Summary

The purpose of this document is to address security in Microsoft Dataverse and provide risk mitigation scenario guidance.

Introduction

What is Dataverse?

Microsoft Dataverse is a cloud-based solution that easily structures a variety of data and low-code business logic to support interconnected applications and processes in a secure and compliant manner. Managed and maintained by Microsoft, Dataverse is available globally but deployed geographically to comply with your potential data

residency. It is not designed for stand-alone use on your servers, so you will need an internet connection to access and use it.

A Dataverse environment is a single instance of Microsoft Dataverse which stores all types of data (tables, documents, events, files, etc.). A *table* is a set of rows (formerly referred to as records) and columns (formerly referred to as fields/attributes). Each column in the table is designed to store a certain type of data, for example, name, age, salary, and so on. Dataverse includes a base set of standard tables that cover typical scenarios, but you can also create custom tables specific to your organization. With standard tables and columns, as well as the ability to easily define relationships between your data, Dataverse was built for powerful, scalable solutions.

You can create one or many instances in Microsoft Dataverse to host data behind your business solutions. Each instance of Microsoft Dataverse will start with the same set of tables to store data, but you can always extend and customize a Microsoft Dataverse environment to meet specific business needs. This means that you can share business solutions that reference standard tables in Microsoft Dataverse across your organization or with any other organization by using it anywhere in the world. The ease of setting up a Microsoft Dataverse instance and a standardized data model under it simplifies your ability to concentrate your efforts on building solutions without worrying about infrastructure, storage, and data integration.

With your data stored in Microsoft Dataverse, there are many ways to access or modify it. You can work with the data natively with tools such as Power Apps or Power Automate. Or through connectors and APIs you can connect to Microsoft Dataverse from any business solution. With the power of features such as role-based security and business rules, you can trust your data is safe no matter how it is accessed.

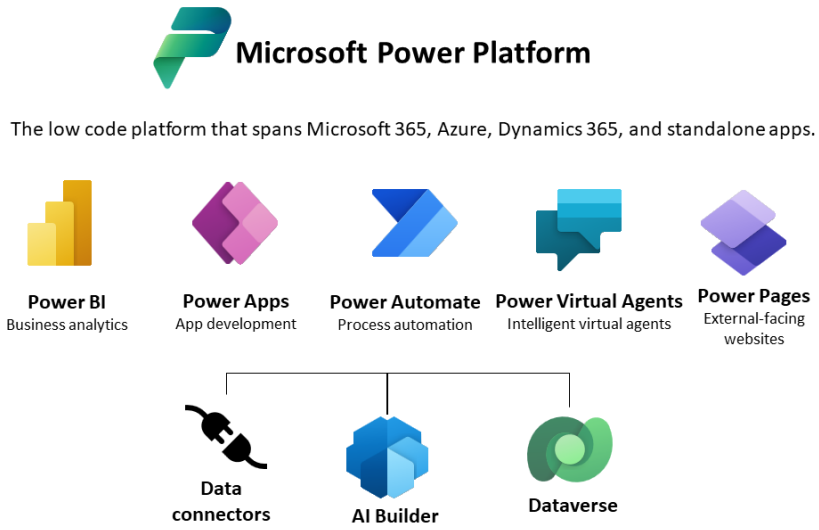
How Dataverse Fits into the Power Platform

Microsoft Dataverse is a cloud-based, low-code data service and app platform, which allows you to leverage the security and connectivity of Microsoft services. Dataverse connects easily to all aspects of Microsoft Power Platform so that you can fully control, automate, and strengthen your business. Dataverse lets you securely store and manage data that's used by business applications.

Microsoft Dataverse and a common layer of admin experiences are the backbone of the Dynamics 365 business. Microsoft Dynamics 365 includes an extensive business

application suite and AI-driven business insights applications. Dataverse also supports Microsoft's low-code platform that includes Power Apps for internal line-of-business applications, Power Automate for process automation, and Power Pages for external business websites. App makers can then use Power Apps to build rich applications that use the data stored in Microsoft Dataverse.

Dataverse is designed to be your central data repository for business data, and you might even be using it already. Behind the scenes, it powers many Microsoft Dynamics 365 solutions such as Field Service, Marketing, Customer Service, and Sales. It is also available as part of Power Apps and Power Automate with native connectivity built right in. The AI Builder and Portals features of Microsoft Power Platform also utilize Dataverse.



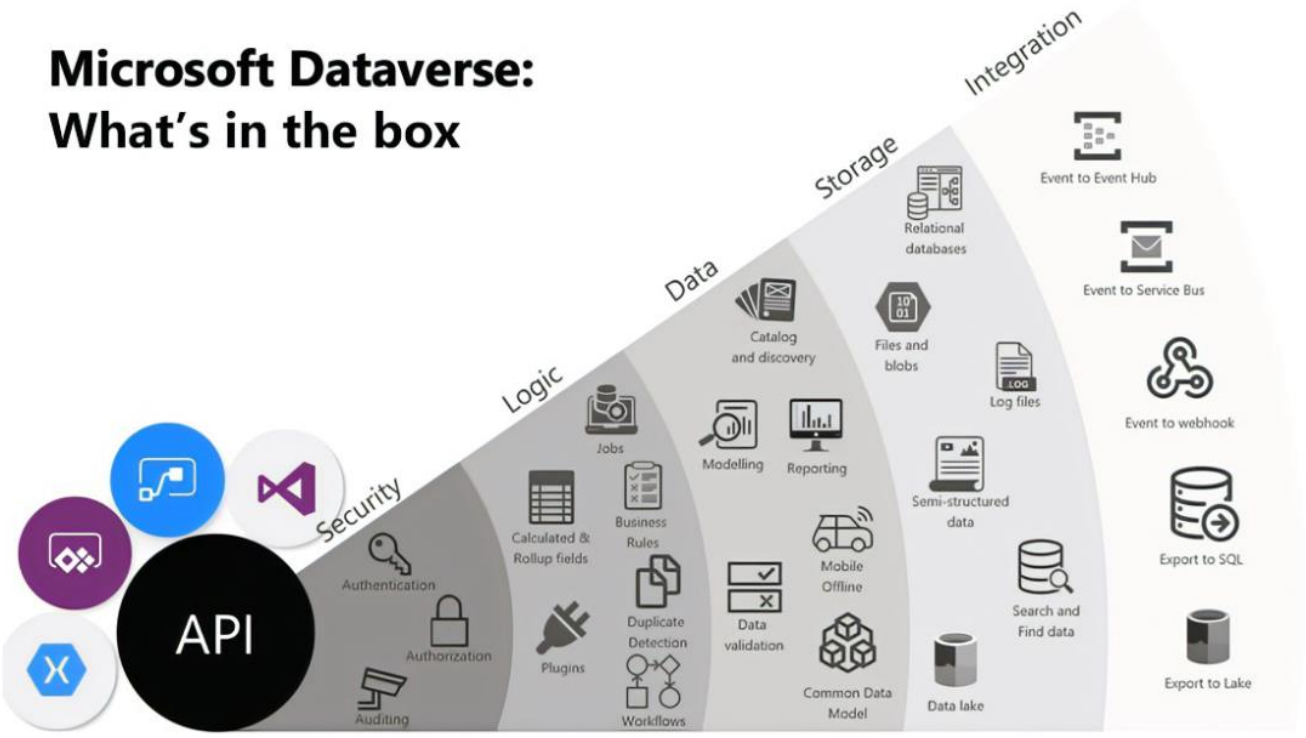
Microsoft Power Platform utilizes Dataverse and related services to provide low-code solutions for enterprise applications.

Why Choose Dataverse?

Here are the main benefits of Microsoft Dataverse:

- **Easy to manage**: Both the metadata and data are stored in the cloud. You don't need to worry about the details of how they're stored.
- **Easy to secure:** Data is securely stored so that users can see it only if you grant them access. Role-based security allows you to control access to tables for different users within your organization.

- **Access your Dynamics 365 Data**: Data from your Dynamics 365 applications is also stored within Dataverse, allowing you to quickly build apps that use your Dynamics 365 data and extend your apps with Power Apps.
- **Rich metadata**: Data types and relationships are used directly within Power Apps.
- **Logic and validation**: Define calculated columns, business rules, workflows, and business process flows to ensure data quality and drive business processes.
- **Productivity tools**: Tables are available within the add-ins for Microsoft Excel to increase productivity and ensure data accessibility.



Above is a visualization that brings together the many offerings of Microsoft Dataverse.

As you can see, Microsoft Dataverse offers a great deal of functionality. Below is a brief explanation of each category of features:

Security: Dataverse handles authentication with Azure Active Directory (Azure AD) to allow for conditional access and multi-factor authentication. It supports authorization down to the row and column level and provides rich auditing capabilities.

Logic: Dataverse allows you to easily apply business logic at the data level. Regardless of how a user is interacting with the data, the same rules apply. These rules could be related to duplicate detection, business rules, workflows, or more.
Data: Dataverse offers you the control to shape your data, allowing you to discover, model, validate, and report on your data. This control ensures your data looks the way you want regardless of how it is used.
Storage: Dataverse stores your physical data in the Azure cloud. This cloud-based storage removes the burden of worrying about where your data lives or how it scales.
Integration: Dataverse connects in different ways to support your business needs. APIs, webhooks, eventing, and data exports give you flexibility to get data in and out.

Microsoft Enterprise Promises

Dataverse delivers on Microsoft Enterprise Promises, particularly focused on safeguarding your data, people, and infrastructure.

Protect everything: Safeguard your entire organization with integrated business security solutions built to work across platforms and cloud environments.

Simplify the complex: Prioritize the right risks with unified management tools created to maximize the human expertise inside your company.

Catch what others miss: Leading AI, automation, and expertise help you detect threats quickly, respond effectively, and fortify your security posture.

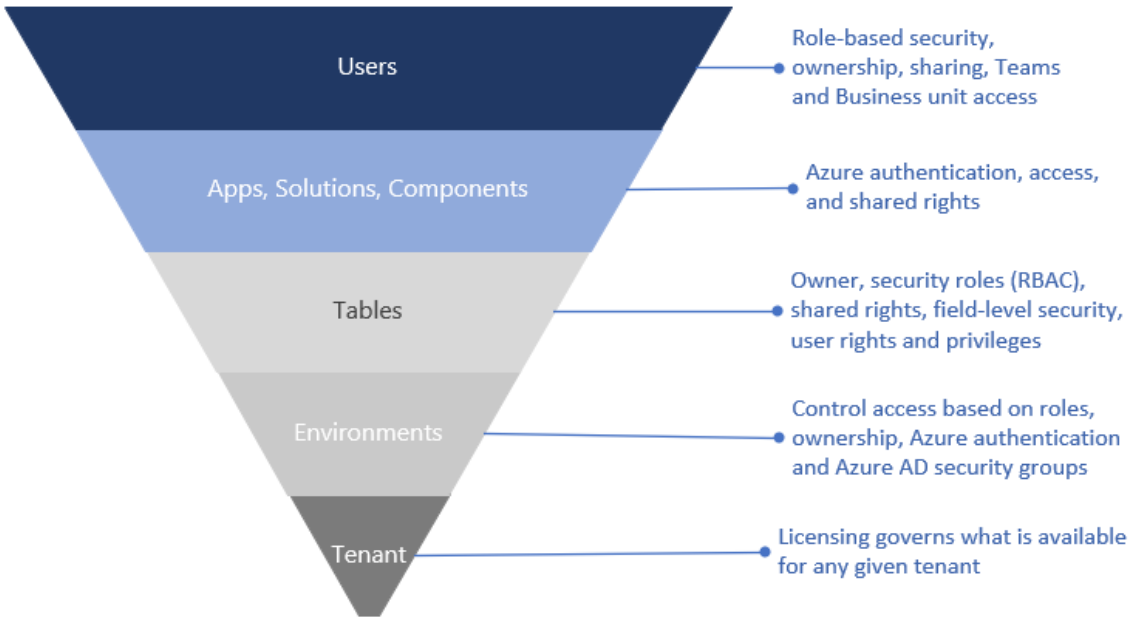
Grow your future: With the peace of mind that comes with a comprehensive security solution, you're free to grow, create, and innovate your business.

Security In Dataverse

What sets Dataverse apart from other low-code options is that everything is governed and authenticated through Azure AD—you need to sign in with your work or school Azure AD account to use this service. This means that as an admin, you have full visibility of everything your makers and users do—it's governable, automatable, auditable, and manageable by default.

- Dataverse uses Azure AD identity and access management mechanisms to help ensure that only authorized users can access the environment, data, and reports.

- Dataverse uses role-based security to group together a collection of privileges. These security roles can be associated directly with users, or they can be associated with Dataverse teams and business units. These privileges provide users access to records.
- In Dataverse, there is another way to grant user access to records other than from security role privileges. Authorized users or owners of records can share their individual rows on a one-by-one basis with another user or team. Because row-level control of access isn't adequate for some business scenarios, Dataverse has a column-level security feature to allow more granular control of security at the column level.
- Dataverse also includes two other data access security models that can be used for hierarchies: the manager hierarchy and the position hierarchy.
    - With the manager hierarchy, a manager must be within the same business unit as the report, or in the parent business unit of the report's business unit, to have access to the report's data.
    - The position hierarchy allows data access across business units.
- Because Dataverse is built on Azure, it benefits from the Azure platform's powerful security technologies. Encryption of data, at rest and in transit, preserves confidentiality.



Security across the stack.

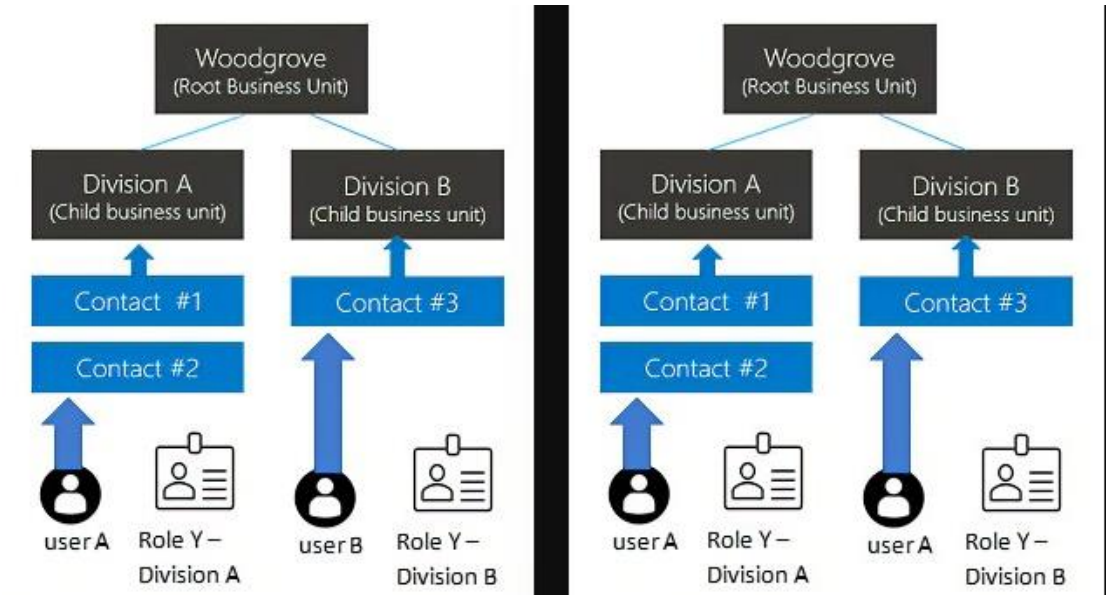
The security model for Dataverse is rooted by Azure Active Directory. Every Dataverse will authenticate its callers through a single **tenant**. A tenant is the base of the security model for Dataverse which holds the identities of the users and service principals. An **environment** is a Dataverse security boundary.

Each environment contains a list of **tables** which are metadata describing the contents of the tables. The **tables** capture the records and data. Both of these are secured with separate privileges. **Apps, solutions, and components** are created to access tables. And finally, **users** take actions against entities.

Dataverse security and data access provides a security model that protects data integrity and privacy and supports efficient data access and collaboration. The goals of the model are as follows:

- Provide users with the access only to the appropriate levels of information that is required to do their jobs.
- Categorize users by role and restrict access based on those roles.
- Support data sharing so that users and teams can be granted access to records that they do not own for a specified collaborative effort.
    - For example: In account-based selling, this enables a new employee added to sales division A to get immediate & secure access to all relevant ongoing opportunities by simply becoming a member of sales division A. Likewise, if an employee moves from division A to division B, just updating sales org role membership ensures appropriate changes in access to opportunities, communication docs, etc. Or if an employee departs, all access is removed automatically (as they depart Azure AD, or if they are removed from the sales role membership).
- Prevent a user's access to records the user does not own or share.

The specific security concepts implemented within Dataverse provide flexibility to create the proper model for your application needs. We continue to grow and change our capabilities to meet our customer’s needs, including the latest addition of Modern Business Units which support business units that are not only hierarchical. Focus on the user in each figure below; the hierarchical configuration maps users based on the owning business unit whereas the Modern Business Unit will allow a user to be a member of multiple business units.



Left is an image of the one-to-one association of a user to a business unit granting access to a record. Right is an image of the many-to-many association of a user to a business unit granting access to records owned by discrete business units.

Risk Mitigation Scenarios

The scenarios below are provided as examples, not a complete prescriptive approach for every organization. Your environment may have special considerations; however, the scenarios, features, and response techniques are provided as references to be implemented within your environment.

#1 Ensure users have the least privilege necessary

I want to minimize access to sensitive data in my applications.

I want to make sure that only users that I allow access based on certain business conditions can sign into my environments and get access to my data.

There are concepts described in the Security In Dataverse section that must be understood to create the right sets of users, permissions, and roles to allow the business to operate. Given the right set of users, you can leverage the Dataverse Authorization Model and Azure Active Directory controls such as Groups. Conditional Access is one aspect of the isolation of an environment's data. The other important consideration is what data is being protected; understanding the data that exists in your environments is critical.

Microsoft Purview Information Protection establishes protection across integrations/environments based on type rather than location of data and provides ways

to combine data sets to be defined that allow data collaboration. IT professionals and administrators can designate containers (Dataverse environments) and folders (data entities) with data sensitivity that defines the boundaries that can isolate data in the organization. The platform also provides ways to designate custom groupings of data connectors to allow collaboration across business units that help users collaborate when necessary.

Additionally, you can leverage Azure AD Conditional Access and location awareness to further control access to environments by trusted devices, locations, and other conditions which can be evaluated for the authentication. For more information see Microsoft Purview Information Protection.

Protect

- Leverage Dataverse Authorization to create the right group and individual access to collections and records. See How access to a record is determined in Dataverse for more details about how to set up the proper authorization model.
- Leverage Azure Active Directory Conditional Access to prevent authentication based on location, device, or other properties of the user's authentication context.

Detect

- Review Audit logs in Azure Active Directory to identify which users who have authenticated to Dataverse.
- Retrieve the history of audited data changes in Dataverse.
- Review Microsoft 365 admin center activity reports.
- Use Microsoft Dataverse usage reports.

Respond

- Disable User from the environment - Delete users from environments.
- Revoke user access in an emergency in Azure Active Directory.
- Microsoft Sentinel SOAR – Create a custom Logic App to handle your unique scenarios.

#2 Manage external or internal access and prevent data loss

I want to make sure users do not have the ability to intentionally leak or allow others to easily access and leak sensitive data in my environment.

Dataverse provides two features that you can easily configure and set up to stop users from data leakage or accidentally providing access to the system that include Data Loss

Prevention Policies with endpoint filtering and actionable controls on all connections (connectors) to your system. The platform also provides additional security using Role-Based Access (RBAC) that system administrators can quickly and easily configure to further lock down access to your organization's tables in the system. The platform also provides additional security using Role-Based Access (RBAC) that system administrators can quickly and easily configure to further lock down access to your organization's tables in the system.

Protect

- Dataverse API - Limit user access with IP firewall.
- Block cookie replay attacks in Dataverse (preview) - Power Platform | Microsoft Learn
- Restrict guest user access permissions through Azure Active Directory.
- Limit IP Surface area by configuring inbound and outbound rules allowing Power Platform. See Azure service tags overview | Microsoft Learn for available service tags.
- Leverage Azure Active Directory Conditional Access to prevent authentication based on IP Address or IP Location for broader access restrictions applied to all Azure Active Directory protected resources.

Detect

- Review Audit Logs for Public IP Address Access to your environment.
- Track user access of the Microsoft Power Platform.
- Use Microsoft Dataverse usage reports.

Respond

- Modify IP Firewall to meet your changing network requirements.

#3: Monitor who is accessing and working with data

I want to make sure I can quickly and easily identify any threats that I define as suspicious activity in the system.

Dataverse Auditing provides ways for system admins to quickly set up audit tracking for their environment. The platform provides the ability to track and log activities that include CRUD operations, opening and viewing records, sharing records, etc. The logs can be easily accessed directly on the client without the need for additional reporting or export of audit activity. It is important to note that Read Auditing is configured separately from Create, Update, or Delete as this audit trail may produce a lot of data; not all environments require read auditing.

Protect

- A baseline for detections will be the enablement of auditing, including User Access Auditing. For details, please review Manage Dataverse auditing. For a functional sample which tests the auditing, review Audit user access.
- Leverage Azure Active Directory Conditional Access to prevent authentication based on location, device, or other properties of the user's authentication context.

Detect

- Review Audit logs in Azure Active Directory to identify which users have authenticated to Dataverse.
- Retrieve the history of audited data changes in Dataverse.
- Review Microsoft 365 admin center activity reports.
- Use Microsoft Dataverse usage reports.

Respond

- Modify the authorization settings for the Dataverse entity to remove inappropriate access.
- In the case of an account compromise, the M365 automations may be applicable.
- Disable User from the environment - Delete users from environments.
- Revoke user access in an emergency in Azure Active Directory.
- Microsoft Sentinel SOAR – Create a custom Logic App to handle your unique scenarios.

#4 Secure data from cloud service operators

I want to make sure Microsoft does not gain unwanted access to my environments and data.

If I decide to leave the cloud service, my data is fully removed and any and all access to the data for both internal and external threats is removed.

Dataverse provides multiple layers for you to protect your data from users gaining access to your sensitive data that include customer exposed features such as Lockbox and Customer Managed Keys as well as internal operational process such as JIT Access and Secure Admin Workstations. With the introduction of Customer Lockbox, the Microsoft JIT Access process includes a customer approval step.

Customer managed keys allow you to revoke the key at any time which prevents any further access to the environment, which in turn, protects your data when leaving the platform. In addition to customer managed keys, admins can easily remove users or delete environments from the Power Apps admin center.
We also fully support the European Union General Data Protection Regulations (GDPR) and will delete all data across environments when asked to do so by a customer.

Protect

- Securely access customer data using Customer Lockbox in Power Platform.
- Configure CMK and Manage the encryption key.

Detect

- Apply Access Monitoring and correlate with Lockbox approvals when a Microsoft domain user is observed.

Respond

- Revoking the encryption/decryption key will mitigate any feasibility of data access.
- Contact your Technical Account Manager or Customer Support.

For additional information, see Dataverse and Security FAQs.

Building Secure Hybrid Environments

As organizations accelerate the transition to the cloud there is a higher need and reliance on advanced technologies when making business and operational decisions. With the move to cloud services and the ability to easily interact across an organization for employees working in the office or remotely and with external customers, there is a higher demand for secure online services. Traditional on-premises application security is no longer enough, companies are looking for cloud services to support native, multi-tiered, defense-in-depth security solutions for their data.

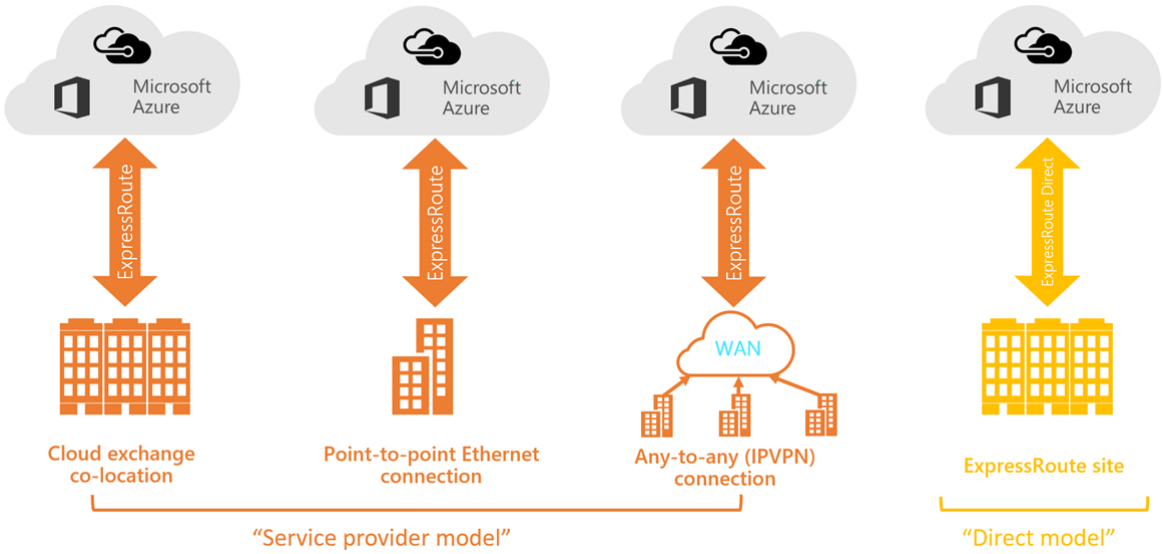
Dataverse puts the power to quickly and easily create end-to-end solutions in the hands of non-professional and professional developers alike. Security is essential for these solutions. The platform offers an array of options for companies to create safe and secure environments with tools to easily define, manage, and configure environments, data, and applications.

Getting your environments secure starts with a multi-layered approach with capabilities that provide tools across the entire stack, starting with your tenant, environments, data, and applications. Dataverse provides you with features and capabilities that cover all aspects of the entire stack that include access controls, data policies, security models, data encryption, and data auditing (both audit log search and Dataverse auditing).

Hybrid Cloud and Data Integrations

The ability to easily set up and configure secure environments with Dataverse starts with how people, both internal and external, gain access to your organizational data and applications. It offers simple and easy configurations and user management tools that start with access based on the Microsoft Azure authentication platform and the Azure AD service. Azure AD provides a fully secured identity federation that enables users to authenticate with credentials to access both on-premises and cloud resources.

Microsoft's global network stands out as one of the largest backbone networks in the world, providing service to not only Microsoft's data centers, but as an extension of your enterprise network through features such as ExpressRoute.



Various ExpressRoute connectivity models are available for your enterprise solutions.

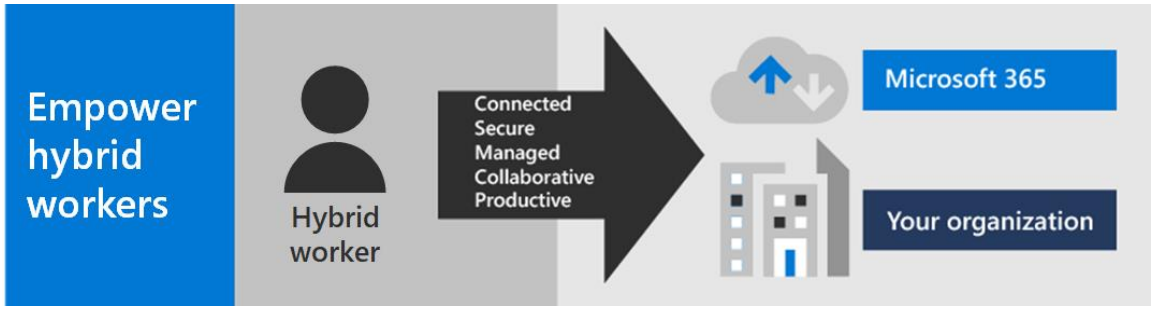
Azure has invested in providing private IP network access technologies for several services which allow enterprises to simplify firewall management and create better clarity around which systems have access to which resources.

Hybrid Worker Infrastructure

To secure and optimize your worker's productivity and collaboration, you need to allow on-site and remote workers to access your organization's on-premises and cloud-based information, tools, and resources easily and securely. This solution steps through the deployment of key layers of infrastructure that empower your workers to do their best work, wherever they are.

Hybrid workers can work on-site or remotely in a combination of locations. Allowing workers to work away from a traditional office is important for many organizations to:

- Hire and retain workers who are unwilling to relocate or require a flexible work environment.
- Reduce worker commuting, leaving workers with more time to be productive and for stress-reducing activities outside of work.
- Save office space.



Microsoft 365 has the capabilities to empower your hybrid workers to work either on-site or remotely.

For IT professionals managing on-site and cloud-based infrastructure to enable hybrid worker productivity, this solution provides these key capabilities:

- **Connected:** From anywhere in the world and at any time, your workers are able to access:
    - Cloud-based services and data in your Microsoft 365 subscription.
    - Organizational resources, such as those offered by on-premises application data centers.
- **Secure:** Sign-ins are secured with multi-factor authentication (MFA) and built-in security features supported by Azure AD which helps protect against malware, malicious attacks, and data loss.
- **Managed:** Your hybrid worker's devices can be managed from the cloud with security settings, allowed apps, and compliance with system health.

- **Collaborative and productive:** Your hybrid workers can be as productive as on-premises in a highly collaborative way with:
    - Online meetings and chat sessions with Teams.
    - Shared workspaces for cloud-based file storage with global accessibility and real-time collaboration with SharePoint and OneDrive.
    - Shared tasks and workflows to divide up the work and get things done.

Data Loss Prevention

The Power Platform and Dataverse protects your data with Microsoft Data Loss Prevention (DLP). It protects sensitive information across devices, cloud services, and on-premises. Data Loss Prevention policies are fundamental to an enterprise's security model. Data is an organization's most valuable and irreplaceable asset and encryption serves as the last and strongest line of defense in a multi-layered data security strategy. Microsoft business cloud services and products use encryption to safeguard customer data and help you maintain control over it.

Access and authentication help secure organizations' data and applications but there is always a need to provide additional layers of security and governance from internal threats when an authorized and authenticated user starts using applications and interacting with data. With the constant threat of losing company and customer sensitive data, building a robust set of data loss prevention policies that further govern data access and interactions are needed to fully secure your organization's data and applications. Dataverse provides additional security for IT professionals and admins with simple and easy ways to define data policies.

Data loss prevention policies (DLP) enforce rules for which connectors can be used together by classifying connectors as either business data only or no business data allowed. Simply, if you put a connector in the business data only group, it can only be used with other connectors from that group in the same application. Admins can define policies that apply to one or all environments within an organization that provide additional layers of security by either granting or blocking access based on DLP policies.

At-Rest Data Protection

Encrypting your information renders it unreadable to unauthorized persons, even if they break through your firewalls, infiltrate your network, get physical access to your

devices, or bypass the permissions on your local machine. Encryption transforms data so that only someone with the decryption key can access it.

By default, Microsoft stores and manages the database encryption key. Dataverse provides customer managed keys (CMK) to encrypt Azure SQL databases that stores transactional data. An administrator can self-manage the database encryption key that is associated with the tenant but is limited to encrypting Azure SQL database storing transactional data only. File, Log, Datalake, and Search encryption will remain managed by Microsoft. Soon, these non-SQL files can be encrypted with the customer managed keys.

Dataverse databases use SQL TDE (Transparent Data Encryption, compliant with FIPS 140-2) to provide real-time I/O encryption and decryption of the data and log files for data encryption at-rest. Azure Storage Encryption is used for data at rest stored in the Azure Blob Storage. These are encrypted and decrypted transparently using 256-bit AES encryption compliant with FIPS 140-2.

In-Transit Data Protection

Azure protects data in transit to or from outside components, as well as data in transit internally, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS1.2 and latest server cipher suites between user devices and Microsoft data centers, and within data centers themselves. To protect your data even more, internal communication between Microsoft services is using the Microsoft backbone network and therefore is not exposed to the public internet. Microsoft uses multiple encryption methods, protocols, and algorithms across its products and services to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure. Microsoft uses the strongest, most secure encryption protocols in the industry to provide a barrier against unauthorized access to your data. Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured.

Data loss prevention policies (DLP) enforce rules for which connectors can be used together. Blue checkmarks indicate features of Microsoft Dataverse and Power Platform.

Authentication, Authorization, and Auditing

Authentication

Security starts with authentication. The security of your organization's data and applications based on conditional access is a top concern when using cloud-based solutions and services. A key aspect of cloud security is identity and access when it comes to managing your cloud resources. In a mobile-first, cloud-first world, users can access your organization's resources using a variety of devices and apps from anywhere. As a result of this, just focusing on who can access a resource is not sufficient anymore. With the ever-growing need for employees and customers to access and use applications and data from anywhere, companies are facing two opposing goals:

- Empower users to be productive wherever and whenever
- Protect the corporate assets at any time

To master the balance between security and productivity, you also need to factor how a resource is accessed into an access control decision. A key advantage of leveraging Azure AD for authentication is that the same policies used to govern a device or user's access via conditional access policies will apply to Dataverse.

Conditional Access

Azure AD provides conditional access that supports automated access control decisions for accessing your cloud apps that are based on conditions. Dataverse honors and

enforces Azure AD conditional access policies, that can be applied to manage the right access under the required conditions. By using Azure AD conditional access, the platform provides added security when needed and stays out the user's way when it isn't.

Several concerns are directly addressed with conditional access that include:

- Sign-in risk
- Network location
- Device management
- Client applications

By providing conditions that trigger access policies, you can control how authorized users access your cloud environments, data, and apps. The objective of a conditional access policy is to enforce additional access controls on an access attempt to a cloud app that is driven by how an access attempt is performed.

Azure AD Security Groups

Customers who are using Azure AD security groups to secure access control of their Azure resources can also extend their security group usage in Dataverse. Dataverse acknowledges the security group membership and grants Azure AD security group members immediate access to Dataverse.

Authorization

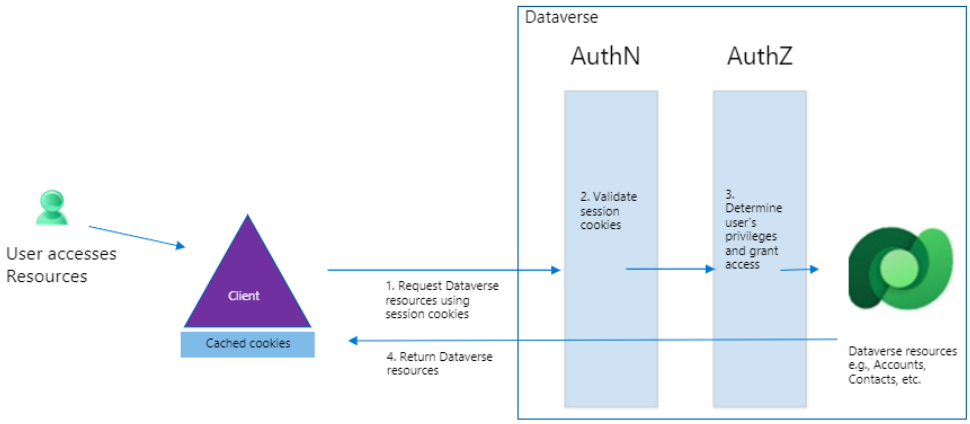
Authorization refers to the mechanisms available inside Dataverse and Dynamics 365 that allow you to control the functionality and data accessible to the users in your environment. You use the security model to protect the data integrity and privacy in a Dataverse environment.

Dataverse authorization is an additional layer of Azure AD authentication. This allows Dataverse to use the information within the user's authentication context to make additional authorization decisions and provides Dataverse administrators more control over the data stored within a specific Dataverse instance. While it may make sense for an enterprise to allow authentications from any IP Location, Dataverse provides control over more fine-grained authorization decisions, such as which IP addresses and Azure AD users are allowed to authenticate to a particular Dataverse environment. Dataverse also enables very fine-grained authorization down to the individual row and column level.

Most operations, support, and troubleshooting performed by Microsoft personnel (including sub-processors) don't require access to customer data. With Power Platform Customer Lockbox, we provide an interface for the customers to review and approve (or reject) data access requests in the rare occasion when data access to customer data is needed. It's used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft. To learn more, see [securely access customer data using Customer Lockbox in Power Platform.]

Authorization flow in Dataverse

Granting permission to secured resources.



AuthZ: IP Binding, Row / Field
Accountability: M365 integration + SIEM

Dataverse provides multiple features and capabilities that can be easily configured and set up using:

- **Role-based security** is where a defined role contains privileges that allow a set of actions to be performed by users within the organization. For example, the salesperson role is assigned a set of privileges that are relevant to the tasks defined for that role. All users must be assigned to one or more predefined or custom roles.
- **Privileges** are the core of the underlying security check. Privileges are "built in" to the product and are used throughout the application and platform layers to allow or restrict access to tables, columns, and rows. The client applications use the privileges to ensure users do not have access to data or applications outside of their defined roles. Privileges cannot be added to or removed from an environment, but you can construct new roles from the existing privilege set.

- **Access levels** provide a hierarchical model that helps govern privileges and access for a given entity type within the organization. Roles can be easily configured to have certain levels of access that include global, business areas or units (deep), local, basic, and none. Each of the levels provides varying degrees of access as you move up and down the pyramid.
    - ***GLOBAL*** gives a user access to all records within the organization, regardless of the business unit hierarchical level to which the instance or the user belongs. Users who have global access automatically have deep, local, and basic access as well.
    - ***DEEP*** grants access to records in the user's business unit and all business units subordinate to the user's business unit.
    - ***LOCAL*** gives a user access to records in the user's business unit. Users who have local access automatically have basic access also.
    - **BASIC** grants a user access to records he or she owns, objects that are shared with the user, and objects that are shared with a team of which the user is a member.
    - ***NONE*** blocks users from accessing any environment including data and applications.

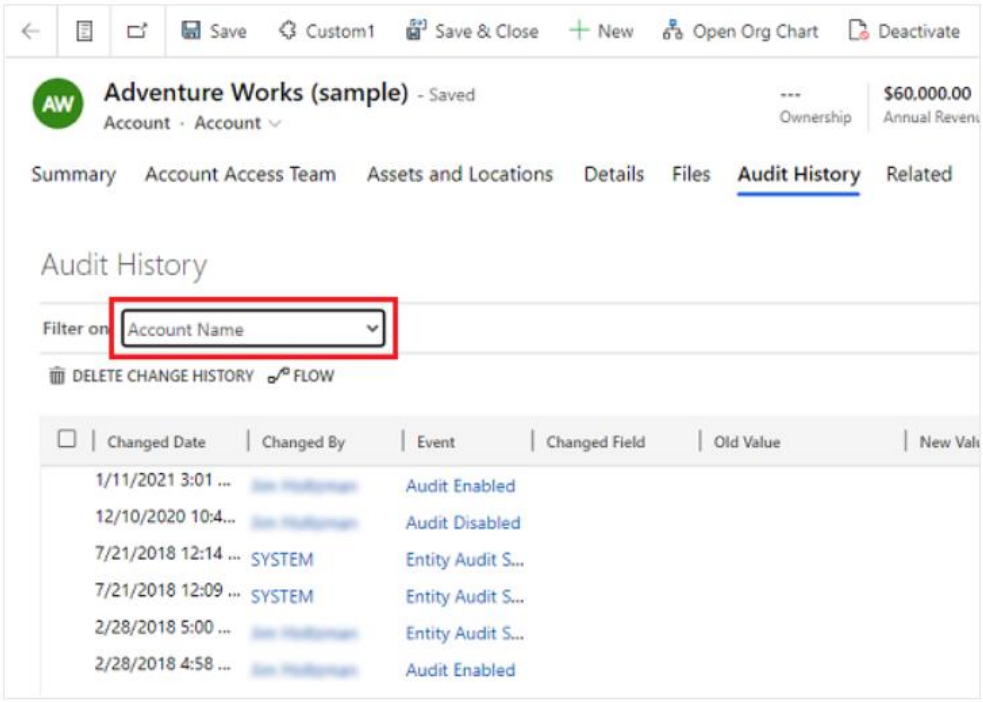
Sharing and collaboration

Authorization in the Dataverse goes beyond just access, it also provides the ability for users to grant access to rows in tables (data) with specific rights to others with access to an environment, organization, data, and applications. This allows owners of data to grant read, write, assign, append, share, and delete rights and privileges. The platform allows users to manage how data is accessed, which further reduces the overhead and the need for system administrators or IT professionals to grant every user in the organization access to specific rows owned by an end user. Using this model, users can easily collaborate across the organization to close deals, solve customer issues, and manage complex marketing campaigns, improving the overall productivity of an organization that drives business results.

Auditing

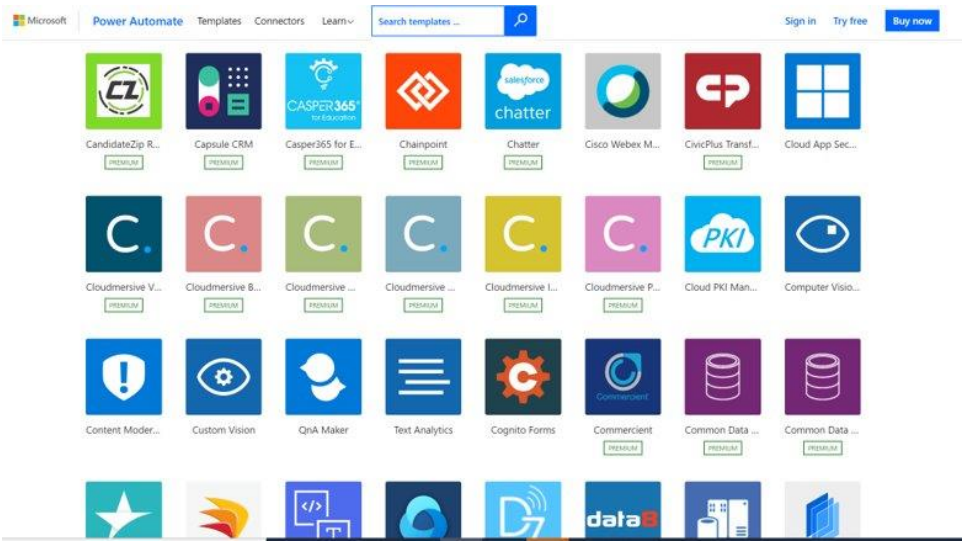
The dataverse auditing feature is designed to meet the external and internal auditing, compliance, security, and governance policies that are common to many enterprises. Dataverse auditing logs changes that are made to customer records in an environment with a Dataverse database. Dataverse auditing also logs user access through an app or through the SDK (Software Development Kit) in an environment.

Dataverse auditing is supported on all custom and most customizable tables and columns. Audit logs are stored in Dataverse and consume log storage capacity. Audit logs can be viewed in the Audit History tab for a single record and in the Audit Summary view for all audited operations in a single environment. Audit logs can also be retrieved using the Web API or the Organization Service.



Example of an audit log.

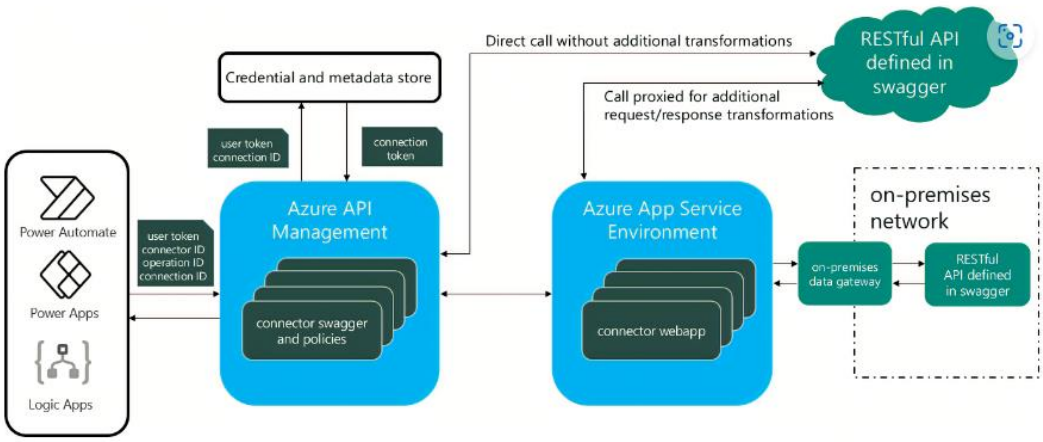
Integration (Connectors)



Wide range of Out of the Box (OOB) data connectors available.

A *connector* is a proxy or a wrapper around an API (application programming interface) that allows the underlying service to talk to Microsoft Power Automate, Microsoft Power Apps, and Azure Logic Apps. It provides a way for users to connect their accounts and leverage a set of prebuilt *actions* and *triggers* to build their apps and workflows. Connectors are classified as either Business Data only or No Business Data allowed. A connector in the business data only group can only be used with other connectors from that group in the same app or Power Automate.

Our large ecosystem of software as a service (SaaS) connectors enable you to connect apps, data, and devices in the cloud. Examples of popular connectors include Salesforce, Office 365, Twitter, Dropbox, Google services, and more.



Runtime flow.

Architecture Components

Here are the architecture components and what they do:

- **Credential and metadata store:** A service to store connector metadata (swagger, connection, ACLs, etc.) and credentials associated with a connection.
- **Connector:**
    - Azure APIM (API Manager) to host all the swagger and policies. In addition to being the entry point for all calls that interact with the connector calls, Azure APIM verifies keys, tokens, certificates, and other credentials.
    - App Service Environment to host connector webapps.

Connector Components

Each connector offers a set of operations classified as *actions* and *triggers*. Once you connect to the underlying service, these operations can be easily leveraged within your apps and workflows.

Actions

Actions are changes directed by a user. For example, you would use an action to look up, write, update, or delete data in a SQL database. All actions directly map to operations defined in the swagger.

Triggers

Several connectors provide triggers that can notify your app when specific events occur. For example, the FTP connector has the OnUpdatedFile trigger. You can build either a Logic App or a flow that listens to this trigger and performs an action whenever the trigger fires.

There are two types of triggers:

- **Polling Triggers:** These triggers call your service at a specified frequency to check for new data. When new data is available, it causes a new run of your workflow instance with the data as input.
- **Push Triggers:** These triggers listen for data on an endpoint, that is, they wait for an event to occur. The occurrence of this event causes a new run of your workflow instance.

Custom connectors

We offer a wide variety of connectors, but sometimes you might want to call APIs, services, and systems that aren't available as prebuilt connectors. To support more tailored scenarios, you can build *custom connectors* with their own triggers and actions. These connectors are *function-based*—data is returned based on calling specific functions in the underlying service.

Future Updates
Connectors for Power Apps and Microsoft Flow are added continuously as we engage partners and ISVs to build them. As the ecosystem grows, we expect more partners to build connectors and get them certified.

Application Security

Plug-ins

A *plug-in* is custom business logic that you can integrate with Dynamics 365 Customer Engagement (on-premises) to modify or augment the standard behavior of the platform. Plug-ins are event handlers since they are registered to execute in response to a particular event being fired by the platform. They provide a way to examine and transform the data passed through the platform operations and initiate additional operations. Plug-ins operate at the deepest level and provide the most robust way to automate business processes regardless of whether they originate from one of the Dynamics 365 Customer Engagement (on-premises) applications, a custom client, data migration, or integration with another system.

A plug-in is a .NET assembly that you can upload to Microsoft Dataverse. Classes within the assembly can be registered to specific events (steps) within the event framework. The code within the class provides a way for you to respond to the event so that you can augment or modify the default behavior of the platform.

The classes in the assembly that can be registered to a step must implement the IPlugin interface. This interface exposes a single method: Execute. When an event occurs that has a class registered to it, contextual data is passed to the `Execute` method. Within the `Execute` method you can:

- Cancel the event and display an error to the user
- Make changes to the data in the operation
- Initiate other actions using the Organization Service to add automation

Plug-ins can be configured to execute synchronously or asynchronously. A synchronous plug-in will cause the operation to wait until the code in the plug-in is completed. This

has an impact on perceived performance of the system. The operations in an asynchronous plug-in are placed in a queue and are executed after the operation is completed so that the operation can be completed with minimal interruption.

When to use plug-ins

People frequently compare workflows and plug-ins as the choices to apply custom business logic. There is a significant overlap in the capabilities of workflows and plug-ins. Plug-ins can do everything workflows can do but the opposite is not true. But this doesn't mean you should just use plug-ins for anything that can't be done with a workflow. There are other capabilities to achieve requirements without using plug-ins.

- Workflows can use custom workflow extensions (workflow activities) which allow you to create reusable conditions and actions with code that can be used within multiple workflows.
- Calculated and rollup fields provide capabilities that could previously only be done using workflows.
- Custom Actions are a type of process similar to workflows that allow for creating reusable messages that can be called from other workflows or from the web service endpoints.
- Azure Service Bus integration and webhooks can be used to push data to external systems where logic can be applied using many different resources.
- Power Automate provides many capabilities that previously were performed using plug-ins.

You have many options available to you. You should evaluate each of them to understand the best way to meet your requirements.

Advantages of plug-ins

These are the main advantages of plug-ins:

- Plug-ins perform well. A well written plug-in provides the most performant way to apply business logic.
- Plug-ins are powerful. Many developers would prefer to use the skills and knowledge they possess to define logic and use the capabilities to work directly with the organization service or external services in code. An experienced plug-in developer can be very productive.

Disadvantages of plug-ins

- Plug-ins require the special skills of a developer to create and maintain. Developers are expensive and many businesses don't have access to one when they have a need. Business processes can change rapidly and providing options to enable change without requiring a developer can allow the system to adapt more rapidly.
- Plug-ins can be abused. A poorly written plug-in can have a significant impact on the performance of the environment. The great power of plug-ins needs to be applied with some restraint and consideration for the impact they have on the system as a whole.

More information: Write Plug-Ins to Extend Business Processes

The Software Development Kit (SDK)

The SDK includes an architectural overview of Dataverse SDK for Apps, the entity model, security model, and web services. Sample code and walkthroughs are provided to guide you through the features. It also contains information that developers can use to customize components within the SDK for Apps through code.
Developers can use the SDK to create and customize:

- Entities (including fields and views)
- Charts and dashboards
- Business processes
- Virtual entities

The SDK can also be used for more advanced scenarios, including:

- Plug-ins, Azure extensions, and webhooks
- Code-based data generation and import
- Solution creation and management (ALM)

APIs

Use Custom APIs to create your own APIs in Dataverse. You can consolidate one or more operations into a Custom API that you and other developers can call in their code or from Power Automate. The Microsoft Dataverse connector enables calling actions in Power Automate.

You can use Custom APIs as business events to enable creating new integration capabilities such as exposing a new type of trigger event in the Microsoft Dataverse connector. More information: Microsoft Dataverse business events.

Custom APIs are an alternative to Custom process actions. Custom process actions provide a no-code way to include custom messages but has some limitations for developers. Custom APIs provide capabilities specifically for developers to define their logic in code with more options. For a full comparison of Custom Process Action and Custom API, see Compare Custom Process Action and Custom API.

Create a custom API

A Custom API may include logic implemented with a plug-in. Using Microsoft Dataverse business events, you may create a Custom API without a plug-in to pass data about an event that other subscribers will respond to.

However, in other cases you will combine a Custom API with a plug-in to define some operation that will delegated to Dataverse to compute and return the result.

There are several different ways to create a custom API:

Method link	Benefit
Plug-in registration tool	An easy-to-use GUI tool integrated with tools used to develop plug-ins.
Power Apps	Using forms to enter data. You don't need to install a separate tool, you must create a separate record for each part of the Custom API.
With Code	After you understand the data model, you can create Custom API very quickly using Postman. Or you can build your own experience to create Custom API.
With solution files	When you use Application Lifecycle Management (ALM) tools you can create or modify Custom API definitions with XML files in a solution that is included in your source code repository. The Custom API will be created when you import the solution generated from your source code.

For more information, see Create and Use Custom APIs.