, will need to do additional manual review of the data or additional review using a third-party eDiscovery tool.

Advanced eDiscovery

The Advanced eDiscovery components build on the Core eDiscovery components to provide a more complete end-to-end eDiscovery workflow, particularly if the case will span multiple geographies. For example, with Advanced eDiscovery an eDiscovery Manager can better manage the hold process by using templates to create customized notifications to users about their data being held as part of an investigation. In addition, the Advanced

eDiscovery features facilitate:

- Searching and indexing non-Microsoft file types (such as PDFs)
- Searching and indexing non-Microsoft data stores (such as Bloomberg, Facebook, Slack, and Zoom)
- Using training and machine learning to improve indexing, message threading, and near duplicate detection (filter for unique data) to reduce nonrelevant data.

Advanced eDiscovery Workflow

An Advanced eDiscovery workflow begins by using Core eDiscovery to create a case, assign permissions, add users (custo-

dians) to the case, and preserve (hold) their data. The eDiscovery Manager can begin processing by conducting initial searches and indexing of held data, which can include non-Microsoft data sources and file types. The real advantage of Advanced eDiscovery occurs in the reviewing and processing stages by:

- Performing near-duplicate detection and message threading
- Performing data relevance checking and data classification
- Reviewing data to redact protected information and annotate data
- Culling nonrelevant documents

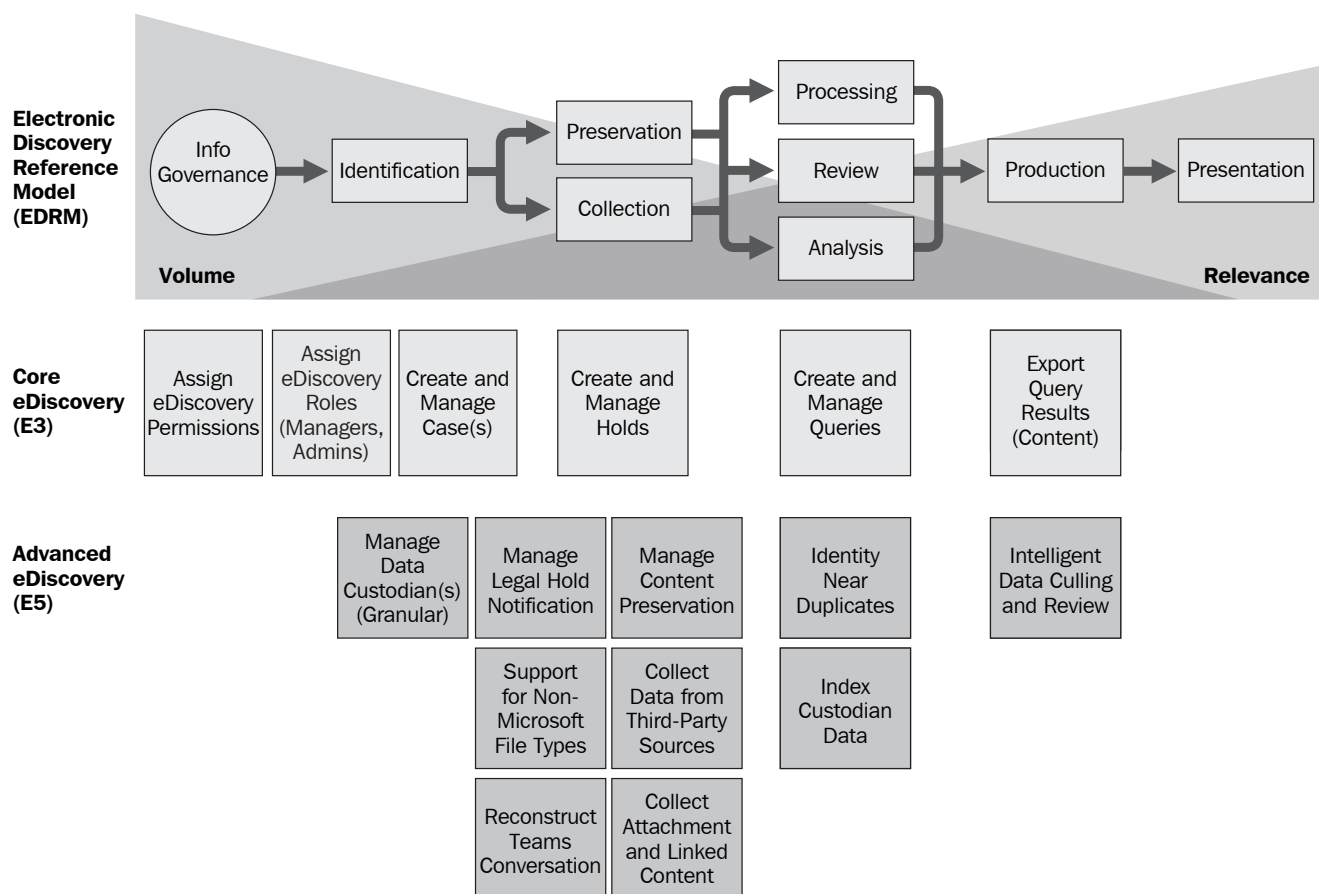
- Exporting the data to hosted or on-premises storage.

Again, organizations will likely need Advanced eDiscovery for any investigation involving large numbers of users, producing a substantial volume of data, or involving investigations that span Microsoft 365 tenancies spanning multiple geographies.

Advanced eDiscovery Licensing

As with Core eDiscovery, licensing Advanced eDiscovery also requires the correct organizational subscriptions (the right to assign licenses for a Microsoft 365 tenancy) and the correct Per-User licenses for users

Comparing Core and Advanced eDiscovery



COPYRIGHT © REDMOND COMMUNICATIONS, INC. REPRODUCTION IN WHOLE OR IN PART IS PROHIBITED.

The Electronic Discovery Reference Model (EDRM) defines an iterative workflow for eDiscovery cases, and Microsoft's eDiscovery feature supports this workflow with Core and Advanced eDiscovery components. The EDRM (top level) specifies a workflow for identifying users; preserving and collecting their data; processing, reviewing, and analyzing the data; and producing and presenting relevant data as part of an internal investigation or litigation.

Core eDiscovery components (middle level) allow for a basic investigation, including assigning permissions to eDiscovery managers and administrators, creating and managing cases, and holding and preserving data, as well as querying the data prior to exporting it for manual review or additional processing with a third-party eDiscovery tool.

Advanced eDiscovery components (bottom level) assist with more granular management of the holds and data by managing additional data sources, identifying the relevant data, and eliminating duplicates prior to exporting it for production or presentation.

Generally, organizations relying on Core eDiscovery, included in Microsoft 365 E3 or Office 365 E3, will need to do additional manual review of the data or additional review using a third-party eDiscovery tool. Using Advanced eDiscovery, which requires having a Microsoft 365 E5 or Office 365 E5 license for each user being investigated, may reduce the amount of data and the need for additional review with other third-party eDiscovery tools. (EDRM model copyright ©2020, EDRM Global, Inc., Creative Commons Attribution 4.0 International, edrm.net.)

in that tenancy. Therefore, to use Advanced eDiscovery, an organization must have one of the following:

- Microsoft 365 E5 or Office 365 E5 subscription
- Microsoft 365 E3 subscription with Microsoft 365 E5 Compliance add-on
- Microsoft 365 E3 subscription with Microsoft 365 E5 eDiscovery and Audit add-on.

(The E5 eDiscovery and Audit suite is a subcomponent of the Microsoft 365 E5 Compliance suite, which is in turn a subcomponent of the full Microsoft 365 E5 suite.)

Each user (custodian of data) must have one of the following licenses, depending on the organization's subscription:

- Microsoft 365 E5 license
- Microsoft 365 E3 license with Microsoft 365 E5 Compliance add-on license
- Microsoft 365 E3 license with Microsoft 365 E5 eDiscovery and Audit add-on license
- Office 365 E5 license.

eDiscovery Updates and Roadmap

Microsoft's eDiscovery focus appears to be on Advanced eDiscovery components. Recent updates include the following:

Relevance component retirement. The original Advanced eDiscovery Relevance component, used to select only data relevant to an investigation, was retired in Mar. 2021. It will be replaced with a predictive coding component.

New predictive coding component. A new Advanced eDiscovery predictive coding component, which allows working with data without having to move it outside of a Microsoft 365 compliance boundary, and which can train data relevance models with as few as 50 sample documents, will become generally available in mid-Apr. 2021. Compli-

ance boundaries are logical areas within an organization used to control who within an organization can access eDiscovery.

License enforcement. In a notice made available to Microsoft 365 administrators in Mar. 2021, Microsoft has indicated that starting in Apr. 2021, all customers using Advanced eDiscovery must have the appropriate licenses discussed earlier in this report. Although this has always been the case, the notice may indicate some form of auditing is starting, and continued use of Advanced eDiscovery features without correct licensing could have audit consequences.

Hold scalability and performance. Core eDiscovery is being improved to reduce hold and retention policy distribution errors caused by the time it takes to place data on hold, particularly when a case involves many users.

UI improvements. Starting in Apr. 2021, a new UI framework will begin to be incorporated into search filtering and querying and search statistics, including estimated search results, condition reports, and top data locations, for easier viewing and navigation.

Recommendations

Many organizations may find Core eDiscovery is a sufficient tool for managing simple investigations, particularly for internal use (violations of organizational policy). It may also be useful for some non-investigatory functions such as finding all project-related data at the end of a project.

Users of Core and Advanced eDiscovery need to carefully monitor the Microsoft 365 Admin Portal messages for changes to eDiscovery. Although most changes have minimal impact, occasionally a case may still be open when a change occurs, and it may be necessary to take steps to preserve the case or migrate data to ensure it will be

available after the change occurs. For example, the change created by the retirement of the relevance module and its replacement with the new predictive coding tool required some intervention because the retirement and replacement dates did not align.

Finally, organizations should have test data to periodically run through Core and Advanced eDiscovery to ensure the components are in fact picking up relevant data, and not missing any relevant data, and to ensure data being turned over in any investigation includes all and only relevant data.

Availability and Resources

Both Core and Advanced eDiscovery are generally available.

For background on eDiscovery investigations, see "Why Bother with eDiscovery? No One Is Suing Us" on page 6 of the June 2019 *Update*.

Core eDiscovery is described in "Getting Started with Core eDiscovery" at <https://docs.microsoft.com/microsoft-365/compliance/get-started-core-ediscovery>.

Advanced eDiscovery is described in "Overview of Microsoft 365 Advanced eDiscovery" at <https://docs.microsoft.com/microsoft-365/compliance/overview-ediscovery-20>.

The relevance module retirement is described in "Retirement of the Relevance Module in Advanced eDiscovery" at <https://docs.microsoft.com/microsoft-365/compliance/relevance-module-retirement>.

The license checking for Advanced eDiscovery is described in "Advanced eDiscovery License Checking" at <https://admin.microsoft.com/AdminPortal/Home?#/MessageCenter:/messages/MC244742>. Microsoft 365 tenancy admin privileges may be required to view this information in the Microsoft 365 message center. 

Turning Off Self-Service Power Platform Purchases

By Joshua Trupin

- Organizations should consider turning off the ability for users to make self-service Power Platform purchases.
- Self-service purchases can raise license costs, increase administrative complexity, and lead to confusion when a user leaves the organization.
- Administrators cannot take full control of self-service licenses after they have been purchased.

Power Apps, Power Automate, and Power BI allow users within an organization to obtain licenses on a month-to-month agreement without going through

centralized IT. Organizations cannot take full control of these licenses, which have additional limitations, and should consider turning off the self-service feature.

End Users Can Acquire Full Licenses

Power Platform is a marketing umbrella encompassing several services, including Power Apps, Power Automate, Power

Virtual Agents, and Power BI. Each service is licensed separately, but other licenses such as Microsoft 365 and Dynamics 365 provide limited rights to use them, and each service provides some rights to use the other services.

Microsoft offers two types of self-service acquisition of licenses for the Power Platform line: self-service sign-up and self-service purchase. Self-service purchase poses more problems for the organization, but self-service sign-up promotes the spread of self-service purchases.

Self-Service Sign-Up

Self-service sign-up allows users to sign up for a free trial of a service, such as a 30-day free trial of Power Apps. Licensed Office 365 and Dynamics 365 users are entitled to a subset of Power Apps and Power Automate features and can use self-service sign-up to temporarily turn on their ability to use premium features such as connectors and Dataverse access.

At the end of the trial period, users need a full license to the service to continue using premium features. If they are unable to obtain a full license from their organization, they can make a self-service purchase.

Self-Service Purchase

Self-service purchase allows an end user to use a credit card to purchase a monthly license to a service. Self-service purchase licenses are purchased at full retail price and are not eligible for discounts provided to the organization. Self-service purchases can be made in two ways: directly from the product Web site or from prompts that appear within applications like Power Automate Desktop.

Any non-guest user with an account in a managed Azure Active Directory (AD) tenancy can make a self-service purchase if the organization has not shut the ability off; the feature does not require the purchaser to have elevated administration rights. The self-service license is associated with the tenancy the user belongs to. End users can purchase multiple self-service licenses and assign them to any user, including guests, within their Azure AD tenancy.

Self-service purchase is not available to customers in the government or education cloud, or in India.

Administration of Self-Service Purchases

Administrators have some control over self-service purchases of Power Platform services. Options include blocking self-service purchases either completely or per product or allowing self-service purchases and managing them within the tenancy.

However, administrators cannot directly terminate a license in their tenancy that was purchased by an end user.

Controlling the Ability to Use Self-Service

Administrators can turn self-service purchasing on or off per license type (plan SKU) or on a tenant-wide basis via PowerShell. Procurement managers, who generally do not have administrative rights, will have to request these operations from their Microsoft 365 or Dynamics 365 administrators.

The Azure AD PowerShell command `AllowAdHocSubscriptions` allows administrators to turn self-service sign-up on or off for all Microsoft cloud-based applications and services at once.

Alternately, administrators can use the MSCommerce PowerShell command `AllowSelfServicePurchase` to turn self-service purchases on or off for specific cloud-based applications and services, but it must be run for each plan SKU. If license types change, the PowerShell command will need to be run again to account for the new SKUs.

Viewing Purchased Licenses

When an end user purchases self-service licenses, he can view, assign, and manage those licenses from a limited version of the Microsoft 365 admin center.

Administrators can view the self-service purchases made within a tenancy through the Microsoft 365 admin center, including product name, purchaser, expiration date, and assigned users. However, administrators cannot cancel or replace those licenses. Administrators can contact the self-service user, request that she cancel her subscription, and replace it with a license procured through an existing agreement.

Administering Already Purchased Licenses

After end users have acquired licenses through a self-service purchase, administrators have limited options to control those licenses. These options include the following:

- Limiting the rights of self-service licenses, such as disallowing them to create new environments within Power Platform services
- Managing the use of data sources (such as Dataverse) to limit the access given to self-service licenses
- Turning off the user's access to premium connectors.

Applying security settings to a self-service license is performed in the Power Platform admin center.

Different Rules for Self-Service Licenses

Licenses to Power Platform services acquired through self-service purchase operate under different rules from those purchased through an organization's subscription, making them less desirable:

Self-service licensees are not eligible for Premier Support; they receive only standard product support. Organizations are not expected to provide support on behalf of the licensee.

The purchaser of a self-service license is billed directly and cannot transfer billing responsibility to the organization.

Organizations cannot add self-service licenses to an existing license agreement at a negotiated discount. A procurement manager must request that the purchaser cancel his license and receive a replacement.

Recommendations

Self-service purchases were introduced in 2019 as a way for Microsoft to encourage so-called citizen developers to create projects outside the purview of centralized IT departments. However, end users do not necessarily have insight into the licenses that may already be available to them through their organization. Self-service purchases could also bypass organizational requirements, such as receiving training before gaining access to a service or understanding regulatory concerns over the service's internal use. For these reasons, organizations should strongly consider turning off the ability for end users to make self-service purchases of licenses.

A user who makes self-service purchases can create risk when she leaves the organization. After she is removed from the Azure AD tenancy, the purchaser no longer has access to her license but could still be financially responsible for the license. The end user must cancel her self-service purchase; an administrator can only request cancellation by contacting Microsoft customer support.

When a user cancels his self-service purchase of a subscription that covers multiple users, the organization must assign IT-controlled licenses to the remaining users to avoid discontinuity of service and possible deletion of their data. This process is especially important for apps that have become important to line-of-business processes. An administrator must then use PowerShell to transfer ownership of any apps and environments to another user, preferably one with an IT-controlled license.

Organizations that choose to leave self-service purchases on must closely track who has been assigned the licenses, and they must be ready to quickly act to ensure that guest users have limited access

to corporate resources. The organization must also ensure it can purchase licenses for any user orphaned when a self-service subscription is canceled.

Resources

Self-service license purchase is discussed at [https://docs.microsoft.com/micro-](https://docs.microsoft.com/micro-soft-365/commerce/subscriptions/self-service-purchase-faq)

[soft-365/commerce/subscriptions/self-service-purchase-faq](https://docs.microsoft.com/micro-soft-365/commerce/subscriptions/self-service-purchase-faq).

Disabling self-service purchases is documented at <https://docs.microsoft.com/power-bi/admin/service-admin-disable-self-service>.

Managing self-service licenses is presented at [https://docs.microsoft.com/micro-](https://docs.microsoft.com/micro-soft-365/commerce/subscriptions/manage-self-service-signup-subscriptions)

[soft-365/commerce/subscriptions/manage-self-service-signup-subscriptions](https://docs.microsoft.com/micro-soft-365/commerce/subscriptions/manage-self-service-signup-subscriptions).

A list of products eligible for self-service purchase is contained at <https://docs.microsoft.com/microsoft-365/admin/misc/self-service-sign-up>. 

Power Platform Improves Governance and Administration Controls

By Joshua Trupin

- Power Apps and Power Automate will be receiving several new administration and governance features in 2021.
- Administrators will be able to better control data usage, preventing intentional or inadvertent leaks of sensitive data.
- Organizations will gain better information about app usage and resources, helping reduce surprise costs.

Power Apps, a graphical application development environment, and Power Automate, a graphical workflow automation engine, are receiving new features and controls through 2021. These controls are part of a larger rollout of Power Platform features and could help administrators better control data leakage through apps and flows, allow more granular control of how the services can access connectors, and improve understanding of app usage and licensing needs. The services will also receive new features for real-time debugging of published apps.

Together, these additions show the Power Platform evolving to be more suitable for corporate projects and professional development.

New Data Protection Features for Power Apps and Power Automate

Many upcoming improvements to Power Apps and Power Automate focus on giving administrators the ability to fine-tune data controls to lessen the chance of a misbehaving app or users from exporting sensitive data outside an organization.

Connectors Gain Finer-Grained Controls

Connectors are components that can link apps created in Power Apps and Power Automate flows to Microsoft and third-party services and data sources through a consistent interface, much like common controls.

Currently, administrators can set a Power Apps or Power Automate connector to one of three states: business (indicating that it may handle sensitive data), non-business

(all other connectors), or blocked (use forbidden in a tenancy). Connectors must be set to the same state (either business or non-business) to interoperate within an app or flow. A preview feature, Connector Action Control, will allow administrators to allow or block specific actions on a per-connector basis rather than blocking the entire connector from any usage. For example, users who access a SharePoint list through a connector could have their access set to read data but not write to the list. This feature could reduce the risk of allowing certain connectors and expand access to previously blocked connectors.

Endpoint Filtering Provides Additional DLP

New tenant isolation capabilities could allow organizations to limit data exfiltration through additional or unintended routes. Endpoint filtering will allow organizations to limit connections to specific lists of tenants and block cross-tenant connections.

This feature could not only protect data from being moved outside an organization but also open up Power Automate architecture to allow an organization with multiple tenancies to more securely work together without opening up connections to the entire Internet.

Email Operations Gain Exfiltration Controls

Administrators will be able to configure rules for e-mail messages that are being sent from Power Apps and Power Automate. This will include blocking e-mail being sent to recipients outside an organization, as

well as blocking specific apps and flows from sending e-mail. The rules are set up similarly to rules in Outlook, with conditions and actions: An administrator can set a rule to automatically delete e-mail sent from specific apps if the recipient is outside the organization and the subject line includes a specific phrase. These controls could help lessen the risk of having sensitive data being sent outside the tenancy via an app or flow, as well as reducing the chance that a poorly designed or tested routine could inadvertently flood users with e-mail.

Sensitive Data Protection Planned

A future update of Power Platform will integrate the services with Microsoft Information Protection, allowing administrators to scan, classify (using sensitivity labels), and protect sensitive data that is handled within Power Platform services.

Expanded Reporting and Diagnostics Features

Several updates could make Power Platform services more attractive to IT organizations that need to monitor usage and assume ownership of user-created apps and flows.

Health and Analytics Reporting Is Being Expanded

Reporting on apps and flows is being expanded to provide health, usage, and adoption analysis across an entire tenant, and all environments within the tenant. Previously, reporting was limited to individual apps and flows. This functionality is available

now for Power Apps and will be rolling out for Power Automate through 2021.

This expanded reporting could help administrators more quickly spot apps that are performing abnormally or that are seeing a sudden surge in adoption and also better plan future capacity licensing needs.

API Usage Reports Included for Power Automate

A preview feature, expected in Apr. 2021, will enhance license reports from the Power Platform admin center will show API usage per flow and per user, which will help administrators determine which flows and users may need additional capacity licensing. However, this update is likely to signal stricter capacity enforcement, based on limits introduced in, but loosely enforced since, Oct. 2019.

Expanded Power Apps Diagnostics in Preview

Power Apps will be expanding several capabilities for debugging published canvas apps. App creators will have improved capabilities to import and export log files, monitor and debug user sessions in real time, and share diagnostic sessions to improve troubleshooting of apps.

This feature could improve the ability of IT departments to provide better application life-cycle management (ALM) for published apps.

Resources

New Power Platform governance controls are described at <https://techcommunity.microsoft.com/t5/microsoft-mechanics-blog/new-controls-to-govern-the-power-platform/ba-p/2220649>.

The Power Platform 2021 Wave 1 release plan is documented at <https://docs.microsoft.com/power-platform-release-plan/2021wave1/power-automate/planned-features>.

Power Apps administration and governance is discussed in a Microsoft white paper that can be downloaded at <https://aka.ms/powerappsadminwhitepaper>.

Power Platform capacity limitations are outlined in “Managing Power Platform Capacity Limits” on page 6 of the Mar. 2021 Update.

Sensitivity labels are discussed in “Executive Focus: Microsoft 365’s Compliance Technologies” on page 25 of the Feb. 2021 Update.

A collection of Power Apps and Power Automate reports is curated in “Kit: Power Platform” at <https://www.directionsonmicrosoft.com/update/secured/2021/03/kit-power-platform>. 

Operator Connect Will Expand Availability of Teams Calling

By Jim Gaynor

- **Operator Connect will enable managed PSTN phone service in Teams in more regions than is possible today.**
- **Customers may be able to leverage their existing telephone operators without additional on-premises infrastructure.**
- **Operator Connect Conferencing will allow customers to use Teams conference dial-in numbers from operators other than Microsoft.**

OPERATOR CONNECT and Operator Connect Conferencing, announced in March and expected in preview in mid-2021, will allow customers to leverage public switched telephone network (PSTN) carriers (which Microsoft calls operators) for calling services in Teams without the on-premises infrastructure required by Direct Routing, Microsoft’s current solution for connecting Teams to utilizing external operators. Operator Connect will provide operator-managed calling infrastructure and could enable customers to leverage their existing operator contracts and use Teams voice calling in more geographic regions than are serviced by Microsoft’s current offerings.

Direct Routing Without Additional Infrastructure

Operator Connect is designed to provide PSTN connectivity for Teams customers without using Microsoft as an operator (as in the hosted Calling Plan service), but without the on-premises infrastructure required to implement Direct Routing (which uses a customer’s contracted operator and on-premises infrastructure).

Operator Connect, similar to Direct Routing, utilizes a session border controller (SBC) to route PSTN traffic between the customer’s phone operator and the customer’s Teams tenancy. SBCs are devices commonly used in Voice over IP (VoIP) deployments to control signaling and media streams between an operator’s network and customers’ networks. However, Direct Routing requires customers to manage their own SBC or contract with a third party for service.

Operator Connect reduces the management overhead and infrastructure requirements of Direct Routing by providing hosted SBCs that are managed by operators that partner directly with Microsoft. Operator Connect can be provisioned by administrators from within the Teams admin center, and it can provide the benefits of Direct Routing without requiring customers to purchase, deploy, or manage their own SBCs. This feature can enable faster deployment of Teams calling compared with Direct Routing while minimizing the in-house expertise and capital expense required.

Operator Connect will offer direct peering between partner operators and Microsoft, and operators will provide shared technical support and service level agreements. Compared with Direct Routing, Operator Connect could improve performance and service quality and reduce technical support conflicts between operators, SBC vendors, and Microsoft.

Operator Connect Conferencing Expands Audio Conferencing Providers

Operator Connect Conferencing will allow customers to add operator-provided phone numbers to Audio Conferencing, a service that allows meeting attendees to use a traditional phone to connect to meetings when they are unable to attend online. Previously, Audio Conferencing required customers to use Microsoft-provided numbers and operator services.

Similar to Operator Connect, operators will partner with Microsoft to provide Operator Connect Conferencing services, including shared technical support and service level agreements. Operator Connect Conferencing could allow customers to leverage their existing operator contracts, while providing users and customers with dial-in numbers in geographic regions not serviced by Microsoft's current offerings.

Availability and Licensing

Operator Connect and Operator Connect Conferencing are expected to enter public preview in mid-2021, with general availability planned for the first half of 2022.

Several operators, including BT, Deutsche Telekom, Intrado, NTT, NuWave, Orange Business Services, and Telenor, are partnering for both Operator Connect and Operator Connect Conferencing. Pure IP, Rogers, Swisscom, and Verizon are partners for Operator Connect only. Additional partners are expected before Operator Connect reaches general availability.

No details regarding pricing and the geographic regions where Operator Connect will be offered have been re-

leased, but further information will likely become available during the public preview. There are likely to be additional costs for the services, which may be dependent on operator and service region.

Operator Connect will require an Office 365 tenancy that includes Microsoft Teams and Phone System. Operator Connect will add additional numbers to an Audio Conferencing bridge, which requires an Audio Conferencing license for the meeting organizer. Phone System and Audio Conferencing are included in Office 365 Enterprise E5 and can be purchased stand-alone to augment Office 365 Enterprise E3.

Resources

Operator Connect was announced at <https://techcommunity.microsoft.com/t5/microsoft-teams-blog/introducing-operator-connect-and-more-teams-calling-updates/ba-p/2176398>.

Telephony Services for Teams, including Calling Plan, Direct Routing, and Phone System, are summarized in the *Microsoft 365 Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/telephony-services>. ➤

In Brief Skype for Business Server 2019 Adds Modern Control Panel

The Modern Admin Control Panel (MACP) for Skype for Business Server 2019 is generally available as part of the March 2021 cumulative update. The MACP is a Web-based control panel implemented in HTML5, and it replaces the original admin control panel that was implemented in Silverlight. Silverlight is supported only on Internet Explorer 10 and Internet Explorer 11 and will reach end of support in Oct. 2021. General availability of the MACP follows two earlier phases released in July 2019 and Mar. 2020, and it enables administrators to manage Skype for Business Server 2019 using modern Web browsers such as Edge

and Chrome. Other improvements in the March 2021 cumulative update include support for OAuth authentication to log into the MACP Web portal and the capability to assign a simplified URL for MACP access. No plans have been announced to bring the MACP to Skype for Business Server 2015 or earlier versions. General availability of the MACP for Skype for Business Server 2019 was announced at <https://techcommunity.microsoft.com/t5/skype-for-business-blog/skype-for-business-server-2019-announcing-the-general/ba-p/2203816>. ➤

Operating Systems & Hardware

In Brief More Time Between Edge Updates

A new Edge Extended Stable channel planned for Sept. 2021 will give enterprise customers more time to plan, test, and deploy updates for Microsoft's Edge Web browser. The Extended Stable channel will have an eight-week release cadence. It will only be available for customers with managed environments, implying it will be controlled by a registry key. Separately, and driving the creation of the Edge Extended Stable channel, the Windows 10 Edge Stable channel will change to a four-week cadence for major updates

with version 94, which is also scheduled for release in Sept. 2021. These channel changes are described in the Windows blog at <https://blogs.windows.com/msedgedev/2021/03/12/new-release-cycles-microsoft-edge-extended-stable>. The tentative Edge release cycle is described at <https://docs.microsoft.com/deployedge/microsoft-edge-release-schedule>. For *Directions on Microsoft's* latest roadmap on Microsoft's Windows Web browsers, see "Edge Update and Roadmap, Feb. 2021" on page 28 of Apr. 2021 *Update*. ➤

Microsoft Defender for Endpoint Platform Support

By Wes Miller

- Microsoft Defender for Endpoint now offers centrally managed threat monitoring for Macs and PCs.
- Microsoft Defender for Endpoint is available for iOS, iPadOS, and Android, but the available features are very limited.
- Most Microsoft Defender for Endpoint capabilities are still exclusive to Windows.

Microsoft Defender for Endpoint is a subscription-based, Microsoft-hosted service that offers endpoint protection on Windows and macOS clients, and on popular mobile devices. Broader capabilities, such as endpoint detection and response (EDR), discovery, and recommendations, began arriving for non-Windows platforms during 2021. Support for iOS, iPadOS, and Android arrived late in 2020 and focuses mostly on malware or malicious site discovery because of design constraints of those platforms. Customers should understand that although Microsoft Defender

for Endpoint supports other platforms, Windows 10 is required to get the most value from Microsoft Defender for Endpoint, and some capabilities are exclusive to Windows 10 Enterprise edition. Microsoft Defender for Endpoint was most recently named Microsoft Defender Advanced Threat Protection (MDATP), but was also known as Windows Defender ATP prior to that.

Microsoft Defender for Endpoint is available for Windows Server but is licensed through two entirely different licensing models and is not available through Microsoft 365 suites. Linux server OS licens-

ing of Microsoft Defender for Endpoint is even more complex. The remainder of this report focuses exclusively on Microsoft Defender for Endpoint for client (PC and mobile device) endpoints. (For more information on Microsoft Defender for Endpoint (server) licensing options, see “Licensing Microsoft Defender for Endpoint on Servers” on page 32.)

Microsoft Defender for Endpoint Basics

The Microsoft Defender for Endpoint software—referred to as a sensor—is in-

Microsoft Defender for Endpoint Features by Platform

Microsoft Defender for Endpoint offers a range of capabilities, but most require Windows 10, and many require Windows 10 Enterprise edition. Shown here in the first column of the chart are the six key capabilities offered by Microsoft Defender for Endpoint.

Microsoft delivered threat and vulnerability management and limited remediation capabilities for macOS during 2020.

Microsoft Defender for Endpoint offers very rudimentary capabilities on mobile devices. The Android client offers anti-phishing and Web protection, malware scanning, and support for Conditional Access enforcement when the device is used to access Azure Active Directory–integrated applications. The client for Apple mobile devices offers anti-phishing and Web protection capabilities, in addition to URL and domain blocking.

Chromebooks are not supported.

Feature	Description	Windows 10	macOS
Managed endpoint protection	Managed antivirus (AV) and antimalware using Microsoft Defender Antivirus on Windows or other Microsoft AV software on non-Windows platforms.	✓	✓
Next-generation protection	Cloud-based Microsoft Defender Antivirus AV capabilities including behavioral, heuristic, and real-time protections and block at first sight.	✓	○
Attack surface reduction	Manage Windows-native threat mitigation capabilities including Windows Defender Application Control and AppLocker. (Many features require recent versions of Windows 10 Enterprise edition.)	✓	○
Endpoint detection and response	Aggregation and analysis of diagnostic data from systems across the organization for alerting, reporting, and hunting.	✓	✓
Threat and vulnerability management	Discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations.	✓	✓
Automated investigation and response	Automated, playbook-based investigation across one or more systems. Can also perform manual or automated remediation.	✓	○

stalled on individual devices (endpoints) and communicates with a Microsoft-hosted service that aggregates diagnostic data from endpoints across the organization, enabling analysis by experts within the organization. It uses the built-in Microsoft Defender Antivirus client software (previously named Windows Defender Antivirus) on Windows and Microsoft antivirus (AV) software on other platforms. Microsoft Defender for Endpoint requires these AV engines and cannot be used with third-party AV on protected endpoints.

Six core features are available with Microsoft Defender for Endpoint when running on Windows 10 Enterprise endpoints. Only recent versions of Windows 10 Enterprise offer the full set of Microsoft Defender for Endpoint capabilities. All other platforms receive a smaller subset of capabilities. (For an analysis of which platforms receive each layer of Microsoft Defender for Endpoint capabilities, see the chart “Microsoft Defender for Endpoint Features by Platform” on page 13. For a score-based summary of how comprehensive the Microsoft Defender for Endpoint capabilities are on each platform, see the chart “Microsoft Defender for Endpoint Platform Support Scorecard” on page 15.)

Managed Endpoint Protection

Endpoint protection includes AV and antimalware, which is built into Windows natively in the form of Microsoft Defender AV. Microsoft Defender for Endpoint adds centralized management and logging to this basic detection engine. Microsoft Defender for Endpoint also offers managed endpoint protection for macOS using a Microsoft-supplied antimalware engine delivered with the Microsoft Defender for Endpoint sensor software. This Microsoft Defender for Endpoint offering replaces System Center Endpoint Protection (SCEP), which used to support Apple Mac devices and Linux but has discontinued both. (SCEP continues to be available for Windows and Windows Server but, compared against Microsoft Defender for Endpoint, offers very limited value other than AV and malware detection.)

Next-Generation Protection

Next-generation protection is a set of cloud-based capabilities unique to the Microsoft Defender Antivirus engine and exclusive to Windows 10 Enterprise endpoints. It includes cloud-based heuristic, behavioral, and block-at-first-sight capabilities built into Windows Defender software. Microsoft’s current antimalware engines for macOS and Linux do not support these capabilities, although comparable capabilities might be added for these platforms in the future.

XDR, Microsoft 365 Defender, and Azure Defender

Customers are likely to increasingly see the terms “XDR”, “Microsoft 365 Defender”, and “Azure Defender”, but what do they mean? Extended detection and response (XDR) is a term used by analysts and some in the industry to describe inputs across a range of traditionally stand-alone security tools, surfaced together in a usable form that is likely to be more powerful than the sum of its parts.

Microsoft uses XDR to describe Microsoft 365 Defender, a brand that unifies the three existing Microsoft Defender services (Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Defender for Office 365) within one console, the Microsoft 365 Security Center. Microsoft 365 Defender is intended to combine related threat information into incidents and allows one service in the suite to inform other related services of actions that should be taken. The Microsoft 365 Defender brand replaces the Microsoft Threat Protection [MTP] brand that first arrived in late 2019.

Although the three Microsoft Defender component services can be licensed independently, and customers often purchase them that way, many of Microsoft’s recent security feature demos and documentation related to the recent Solarigate and HAFNIUM attacks require that all three services be licensed to enable the capabilities being demonstrated. (Many demos also require Azure Sentinel, which is not a part of any Microsoft 365 suite and must be licensed independently.)

Microsoft 365 Defender demonstrates the tighter integration between security services that Microsoft is likely to expand on over the coming years, making it increasingly difficult to license just one or two Microsoft 365 security or compliance services.

Azure Defender is similar to Microsoft 365 Defender in that it is not a service or product licensed independently, but a similar XDR offering that can correlate information from across a range of security services with “Azure Defender” in their name. These services primarily secure Azure services and resources, but some can work with VMs/servers on-premises or in other clouds, using Azure Arc management tooling.



Attack Surface Reduction

Attack surface reduction is a set of Microsoft Defender for Endpoint security capabilities integrated exclusively to Windows endpoints. It includes a range of security capabilities built directly into Windows OSs, including AppLocker (which blocks and allows applications based on company policy) and Windows Defender Application Control. Microsoft Defender for Endpoint can be used to centrally manage and control these components, but all of them require Windows OSs, and many require Windows 10 Enterprise. Comparable capabilities are not offered for non-Windows platforms and are likely to remain exclusive to Windows for the foreseeable future.

Endpoint Detection and Response

EDR aggregates data from endpoints into the Microsoft Defender for Endpoint hosted service and includes malware analysis, hunting (research) of threats across systems, and alerting (notification) capabilities. The most comprehensive EDR coverage is available for Windows, followed by macOS. Microsoft is likely to continue to invest across all platforms supported by Microsoft Defender for Endpoint. (EDR is

not to be confused with eXtended detection and response [XDR], an analyst term that Microsoft began using during 2020 alongside the overloaded Microsoft 365 Defender brand. For more information on XDR and Microsoft 365 Defender, see the sidebar “XDR, Microsoft 365 Defender, and Azure Defender” on this page.)

Threat and Vulnerability Management

Threat and vulnerability management includes automatic analysis of aggregated endpoint data by the hosted service to discover potential threats the organization is likely to be impacted by and vulnerabilities within OS and application software that Microsoft Defender for Endpoint has discovered on endpoints. This capability was originally limited to Windows endpoints, but the feature was recently delivered for macOS.

Automated Investigation and Response

Automated Investigation and Response (AIR) provides scripts for automated investigation of threats and remediation tools. It uses the existing hunting playbooks created by security analysts to discover threats, generate alerts, and potentially remediate threats discovered across one or more end-

points. This capability performs hunting in aggregate across endpoints, not just on a system-by-system basis.

This capability is available only for Windows at this time but could arrive for macOS at some point in the future. Currently, some limited remediation tools are available for macOS.

Remediation tools are unlikely to ever arrive for the mobile device OSs supported by Microsoft Defender for Endpoint because of the constraints of those platforms.

Mobile Device Client Support

Microsoft delivered Microsoft Defender for Endpoint clients for iOS, iPadOS, and Android late in 2020, but formal endpoint protection like that offered for Windows and macOS is not possible because these platforms do not permit third-party software to interact with them at the level required to implement full malware detection scanning and remediation.

Although they cannot offer the level of protection and insight delivered by the Endpoint client on Windows 10 or macOS, these new clients should help organizations ensure a level of security on these popular mobile device OSs, particularly when users are connecting to organizational resources.

The Android client offers anti-phishing

and Web protection, malware scanning, and support for Conditional Access enforcement when the device is used to access Azure Active Directory-integrated applications.

The client for Apple mobile devices offers anti-phishing and Web protection capabilities, in addition to URL and domain blocking.

Mobile clients are managed from Microsoft Defender Security Center, where events are centrally logged, and Microsoft Defender SmartScreen is used to screen URLs. The Android client is available in the Google Play Store, and the Apple client is available in the App Store on devices running iOS and iPadOS. Users licensed for Microsoft Defender for Endpoint are permitted to install and run the software on up to five mobile devices of any type.

Licensing and Resources

For a visual summary of which Microsoft 365 suites include rights to Microsoft Defender for Endpoint, see the chart “Microsoft Defender for Endpoint Suite Licensing” on this page.

The roadmap for Microsoft Defender for Endpoint is discussed in the *Microsoft 365 Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/microsoft-defender-endpoint>.

Microsoft Defender for Endpoint licensing is discussed in the *Licensing Reference Set* at <https://www.directionsonmicrosoft.com/licensing/microsoft-defender-endpoint>.

Microsoft Defender for Endpoint (server) licensing is discussed in “Licensing Microsoft Defender for Endpoint on Servers” on page 32.)

Microsoft Defender for Endpoint documentation is at <https://docs.microsoft.com/microsoft-365/security/defender-endpoint>.

General availability of Microsoft Defender for Endpoint mobile clients was announced at <https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-on-ios-is-generally-available/ba-p/1962420>.

New UEFI scanning capabilities for Microsoft Defender for Endpoint on Windows were first announced at <https://www.microsoft.com/security/blog/2020/06/17/uefi-scanner-brings-microsoft-defender-atp-protection-to-a-new-level>.



Microsoft Defender for Endpoint Platform Support Scorecard

Microsoft 365 security and management services offer different capabilities depending on the platform that is being used with them. This chart shows a simple score for each of the four primary client platforms supported by Microsoft 365 suites. Here, the breadth of features available for Microsoft Defender for Endpoint on each platform was compared to arrive at a *Directions on Microsoft*–assigned score. The explanation column provides a high-level synopsis of features available for each platform that helped determine the score.

For simplicity, this chart combines iOS and iPadOS. To date, the features of this service that are available to those two platforms are identical.

Platform	Score	Score Explanation
Windows 10	4	Full AM, EDR and OS protection capabilities
macOS	3	AM, key EDR features, basic remediation
iOS/iPadOS	2	Anti-phishing, Web protection
Android	2	Malware scanning, anti-phishing, Web protection

COPYRIGHT © REDMOND COMMUNICATIONS, INC. REPRODUCTION IN WHOLE OR IN PART IS PROHIBITED.

Microsoft Defender for Endpoint Suite Licensing

Not all Microsoft 365 security and management services are available with all Microsoft 365 suites. This chart shows which Microsoft 365 suites for enterprise businesses include Microsoft Defender for Endpoint. (Microsoft Defender for Endpoint is included in Windows 10 Enterprise E5, and suites that include it.)

Customers should be careful if they do not plan to license all users in the organization for the full Microsoft 365 E5 suite. Mixing features across a tenancy of Microsoft 365 services can lead to license shortfalls and a significant unexpected expense when an audit occurs.

Suite	Included
Microsoft 365 F1	☐
Microsoft 365 F3	☐
Microsoft 365 E3	☐
Microsoft 365 E5	☒

COPYRIGHT © REDMOND COMMUNICATIONS, INC. REPRODUCTION IN WHOLE OR IN PART IS PROHIBITED.

Azure Defender Can Secure a Range of Azure Services

By Wes Miller

- Azure Defender is a family of freestanding, paid services used to secure Azure resources.
- Some Azure Defender services can be used with resources that are on-premises or in other clouds.
- Third parties are unlikely to match the level of security integration with Azure that Microsoft provides.
- Customers may need to augment Azure Defender with Azure Monitor and Azure Sentinel for a complete solution.

Azure Defender is a family of independent security services designed primarily to help secure resources running in Azure. The Azure Defender brand replaces the paid Standard tier of Azure Security Center. The free tier of Azure Security Center continues to be available but does little other than assist with security recommendations and assessments of the organization's Azure resources.

Azure Security Center: Recommendations and a Portal

Azure Defender services take advantage of the Azure Security Center portal for centralized management and, therefore, the portal play an important role in the use of Azure Defender services.

On its own, Azure Security Center is a free service that offers recommendations primarily intended to secure Azure resources and provide assessments of an organization's security posture. Microsoft refers to Azure Security Center as security posture management—it is about recommendations and alerting, not active defense, analysis, and mitigation of threats.

However, administrators can use the Azure Security Center portal to manage security issues with Azure resources and resources managed using Azure, including Azure Arc enabled resources.

Azure Defender: An Umbrella Brand for Services

Azure Defender is a family of services that each deliver proactive defenses, detection, logging, and alerting specific to the Azure service or resource they are protecting. The alerts and information generated by each Azure Defender service are integrated into the basic security tools and management plane included with Azure Security Center. Microsoft refers to this approach using the industry analyst term “extended detection and response” (XDR). (For more information on XDR and Azure Defender, see the sidebar “XDR, Microsoft 365 Defender, and Azure Defender” on page 14.)

“Azure Defender,” like “Microsoft 365 Defender,” is an umbrella brand of services and each service can be licensed stand-alone, but the services are likely to deliver the most value when used together with findings in Azure Security Center. Although Microsoft does not group them as such, the security services available under the Azure Defender umbrella brand can be organized into four loosely defined categories of services:

Workload defense is where Azure Defender services can protect application workloads running in Azure, like Azure VMs (and VMs and physical servers in select other configurations outside Azure), Azure App Service, and Azure container-based application services running on Linux.

Database defense is where Azure Defender services can be used to protect database workloads, like SQL Server inside and outside of Azure and multiple types of Azure Platform as a Service (PaaS) database offerings.

IoT defense is where Azure Defender offers two models for securing and auditing Internet of Things (IoT) systems.

Infrastructure defense is where Azure Defender secures several categories of Azure infrastructure, such as Azure Resource Manager (ARM), Azure Storage, and Azure Key Vault.

(For more information on the range of Azure Defender services, see the chart “Family of Azure Defender Services” on page 17.)

While organizations may find third-party offerings that secure certain Infrastructure as a Service (IaaS) and externally connected Azure workloads, like Azure VMs, SQL Server, and IoT devices, it is difficult or impossible for a third party to achieve the deep integration Azure Defender provides for Azure PaaS services and Azure infrastructure defenses.

Strongest Offerings Are Securing VMs and SQL

Two of the oldest and most comprehensive Azure Defender offerings are the services most organizations would be likely to use: Azure Defender for Servers and Azure Defender for SQL.

Azure Defender for Servers

Azure Defender for Servers was originally designed for use with Azure VMs. Two of its features still only make sense with Azure VMs and are not available when the service is used with VMs or server operating system environments (OSEs) outside Azure:

- Just-in-time (JIT) VM access, which controls administrative access to VMs
- Adaptive network hardening, which provides recommendations on network ports that should be disabled to maximize security.

Azure Defender for Servers is also one of the two ways to license Microsoft Defender for Endpoint (server) for Windows Servers. Microsoft Defender for Endpoint (server) is the confusingly named offering of Microsoft Defender for Endpoint software when it is used with servers inside or outside of Azure. Windows Defender for Endpoint (server) can also be installed on a Windows Virtual Desktop (WVD) host running Windows 10 Enterprise multi-session. (Azure Defender for Servers does not confer rights to run Microsoft Defender for Endpoint on a Linux server. For more information on Microsoft Defender for Endpoint (server) licensing options, see “Licensing Microsoft Defender for Endpoint on Servers” on page 32.)

In addition to Microsoft Defender for Endpoint (server), Azure Defender for Servers includes vulnerability and patch assessments for Windows Server and Linux VMs in Azure and elsewhere and memory-based forensics, which helps analysis of fileless memory exploitation, code injection, and execution of malicious payloads. (For detailed descriptions of the features in Azure Defender for Servers, see the chart “Azure Defender for Servers Features” on page 18.)

Azure Defender for Servers is available for Windows Server VMs and physical servers external to Azure using Azure Arc. There is no price difference for Azure Defender for Servers when used with Azure VMs or externally using Azure Arc.

Some Azure Security Center features that are free for use with Azure VMs, like OS patch management, security management

Family of Azure Defender Services

A range of security services are available under the Azure Defender brand. Each service is licensed independently and secures a different type of service or infrastructure within Azure. Some services can also secure assets on-premises or in other clouds, typically using Azure Arc.

Azure Defender for Servers includes up to 500MB of data ingestion into Azure Monitor per day, for the standard retention period of up to one month. Additional data storage or an extended retention period and use of Azure Monitor's Log Analytics capabilities by any of the other Azure Defender services require additional licensing.

Service Name	Core Capability	Azure Resources Only	Licensing (US\$)
Workload Defense			
Azure Defender for Servers	Secures Azure Virtual Machines, Azure Arc enabled VMs, and bundles Microsoft Defender for Endpoint (Windows only).	☐	\$0.02 per server, hourly
Azure Defender for App Service	Secures deployments of Azure App Service, including detection of vulnerability scanners or fileless attacks and digital currency mining attacks.	☒	\$0.02 per app service application, hourly
Azure Defender for Kubernetes	Secures Azure Kubernetes Service (AKS) nodes, including detection of exposed Kubernetes dashboards, creation of high-privileged roles, and the creation of sensitive mounts (Linux only).	☒	\$0.00268 per vCore, hourly
Azure Defender for ACR	Scans Azure Container Registry (ACR) images using Qualys vulnerability scanning tools (Linux only).	☒	\$0.29 per protected image
Database Defense			
Azure Defender for SQL on Azure	Uses real-time anomalous activity detection to notify administrators when unusual access attempts on Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics are detected. Includes brute force attack prevention.	☒	\$0.021 per instance, hourly
Azure Defender for SQL outside Azure	Uses real-time anomalous activity detection to notify administrators when unusual access attempts on SQL Server databases outside Azure are detected. Includes brute force attack prevention.	☐	\$0.015 per vCore, hourly
Azure Defender for MySQL	Uses real-time anomalous activity detection to notify administrators when unusual access attempts on Azure Database for MySQL are detected. Includes brute force attack prevention.	☒	Free during preview
Azure Defender for PostgreSQL	Uses real-time anomalous activity detection to notify administrators when unusual access attempts on Azure Database for PostgreSQL are detected. Includes brute force attack prevention.	☒	Free during preview
IoT Defense			
Azure Defender for IoT – IoT Hub Per Device	Uses on-device agents to gather security events from IoT devices. Requires Azure IoT Hub.	☐	\$0.001 per device, monthly
Azure Defender for IoT – IoT Hub Per Message	Uses on-device agents to gather security events from IoT devices. Requires IoT Hub.	☐	\$0.20 per 25,000 transactions
Azure Defender for IoT – Agentless	Uses sensors (VM or appliance) to gather security events based on IoT network traffic. Uses on-premises software and console.	☐	\$2,000 per 1,000 devices, monthly
Infrastructure Defense			
Azure Defender for Storage	Secures Azure Blobs, Azure Files, and Azure Data Lake Storage Gen2 resources, including detection of anonymous access, compromised credentials, social engineering, privilege abuse, and malicious content.	☒	\$0.02 per 10,000 transactions per subscription
Azure Defender for Key Vault	Watches for unusual and suspicious activity in Azure Key Vaults.	☒	\$0.02 per 10,000 transactions
Azure Defender for ARM	Watches for suspicious operations, exploit toolkits, and lateral movement operations upon Azure Resource Manager (ARM) elements.	☒	Free during preview
Azure Defender for DNS	Watches for DNS tunneling exfiltration, command and control (C&C) and malicious domain communication, and DNS attacks.	☒	Free during preview

Azure Defender for Servers Features

Azure Defender for Servers includes several features, but not all are available in all scenarios. Originally only available for Azure VMs, many features of Azure Defender for Servers are now available for use with on-premises VMs or physical servers, and in VMs running in third-party clouds, connected via Azure Arc.

Some features are only available for operating system environments (OSEs) running Windows Server, and some features are only available on Linux.

Some features are not available for OSEs running within Azure VM scale sets.

Azure Defender for Servers includes up to 500MB of data ingestion into an Azure Monitor Log Analytics workspace per day for the standard retention period of up to one month. Additional data storage or an extended retention period requires additional licensing.

Feature Name	Feature Description	Azure Virtual Machines	Azure VM Scale Sets	Azure ARC Enabled Systems (external to Azure)
System Security Management				
Microsoft Defender for Endpoint	Real-time attack surface reduction with endpoint detection and response (EDR) (Windows Server only).	✓	✓	✓
Behavioral analytics and security alerts	Automatic blocking of security threats using Microsoft Defender for Endpoint and generation of alerts on events.	✓	✓	✓
Endpoint protection management ¹	Management of Microsoft and third-party endpoint protection software.	✓	✓	✓
OS patch management ¹	Real-time patch management analysis for supported OSs.	✓	✓	✓
Security misconfiguration assessment ¹	Assessment of systems for configuration settings that could result in poor security posture.	✓	✓	✓
Fileless security alerts	Real-time memory-based forensics of potential memory exploitation, code injection, and execution of malicious payloads (Windows only).	✓	✓	✓
File integrity monitoring	Real-time analysis of VMs to watch for and alert on modification of key files and registry data.	✓	✓	✓
Docker container recommendations and threat protection	Recommendations and threat protection of Docker-hosted IaaS containers (Linux only).	✓	✓	✓
Adaptive application control	Proactive tool that uses machine learning to enforce whitelisting of applications on Windows Server VMs.	✓	○	✓
Network-based vulnerability assessment	Automatic assessment of vulnerabilities on Windows Servers.	✓	○	✓
Disk encryption assessment	Assessment to ensure that Azure VM OS and data disks are encrypted using BitLocker.	✓	✓	○
Azure VM Security Management				
Just-in-time VM access	Proactive tool that leaves network ports for remote administration closed until required and activated.	✓	○	○
Adaptive network hardening	Proactive tool that uses machine learning to establish and enforce rules about what network connections should be allowed to Azure VMs.	✓	○	○
Security Basics and Third-Party Integrations				
Regulatory and compliance dashboard and reporting	Dashboards and reporting to help organizations assess the compliance of their resources.	✓	✓	✓
Network map tool and security assessments	Network map and network security hardening recommendations.	✓	✓	○
Third-party vulnerability assessments	Security analysis of Azure resources using third-party software to provide recommendations.	✓	○	✓

¹ Endpoint protection management, OS patch management, and security misconfiguration assessment are free Azure Security Center capabilities for Azure VMs, but they require Azure Defender when used with OSEs outside of Azure.

assessments, and endpoint management, require Azure Defender for Servers when used with OSEs outside of Azure.

Azure Defender for Servers has an hourly price of US\$0.02 “per server” (US\$14.60 per month), where Microsoft defines a server as a virtual OSE or physical OSE. This means that every VM and physical host must be licensed individually. Licensing a physical host for Azure Defender for Servers confers no rights to use the service—or Microsoft Defender for Endpoint (server)—within VMs on that server. Each licensed OSE includes 500MB of data ingestion into Azure Monitor’s Log Analytics feature, which is used by several features included in Azure Defender for Servers, like OS patch management.

Azure Defender for SQL

Azure Defender for SQL offers several layers of protection for SQL Server running in Azure VMs or outside Azure, as well as Azure SQL PaaS offerings; Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics, as follows:

- Helps prevent potential brute force attack attempts where a large number of failed login attempts have been observed
- Generates alerts for SQL injection attempts, which could help identify attacks before they breach systems and escalate.

The service also includes vulnerability assessments and information protection for instances of Azure SQL PaaS offerings. Vulnerability assessments are used to help discover and remediate vulnerabilities in the database, such as unmodified default administrator accounts and lack of encryption. Information protection helps identify and classify potentially sensitive data. Both vulnerability assessments and information protection require manual effort and are also included in SQL Server Management Studio for free with SQL Server.

Azure Defender for SQL also offers anomalous activity detection for SQL Serv-

er and Azure SQL PaaS offerings, alerting on unusual activity such as when databases are accessed:

- From an unexpected geographic location
- From an unexpected Azure data center
- By an unexpected security principal (user)
- By a potentially harmful application (which may indicate attack tools or a penetration test).

Similar, but more limited offerings are available for Azure open-source SQL database services; Azure Database for MySQL and Azure Database for PostgreSQL, both currently free while the services continue in a long-running public preview.

Azure Defender for SQL on Azure has an hourly price of US\$0.021 “per instance” (US\$15 per month), where an instance is defined as:

- An Azure VM running Windows Server or Linux with SQL Server installed
- A deployment of Azure SQL Database (single database or elastic pool)
- An Azure SQL Managed Instance database
- An Azure Synapse Analytics dedicated SQL pool.

Azure Defender for SQL outside Azure has an hourly price of US\$0.015 (US\$10.98 per month per vCore). Since SQL Server running in a VM requires a minimum of four vCores, the minimal cost for a single instance of a VM or physical server running SQL Server outside of Azure is US\$43.80, almost triple the cost of running Azure Defender for SQL on an Azure VM, with no additional value provided for the price difference.

Beware, Batteries Are Not Included

Making the most of Azure Defender services is likely to result in numerous unexpected charges that organizations should understand before broadly adopting Azure Defender services:

- Azure Monitor’s Log Analytics capabil-

ity is used by multiple Azure Defender services, and storage charges can be difficult to estimate prior to production deployment

- To use the full breadth of XDR scenarios demonstrated by Microsoft, organizations will likely need to license Azure Sentinel

• Azure Defender for IoT deployments that rely on Azure IoT Hub require the use of that service for message transfer; as with Log Analytics, these costs can be hard to estimate prior to deployment

• An agentless deployment of Azure Defender for IoT requires a predefined minimum commitment of managed devices from within the Azure portal; this is used to activate the on-premises software console used to manage the service

• Azure Defender for SQL outside Azure is considerably more expensive than Azure Defender for SQL on Azure, as the former is licensed per OSE instance, while the latter is licensed per vCore

• When Azure Defender is enabled for Azure resources, the change is logged in the Azure activity log, giving organizations some insight into who turned the service on for which resources, and when the action was taken.

Resources

Azure Defender documentation is at <https://azure.microsoft.com/services/azure-defender>.

Azure Defender pricing information is at <https://azure.microsoft.com/pricing/details/azure-defender>.

Azure Security Center documentation is at <https://docs.microsoft.com/azure/security-center/security-center-introduction>.

A comparison of Azure Defender to Azure Security Center is at <https://docs.microsoft.com/azure/security-center/security-center-pricing>.

Microsoft Defender for Endpoint capabilities are described in “Microsoft Defender for Endpoint Platform Support” on page 13. ➤

Consolidating Azure Deployments During M&A

By Rob Sanfilippo

- Azure deployments under different Azure Active Directory tenancies resulting from mergers and acquisitions should be consolidated under a single tenancy.
- The difficulties and risks of consolidation may be best handled with the assistance of an external consulting partner.

Mergers and acquisitions (M&A) are a regular occurrence for some organizations. M&A can result in the existence of multiple Azure Active Directory (AAD) tenancies within an organization, and more than one of these tenancies may have an Azure deployment (that is, different Azure subscriptions may be linked to different tenancies). Organizations should pursue consolidation of such deployments. However, the processes involved could be complex, so organizations that rarely engage in M&A may find it more cost effective to use an external consulting partner rather than developing processes they are not likely to reuse.

This report focuses on the consolidation of multiple Azure deployments that were created under different AAD tenancies. There are other Azure deployment considerations and opportunities that could arise during M&A that are not addressed in this report.

Problems with Azure Deployments Under Different Tenancies

Maintaining Azure deployments that use different tenancies usually brings complexity and risk. Such a practice may be necessary because of security or compliance requirements or the lack of resources to perform a consolidation. However, in most cases, organizations should pursue consolidation of Azure deployments into a single tenancy for the following reasons:

Access management. An Azure subscription cannot be configured for access with accounts from more than one tenancy. Azure uses a role-based access control (RBAC) system to assign access to administrators using AAD accounts. Maintaining multiple Azure subscriptions that use different tenancies requires creating and maintaining separate accounts and roles for the same users and purposes in each deployment. This duplication adds management overhead and risk of assigning unnecessary access.

Governance. Azure governance includes processes that work with policy, compliance, security, and management using various Azure services and tools. Keeping Azure deployments under different tenancies requires applying the same governance in each deployment, which adds a burden to duplicate the governance configurations for each tenancy that has linked Azure subscriptions and a risk of having those configurations become inconsistent.

Redundant solutions. Keeping deployments under different tenancies may lead to maintaining multiple instances of the same or similar solutions. For example, M&A could result in multiple Azure deployments that host expense reporting applications, leading to redundant management tasks, difficulties with scaling, and extra cost.

Determining What Is Running in Acquired Azure Deployments

An early step in consolidation is determining the purpose and contents of Azure deployments that arrive during M&A. An organization may find it owns and must take over management of Azure deployments that it was not involved in creating, and the original IT and development teams responsible for the deployments may not be available. Discussions between the new and previous teams should be held as far in advance of a transition as possible, but these interactions may be prevented by the legal processes of M&A, giving the new teams a short time to understand and take over Azure deployments.

The worst case of an Azure deployment transition is when it is not known what the deployment contains, previous team contacts are not available, and there is insufficient documentation provided. Exploring and inventorying an Azure deployment and determining interdependencies among resources in such cases can be done with various ad-hoc tools and processes (given appropriate security access), including the following:

The **Azure portal** can be used to explore the resources in a deployment using the “Resource groups” and “All resources” views and views that show all instances of particular resource types, such as VMs and SQL Databases.

The **Azure Network Watcher topology** view can be used to explore existing networking configurations, such as virtual networks, network interfaces, and network security groups to help understand connectivity in the deployment so it can be replicated in the target deployment.

Azure Monitor can be used to run custom queries on the deployment to, for example, create reports on particular types and names of deployed resources. The Service Map solution that works with Monitor can be used to discover certain resource interdependencies.

Azure Resource Manager (ARM) templates can be viewed and exported to collect the JSON-based files, which provide meta-data (and some data) of existing resources. These templates can be used to understand deployment configurations and speed their replication by importing the templates in the target deployment, usually with some modification.

Azure PowerShell cmdlets and the Azure CLI can produce deployment inventory lists at different levels of specificity. The tools could be used to create scripts that produce custom reports as an alternative to manual exploration of a deployment.

The **Azure Migrate service**, typically used to assess on-premises VM deployments for migration to Azure, could be used to assess VMs in an Azure deployment so they can be moved to a different Azure deployment in a lift-and-shift fashion.

How to Consolidate

Consolidation of Azure deployments under a single tenancy can be performed in two primary ways: using a tenancy transfer tool in the Azure portal or manually recreating resources in the destination with various tools and processes.

Both options require planning and could entail significant challenges and risks of error. Selection factors vary by scenario, and a strategy that uses both options may be necessary. Factors include the acceptable amount of downtime, the size and complexities of the deployments, and the available budget, expertise, and time to complete the consolidation. The difficulties of performing certain consolidations may make the usage of an external consulting partner the best approach.

Transferring Subscriptions Using the Azure Portal

The Azure portal provides a tool for transferring a subscription across tenancies. A subscription contains Azure resources (such as VMs) controlled by a single tenancy and billing owner. A billing ownership change to a subscription, which is likely for M&A consolidations, also can be performed in the Azure portal. Azure deployments commonly have multiple subscriptions, and the tool must be run separately for each subscription. Additional manual steps must be performed before and after using the tool, and solution downtime is likely.

Several elements of a subscription are not transferred by the tool, including:

- RBAC role assignments, custom roles, and managed identities
- Portions of resource configurations for certain services, such as SQL Database, Storage, Azure Kubernetes Service, Key Vault, Files, and Data Lake Storage
- Policies, which must be exported, imported, and assigned in the new tenancy.

The procedure for using the tool includes preparation steps to gather lists of the elements that must be manually reconfigured after the tool is used. These lists are usually generated using PowerShell or the Azure CLI.

There are several means of access that may remain available to previous administrators or users after the tool is used to change tenancies. For example, access keys to services, management certificates that allow administrator access, and remote access credentials for VMs remain unchanged after a tenancy transfer. These items could preserve undesired deployment access creating security weaknesses after the consolidation, so they should be carefully investigated after using the tool to transfer a tenancy.

A tenancy transfer performed using the tool does not physically move resources across regions; it performs a logical configuration change. Azure Resource Mover, a separate tool, can be used to move resources physically across regions after a tenancy

is changed if that is required for compliance or other organizational reasons.

Redeploying Resources Manually

A fully manual approach to consolidating deployments under a tenancy can be employed. This option gives more flexibility to what, when, and how parts of a deployment are moved. For example, it enables the physical movement of resources across regions. However, the approach involves several diverse tools and significant customization, making it error prone if not precisely planned and executed.

A manual redeployment process can be performed using the tools and techniques such as the following:

- Azure Site Recovery and Azure Migrate can be used to move VMs
- Databases can be moved using extract, transform, and load (ETL) tools (such as Azure Data Factory), the Azure Database Migration Service, or backup and restore tools that vary by database type
- Azure Storage accounts can be moved using tools such as Data Factory, AzCopy, and the Azure Storage Data Movement Library
- Virtual networks can be peered between Azure deployments in different tenancies, allowing fast, secure data transfer during a consolidation
- ARM templates can be exported from the source deployment, modified, and imported in the target deployment
- The Azure Import Export service and Data Box devices can be used to transfer data from the source to target deployments using physical appliances
- Applications that are deployed from source control systems such as GitHub and Azure DevOps can be published into the desired deployment by modifying pipeline targets.

Manual redeployment is a complex method because there are more than 200 Azure resource types, many of which require unique processes to replicate. For example, there are many networking resource types that must be reconfigured to work with network address spaces in a different environment; Azure Monitor Log Analytics workspaces are likely to be combined in the destination deployment, rather than added to it; and Azure portal dashboards may need to be rebuilt instead of moved when consolidating.

Other Planning Considerations

Organizations consolidating Azure deployments may want to break the process into phases and make changes to the deployments while consolidating.

Phasing the Consolidation

Larger deployments should typically be consolidated using a phased effort that subdivides the process over time to maintain application availability and simplify validation of the consolidation.

Phases might be performed using solution, subscription, resource group, or resource type boundaries, although the plan should prevent situations where portions of a critical solution are split between deployments, making it unavailable.

It may be necessary to perform a consolidation over an extended period, such as months or years, so a hybrid stage, where both tenancies are maintained, could be employed. However, for reasons mentioned earlier, it is best to plan for ultimately merging all Azure deployments under a single tenancy.

Making Deployment Modifications During Consolidation

Consolidating Azure deployments under a single tenancy could present opportunities to make changes that improve solutions and realize other optimizations. However, the time and budget available to complete a consolidation and the compounded complexity of making changes while consolidating may prohibit such modifications. Nevertheless, a consolidation period is a good time to explore potential improvements that could be planned for the future.

Modifications to be considered for a consolidated deployment include the following:

Redundancy elimination could be achieved by reviewing solutions in the source and target deployments for overlap and choosing the optimal solution to preserve. For example, multiple line-of-business applications designed for the same purpose may exist. Furthermore, components across solutions might be consolidated, such as databases and machine learning models with similar purposes.

Cleanup and organization improvements could be made while deployments are inventoried and reviewed during a consolidation. Older deployments may have been poorly planned or expanded erratically over years. For example, naming schemes, hierarchical organization (management groups, subscriptions, and resource groups), and Azure tag usage might require improvements. Governance controls, such as policies and RBAC settings, also should be examined and strengthened where necessary.

Unused resources could be located during a consolidation. Such resources might be creating unnecessary costs. For example, unused VMs and other orphaned resources might exist, and abandoned, temporary, and experimental solutions that are no longer used may still be deployed.

Right-sizing changes to a consolidated deployment could be made to optimize costs. Native Azure tools such as the Advisor and Cost Management services could help locate right-sizing opportunities.

Licensing changes, such as the use of the Azure Hybrid Benefit and purchase of reservations may provide benefits when making deployment consolidations due to M&A.

Development tasks may be required during a consolidation. Certain applications may contain code that references metadata specific to a tenancy or deployment, such as subscription IDs and URLs, requiring updates to the code to keep applications running properly after a consolidation.

Solution improvements could be made to optimize, enhance, or replace existing solu-

tions. M&A could deliver superior solutions or functionality that was not previously available. Azure capabilities could be leveraged to refactor, rearchitect, or rebuild solutions. For example, Platform as a Service (PaaS) and serverless services could be used to improve solution performance and reduce costs, and incorporation of machine learning and IoT technology could deliver new features.

Resources

Azure Active Directory tenancy considerations are discussed in “Do Multiple Microsoft 365 Tenancies Make Sense?” on page 19 of the Dec. 2019 *Update*, “AAD Tenancy Strategies for Complex Organizations” on page 17 of the Jan. 2017 *Update*, and the *Microsoft 365 Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/azure-active-directory>.

[directionsonmicrosoft.com/roadmap/ref/azure-active-directory](https://www.directionsonmicrosoft.com/roadmap/ref/azure-active-directory).

Azure deployment hierarchies are discussed in the *Azure Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/azure-deployment-hierarchies>.

Azure Resource Mover is discussed in “Moving Azure Resources Across Regions” on page 18 of the Apr. 2021 *Update*.

Moving resources logically is discussed in “Moving Azure Resources Across Subscriptions and Resource Groups” on page 20 of the Apr. 2021 *Update*.

Azure Governance resources are available in “Kit: Understanding Azure Governance” at <https://www.directionsonmicrosoft.com/update/secured/2020/05/kit-understanding-azure-governance>. 

SQL Server Database Options in Azure & On-Premises

By Andrew Snodgrass

- Azure SQL Server-based PaaS and cloud offerings provide a viable alternative to most on-premises SQL Server deployments.
- They are easier to deploy, scale, and manage, and they can help organizations avoid upfront cost with licensing migrations options that protect existing investments.
- They are mostly compatible with the full SQL Server product but lack some features, control, and flexibility of a traditional SQL Server deployment.
- Choosing a destination is becoming easier as compatibility differences decline and deployment options increase.

Microsoft provides multiple offerings (on-premises and in Azure) for deploying SQL Server databases, including the traditional SQL Server software, several Platform as a Service (PaaS) offerings, and new PaaS on-premises and edge options. The offerings vary in features, capacity, and licensing, but all rely on the same database engine, providing opportunities for migrating workloads with minimal modifications. (For a comparison of capacities and features, see the chart “SQL Server Database Offerings Comparison” on page 23.)

SQL Server On-Premises

SQL Server on-premises is the traditional deployment model and provides all the features and roles needed to host transactional databases and data warehouses. SQL Server is available on Windows Server and Linux, although the Linux offering lacks some roles, such as Reporting Services and Analysis Services. SQL Server on-premises is available in multiple editions, with

Standard and Enterprise most typically deployed by enterprises.

On-premises deployments provide the greatest level of control and configuration, allowing customers to create simple or complex environments that are highly customized to their workloads.

However, on-premises deployments mean customers are responsible for all associated data-center costs, including hardware, back-end infrastructure, network connectivity, storage, security and authentication, and administration, as well as other servers and software licensing requirements. This includes initial capital expenditures plus depreciation expenses.

Software licenses are available under a per-core and a server plus Client Access License (for Standard edition only) model through Microsoft volume licensing.

SQL Server on Azure VMs

SQL Server in Azure VMs provides the same feature set as SQL Server on-premises, although with potentially lower

hardware limits for memory and cores and is available in a pay-as-you-go licensing model. The back-end infrastructure is managed by Microsoft, but customers are still responsible for maintaining the OS and server software.

Deploying SQL Server to Azure VMs will interest customers performing lift-and-shift migrations to Azure and who prefer an Azure environment that mimics their on-premises or hosted data center. It provides control over when patches and updates are applied and supports complex applications that need low-level granular control of the database software and server or specialized failover and replication configurations. The VM configuration also allows co-location of applications, databases, and other features on a single VM, which is not available in any of the PaaS offerings.

SQL Server in Azure VMs is available in two license models. Customers may purchase licenses through Microsoft volume licensing and reassign them to Azure (known as Azure Hybrid Benefit), or they may li-

SQL Server Database Offerings Comparison

The chart compares SQL Server database on-premises with Azure SQL offerings. The chart uses Enterprise edition for on-premises and highlights differences in key areas.

The cloud Platform as a Service (PaaS) services offer many common database management features and APIs offered with the SQL Server software, although they tend to have capacity and features limitations and they lack other SQL Server roles, such as Reporting Services, Integration Services, and Analysis Services, which can be found in other Azure services. Consequently, choosing an Azure destination includes trade-offs, and comparing costs may be difficult.

Feature	Description	SQL Server On-Premises	SQL Server in Azure VMs	Azure SQL Managed Instance	Azure SQL Database Single Database	Azure SQL Database Elastic Pool	Azure Synapse Analytics	Azure SQL Edge
Tenancy	The location and hosting environment	Customer premises	Microsoft data center (multitenant VM hosting)	Microsoft data center (multitenant hosted platform)	Microsoft data center (multitenant hosted platform)	Microsoft data center (multitenant hosted platform)	Microsoft data center (multitenant hosted platform)	Customer premises
Product update control	Customer-managed SQL Server updates and maintenance	✓	✓	✓	○	○	○	✓
OS control	Customer-managed OS updates and maintenance	✓	✓	○	○	○	○	✓
Physical updates	Customer-managed hardware updates and maintenance	✓	○	○	○	○	○	✓
Performance scaling	Scaling technique to increase performance to address workload demands	Scale up to higher spec hardware	Scale up to higher-performing VM	Scale up to higher tier and performance level	Scale up to higher tier and performance level	Scale up to higher tier and performance level	Scale compute and storage resources independently	Scale out clustering
Max database size	Maximum database size	524PB	524PB	4TB - 8TB	2GB - 4TB (Hyperscale 100TB)	156GB - 4TB	Multiple petabyte	524PB
Max memory size	Maximum memory available	Hardware limit	5700GB	396GB	48GB - 396GB (Preview 3767GB)	396GB (Preview 3767GB)	Service limit	64GB
Max cores	Maximum number of server cores	Hardware limit	208	80	8 - 128	80 - 128	Service limit	8
Database backups	Scheduled full, incremental, and log backups for restoration	Customer managed	Customer managed	Microsoft and customer managed	Microsoft managed	Microsoft managed	Microsoft managed	Customer managed
Replicas for high availability and disaster recovery	Secondary replicas used for high availability, disaster recovery, and reporting	Up to eight customer-managed replicas	Up to eight customer-managed replicas	Two high-availability replicas and up to four disaster recovery replicas	Two high-availability replicas and up to four disaster recovery replicas	Two high-availability replicas and up to four disaster recovery replicas	Microsoft-managed high-availability and disaster recovery replicas	None
Database replication	Database replication and mirroring to create backup copies	✓	✓	✓	Limited	Limited	Through ETL component	None
Pricing	Base pricing methodology	Licensing	Capacity and licensing	Capacity and features	Capacity and features	Capacity and features	Capacity and components	Per-device

cense SQL Server on Azure in a capacity-based, pay-as-you-go model, where all costs for the SQL Server software are covered by an hourly fee. In both cases, the cost of the underlying Windows Server VM is billed separately. Additional licensing options include reserved capacity, which provides a discount in exchange for a one- or three-year commitment.

Customers can choose from a variety of server families and sizes. VM images range significantly in price per hour depending on the edition of SQL Server selected and the number of virtual cores used for the instance. CPU resources, memory, and features such as load balancing and auto-scaling all affect the cost of the underlying VM. Additional costs include storage of the VM and associated data in Azure, as well as charges for outbound data transfer.

Cloud PaaS Offerings

Microsoft provides several SQL Server PaaS offerings that share many similarities but are designed for different workloads and therefore have trade-offs on features, performance, capacity, and cost:

- Azure SQL Database
- Azure SQL Managed Instance
- Azure Synapse Analytics

The offerings are designed for organizations seeking a relational database cloud service with low cost, quick deployment, scalability, and global reach. Microsoft manages and updates the underlying infrastructure, including servers, OSs, and SQL Server software, which removes most of the overhead associated with installation and maintenance of the host OSs and server applications. They include high-availability and replication features, providing globally distributed data sharing and disaster recovery, and provide access to Azure security services.

The services use SQL Server's database engine and offer many of the most common database management features and APIs in the full SQL Server software product. However, they lack some advanced features and low-level controls that may be critical to complex workloads, such as using buffer pool extensions, database mirroring, multiple log files, or configuring Always On Availability Groups, differential backups, and snapshots. They are also limited to providing the database engine only; no other SQL Server roles, such as Reporting Services, Integration Services, and Analysis Services, are supported. These roles are available in various combinations in other Azure services, including Power BI, Azure Data Factory, and Azure Analysis Services.

Pricing for the PaaS offerings varies significantly, but they all support Azure Hybrid

Benefit for deployments using virtual core pricing and other purchasing options that can reduce the costs for continually running PaaS offerings if applied for an extended period.

Azure SQL Database

Azure SQL Database is the original SQL database offering. It is a multitenant cloud service that supports deployment of stand-alone databases within an instance, where each database is independent of other databases. For example, a stand-alone database might support a departmental application or a self-contained business intelligence (BI) database. SQL Database supports most of SQL Server's database management features but is the most restrictive of the PaaS offerings and has a longer list of unsupported features than the others, adding lack of support for cross-database queries and the SQL Server agent.

SQL Database is available in two deployment models: single database and elastic pool. Single database deployments have guaranteed resources (compute and memory), while elastic pool is primarily for ISVs and organizations that have multiple single databases (with variable use patterns) that can share resources to help control cost.

Both deployment models can be purchased by capacity (referred to as vCores) or tier-based (referred to as Database Throughput Units).

Capacity pricing is calculated on a combination of computing power (vCores and memory), storage, and number of operations. Customers can choose between several capacity levels (Serverless, General Purpose, Business Critical, and Hyperscale) that vary in hardware selection, virtual cores, memory limits, and availability.

Tier-based purchasing is available in three tiers (Basic, Standard, and Premium) that are distinguished by maximum database size, computing resources, and features.

Costs accumulate for every hour the database exists (except for the serverless deployment option) and the database cannot be shut down, although customers can modify the performance level to match expected expenditures. The cost of database storage is included with throughput tiers, while storage is priced separately with virtual core pricing. Additional costs include optional disaster recovery features and backup storage.

Azure SQL Managed Instance

Azure SQL Managed Instance closely resembles a traditional on-premises SQL Server instance. Managed Instance was originally included in the SQL Database offering but was made a separate service

in 2020. It continues to receive unique features that are not available in SQL Database, such as cross-database queries and SQL Server's Machine Learning Services.

Managed Instance solves the single database deployment limitation of SQL Database by allowing customers to deploy SQL Server instances as they would on-premises. This approach provides a practical way to migrate SQL Server applications with complex database requirements, such as the need to group a collection of databases in one location, have shared security controls, or to failover as a group. Managed Instance also provides instance-level features, like access to the resource governor, and security features that are often requirements for many enterprises. The service is also previewing more on-premises capabilities, including language tools and support for distributed transactions across hosted databases.

Managed Instance can be purchased exclusively by capacity with vCores. Pricing is based on a combination of compute power (including virtual cores and memory), storage, and number of operations. Customers can choose from among several tiers (General instance pools, General single instance, and Business Critical single instance) that vary in capacity and memory limits and features. Additional costs for optional disaster recovery features, as well as charges for outbound data transfer and backup storage, should be expected. Automated backups and a limited storage capacity are included with each tier; however, it is likely that some tiers will incur additional backup storage costs.

Azure Synapse Analytics

Azure Synapse Analytics (formerly SQL Data Warehouse) combines a traditional data warehouse service based on SQL Server with a general use analytics platform, specifically for organizations with skills in SQL Server's T-SQL and Apache Spark. It provides petabyte-level data storage for data warehouses and can be used as an alternative to traditional on-premises data warehouse deployments. However, the data warehouse relies on the use of SQL Server's ColumnStore Indexing (a storage method that helps speed aggregation of large datasets), which may require restructuring existing data warehouses and applications to work in the service.

The service will likely interest customers with plans to move SQL Server data warehouses to Azure, organizations that are expanding into Spark and other analytics languages, and environments with a mix of data types (structured, semi-structured, and unstructured) that need to perform

near-real-time analysis or historical reporting. It supports most of the SQL Server features used in data warehouses on-premises but also provides features, like scale-out computing, that are unique to the service. To fully take advantage of Synapse Analytics will likely require restructuring some data structures and adopting new query methods.

Synapse Analytics provides:

- Data hosting and management of SQL Server data warehouses (into the petabyte scale) and Spark SQL tables

- Query and analytics using SQL Server and Apache Spark to perform routine and ad-hoc queries against any type of data

External data access, a key feature of data warehouses, is available using:

- SQL Server's external and linked table capabilities

- Direct access to Azure Data Lake Storage (ADLS) Gen 2 data

- Synapse Link, a separate component that uses distributed queries to access other Azure services

- Synapse Pipelines, an embedded extract, transform, and load (ETL) capability based on Azure Data Factory.

Synapse Analytics components are priced separately. Data warehouse features scale storage and computing resources independently and are priced by provisioned compute resources called data warehouse units (DWUs), which represent the relative power of the service as a blended measure of CPU, memory utilization, and read-write rates. Newer analytic features are priced on the node size (based on vCores and memory), the number of nodes, and autoscale settings. Synapse Pipelines loosely follows the Data Factory native-mode V2 pricing structure, which is based on the number of operations (read, write, and monitoring), pipeline orchestration runs, and execution runtime hours. Storage charges are based on Azure Premium Storage rates. Additional charges apply for optional, geo-redundant storage (across multiple Azure regions). Operations that move data out of the data warehouse, such as retrieving data via a query or exporting data for some other purpose, carries Azure's regular outbound data charges.

On-Premises PaaS Alternatives

Microsoft also is pursuing new deployment options that extend PaaS and other Azure services to a customer's location. These options provide several benefits over traditional on-premises deployments, including the following:

- Quick deployment and simplified management

- On-demand scaling, which can help

control cost for applications with variable-use patterns

- No upfront purchase of server licenses, which can reduce costs for SQL Server.

However, they also grant Microsoft some ongoing access to customer-hosted environments. Although customers can limit when the access occurs, this access could expose sensitive data and processes, which in turn could violate privacy regulations and security standards, or open avenues for future software license audits.

Arc Enabled Data Services

Azure Arc is a set of capabilities for using Azure management interfaces to work with deployments hosted outside of Azure. Arc could simplify managing a combination of services hosted in Azure, on-premises, and in other clouds, such as Amazon Web Services. It allows customers to have a mix of Azure-hosted and non-Azure deployments that can be managed together, ensuring a consistent application of policies and services.

Azure Arc enabled data services (currently in preview) is the Arc service that supports deployment of SQL Managed Instance on-premises. This scenario will most likely interest customers with on-premises regulatory or compliance requirements, hybrid environments that need consistency between cloud and local deployments, or migration plans that will benefit by moving to Managed Instance locally prior to migrating to Azure to reduce risk.

Arc enabled data services includes most of the features in the cloud offering but has technical and management requirements, such as deployment uses a local Kubernetes cluster, and the local deployment must occasionally connect to Azure for updates and billing purposes. Additionally, there are several capabilities not available that may arrive in future updates. For example, SQL Managed Instance on-premises does not support merge replication, linked servers, Always On availability groups, managed backups, Active Directory authentication, and certain other features supported by the Microsoft-cloud offering.

The offering is in preview, and pricing is not currently available.

Azure SQL Edge

Azure SQL Edge is a small-footprint deployment option for low-powered devices, gateways, and edge servers running near Internet of Things (IoT) devices. It includes a special edition of SQL Server's database engine that is optimized for such devices. Like its parent, SQL Edge can process relational data, nonrelational JSON data, and graph and time-series data. It also includes

a local data streaming engine and unique machine learning capabilities for capturing and processing real-time data streams.

SQL Edge will most likely interest customers with point-of-sale systems and smart scanners that need to run some local data processing, edge gateways that gather data from multiple devices and process and aggregate the data, or edge servers that support complex devices like robotic equipment that need to perform sophisticated analysis locally to detect anomalies in equipment performance and take corrective action. It is a more capable solution than SQL Server Express and SQL Server Compact because it includes most of the SQL Server Enterprise Edition security and performance, and it has additional machine learning and data streaming capabilities. It also helps address device memory constraints that prevent deploying the full SQL Server product on such devices since it requires less than 500MB.

SQL Edge can be deployed in two modes:

- Connected deployment uses an IoT Edge module (a local deployment of Azure IoT services and software), where SQL Edge can receive data from other IoT Edge modules and store data locally on the edge server or in Azure-hosted databases

- Disconnected deployment is for local installation on a customer's device (without IoT Edge), where customers can deploy SQL Edge container images as stand-alone containers or on a Kubernetes cluster.

SQL Edge pricing is per device, and it is available in developer and production editions.

Resources

The SQL Server roadmap is discussed in the *On-Premises Software Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/sql-server>.

Azure SQL Database is discussed in the *Azure Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/azure-sql-database>.

Azure SQL Managed Instance is discussed in the *Azure Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/sql-managed-instance>.

Azure Synapse Analytics is discussed in the *Azure Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/synapse-analytics>.

Azure Arc enabled database services are discussed in "Azure Arc Data Services On-Premises Explained" on page 32 of the Jan. 2021 *Update*.

Azure SQL Edge is discussed in the *Azure Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/sql-edge>.

Licensing SQL Server is covered in the *Licensing Reference Set* at <https://www.directionsonmicrosoft.com/licensing/sql-server>.

Analysis Services options are compared in “Comparing SQL Server Analysis Services

Offerings” on page 26 of the Nov. 2020 *Update*.

Reporting Services options are discussed in “SQL Server, Power BI On-Premises Reporting Roadmap” on page 19 of the Sept.

2020 *Update*.

Integration Services options are discussed in “Comparing Data Integration and Transformation Offerings” on page 3 of the Feb. 2020 *Update*. 

Cognitive Services Simplifies Machine Learning Deployments

By Andrew Snodgrass

- Azure Cognitive Services can speed development and deployment of applications that need artificial intelligence analysis.
- Prebuilt machine learning models for common business needs reduce creating, testing, and training requirements.
- Local deployment options provide isolation, tighter security, and faster response times.
- Limited customization means complex workloads may be better handled by other Azure services.

Azure Cognitive Services is a collection of machine learning services that allow developers to add artificial intelligence (AI) to bots and other applications, with reduced upfront cost and expertise. They are less expensive to deploy and scale than comparable machine learning environments built separately.

Overview

Cognitive Services machine learning services include complete models for a range of common business needs, such as image analysis, search and indexing, and anomaly detection. The services are designed to be incorporated into custom applications and processes by developers, rather than being called independently by end users. They are built using Microsoft's internal machine learning expertise and data stores, which help provide advanced services that are beyond what most organizations can create on their own, including language translation (for over 90 languages) and speech-to-text conversion.

However, the services limit customizations and they are less flexible than other Microsoft offerings, such as Azure Machine Learning, SQL Server Machine Learning Services, and ML.NET, an open-source library of machine learning algorithms. Consequently, customers with unique requirements, such as complex anomaly detection or business-specific machine learning needs, may find Cognitive Services too restrictive. (See the sidebar “Alternatives to Cognitive Services” on page 27.)

The services will most likely appeal to customers in the following scenarios:

- Workloads that closely match the task supported by a specific service (such as

anomaly detection) with minimal customization

- Organizations with limited machine learning skills that want to include advanced analytics in their applications
- Developers wanting to include advanced language, speech, and search in their applications with minimal effort
- Data specialists performing proof of concept on machine learning processes.

Some of the services like language translation are fully trained, while others like facial recognition will require upfront effort to gather and cleanse training data. Additionally, using services that process personally identifiable and sensitive data will require new data governance policies and procedures.

Service Categories

Cognitive Services offerings are referred to as APIs and are grouped by Microsoft's documentation into the following categories. (Overlaps exist between the groups, so developers should review all the services and capabilities to ensure they are choosing the fewest services and most complete set of features.)

Vision services can recognize objects in images and assign custom classifications, identify people's faces and emotions, process video content by creating an index of transitions and images, and extract table data from forms. For example, they can evaluate a PDF file to detect tables and cells and then output the results to a JSON document with coordinates and details for further processing. The APIs in Vision include Computer Vision, Custom Vision Service, Face, Form Recognizer, and Video Indexer. Most of them require training with customer-supplied data.

Speech services can convert speech to text and vice versa, perform advanced speech recognition (such as on samples with high background noise), build transcriptions of conversations, and identify people by their voice signature. For example, voice recognition features can be incorporated into medical applications to provide hands-free authentication. The only API in this category is Speech service, which requires customer data training for voice recognition features.

Language services can analyze text conversation to predict meaning and extract relevant data, support chatbots to recognize questions and find responses in local knowledge bases, perform real-time translations on more than 90 languages, and determine the topics and sentiment of text. Language services also support natural language interfaces that let users submit queries (in text or speech) that are converted to complete queries. Additionally, the service now includes an immersive reading feature to help new readers and individuals with reading difficulties. For example, organizations can use the immersive reading API to provide a more accessible method for sharing the contents of their Web site with users. The APIs in this category include Language Understanding (LUIS), QnA Maker, Text Analytics, Translator, and Immersive Reader. Some of the features, such as QnA Maker, require first indexing knowledge bases and then training and tuning the service on correct responses.

Decision services can monitor and detect anomalies in time series data, provide customized anomaly detection on multi-variate time series data, moderate content for potentially offensive or undesirable content, and provide personalized user experiences

Alternatives to Cognitive Services

Cognitive Services does not encapsulate all of Microsoft's machine learning-related offerings, just those provided by a particular group within Microsoft. Other Microsoft machine learning options that developers use generally fall into two major categories:

Full-featured offerings, such as Azure Machine Learning, Databricks, HDInsight, SQL Server, and ML.NET support machine learning capabilities for professional data engineers and scientists. They use a variety of machine learning languages like Python, Spark, and R to enable development of sophisticated machine learning models and scripts to address any requirement, whether simple or complex. As such, they generally require more effort to deploy and use than Cognitive Services but can enable more targeted solutions.

Self-service offerings, such as Power BI, AI Builder, and Excel, provide machine learning abilities for professional and nonprofessional users. They include basic predefined models (similar to some in Cognitive Services) that users can modify and customize to meet their needs and train with their own data. The models typically run within the product in which they were created, but some can export or publish their models to other Microsoft offerings to be part of a larger application.

Another service called Cognitive Search (not part of Cognitive Services) is a cloud-based, full-text search service for application developers to call from within their applications. The service is designed for indexing and searching customer-supplied content, such as knowledge bases and internal documentation. Cognitive Search can call Cognitive Services offerings, such as calling image and text analysis, to extend its functionality. ▶

based on real-time behavior. For example, the anomaly features can be trained with customer-supplied historical equipment data to create boundaries of acceptable results and set to receive and evaluate an ongoing stream of equipment data to monitor for abnormalities. The APIs in this service include Anomaly Detector, Content Moderator, Metrics Advisor, and Personalizer. Most of the features require cleansed customer data for training.

Search services are based on numerous Bing Search capabilities that can access Bing's search engine, suggest related search terms, perform precise news, image, and video searches, and use Bing statistics to analyze query usage for performance tuning. For example, a custom sales app can use the Bing local business search API to help find potential customers. This service uses the numerous Bing Search APIs, including news, spell check, video, Web, autosuggest, entity, image, and visual.

Development Options

Developers incorporate the services in their applications and processes through various methods:

REST APIs and client libraries provide programmatic access to all services and the most capabilities.

Connectors to Azure data services (called Cognitive Services for Big Data) allow de-

velopers using Azure Synapse Analytics and Databricks to send streaming data to certain Cognitive Services offerings for real-time processing. The Cognitive Services offerings supported include Computer Vision, Face, Speech, Anomaly Detector, Text Analytics, and Bing Image Search.

Direct integration with select Azure services enables use of Cognitive Services features on data being processed by those services. Supported Azure offerings include Azure Functions, App Service Web Jobs, Azure Logic Apps, Power Automate, and AI Builder.

Deployment Options

Deployment options include connecting to Cognitive Services in Azure, but also support running some services locally on customer-supplied hardware in a disconnected or occasionally connected mode. Running locally can help improve security, reduce latency, or simplify regulatory compliance. The advantages can be critical in, for example, equipment operation solutions that could result in costly downtime if not addressed in near real time. Customers also have control over when local services are updated, ensuring changes are only applied once they have been tested and validated.

Local deployment is available in two configurations:

Docker container images allow organiza-

tions to deploy select services using Azure Kubernetes Service, Azure Container Instances, and Kubernetes deployed to Azure Stack. Local deployments are mostly disconnected, but they must be configured to allow periodic connection to Azure for billing purposes.

Azure IoT Edge includes a module for Cognitive Services that supports running select services with other deployed IoT Edge modules. IoT Edge is a collection of runtime modules that enables certain Azure functionality to run locally on or near IoT devices.

Services available for local deployment include anomaly detection, language understanding (LUIS), and text analytic features, such as speech-to-text and text-to-speech, sentiment analysis, and phrase extraction. A preview of local deployment for vision services and some additional speech capabilities is also available.

Roadmap

Cognitive Services receives frequent updates to the individual services and occasionally introduces new services, although many offerings remain in preview for extended time periods. Key plans include the following:

- New services will include gesture-based control APIs, which can help developers add hand-gesture input processing to applications, and event tracking APIs, which can return events associated with Wikipedia entries

- Azure Percept is a hardware-software platform for devices such as security cameras that will use Cognitive Services and other Azure services for local vision and audio analysis

- Speech Services will eventually replace the earlier Bing Speech service; however, Bing Speech retirement has been delayed to Nov. 1, 2021 (from Jan. 14, 2020).

Pricing and Resources

Pricing plans vary substantially by API and are based on number of transactions, instances, hours, images, documents, or characters. For example, certain image recognition APIs cost US\$1 per 1,000 transactions for the first 1 million per month, and the rate decreases in steps to a minimum of US\$0.65 per 1,000 transactions for usage above 5 million per month. Most services provide a monthly free usage allowance, and some of the APIs are in preview with reduced price rates in effect.

Microsoft AI updates are discussed in "Artificial Intelligence Offerings Receive Updates" on page 11 of the Apr. 2019 *Update*. ▶

Azure IoT Services

By Barry Briggs

- Connecting industrial devices to the cloud in IoT systems can yield significant benefits such as analytics, supply chain optimization, and predictive maintenance.
- Azure can ingest, store, and analyze device data at massive scale to enable applications that are difficult or impossible on-premises.
- A complete IoT solution may involve connecting many Azure services that add to the cost.

Azure provides a comprehensive, and occasionally overlapping, set of services supporting commercial Internet of Things (IoT) deployments. By leveraging massively scalable services such as Azure networking and storage, analytics, and business intelligence, IT and operational technology (OT) professionals can create end-to-end applications providing near-real-time visibility and control of IoT devices, as well as analytics-based applications for tasks such as predictive maintenance. Many of the Azure services can be deployed

either in the public cloud or at the edge (on-premises or on-site) depending on latency, connectivity, and compliance requirements. However, use of these services may add to the overall cost of an IoT solution.

Connected IoT Devices Unlock New Value but Come with Challenges

Organizations increasingly find value in connecting devices, such as programmable logic controllers (PLCs), sensors, manufacturing devices, and medical equipment to cloud services such as analytics, visual-

ization, and machine learning. (In manufacturing applications, this digitization is often termed “Industry 4.0.”) Azure’s native abilities to scale and ingest huge amounts of data from external sources benefit IoT scenarios, including predictive maintenance, forecasting, supply chain visibility and optimization, and many others.

However, a number of challenges exist, including the variation of computing capability on these devices, especially limited on legacy devices; the event-driven and real-time nature of IoT; as well as security

Understanding Azure IoT Hub and Azure Event Hubs

Azure IoT Hub contains an instance of Azure Event Hubs. Both receive events from external software and devices at scale. Sharing a common underlying architecture, both support partitions, which enable incoming messages to flow to different locations, thus reducing or preventing contention. Both can support ingestion, or receive rates, in the millions of messages per second. Unsupported protocols, such as Constrained Application Protocol (CoAP), can be connected through third-party add-ons.

However, there are important differences. Azure IoT Hub specifically targets IoT scenarios, so it includes features for device provisioning and per-device security (and smaller message sizes). IoT Hub (in its Standard tier) supports bidirectional (device to cloud and cloud to device) communications. Event Hubs, which is receive-only, by contrast focuses on general-purpose event processing—such as receiving data from external applications like business-to-business data—and does not natively support Message Queueing Telemetry Transport (MQTT), a common IoT protocol. Event Hubs may be the better option for scenarios such as queuing messages between local systems or across data centers.

Feature	Azure IoT Hub	Azure Event Hubs
Receive events and data from devices at scale	✓	✓
Partition support	✓	✓
Bidirectional (events and commands) communication with devices	✓	○
Device identity and provisioning	✓	○
Device-level security	✓	○
Maximum message size	Receive: 256k Send: 64kb	Receive: 1MB
HTTP(S) protocol support	✓	✓
AMQP protocol support	✓	✓
MQTT protocol support	✓	○
Kafka event streaming	○	✓
Pricing	Tiers and # messages	Tiers/events or Capacity units

and the need to scale to perhaps millions of devices. Additionally, unlike the public Internet and Web, which have largely standardized on HTTP, IoT devices and gateways may use one of a number of other protocols including the Advanced Message Queueing Protocol (AMQP), Message Queueing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and others.

Azure IoT Services Overview

Azure provides a number of services designed for industrial and commercial IoT computing scenarios and targeting the challenges noted above. These services can enable sophisticated deployments; however, they are evolving, which introduces the risk of change, and they overlap in places, which means customers should develop an understanding of the differences before deploying services.

For an illustration that shows how various services interact implementing an IoT deployment, see “Azure IoT Solution Architecture” on page 30. This report focuses on the Azure services in the illustration that specifically support IoT.

Connecting to Devices Using PaaS: IoT Hub

Azure IoT Hub is Microsoft’s Platform as a Service (PaaS) solution for connecting devices to Azure. IoT Hub supports bidirectional communications with devices—receiving events and sending commands and updates—as well as several IoT protocols, such as MQTT and AMQP. (See the sidebar “IoT Protocols” on this page.) IoT Hub is used as the interface between devices and other Azure services and helps developers address the challenges of protocol diversity, security, and high message ingestion (receive) rates.

Incoming messages can be routed to customer apps and/or any of a number of Azure services. For customer applications, IoT Hub also supports Client Service SDKs enabling applications to interact with IoT devices for several programming languages, including C#, C, Java, and JavaScript via [Node.js](#). Incoming IoT messages can be routed to these applications, which can then perform actions such as sending a response or a command to another IoT device (for example, turning on climate control in response to a temperature change). Alternatively, or in addition, messages can be directed to Azure Stream Analytics for near-real-time analytics (such as monitoring device behavior within a time window) and/or to Azure Cosmos DB or Azure Storage for later analysis by Azure Machine Learning or other services.

Each IoT Hub instance includes a built-in instance of the Azure Event Hubs service. Event Hubs by itself can be used for receiving IoT data; however, Event Hubs cannot send messages to devices, and there are other differences. (See the chart “Understanding Azure IoT Hub and Azure Event Hubs” on page 28.)

IoT Hub maintains device metadata and status in documents called “device twins” (not to be confused with a “digital twin” discussed later). Developers can query these documents using SQL-like syntax. It also supports message routing based on both metadata (for example, device ID) and/or message contents; for example, if a sensor registers a temperature higher than 50 degrees, the message can be forwarded to an application or another endpoint.

Azure IoT Hub Device Provisioning, described by Microsoft as a “helper service” for IoT Hub, enables operators to quickly provision certain IoT devices at scale. Provisioning gathers and adds device information such as manufacturer, model, and device ID to IoT Hub, creating a device twin. In addition, device provisioning involves creating the security environment for the device, using either symmetric or X.509 PKI keys for secure communications. Device Provisioning depends on the manufacturer having

preconfigured the device to support it. A related service, Azure IoT OPC Twin, enables automated discovery of devices conforming to the OPC UA standard, a standard for process control systems. (A reference implementation for the connected factory scenario can be found at <https://www.azure-itsolutions.com/Accelerators#description/connected-factory>.) Device twins can also be created programmatically (for example, via PowerShell).

Connecting to Devices Using SaaS: IoT Central

Azure IoT Central is an Azure Software as a Service (SaaS) solution that enables operators and administrators to connect devices, create rule-based IoT applications, and monitor the operation of the IoT ecosystem. IoT Central can be white labeled for customer applications. IoT Central can connect directly to devices or to intermediaries such as gateways or edge devices.

IoT Central uses IoT Hub services internally, including the Device Provisioning Service. Rule-based apps can trigger various actions in response to device events, such as sending an e-mail or triggering a Power Automate flow. IoT Central provides built-in dashboards for IoT activity; and templated solutions for IoT Central are available sup-

IoT Protocols

Industrial devices commonly use one of a variety of networking architectures and protocols to communicate with on-premises or on-site controllers, or the cloud. Some of the more common protocols include the following:

Message Queueing Telemetry Transport (MQTT), originally developed by IBM, is a lightweight publish and subscribe transport. Senders publish to a “topic” in “namespace” and consumers pick messages off the topic queue. MQTT is designed for short messages such as device telemetry and does not support higher-order concepts like transactions. MQTT can be secured with Transport Level Security (TLS).

Advanced Message Queueing Protocol (AMQP) targets message-oriented middleware but is also used in IoT applications. AMQP, which also implements a publish-and-subscribe architecture, requires a larger on-device footprint and possesses a chattier wire protocol than MQTT, but comes with additional features commonly found in enterprise-class messaging such as transactions, delivery options (at-least-once, at-most-once, exactly-once), and message rejection, among others.

Constrained Application Protocol (CoAP) targets highly constrained devices and layers on top of the User Datagram Protocol (UDP), not TCP. It does not implement a publish-and-subscribe model but rather a client-server architecture; messages can either be acknowledged by the receiver or be “fire and forget.”

HTTP or HTTPS is the most common Web protocol based on TCP/IP. HTTP and HTTPS are half-duplex, connectionless protocols, meaning that protocols that do support connections, such as MQTT, can be faster.

WebSockets is a full-duplex implementation on TCP. MQTT and AMQP can also be used over WebSockets.

The OPC Foundation provides a set of reference architectures, standards, data models, and protocols for the industrial IoT and SCADA communities. ➤

porting a number of vertical industries including logistics, in-store analytics, inventory management, and video analytics on the Azure IoT Accelerators site. Solution developers can customize dashboards in IoT Central and can create custom industry templates and templates for new devices.

Other Azure IoT Services

Azure IoT Protocol Gateway is a software framework for either customizing supported protocols such as MQTT or for creating

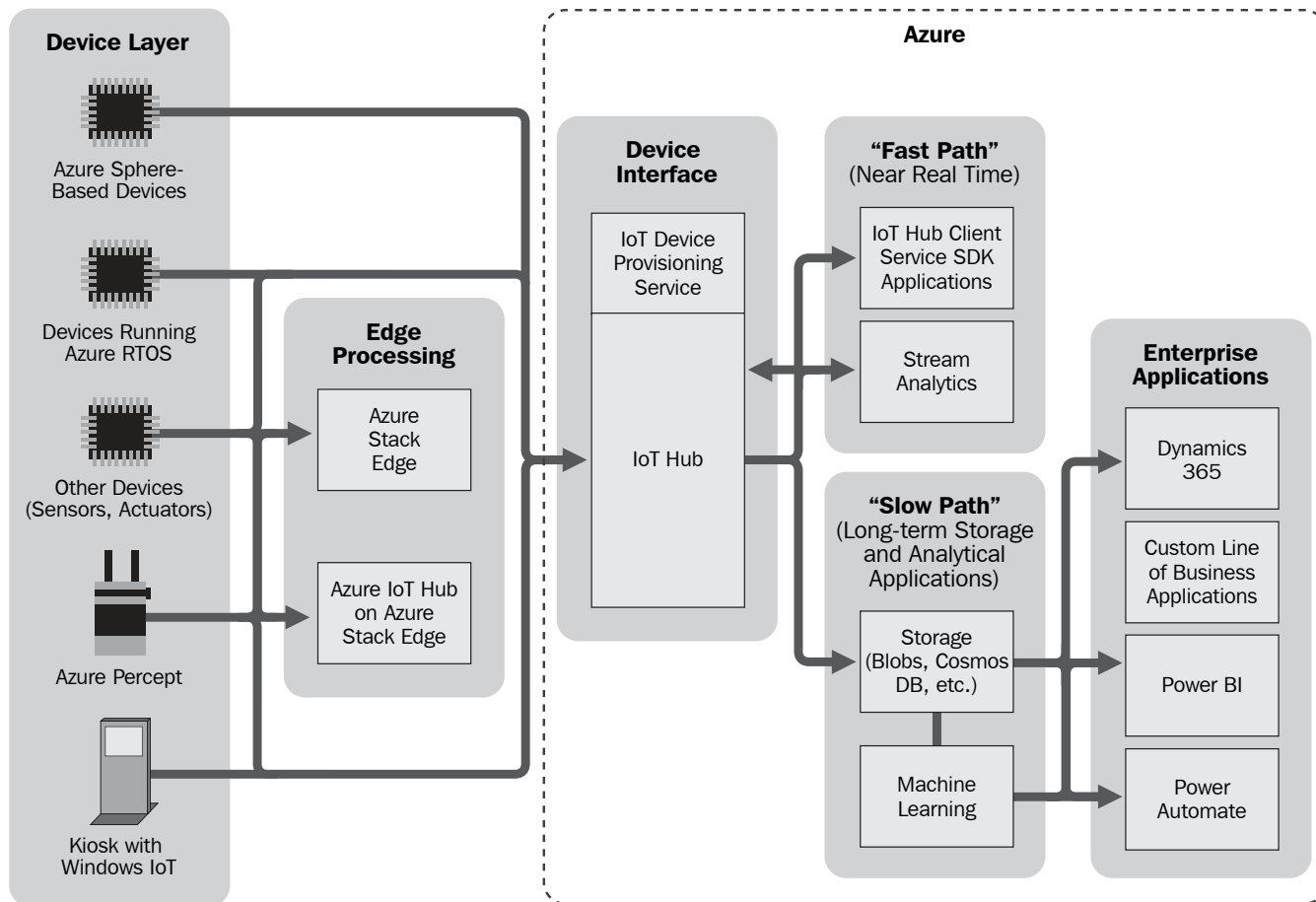
adapters for protocols not natively supported by IoT Hub, such as CoAP or legacy protocols. The protocol gateway can run as a microservice in Azure Service Fabric or in an Azure VM.

Azure Defender for IoT, available as an option for IoT Hub, provides a lightweight agent for capable IoT devices and device inventory, as well as agentless network monitoring to detect anomalous behavior. (For more detail, see “Azure Defender Can Secure a Range of Azure Services” on page 16.)

Azure Digital Twins is an Azure service that enables customers to model and simulate complex IoT environments, such as factories with hundreds of individual interconnected devices. Azure Digital Twins can receive real-time data from real devices via IoT Hub while permitting users to perform what-if simulations. Developers create models of IoT environments using the JSON-based Digital Twin Definition Language (DTDL).

Azure Time Series Insights aims to simplify

Azure IoT Solution Architecture



A full-featured IoT deployment consists of many layers that connect devices (left) to Azure cloud services, not all of which are shown in this diagram. In this scenario, the wide range of IoT device types, from simple sensors to full PC-based devices (for example, kiosks), are shown at left. Messages are transmitted from the devices on one of a variety of protocols, including HTTP, MQTT, AMQP, and others. (See the sidebar “IoT Protocols” on page 29.) Optionally, organizations may deploy Azure services at the “edge,” that is, in locations near the devices, to satisfy demanding latency, connectivity, or security requirements.

The architecture centers on Azure IoT Hub, which receives from and sends messages to devices, as well as providing device identity and security. The Device Provisioning Service sets up devices to communicate with IoT Hub and provides firmware and software updates.

IoT Hub routes data between devices and applications via a “fast path” (top) or a “slow path” (bottom).

Fast-path scenarios require near-real-time functionality. For these, developers can write applications using the Client Service SDK that receive messages from devices and immediately send a response. Alternatively, messages can be directed to Azure Stream Analytics for near-real-time processing.

In slow-path scenarios, IoT Hub forwards messages to various Azure storage and analytical services. Messages can be stored in high-volume storage such as Azure Blob Storage, HDInsight, or Cosmos DB; other services such as Azure Machine Learning and Power BI can then perform analysis.

analyzing event streams such as those arriving from IoT devices or applications. The service provides a dashboard of visualization tools (such as filtering and sorting controls, line charts, and heat maps) for exploring the data in near real time as it arrives.

Many other Azure services, such as Cosmos DB, Power BI, and Machine Learning, can be leveraged for increased insight and control over the IoT deployment; however, use of them will add cost.

Azure IoT Edge Services

In many cases, IoT services must be located close to the devices they manage. For example, manufacturing or medical devices may require the predictable latency not available from the public Internet. In other scenarios, devices must continue to run even if connection to the public cloud is lost. Finally, in some cases security or compliance requirements mandate infrequent or no connection to the cloud. Microsoft offers a range of solutions for processing IoT data at the edge, that is, on-premises or on-site:

Azure IoT Hub on Azure Stack Hub (in preview) provides the full capabilities of IoT Hub on-premises for scenarios where processing must remain local.

Azure Stack Edge is a cloud-managed appliance (available as 1U rack-mountable or in portable, ruggedized versions) supporting edge operations such as local compute and storage. The devices are equipped with GPUs to accelerate machine learning inferencing.

Azure IoT Edge, which is open source, runs on customer hardware or devices and

supports certain Azure services such as Stream Analytics, Functions, and Machine Learning running in containers as well as customer applications on-premises.

Azure IoT Devices and Software

In addition, Microsoft offers the following products to run on IoT devices:

Azure Sphere, a reference design for a secure, Azure-connected microcontroller unit (MCU). Microsoft has a number of hardware partners building Sphere-based MCUs.

Azure RTOS, a real-time OS featuring Azure connectivity for resource-constrained IoT devices.

Azure Percept, a first-party hardware and software platform for building and deploying artificial intelligence (AI) solutions at the edge.

Windows offers editions targeting IoT devices, including Windows 10 IoT Core, for constrained devices such as Raspberry PI; Windows 10 IoT Enterprise, targeting interactive devices such as kiosks; and Windows Server IoT 2019 available to OEMs and intended for fixed-purpose IoT deployments. It is expected that Windows 10 IoT Core and Windows 10 IoT Enterprise will be merged in 2021.

Recommendations

Industrial and commercial IoT environments can be complex, and topologies and configurations vary widely. Customers should carefully consider if their applications require processing at the edge, for reasons listed above. The need for custom code or legacy device support may be reasons to favor the PaaS-model IoT Hub over

IoT Central; alternatively, the desire for a managed SaaS service might suggest IoT Central as a choice.

Availability and Resources

Pricing an IoT system on Azure will be complex because each service has its own pricing model. For example, IoT Hub is priced by tier. The Basic tier supports a limited set of features (for example, Basic does not support cloud to device messaging) and is further broken down by throughput (that is, by the number of messages per day). The Standard tier supports all features and like the Basic tier is further broken down by throughput. A free tier, intended for evaluation and development, supports all features but only supports a small number of messages per day.

IoT Central is priced by tier and by the number of devices connected. The lowest tier is intended for devices sending a few messages per day; the highest, a message every few minutes.

The IoT Hub Device Provisioning Service costs US\$0.10 per 1,000 operations.

IoT Hub, IoT Central, and other IoT services (except for Azure IoT Hub on Azure Stack Hub, which is in preview) are generally available.

The roadmap for Azure IoT is discussed in the *Azure Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/iot-services-and-software>.

Azure IoT Hub documentation is at <https://docs.microsoft.com/azure/iot-hub>.

Azure IoT Central documentation is at <https://docs.microsoft.com/azure/iot-central>. 

In Brief **Previews of Java Distributions Available**

A preview of the Microsoft Build of OpenJDK became available in Apr. 2021. The offering shows Microsoft's commitment to the Java programming language, which could reduce risk for organizations moving Java-based solutions to Azure and developers adopting Microsoft tools for Java software projects. OpenJDK is an open source software implementation of the Java platform, including development and runtime components. The preview, which is based on

Java 11 (a Long-Term-Support release), is supported on servers and clients on Windows, Linux, and macOS OSs. A refresh of Microsoft's Early Access release of OpenJDK for Windows ARM devices (such as the Surface Pro X), which is based on Java 16, also became available in Apr. 2021. The Microsoft Build of OpenJDK is available at <https://www.microsoft.com/openjdk>, and it is also supported in the Azure Cloud Shell, which is accessible in the Azure portal.

Nuance Communications Acquired by Microsoft

Nuance Communications, a provider of speech recognition software, has agreed to be acquired by Microsoft. Nuance pioneered Interactive Voice Response (IVR) and other speech technologies and supplied Apple's original implementation of its Siri virtual assistant. Today it focuses on the application of speech in vertical industries, most notably healthcare. Nuance's technologies, which are widely used for exam room and radiology reporting, will likely first be integrated into Microsoft's Cloud for Healthcare, one of several "industry clouds" announced

in February, and subsequently in other Azure, Dynamics, and Teams services and vertical solutions. This acquisition, once concluded, will be the second largest in Microsoft history (after LinkedIn). Nuance will report into Microsoft's Cloud & AI group. Microsoft's press release is at <https://news.microsoft.com/2021/04/12/microsoft-accelerates-industry-cloud-strategy-for-healthcare-with-the-acquisition-of-nuance>; Nuance Communications is at <https://www.nuance.com>.

DAPR Can Simplify Creation and Management of Microservices

Microsoft's Distributed Applications Runtime (DAPR) can simplify creation of microservice-based cloud applications. Microservices are typically small portions of functionality that can work together to comprise an application or service. DAPR provides a combination of developer-focused capabilities and common interfaces to other cloud services that could make microservice-based applications more secure, more resilient, and faster to build, deploy, and monitor. Like the popular open-source service mesh Istio, DAPR runs as a "sidecar," meaning it operates alongside the microservice, and can be hosted with Kubernetes pods

or VM-based applications. DAPR exposes a programming model and a set of distributed building blocks that make it easier to invoke and interface with other services, manage secrets using key vaults, and enable other capabilities beyond the networking services that are typically provided by a basic service mesh offering. DAPR supports a variety of programming languages, is portable across Windows, Linux, and MacOS, and is free of charge and open source, but relies on the open-source community for support and updates. DAPR's home page is at <https://dapr.io>. Istio's home page is located at <https://istio.io>.

Azure Synapse Pathway Simplifies Data Warehouse Migration

Azure Synapse Pathway (in preview) is data warehouse migration software that helps automate the conversion of data warehouses (on-premises and hosted) to Azure Synapse Analytics. Synapse Analytics is a multipurpose analytics and data warehouse service designed for organizations with SQL Server T-SQL and Apache Spark expertise. The Synapse Pathway software will interest customers with older data warehouses needing assistance in migrating to Synapse Analytics. Synapse Pathway includes assessment and conversion features to determine a source data warehouse's suitability for Synapse Analytics and convert the database, schema, and tables by creat-

ing scripts that run in Synapse Analytics. Plans call for automated assessment and conversion of database views, procedures, and functions to Synapse Analytics T-SQL, which is often a manual effort that takes considerably longer than the migration of data. Pathway currently supports IBM Netezza, Snowflake, and SQL Server, with plans for Google's BigQuery, Hive-based Hadoop solutions, Redshift, and Teradata in the future. Pathway does not create the destination data warehouse, nor does it transfer the data. Additional details are discussed in the *Azure Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/synapse-analytics>. 

Licensing & Support

Licensing Microsoft Defender for Endpoint on Servers

By Wes Miller

- Microsoft Defender for Endpoint offers endpoint security for servers, with potential savings for existing Microsoft 365 E5 customers.
- Organizations will need to compare costs over time, as one licensing avenue is more flexible but far more expensive.
- Licensing rights for Microsoft Defender for Endpoint on Linux-based servers are not as liberal as for Windows Server.

Microsoft Defender for Endpoint (server) offers endpoint detection and response (EDR) to identify and help remediate malware attacks on servers running Windows Server or Linux. Organizations looking to license Microsoft Defender for Endpoint on Windows Server face complicated licensing options, with dramatically different costs, and varying flexibility depending on which license option is chosen. Only one licensing option is available for Linux servers.

Server Licensing Options for Microsoft Defender for Endpoint

Microsoft Defender for Endpoint (server) is licensed Per-OSE (operating system envi-

ronment), where the OS is running in a VM or on a physical server. Unlike Windows Server, licensing a physical server with Microsoft Defender for Endpoint (server) confers no rights to run the Microsoft Defender for Endpoint (server) within VMs on that server; instead, each VM must be licensed individually and in addition to the license for the physical server.

Two options are available for organizations to license Microsoft Defender for Endpoint (server) for Windows Server VMs and physical servers.

- A stand-alone Microsoft Defender for Endpoint (server) license
- Azure Defender for Servers hosted service, which includes a license for Microsoft

Defender for Endpoint (server) along with other benefits.

Although the Microsoft Defender for Endpoint features and capabilities are identical regardless of which option is chosen to license Windows Server either physical or virtual, the prerequisites and costs are very different.

Microsoft Defender for Endpoint (Server)

The stand-alone license for Microsoft Defender for Endpoint (server) is available under the following terms:

Licensing prerequisites specify that an organization must already have 50 users licensed for Windows Enterprise E5/A5, or

a Microsoft 365 suite containing it.

Applicable licensing agreements include an Enterprise Agreement (EA), Enrollment for Education Solutions (EES), or a Microsoft Customer Agreement (MCA).

Licensing rights include the right to run Microsoft Defender for Endpoint (server) on one OSE instance of Windows Server or a Linux server running on-premises, in Azure, or in a third-party cloud as permitted under the licensing terms. (The current licensing terms do not forbid or otherwise limit the use of the Microsoft Defender for Endpoint (server) software in any third-party cloud.)

License duration is defined by the terms of the agreement the service is licensed under.

Cost for the stand-alone license is US\$5.02/month as of Apr. 2021 using EA Level A pricing.

Licensed OSs include Windows Server and Linux server, and Windows 10 Enterprise multisession running in the Windows Virtual Desktop (WVD) service.

This stand-alone license is currently the only option for licensing Linux servers.

Azure Defender for Servers

When Microsoft Defender for Endpoint (server) is licensed using Azure Defender for Servers, the following terms apply:

Licensing prerequisites do not apply; unlike the stand-alone licensing, no prior licensing of users for Windows Enterprise E5/A5 is required.

Applicable licensing programs include all programs that Azure can be purchased under, which includes all programs listed above, plus the pay-as-you-go Microsoft Online Services Program (MOSP).

Licensing rights include the right to run Microsoft Defender for Endpoint (server) on one OSE instance of Windows Server running on-premises, in Azure, or in a third-party cloud as permitted under the licensing terms. (As noted earlier, current licensing terms do not forbid or otherwise limit the use of the software in any third-party cloud. Note that Azure Defender for Servers licensing currently specifically excludes rights to run the software on Linux systems.)

License duration is more flexible than the stand-alone license, as organizations can onboard/offboard servers under the Azure Defender for Servers service as required, paying only for running instances of the service.

Cost for the stand-alone license is US\$14.60 per month (US\$0.02/hour) using U.S. Azure MOSP pricing as of Apr. 2021.

Licensed OSs include Windows Server and Windows 10 Enterprise multisession running in the WVD service.

Which Licensing Avenue to Choose

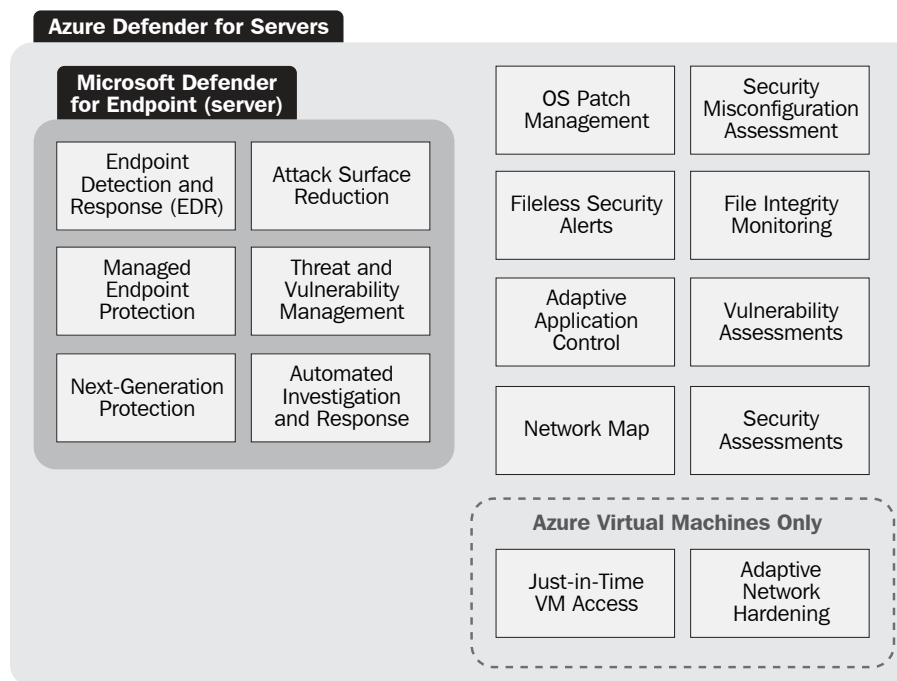
Licensing servers for Microsoft Defender for Endpoint using Azure Defender for Servers is significantly more expensive than licensing the stand-alone Microsoft Defender for Endpoint (server) software. However, it might make sense for customers who:

- Have not, and do not plan to, license Windows Enterprise E5 or Microsoft 365 E5-level security services that include it
- Do not need to license Linux servers
- Have VMs and servers that will benefit from the additional capabilities included with the Azure Defender for Servers service, particularly including OS patching, and vulnerability and security assessments.

Customers need to understand the additional features included in Azure Defender for Servers in order to decide which option to choose. (For a snapshot of the benefits included with Azure Defender for Servers, see the illustration “Comparing Microsoft Defender for Endpoint Server Licensing Options” on this page. For additional details, see the chart “Azure Defender for Servers Features” on page 18.)

Customers can use both licensing options concurrently, which may make sense when the Windows E5 licensing prerequisites have already been met and the additional Azure Defender for Servers capabilities

Comparing Microsoft Defender for Endpoint Server Licensing Options



Organizations have two choices to license Microsoft Defender for Endpoint (server) for Windows Server. A freestanding license is available, but only for organizations with at least 50 users licensed for Windows 10 Enterprise E5 or a suite that includes it.

Azure Defender for Servers includes all of the same Microsoft Defender for Endpoint (server) capabilities, but also adds several features designed for use in Azure VMs, on-premises VMs or servers, and VMs in third-party clouds. Two capabilities are exclusively available for use in Azure VMs.

ties are not needed for some VMs or hosts but are needed for others.

Regardless of which option is chosen, data from the servers can be configured to be viewable in the Azure Security Center portal or the Microsoft 365 security center.

Customers who acquire stand-alone Microsoft Defender for Endpoint (server) licenses and later choose to cover the same servers with Azure Defender will be eligible

for a credit toward Azure Defender. (These terms are not defined, but the offer is noted in the Microsoft Product Terms documentation as of Apr. 2021.)

Resources

Azure Defender for Servers documentation is at <https://azure.microsoft.com/services/azure-defender>.

Azure Defender pricing information is at

<https://azure.microsoft.com/pricing/details/azure-defender>.

Azure Defender for Servers capabilities are described in “Azure Defender Can Secure a Range of Azure Services” on page 16.

Microsoft Defender for Endpoint capabilities are described in “Microsoft Defender for Endpoint Platform Support” on page 13. ▶

Power BI Premium Introduces Per-User Licensing

By Andrew Snodgrass

- A new Power BI license will help groups that need premium Power BI reporting on a small scale.
- It provides most of the features offered in Premium capacity subscriptions, but at a lower-cost entry point.
- Sharing content could force licensing more users than planned.

POWER BI PREMIUM PER-USER (PPU) is a new licensing option that will most likely interest small groups or departments that need Premium features but do not have the budget or number of users to justify the more expensive Premium-capacity license. However, customers should evaluate PPU cautiously, as it can result in the need to increase licensing for all users who interact with PPU hosted content.

Premium Overview

Power BI includes software and cloud services that provide data management, data analysis, and reporting. Power BI offers multiple back-end hosting platforms that enable publishing and distribution of shared datasets and reports, processing data to produce (render) reports, managing user access, and delivering reports through clients. (See the illustration “A Licensing Overview of Power BI Back-End Platforms” on page 35.)

Power BI Premium is the most capable of the Power BI back-end hosting platform, designed for enterprises with thousands of users. It offers exclusive features, such as paginated SQL Server reports, Analysis Services Tabular data models, and high-end security. The original Premium P offering starts at US\$4,995 per month, which can be a hindrance for many organizations and departments that need the advanced features of Premium but have a small number of users.

Premium Per-User Lowers Entry Point

PPU, available for US\$20 per user per month, offers a lower entry point for access to Premium features. It will most likely interest organizations, departments, or small groups in the following scenarios:

- Departments that typically use paginated reports, such as finance groups
- Enterprises new to Power BI that plan to expand its use
- IT departments evaluating Premium features
- International offices that need content (reports and data) stored locally for data residency requirements.

PPU features and licensing are applied at the Power BI

workspace, which is a secure area for sharing content in Power BI. Once an administrator applies the PPU status to a workspace, only PPU licensed users can access reports, data, and other content in the workspace.

PPU workspaces have most of the features available in a full-size Premium-capacity environment with some notable exceptions, such as large data model sizes, customer control of encryption keys, global distribution of reports, and rights to Power BI Report Server on-premises. PPU also limits the use of the Export API and does not provide the same level of administrative controls as Premium-capacity environments.

Sharing Content Impacts Licensing

Customers can have a mix of PPU, Power BI Pro, and Premium-capacity environments, but there are limitations on sharing content between users of those environments. PPU users may access content hosted in Power BI Pro and Premium-capacity deployments, but only users licensed with PPU may access content hosted in a PPU workspace.

There are no technical controls that prevent an author from building a report using PPU-hosted data and publishing that report to a Power BI Pro or Premium environment. However, there are licensing controls to enforce Microsoft’s multiplexing (indirect access) rules that block users without a PPU subscription from opening the report. For example, a financial report that uses data from a dataset hosted in a PPU workspace requires everyone who accesses the report to have a PPU subscription license, even if the report itself is hosted in a Power BI Pro workspace.

This licensing requirement follows the lineage of PPU hosted content, regardless of how many levels the data goes through before a user accesses it, which can result in unplanned licenses purchases.

Recommendations

Directions on Microsoft provides the following recommendations for using PPU capabilities:

- PPU environments works best for small groups or organizations planning to expand into a Premium capacity
- Mixing PPU workspaces with existing Power BI Pro

or Power BI Premium environments should be done cautiously to avoid unintended multiplexing

- Adding PPU workspaces should be limited to well-isolated situations or where the PPU workspace is at the end of the line in providing content to users.

Migrating from PPU to a Premium capacity is relatively straightforward, which could allow customers to start with PPU and then upgrade to Premium as they expand. PPU workspaces are compatible with Premium capacity workspaces and can be migrated without rebuilding or redeploying the environments. The only requirement is

that datasets and data models must be fully refreshed in the Premium capacity to establish the new connections.

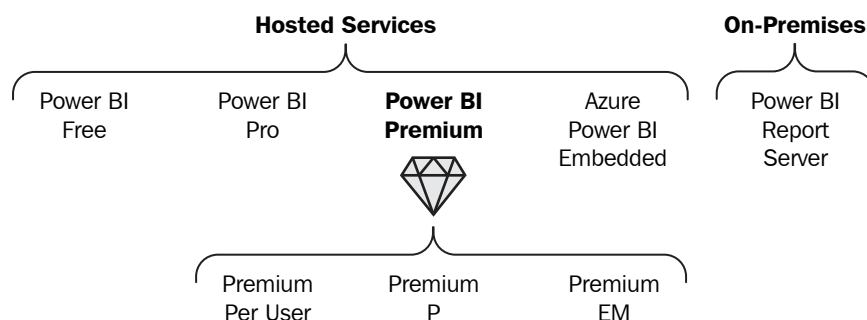
Resources

Licensing Power BI is discussed in the *Licensing Reference Set* at <https://www.directionsonmicrosoft.com/licensing/power-bi>.

Power BI is covered in the *Microsoft 365 Roadmap* at <https://www.directionsonmicrosoft.com/roadmap/ref/power-bi>.



A Licensing Overview of Power BI Back-End Platforms



Microsoft offers customers several Power BI back-end hosting platforms (shown here), including multiple cloud services and an on-premises Power BI Report Server. They vary by licensing model and on support for content types, client tools, capabilities, performance, scaling, security, and licensing.

Back-End Hosting Functions

The back-end hosting platforms act as repositories for several components:

- Reports
- Datasets (built using Power Query)
- Tabular semantic data models (using Analysis Services)
- Data integration pipelines.

They are also the workhorse for authenticating, executing queries, accessing external data, scheduling data refreshes, and running integration pipelines, as well as rendering, publishing, and distributing reports. They also respond to user interaction for real-time analysis.

Back-End Platforms Overview

Power BI offers the following back-end hosting platforms:

Power BI Free is designed for small businesses, individual users, and occasional consumers of reports. It lacks security controls, provides limited data storage capacity and refresh rates, and has other significant shortcomings that typically make it unsuitable for midsize and large organizations.

Power BI Pro is designed for organizations with relatively few users (typically less than 500) authoring or consuming Power BI-based reports or dashboards, and it lacks high-end capabilities and advanced security and control features that are available in Premium. It is licensed per user.

Power BI Premium is the high-end offering with a superset of the Power BI Pro features and is licensed primarily by capacity, which allows customers to provide access to an unlimited number of internal and external users, removing the need to license users individually. Premium is designed for enterprises with a large number of users that need exclusive Premium features not available in Power BI Pro, such as larger data models, SQL Server paginated reports, Analysis Services Tabular data models, data integration pipelines, and high-end security.

Premium is available in three options:

Premium P is the highest level with all capabilities and is licensed by capacity with tiers ranging from P1 to P5 that differ in the number of virtual cores

Premium EM is licensed by capacity with most Premium P features but is limited to sharing reports through internal line-of-business applications and Web sites; it is licensed by capacity with tiers ranging from EM1 to EM8 that differ by the number of virtual cores

Premium Per-User (PPU) has most of the features of Premium P but fewer security controls; it is licensed per user (rather than capacity) and has sharing restrictions.

Azure Power BI Embedded has similar capabilities and limitations as Premium EM but is designed for ISVs and developers to deliver reports to external users through custom applications and Web sites. It is licensed by capacity and has cost-control features not in Premium EM, such as the ability to pause the service.

Power BI Report Server is an on-premises edition of SQL Server Reporting Services that can host Power BI (.pbix) reports. It can be licensed with SQL Server Enterprise edition with active Software Assurance (SA) or with on-premises rights provided through a Premium P subscription. Purchase of Power BI Premium P include rights to deploy Power BI Report Server on-premises using the same number of cores included in the Premium P capacity simultaneously, which will most likely appeal to organizations with a mix of reporting workloads, where some reports are hosted in the cloud for external access and sensitive reports are hosted on-premises.

Report Authoring Licensing Requirement

All platforms (except for Power BI Free) require Power BI Pro or PPU licenses for individuals who create, contribute to, or publish Power BI content. These individuals, often referred to as report authors or data engineers, must have a Power BI Pro or PPU subscription, regardless of where the content is hosted and shared, except when the content is hosted in a PPU workspace. Then the individual must have a PPU subscription.

Directions on Microsoft (DOM) is an independent IT planning information and advisory service focused exclusively on Microsoft enterprise technologies since 1992. DOM membership gives you access to an all-in-one-place source of objective and accurate facts about Microsoft roadmaps, products, and licensing policies that will help you make faster, better decisions about your Microsoft investments.

Directions on Microsoft services include:



DOM equips you with the essential knowledge you need to take full control of your Microsoft investments. To schedule a demonstration of the DOM portal, please call +1 425.739.4669 or e-mail info@DirectionsOnMicrosoft.com.

Product & Services Roadmaps

DOM Roadmaps summarize essential facts about Microsoft enterprise products and cloud services, including code names, release dates, new features, key use scenarios, and support deadlines. Use them to build your Microsoft IT plans and budgets and proactively prepare for disruptive changes in Microsoft technologies and services.

Technology Reports

DOM Reports drill down into key Microsoft technologies and initiatives to help you understand the technical and business significance that can affect your organization. Use them to cut through the marketing hype that surrounds Microsoft technologies and focus your attention on facts that matter to IT decision makers.

Licensing Reference Set

The DOM Licensing Reference Set is an up-to-date wiki of licensing rules and programs for Microsoft enterprise products and cloud services. Use it to quickly find answers to your Microsoft licensing questions and verify what Microsoft or your reseller is telling you.

Analyst Webinars

DOM Webinars are monthly conference calls consisting of a 20-minute presentation by DOM subject matter experts followed by a question-and-answer period. Use them to get clarity about new Microsoft technologies, roadmaps, and licensing policies in the most time-efficient way possible.

Licensing Boot Camps & EA Negotiation Workshops

The two-day DOM Licensing Boot Camp and one-day EA Negotiation Workshop (now in an online format) are intensive trainings that teach you how Microsoft licensing really works. Use them to get the information and knowledge you need to optimize your agreements.

Advisory Services

DOM subject matter experts apply an institutional understanding of Microsoft technologies, roadmaps, and licensing to elevate your Microsoft IT strategy and help you negotiate the best terms possible on your Microsoft agreements.

You get thinking and advice you'd expect from a top consulting firm for a fraction of the cost.

