Enterprise Security with Microsoft Power Platform

Authors:

Rahul Ranjit Kannathusseril, Microsoft
David Yack, Colorado Technology Consultants

Power Patterns & Practices:
Robert Standefer (Robert.Standefer@microsoft.com)

Table of Contents

Security is a top priority for any organization that wants to succeed in the digital age. You need to safeguard your assets from threats and follow your organization's security policies. Microsoft Power Platform can help you achieve both goals with its low-code application platform that lets you build and manage apps and data easily and securely.

This white paper shows you how to align Power Platform with your security practices. You'll learn how to use the tools and technologies in Power Platform to configure and manage your apps and data according to your security requirements. You'll also discover the benefits of using Power Platform to empower your security team and accelerate your digital transformation efforts.

Cybersecurity landscape

Cybersecurity is a defining challenge of our time. Organizations everywhere, of every size and in every industry, feel the urgency and pressure of protecting against increasingly sophisticated attacks.

In this paper, we'll explore how the built-in security capabilities of Microsoft Power Platform work with Microsoft's robust security foundation to handle the cybersecurity challenges that organizations face as they update and improve their business applications.

Typical business application challenges

Your business applications are vital for your organization. They store some of your most sensitive data and run your essential processes. But they also attract attackers who want to steal or damage your assets.

You don't have to look hard to find headlines about hackers who sell customer records on the dark web or access customer names and emails. These breaches can cause significant harm in many ways, such as exposing customer data, disrupting business processes, losing revenue, and damaging your organization's reputation.

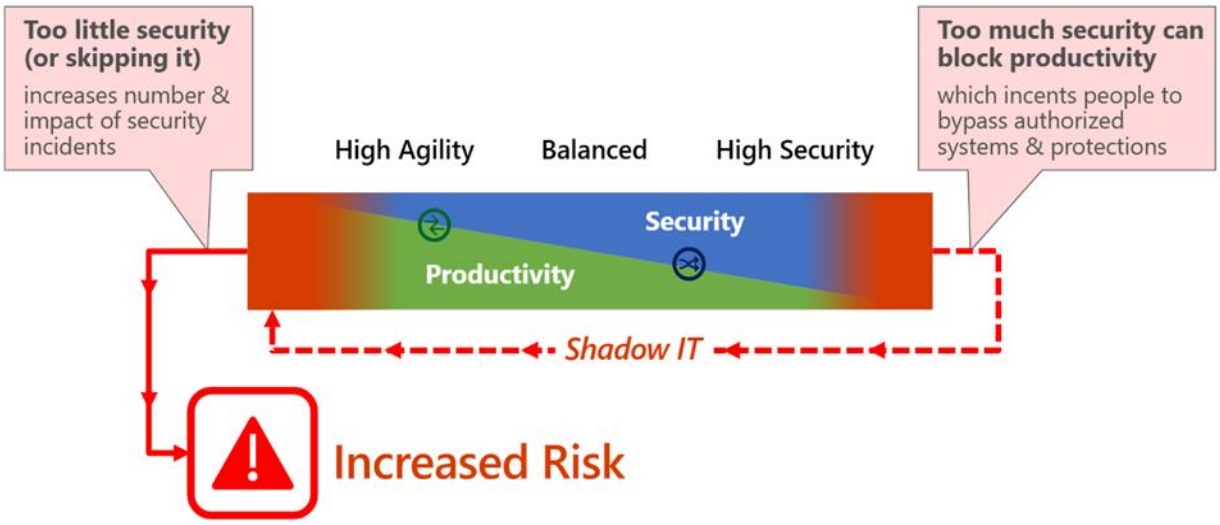
Most business applications have few controls to stop attackers once they get in. Some attackers are insiders who have permission to use the systems. They know how to avoid the built-in controls and exceptions in your organization. They don't always make drastic changes to data or processes. The hardest attacks to detect are the ones that make minor adjustments that benefit them but harm you.

You can't rely on monitoring the activities of your business applications to spot problems. You need to connect them with other data sources to find and respond to activities that might otherwise go unnoticed.

Your security team might not know much about your business applications and how they work. The business application users know their processes well, but they might not have the security skills and awareness to recognize threats. All this can leave gaps in your security efforts.

Low-code platforms let users from different parts of the organization build business applications. These users know their business processes well, but they might not have much technical experience. They need extra guidance to make sure that they use the right security controls and guardrails to protect organizational data and processes from harm.

Organizations need to find the right balance between security and productivity. They need enough security to keep their assets safe, but not too much security that slows down their work. Users who feel frustrated by security measures they don't understand the need for might try to work around them to get things done faster.



Top 10 low-code/no-code security vulnerabilities

Using a low-code/no-code platform for your business applications can reduce some security risks, but not all of them. These risks are common to any low-code/no-code platform. You need to address them by using both the security features in the platforms and the security processes in your organization.

The Open Worldwide Application Security Project® (OWASP) is a nonprofit foundation that works to make software more secure. It has identified the top 10 low-code/no-code security risks that you should know about if you use low-code/no-code solutions. OWASP updates the list based on feedback from the security community. Here's the current list:

- Account impersonation
- Misuse of authorization
- Data leakage and unexpected consequences
- Failures of authentication and secure communication
- Misconfigured security
- Injection handling failures
- Vulnerable and untrusted components
- Failure to handle data and secrets properly
- Failure to manage assets securely
- Failures of security logging and monitoring

On the OWASP website, you can view full details, including a description of each risk, example attack scenarios, and how to prevent them. The guidance that OWASP provides is general and applies to any product and organization. You need to tailor it to your specific situation.

In the rest of this paper, we'll show you how to use the security features of Power Platform with your governance and SecOps processes to address these challenges in your organization.

Microsoft security foundation

Organizations don't exist in isolation. They work with each other and their customers. They form the vital supply chains we all depend on. We need to work together to protect our people, data, and infrastructure. Microsoft will be bold with a comprehensive approach to security that is end-to-end, best-in-breed, and AI-powered.

Microsoft works toward this goal by focusing on tools and capabilities that support the following high-level goals:

- **Protect everything.** Keep your entire organization safe with integrated business security solutions that work well across platforms and cloud environments. This goal includes making your organization's Power Platform solutions part of your protected resources.
- **Simplify the complex.** Prioritize the right risks with management tools that make the best use of the human expertise in your company. Show the security management of Power Platform business applications in your management tools so that it doesn't add more complexity.
- **Catch what others miss.** Use leading AI, automation, and expertise to find and stop cyberthreats fast and fortify your security position.

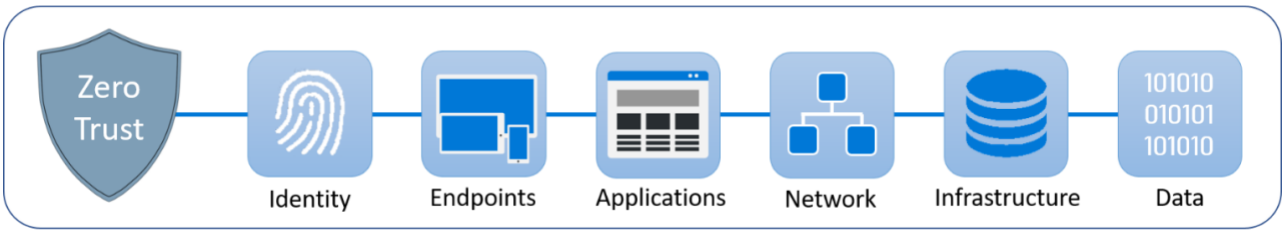
These security goals drive the innovation in the following Microsoft integrated security products.

- **Microsoft Defender:** Stop cyberattacks on your devices, identities, apps, email, and clouds with industry-leading extended detection and response (XDR) products.
- **Microsoft Sentinel:** Stay ahead of cyberthreats with AI-powered security information and event management (SIEM) that aggregates data from your entire enterprise to give you unmatched visibility.
- **Microsoft Entra:** Verify every identity and access request across your clouds, platforms, and devices with a unified set of identity and access products.
- **Microsoft Purview:** Protect data wherever it is with information protection, governance, and compliance products that are designed to work together.
- **Microsoft Priva:** Respect customer and employee privacy with products that reduce risk and manage compliance on a single platform.
  Microsoft Intune: Strengthen device security and enable seamless hybrid work experiences with a family of endpoint management products.

These products work together to form a stronger defense. Microsoft Power Platform builds on this foundation to add security to the business applications you make.

Together, these products can help you adopt a Zero Trust end-to-end strategy for not only your basic productivity applications but also your business applications that are built on Power Platform.

A Zero Trust strategy will monitor and control the six main pillars of security: identity, endpoints, applications, network, infrastructure, and data.



Zero Trust is a multilayered approach to security. In this paper, we'll show you how the Power Platform business applications that you build can join in multiple layers of security.

Zero Trust isn't a product. It's a strategy you need to follow to gain the benefit. At the core of the strategy are the following Zero Trust principles:

- **Verify explicitly.** Zero Trust requires strict identity verification for every user and device that wants to access resources. With Zero Trust, the identity verification of users and devices is an ongoing process, often at multiple levels. This makes sure that you always check and confirm who can access what.
- **Use least privilege access.** Make sure that user access is limited, with just-in-time and just-enough access. This means only giving access to systems and applications to authorized users for specific tasks for a short time.

- **Assume breach.** Assume that attackers are already in your network and are trying to move around and get more information. It uses a deny-all approach and real-time monitoring to compare every request with known behaviors to limit and control access. Assume breach is the mindset of creating the necessary separation of access to keep the damage in a small area, and by doing that, minimizing the impact on your business.

As you read the rest of this paper, you'll see how many of the Power Platform security features can help you adopt a Zero Trust strategy.

Power Platform overview

Microsoft Power Platform gives you a comprehensive set of tools and technologies that help you make and update your applications quickly and effectively. Power Platform lets you build and deploy custom

applications with a low-code approach, which means you don't need much coding or development work. This lets business users and citizen developers take an active role in the modernization process, speeding up application delivery and reducing their dependency on IT teams.

Power Platform components

Each product in the Power Platform family has a different focus area, so you can use them individually or together based on your needs. When you use them together, the interconnections between the products make them work seamlessly together. The products try to use the same security concepts and features when they can. Here's a high-level description of what each Power Platform product can do.

- **Power Apps:** Power Apps lets you build custom apps fast. You can use data and services from more than a thousand connectors in your app. The apps can run in the browser, on the desktop, or on mobile devices.
- **Power Automate:** Create automated workflows that work with services using connectors. Power Automate can use digital process automation (DPA) to automate processes in applications that have an API. When connectors aren't available, you can use robotic process automation (RPA) to automate repetitive tasks that you do in a browser or the user interface of a Windows app. Your workflows can run when something happens in other systems and services or schedule them to run at a specific time.
- **Power BI:** Power BI helps you find and understand insights from your organization's data. You can use automated machine learning to make predictions, AI visualizations to drill down into root causes, and Q&A visualization to ask questions about your data. Power BI isn't covered in-depth in this paper. Refer to Power BI security white paper for details.
- **Power Pages:** Power Pages lets you make data-driven, low-code websites that users inside and outside your organization can use. You can quickly make websites that support business processes like getting permits and licenses and reporting outages. You can also show data that's relevant to the business process and specific to each user.

Power Platform concepts

Besides the products above, some other features and concepts are important to know the platform's capabilities. Here are the ones you need to understand.

- **Connectors:** Connectors are key to the strategy for making low-code and traditional coding work together. Connectors are a wrapper around an API that lets Power Apps and Power Automate use the services behind the API. You can use more than a thousand connectors that are already made, or you can make your own for any RESTful API. The connector definition includes the information you need to make the API easy for low code to use. For example, you could make a custom connector for an internal microservice to let apps and automations use it while keeping the back-end data safe.
- **Dataverse:** Dataverse is a cloud-scale data store that works with different types of data and is built on Azure data management services. Dataverse makes the underlying services simpler to offer a secure place for business data. You can define business rules and logic on the data and use them in

apps and APIs that use the data. You can make external data look like a Dataverse table with virtual tables. Dataverse has built-in support for multi-language and multi-currency apps. The Dataverse metadata helps you make applications quickly from the data model, making it one of the fastest ways to build an application that shows data in a form.

- **AI Builder:** AI Builder and Power Platform Copilots are a key part of using AI to build solutions and adding AI to Power Platform solutions. AI Builder is a platform feature that lets you easily add AI to Power Automate and Power Apps. With AI Builder, you can use many Azure Cognitive Services from low code, but you can also train custom models with low code ways to support Power Platform solutions.
- **Copilot:** Copilot gives you AI-powered help across Power Platform to make users and developers more productive. Developers can build low-code apps faster by using Copilot to frame the low-code resource first. Copilot can also help developers do things like making a screen that adjusts to different devices with a specific layout, just by asking in natural language. Developers can also add copilots to apps to let users talk to them to understand data. Users access to data through Copilot with the same authorization systems as the rest of Power Platform.
- **Environments:** Power Platform environments are spaces to keep Power Platform resources and let administrators manage and secure them. For example, a simple implementation would have an environment for development, test, and production. You can make environments Managed environments, which let you set up more security features.
- **Dataverse solutions:** The Dataverse solutions framework lets you use solutions as containers to track and manage customizations in an environment with Dataverse. This includes flows, canvas and model-driven apps, table metadata, forms, views, and other resources you need to run the app, including code assets that developers made. A solution starts in a development environment where the app or a flow is created, and then you can use it to move the contents to other environments like test and production. Solutions let you control code sources and do other tasks that are part of an application lifecycle management (ALM) process. You can use the solution checker to check for performance, security, stability, and reliability problems with the solution contents.
- **Power FX:** Microsoft Power FX is the low-code language for expressing logic in Power Platform. Inspired by Microsoft Excel formulas, it's a language that has clear types, states what to do, and uses functions. Power FX is open-source[1], so you can use it for any purpose.

Power Platform adoption

The low-code development features in Microsoft Power Platform help you build and deploy modern applications quickly. These features can help your organization adapt quickly as business needs and markets change.

As a security professional, you need to make sure that your organization uses Microsoft Power Platform in a way that follows your organization's security policies and compliance requirements.

[1] https://github.com/microsoft/Power-Fx

Every organization is different, but these are the steps that many organizations take as they add Power Platform to their security architecture:

- **Learn:** You're starting here with this paper as you discover what Power Platform can do for security. Your team can learn more using the many resource links in this paper.
- **Assess:** This is where you look at how you use Power Platform now. You should also check the current security settings as you will make plans to adjust them based on your needs.
- **Plan:** Using what your team learned and your organization's security policies and compliance requirements, you will develop a security plan.
- **Implement:** This is where you'll roll out the changes you need to follow your security plan. You must be careful not to disrupt any current Power Platform resources. You must also think about the training that users need to understand how to work within your security plan.
- **Monitor, review, adapt:** With the ever-changing security threat landscape and evolving business needs, you must keep your security plan up to date. You should include this process in any security plan and do it regularly to review and improve how you secure your Power Platform resources. You should also plan to use new features of Power Platform that continue to evolve as well.

Security development lifecycle

Developing secure software is important whether you use Power Platform or traditional coding techniques. In this paper, you'll learn about the platform's features that you can use to make your security position stronger. By using those features, you have set up guardrails to help users make solutions on the platform that follow your organization's security policies. You should combine these guardrails with a low code security development lifecycle (SDL) that focuses on the people and process parts that can make the solutions you build more secure. Most of the time, users don't mean to build apps and automations with security problems. They just don't know better. Establishing an SDL that's right for low-code solutions can lead to more secure solutions with fewer and less serious vulnerabilities.

SDLs aren't one-size-fits-all. You have to tailor them to your own needs and include anything that's unique to your own risk and compliance requirements. Microsoft's Security Development Lifecycle consists of seven components, including five core phases and two security activities that support them.

The five core phases are requirements, design, implementation, verification, and release. Each phase has required checks and approvals to make sure that you meet all security and privacy requirements and best practices. The two supporting activities are training and response. Working with the users and teams as they start building solutions is a better way to collaborate than waiting until they want to get approval to deploy, and you stop them from going live.

Training

Training is one of the most important phases because many times the people who build the applications don't know the risks you're concerned about. If your organization does any training on how to build on Power Platform, you could add this to those efforts. Your training should include educating users about the types of data loss prevention policies you have established and other settings that might need to be

changed as they develop their solutions and how they should ask for those changes. This training is also where you teach them about the other phases and what to look for in their solutions to keep them secure. Make clear how you'll collaborate with them to move forward from each phase as they build their solutions.

Requirements

As the makers plan the solution is the best time for the team to consider the data the solution will handle, known threats, regulations, and industry requirements. The team should review with your security team to see if the proposed solution is feasible.

Design

In this phase, the team that's building the solution should check the security and privacy requirements and evaluate how they will affect their design. For example, they might decide to use Dataverse to store the data because it can protect the data with role-based column-level security. You can use threat modeling to document the design process more formally if your organization needs that. Your security team should be ready to help the design team with suggestions on how to solve security challenges for their requirements. The teams should agree on any security logging they need to add. The checkpoint for this phase is sharing the solution's security design and approving how to fix any security issues that are found.

Here are some examples of considerations that are related to security design:

- **Data security:** Make sure that all services that connectors or HTTP actions use are encrypted (HTTPS).
- **Error messages:** Avoid leaking sensitive data or giving information that could help someone work around security.
- **Access control:** Use Dataverse security roles that give users and applications only what they need to access Dataverse data. Avoid complicated security models that make people want to work around security blocks.
- **Hard coding:** Avoid putting URLs and keys in your code. For example, don't hard-code the URL or key to the back-end service in a Power Automate HTTP action. Instead, use a custom connector or an environment variable for the URL, and Azure Key Vault for the API key.
- **Security by obscurity:** Hiding columns on forms isn't security. Users can access the underlying data in other ways. Instead, use techniques like Dataverse column-level security to protect the data.
- **Elevated permissions:** Make sure that any automation that runs as a service account or service principal doesn't use elevated permissions to access or change data more than what the user should be able to access.
- **Custom code:** All custom code should follow traditional secure coding practices and reviews. This includes Power Apps Component framework and Dataverse code plug-in logic.

Implementation

The implementation phase is where you configure or create the Power Platform resources and the design comes to life. Like traditional code, having reviews by peers and keeping security in mind can help you avoid common mistakes. Using any tools available can also help. For example, running the

Power Platform solution checker regularly basis can help you find problems earlier. Using automated testing tools like Power Apps Test Studio, you could create tests where appropriate to look for security issues that might be relevant.

Verification

Verification happens before the solution goes live to make sure that it follows the SDL. It should require that other people check the work, not the people who developed the code. Separation of duties is an important control in this step to make sure that no one can write and release code by themselves that could cause accidental or malicious harm. In this phase, you could use some of the following security checks:

- **Static code analysis:** You could use the solution checker for Power Platform resources and check the source code for potential security problems, including having passwords in code.
- **Credential and secret scanner:** Find places where credentials like passwords and secrets are exposed in source code and configuration files. This is a good time to review how connection credentials will be handled in production.
- **Fuzz testing:** Use bad and unexpected data to look for vulnerabilities and make sure that error handling works. This can be particularly important with solutions that include Power Pages.
- **Configuration validation:** Check the configuration of production systems against security standards and best practices.
- **Component governance:** Find and check open-source software for version, vulnerability, and legal obligations. There are more open-source Power Platform resources now, so don't overlook this step. When you can, talk about this in the design phase to avoid last-minute problems.
- **Penetration testing:** Microsoft performs extensive testing on the underlying platform components, but in some solutions, it would be proper to do more penetration testing at the solution level. Make sure that you follow the testing guidelines that we'll discuss later.

Release

After you finish all security tests and reviews, the solution is ready to go live. You should use repeatable processes that include the right approvals and actions done by the right people. You can use Power Pipelines or Power Platform build tools to make these automations that you can use again. Both tools let you set up continuous integration and continuous deployment (CI/CD) and when you need to, you can include approvals as part of the processes.

For solutions that are used in multiple Power Platform environments, using a safe deployment process that releases updates incrementally can help you find problems with the smallest group of users possible.

Response

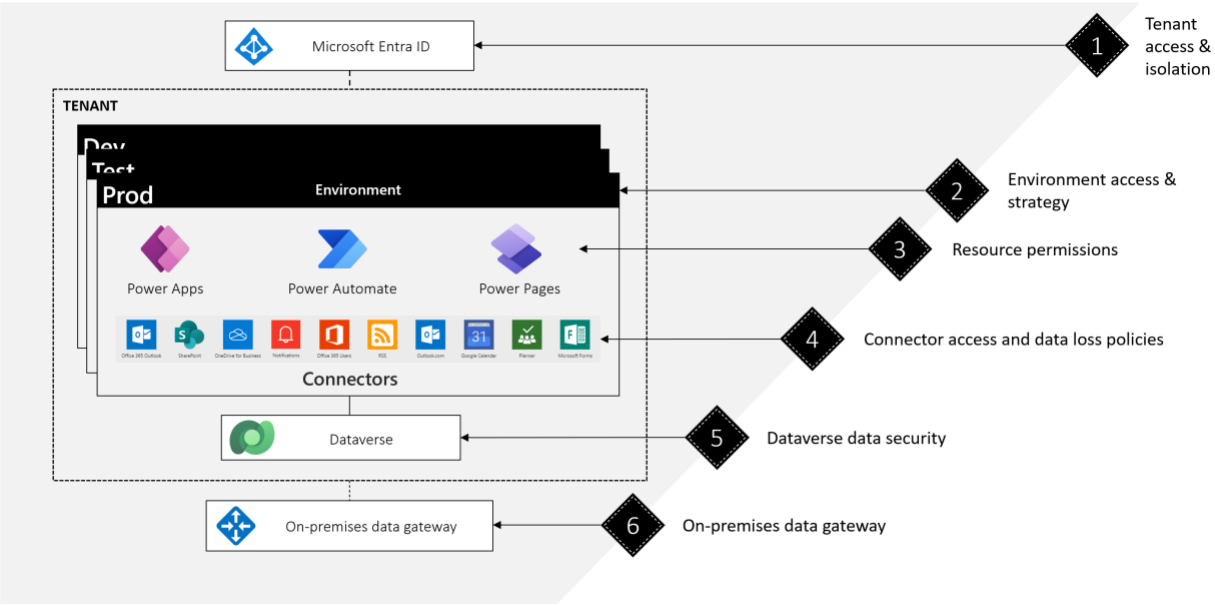
Response is how an organization handles a security problem that's caused by the solution. During the design and implementation, you should identify any logging you need. You should also talk about how security will monitor any logging after release and how you'll respond to a security incident.

You have to adapt your SDL to suit your organization's needs. You'll probably find that it needs to be flexible for different sizes of solutions and how important they are to your organization.

Power Platform security model

Power Platform has strong security because it builds on the foundation of broader Microsoft security features. Power Platform augments those features for quick and easy app development and deployment. If you work with Microsoft tools, you already understand how to secure your data and apps in Power Platform.

The Power Platform security model lets users do the work they need to do with the least amount of friction, while still protecting the data and services. It operates with multiple layers of defense, as shown in the following diagram:



The Power Platform security model includes the following layers to keep your apps and data safe:

- Users are authenticated by Microsoft Entra ID and their use follows conditional access policies.
- Users can only see and use Power Platform resources that their security roles make available to them or that have been shared with them.
- Security roles in environments control who can create apps and workflows.
- Power Automate flows and Power Apps canvas apps connect to other services with connectors. The connectors use the credentials and permissions of the connection.
- Environments that have a Dataverse instance have more advanced options to control access to data and services in that instance.
- Data loss prevention (DLP) policies can limit which connectors can be used together.
- Cross-tenant restrictions can block or allow connectors from other tenants.
- Data gateways can security connect Power Platform cloud resources with on-premises resources.

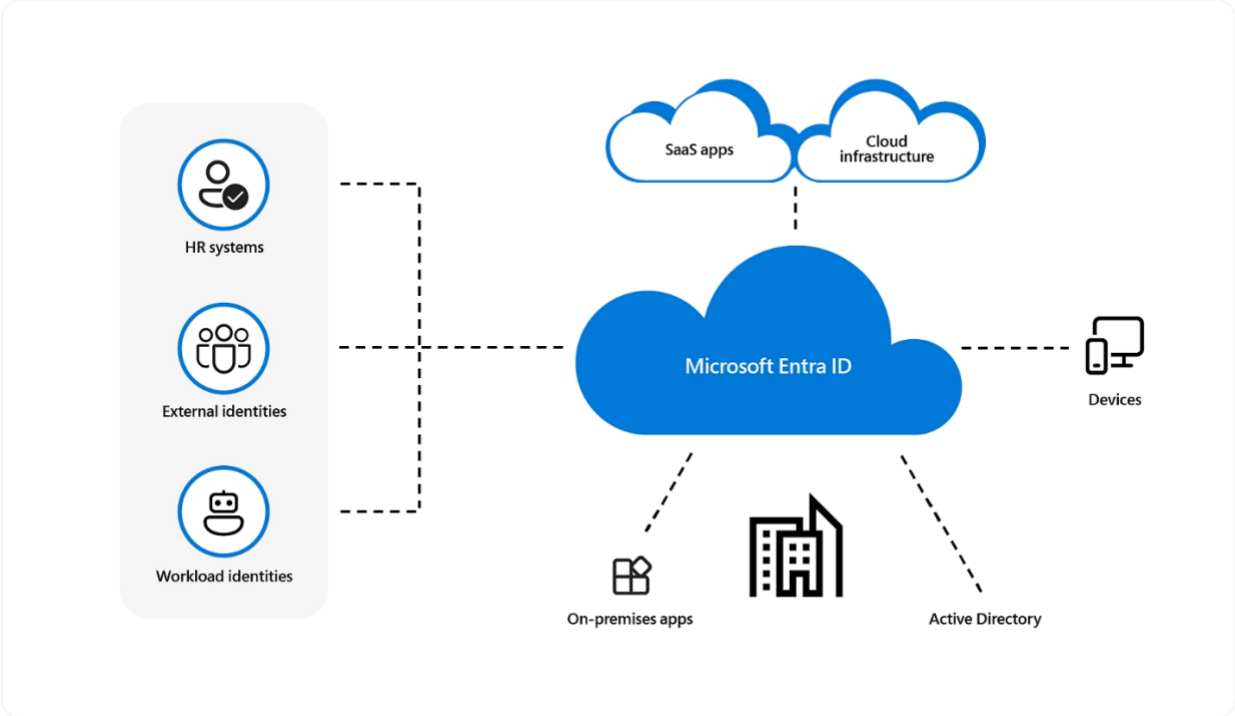
- Guest users can access Power Platform resources and environments with extra security measures.

Power Platform access controls

Access control is a vital part of how Power Platform keeps your apps and data safe. It makes sure that the right users—and only the right users—have access to Power Platform resources. In this section of the paper, we'll explore the ways you can set up access control and their role in your overall security strategy.

Microsoft Entra ID

All Power Platform products use Microsoft Entra ID (formerly Azure Active Directory or Azure AD) to manage who can sign in and what they can do. Microsoft Entra ID helps you protect and control identity for your hybrid and multi-cloud environments. Microsoft Entra ID is essential for letting business guests use Power Platform resources. Power Platform also uses Microsoft Entra ID to let other applications work with Power Platform APIs using service principals. Using Microsoft Entra ID, Power Platform can take advantage of Microsoft Entra ID's more advanced security features like conditional access and continuous access evaluation.



Service admin roles

Microsoft Entra ID has a set of admin roles that let you delegate administrative tasks without granting global admin privileges. The two main admin roles are:

- **Power Platform administrator:** This role can perform all admin functions in Microsoft Power Platform, regardless of security group membership at the environment level.

- **Dynamics 365 administrator:** This role can perform most admin functions in Power Platform, but only for environments where they belong to the security group.

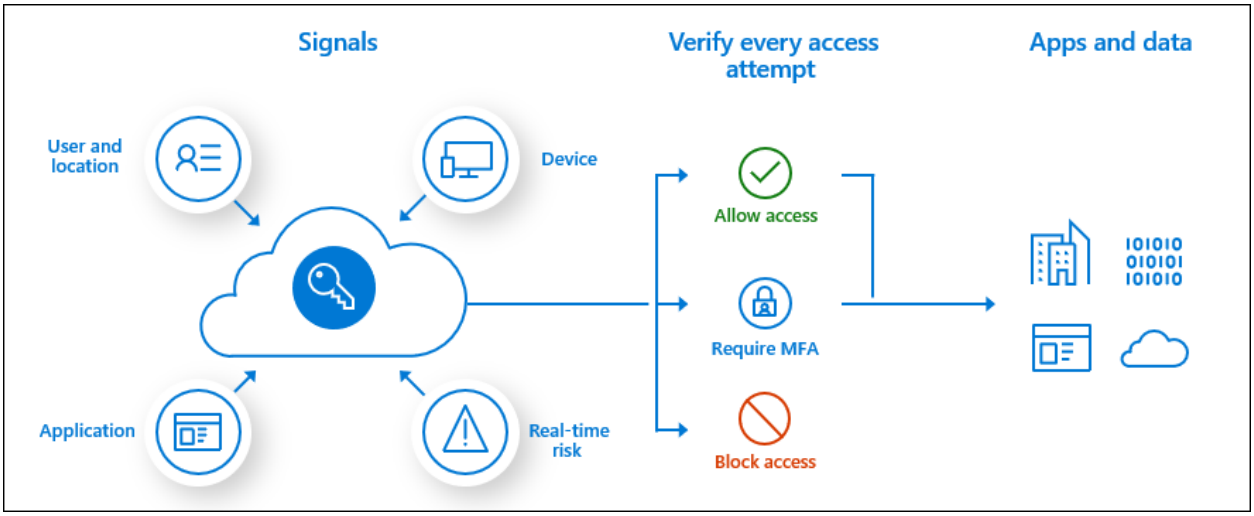
Neither of these roles can do tasks that only the Microsoft 365 global admin can do, such as managing user accounts, subscriptions, and access settings for other Microsoft 365 apps. You might need to assign additional roles to admins who need to perform those tasks. Review the permission matrix for more details of each role's privileges.

You can also use Privileged Identity Management (PIM), a feature of Microsoft Entra ID, to manage, control, and monitor the use of these high-privilege roles. PIM lets you grant just-in-time access to these roles and can incorporate your policies and procedures, such as approvals and justifications. PIM for Power Platform is in public preview. Check the release plan for its general availability date.

Conditional access

Conditional access, a feature of Microsoft Entra ID, lets you apply policies based on signals about the user's situation. These signals help you assess the risk level and enforce appropriate actions. Conditional access policies, at their simplest, are if-then statements that define what users must do to access a resource. For example, you can require users to use multifactor authentication if they want to access a Power Apps canvas app that tracks a compliance process.

The following diagram illustrates how signals are used to decide what action must be performed to access the target apps and data:



You should plan how to use policies to enforce your security guidelines for Power Platform. For example, you can use a policy to limit Power Platform access to specific users or conditions, such as where they're located, the device they're using and the apps that are installed on it, and if they use multifactor authentication.

Conditional access is very flexible, but that flexibility can allow you to create policies that have undesirable results, including locking your own admins out. The planning guide can help you think through how to plan for using conditional access.

Continuous access evaluation

Continuous access evaluation is a feature of Microsoft Entra ID that monitors certain events and changes to decide if a user should keep or lose access to a resource. Unlike OAuth 2.0 authentication, which only checks access token expiration, continuous access evaluation checks critical events such as credential changes or high user risk and network location changes in real time. These checks can trigger early termination of active sessions or require reauthentication. For example, if a user account is disabled or moves to an untrusted network, they should lose access to the app.

Right now, only Dataverse supports continuous access evaluation in Power Platform. Microsoft is working to add support to other Power Platform services and clients.

As organizations continue to adopt hybrid work models and cloud applications, Microsoft Entra ID is a key primary security perimeter that protects users and resources. Conditional access extends that perimeter beyond a network boundary to include user and device identity. Continuous access ensures that access is re-evaluated as events or user locations change. By using Microsoft Entra ID with Power Platform products, you can apply consistent security governance across your application portfolio. Review these identity management best practices for more tips on how to use Microsoft Entra ID with Power Platform.

Authentication in Power Pages

Power Pages handles authentication differently from other Power Platform services because it's designed to create sites for both external and internal users. You can select an authentication provider for each site or allow anonymous access. Power Pages authentication is based on Microsoft Identity Platform, which offers identity-as-a-service and supports authentication and authorization with standard protocols such as OpenID Connect, SAML 2.0, WS-Fed, and OAuth 2.0. Review the list of common identity providers for how to set up each one with Power Pages.

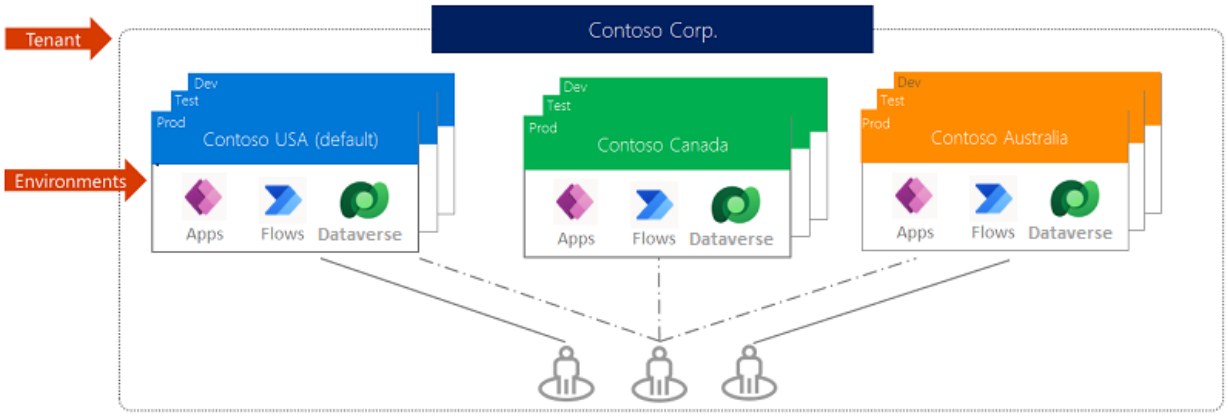
Authentication in Microsoft Copilot Studio bots

Microsoft Copilot Studio (formerly Power Virtual Agents) also handles authentication differently from other Power Platform services because it's designed to create conversational agents for both external and internal users. Authentication allows users to sign in, giving your bot access to protected resources or information. Users can sign in with Microsoft Entra ID or any OAuth2 identity provider, such as Google or Facebook. You can choose the type of authentication for each bot in its settings. This flexibility allows you to match the authentication to your use cases. Review the user authentication options and how to configure them. Power Platform admins can also apply data loss prevention policies and turn off the publishing of bots with AI features at the tenant level.

Power Platform environments

Environments are containers where you can store and control Power Platform resources, such as apps, automations, and connections. Environments help you protect your resources and data from unauthorized access. They are created in a Microsoft Entra ID tenant and tied to a geographic location, which can help you comply with data location requirements. The location of an environment determines the geographic location of any component you create in it.

You can also create a Dataverse database in an environment. Each environment can have only oe Dataverse database. When you use Dataverse in an environment, you can apply more detailed security controls, such as complex business application security models.



Power Platform creates a default environment in each tenant. You can't delete this environment, and all employees can access it. You can take steps to increase the security and governance of the environment. For example, you can restrict sharing with everyone and apply data loss prevention policies such as limiting or blocking connectors. Review how to secure the default environment for more steps you can take. You can also use environment routing to direct makers to their own separate developer environments. Pipelines in Power Platform can automate and control the promotion of resources from development to other environments. Pipelines can include review and approval gates to enforce any security and governance rules you want to apply.

You can create different types of environments to manage your Power Platform resources according to your security, compliance, governance, and user needs. Your capacity and the type of environments you create limit how many environments you can have. You can choose from several types of environments (production, sandbox, trial, developer), each with different features and purposes. From a security perspective, production, sandbox, and trial environments provide similar options for admins to control access. The other types have the following differences:

- **Default:** All new users can create resources in this environment. Review how to secure the default environment for how to apply specific controls.
- **Developer:** Personal environments only for the owner's use. You can't assign security groups to developer environments.
- **Dataverse for Teams:** Special environments that are linked to a specific team the first time an app is installed or created in it. Security depends on the team's membership type. Learn more about Dataverse for Teams environments.

You can use the Power Platform admin portal to restrict who can create environments in the tenant, such as only global admins, Dynamics 365 admins, or Power Platform admins. You can set different permissions for production and sandbox environments, trial environments, and developer environments. For example, you might let users create their own developer environments but not the other types.

Managed Environments

Managed Environments is a set of premium features that you can turn on in an environment to make it easier to manage at scale. When you turn on Managed Environments, you can use the premium governance and security features of Power Platform to get more visibility and control with less effort.

Managed Environments isn't a separate license. It's an entitlement that's included in the standalone Power Platform licenses. Managed Environments is turned off by default. When you turn it on, you unlock several security and compliance features, such as:

- Limit sharing
- Data policies
- IP firewall
- IP cookie binding
- Customer-managed keys
- Lockbox
- Data loss prevention policies for desktop flows
- Extended backups
- Solution checker enforcement

Microsoft adds new features to Managed Environments often. Review the full Managed Environments feature list for the latest information.

Environment groups

When you activate Power Platform in your organization, you can create different environments for different purposes. You might want to group some environments together and apply the same rules to them. A new feature allows you to place environments into logical groups and apply a common set of rules. When a new environment is created manually, you can place it in an environment group and the rules are applied automatically.

You can use environment routing with groups so that when a new maker creates a developer environment, it's automatically added to a designated group and follows the group's rules. This feature helps you maintain consistency and security for developer environments.

Environment strategy

You should have a strategy for how to create and manage your Power Platform environments. Your strategy should meet both security and compliance requirements and operational and administrative needs. It should support the application lifecycle management (ALM) processes of the different solutions you build on Power Platform. A good strategy is one that you share clearly with your users and that has the tools and processes to support the productivity of the users who are building apps and using the Power Platform.

A good starting point for your environment strategy is to make changes to control your existing environments and the creation of new ones. Take the following key steps:

- Assign your admins to the Power Platform and Dynamics 365 roles.
- Restrict creation of new environments.
- Establish a process for users to request new environments.
- Use security groups to protect environments.
- Establish data loss prevention (DLP) policies at both the tenant and the environment level.
- Minimize the use of the default environment by using environment routing to send makers to their own separate developer environments and don't use it for business-critical apps and automations.
- Use environment groups and rules to apply settings to many environments at once and pipelines to make deployment from the default environment to other environments easier.

You might need to isolate users, resources, and data into separate environments for security or data compliance purposes. You can use Microsoft Entra ID security groups to make sure that users can access the proper environments, resources, and data. You can use environment automation tools to manage many environments at once. But as a rule, you should aim to have fewer environments rather than more. Review how to develop an environment strategy for a more in-depth discussion.

Tenant Isolation

Tenant isolation is a feature of Power Platform that lets you control how connectors that use Microsoft Entra ID authentication can access data from other tenants. By default, tenant isolation is off and connectors can access data across tenants unless you have other data policies in place. Tenant isolation applies to all connectors that use Microsoft Entra ID authentication. You can't choose different settings for different connectors, but you can use data loss prevention policies for that. You might want to turn on tenant isolation and define DLP policies for more detailed control of specific connector usage.

When you turn on tenant isolation, Power Platform blocks all cross-tenant connections. Admins can make rules that can allow some connections to ignore tenant isolation. These rules can allow inbound, outbound, or both between your tenant and another tenant. Admins can use a wildcard ("*") to apply the rule to all tenants.

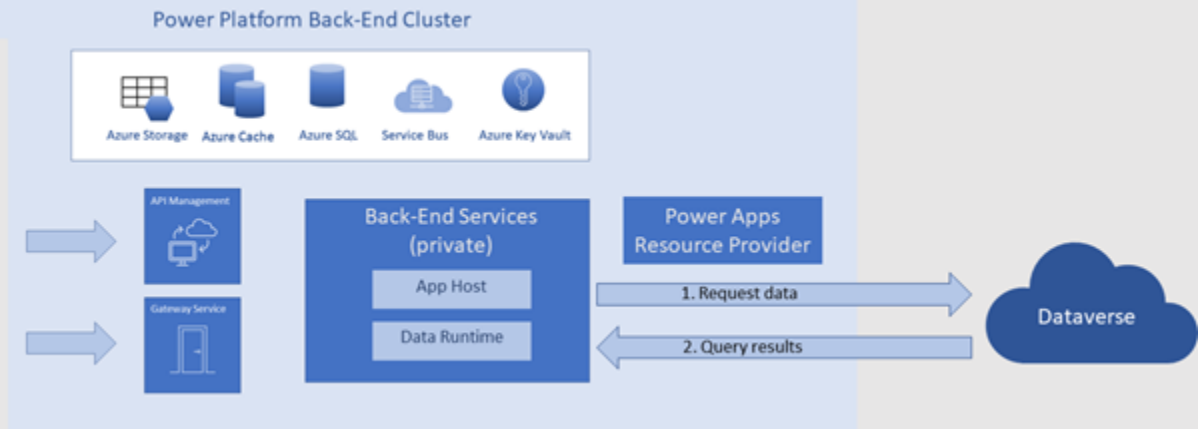
When you turn on tenant isolation, it can affect existing apps and automations that have cross-tenant connections. These resources will stop running correctly. New attempts to create apps and automations that violate the tenant isolation policies will be stopped during the development stage, preventing the connection. Turning on tenant isolation early in the adoption of Power Platform can help minimize the impact on users. You can use cross-tenant isolation reports to assess the impact and add exception rules ahead of time.

Network security

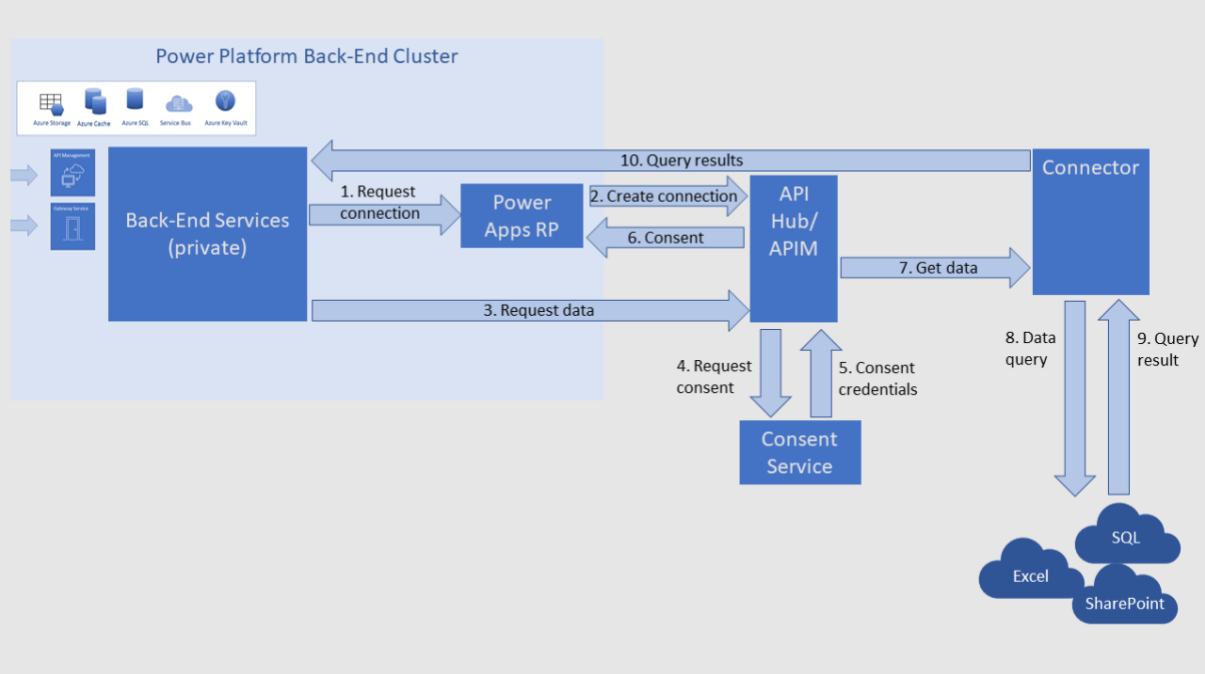
Power Platform service architecture lets you build end-to-end business app solutions that can use data from both internal and external services with connectors. Many solutions can also connect to your organization's on-premises and cloud resources. In this section of the paper, we'll explore the network security features of Power Platform and help you learn how to fit Power Platform services and solutions into your network security design.

Data source connections

Power Platform services use different methods to connect to external data sources, but the general pattern is similar. From the perspective of a maker building an app or automation, they access data and services by setting up a connection with a connector. Behind the scenes, Power Apps canvas and model-driven apps connect directly to Dataverse without needing a separate connector. This lets the Power Apps back-end service ask for data directly from Dataverse using a Power Apps resource provider. Power Automate authenticates using an API Hub, but all data interactions after that are also direct to Dataverse.



For connections to other external data sources, Power Platform services use an [Azure API Management] connector, as shown in the following diagram:



Users authenticate to the Power Platform service first, then, separately, to a data source using the credentials the connector requires. The API Hub credentials service always stores and manages credentials.

Authentication to a data source is specific to that source and depends on the method the maker chooses when they create the connection. Power Apps offers two types of data source authentication methods:

- **Explicit authentication:** The app uses the app user's credentials to access the data source.
- **Implicit authentication:** The app maker provides credentials for the app to use.

We recommend using explicit authentication when possible. It's more secure and doesn't give the app user elevated permissions when they use the app. Learn more about the differences between explicit and implicit authentication.

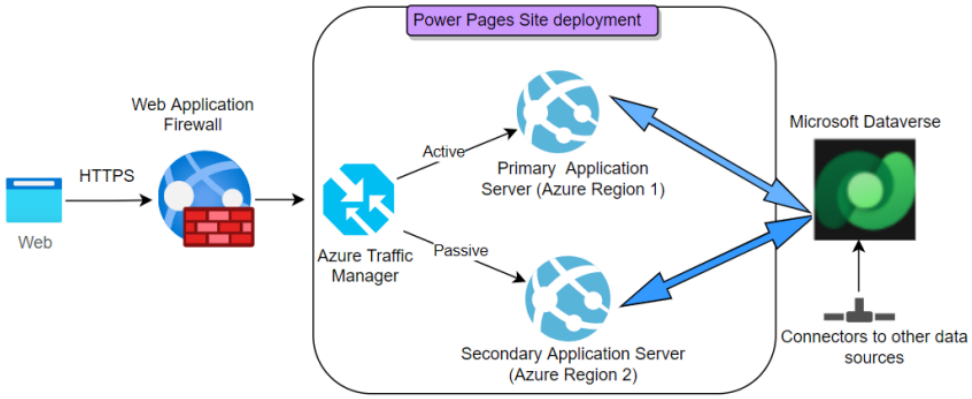
Mobile platforms

Power Platform mobile applications use the same connection and authentication sequences that browsers use. Android and iOS apps open a browser session in the app and support certificate-based authentication. Windows apps use a broker to establish a communication channel with the Power Platform services for the sign-in process.

Protecting Power Pages

Power Pages is different from some other Power Platform services in that it lets you create websites that face the outside world. But like other Power Platform services, Power Pages runs on Azure, so it benefits from Azure's scalability, reliability, and security features.

You can make your Power Pages websites even more security by using Azure Web Application Firewall to monitor, filter, and block malicious requests.



Web Application Firewall policies are based on Azure Front Door profiles with prevention mode turned on. In prevention mode, requests that match the rules that are defined in the managed rule set are blocked. Learn how to turn on Web Application Firewall for production sites in the Power Platform admin center.

Power Pages offers a subset of the Azure-managed DRS 2.0 rule sets. These rules give you more security against common threats.

Power Platform network service tags

Service tags represent a group of IP address prefixes from a service. You can use Power Platform service tags to control network access on network service groups, Azure Firewall, and user-defined routes. Service tags make it easier to manage address changes and network security rules updates.

The following are the service tags for Power Platform and Dynamics 365:

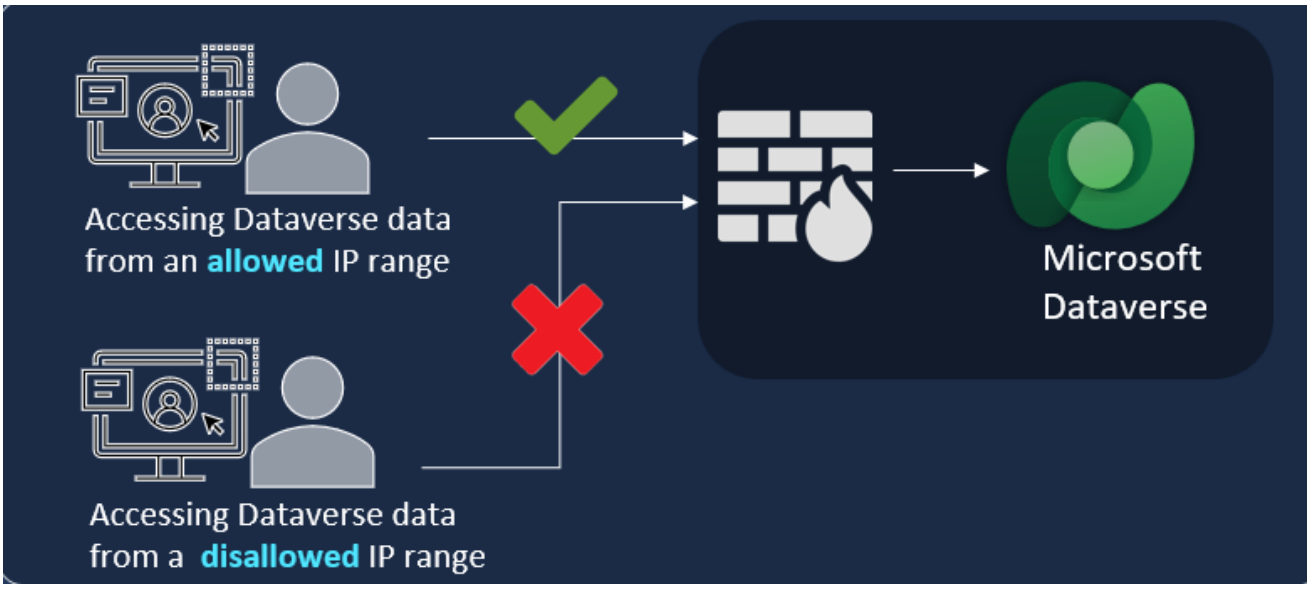
Tag	In/Out	Regional?	Azure Firewall
Dynamics365ForMarketingEmail	Both	Yes	Yes
Dynamics365BusinessCentral	Both	No	Yes
Power BI	Both	No	Yes
PowerPlatformInfra	Outbound	Yes	Yes
PowerPlatformPlex	Inbound	Yes	Yes

Refer to the full list of available service tags to find other service tags for the broader set of Azure services that might be helpful in configuring network security rules.

Connectors need access to the outbound IP addresses in your datacenter region. If your environment or firewall blocks these addresses, the connectors won't work. Most connectors use HTTPS port 443, but some use other protocols. Check the connectors you use to see what they need. IP addresses and service tags depend on the region and the environment where the app or flow is located. Refer to the full list of Power Platform IP addresses and service tags to set up your allow list correctly.

IP firewall for Power Platform environments

IP firewall is a feature that you can turn on and set up for managed environments. It protects your data in real time at the network layer, evaluating requests after they're authenticated and limiting access to Dataverse only to users from allowed IP locations.



The IP firewall feature helps you keep your data safe from requests from unauthorized network locations. For example, if you turn on the IP firewall and allow only your office network IP addresses to access Dataverse, a user can't get to Dataverse from other locations.

The IP firewall also stops token replay attacks. A user can't use an access token from a network location that's not allowed. The request will fail.

Since the IP firewall works at the network layer, it affects both apps and APIs that use Dataverse.

You can set up the IP firewall for each environment. This lets you choose which environments need more protection. For example, you might allow unrestricted access to your development environments, but limit access to your test and production environments.

Learn how to turn on the IP firewall in an environment.

Protect against cookie replay attacks

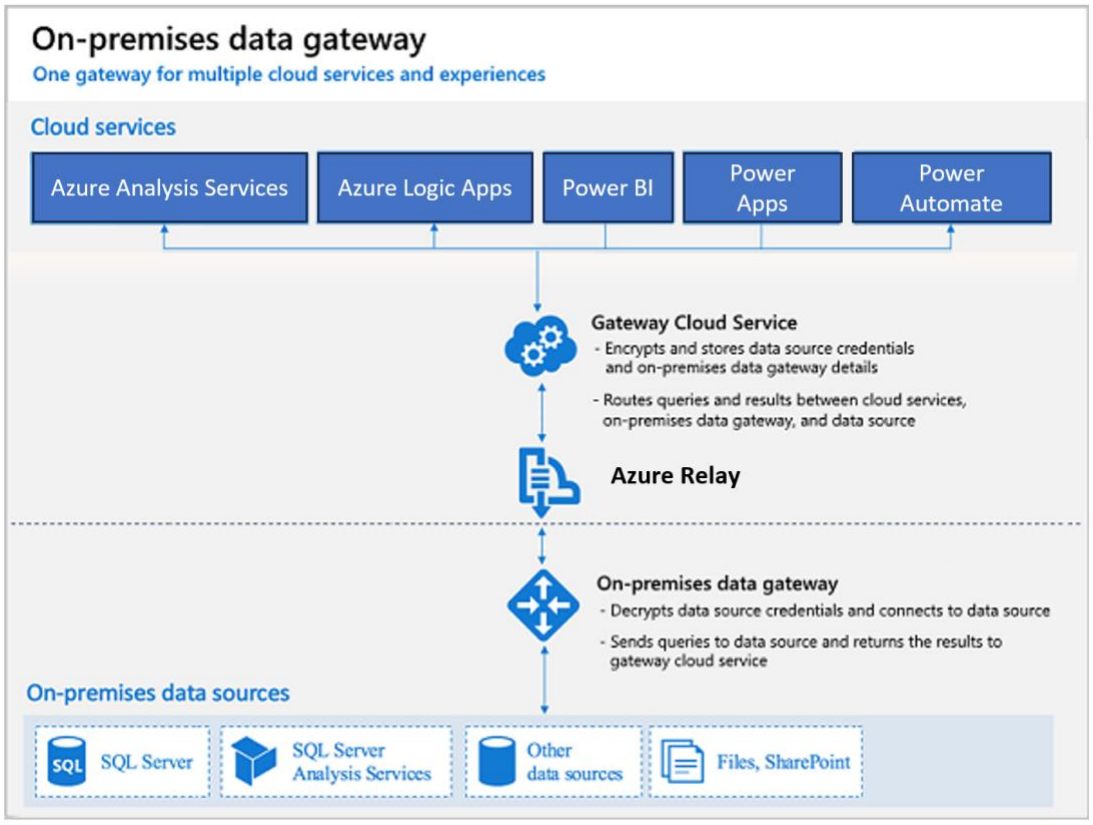
In a cookie replay attack, an attacker intercepts a valid cookie and uses it to impersonate the user who created it. Power Apps model-driven apps use a cookie called *CrmOwinAuth*. You can turn on IP-based cookie binding to protect it. IP-based cookie binding is a feature of Managed Environments. When you turn it on, it compares the IP address of the cookie and the IP address of the request. If they don't match, it blocks the request and shows an error message.

A different IP address doesn't always indicate an attack. Sometimes, the user changes their network connection and gets a new IP address. For example, a user works on a laptop in the office. The cookie is created with the office IP address. Then the user goes to a customer location and connects with a VPN. The VPN is assigned a new IP address. Since the IP address is different from when the user was working in the office, the user has to sign in again if IP-based cookie binding is turned on.

Connect Power Platform to on-premises resources

The on-premises gateway allows Power Platform cloud apps and automations use on-premises resources securely. You can use a gateway to connect to on-premises data from sources like a file system, DB2, Oracle, SAP ERP, SQL Server, and SharePoint. The gateway uses Azure Relay to allow access to on-premises resources securely. Azure Relay can securely expose services inside your network to the public cloud without having to open a port on your firewall. The gateway uses these outbound ports: TCP 443, 5671, 5672, and 9350–9354. The gateway doesn't require inbound ports.

The following diagram illustrates how data flows from on-premises sources to cloud services through an on-premises data gateway, Azure Relay, and cloud data gateways.



One gateway can allow multiple users to access multiple data sources. You can control who can install an on-premises data gateway in your tenant, but not at the environment level. The following gateway roles manage the security of the gateway and its connections:

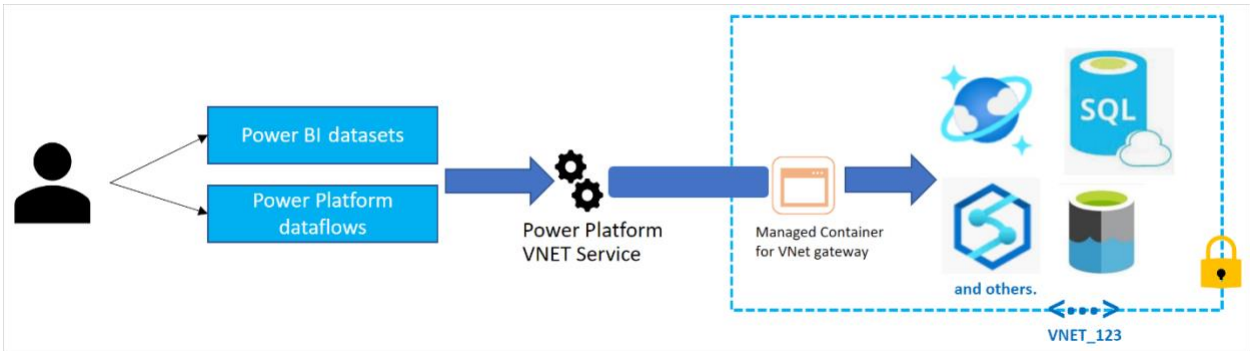
- **Admin**: Any user who installs a gateway is automatically assigned the admin role. An admin can manage and update the gateway, create connections to data sources, manage access to all connections, and manage other users on the gateway.
- **Connection creator**: You can create and test connections on the gateway, but you can't manage or update it or add or remove other users.
- **Connection creator with sharing**: You have the same permissions as a connection creator, plus you can share the gateway with other users.

For connections that you create for Power Apps and Power Automate, you can limit the connection types that are available to users when you assign the role. You can use your standard network controls on the gateway server to limit what data sources the gateway can access.

Clustering gateways can make them more reliable and faster for critical business needs. You can also use different clusters for different purposes, such as supporting the application lifecycle, dividing your organization, or isolating services. This approach can help you meet different compliance or security requirements for different data sources.

Virtual network data gateways

With virtual network data gateways, Power BI and Power Platform dataflows can connect to data services in an Azure Virtual Network without needing an on-premises data gateway on a virtual machine inside the virtual network. The following diagram shows an example:



Find a list of supported data services for Power BI datasets. Find a list of supported data sources for Power BI paginated reports. Find a list of supported data sources for Power Platform dataflows.

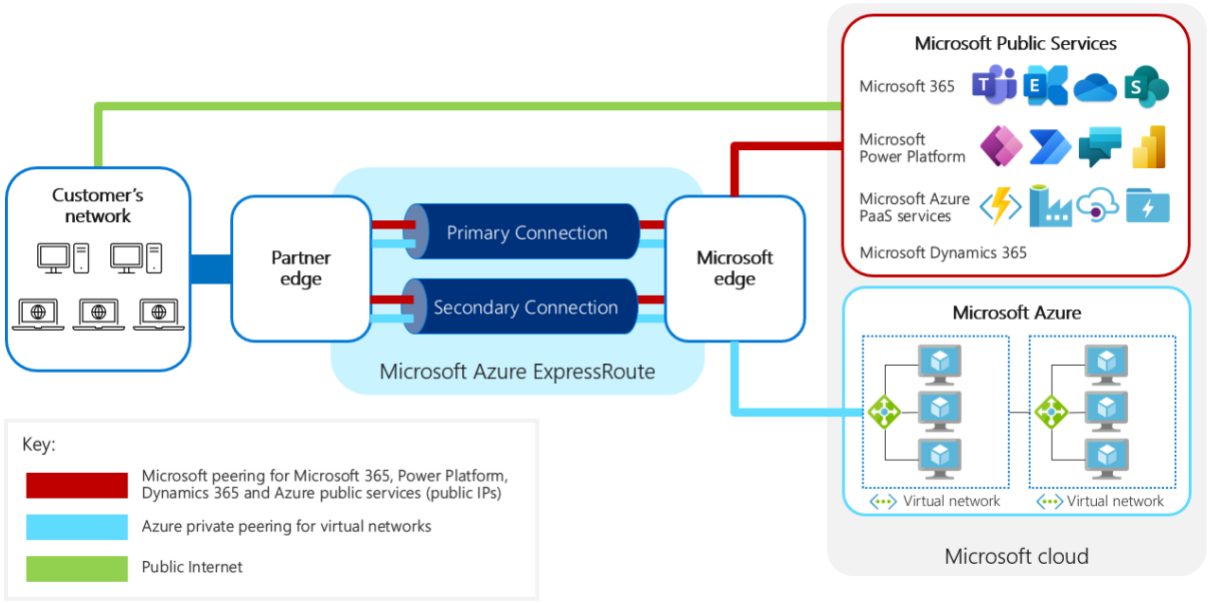
Azure Private Link

Azure Private Link and private endpoints in Azure network services allow Power BI to be accessed securely. Private endpoints send data traffic privately through Microsoft's backbone network infrastructure, not the Internet. Private endpoints make sure that your Power BI resources, like reports or workspaces, always use your private link network path.

Azure ExpressRoute

Azure ExpressRoute offers an advanced way to connect your on-premises network to Microsoft cloud services using private connectivity. You can use one ExpressRoute connection to access multiple online services, such as Power Platform, Dynamics 365, Microsoft 365, and Azure, without traversing the public Internet. ExpressRoute requires significant planning and configuration and costs more for the ExpressRoute service and the connectivity provider.

The following diagram illustrates an ExpressRoute connection:



ExpressRoute doesn't encrypt or filter traffic natively (unless you use ExpressRoute Direct with MACsec enabled). It only establishes a private connection between the Microsoft and customer datacenters through their connectivity provider.

Any request from any Microsoft online service or Azure service to the subnet that ExpressRoute advertises will use that circuit, no matter what the service or customer is. Because the request is routed at the network layer, you can't control it at the application level.

Microsoft services can be accessed directly over the public Internet because they use application-level authentication and authorization to control access. They also have infrastructure-level protection against attacks and threats. For on-premises services, you need to provide your own protection when they receive traffic from Microsoft services across an ExpressRoute connection.

You might face a challenge if you want to use ExpressRoute for some Microsoft cloud services but not others. The peering options give you some control, but they don't let you choose specific services of the same peering type (for example, to enable routing only to Azure virtual machines but not to Microsoft 365). You can use Border Gateway Protocol (BGP) communities to route traffic for certain services only. This applies to Power Platform services that have a Microsoft 365 presence. You might want to route some of them through ExpressRoute but not all, or only some Microsoft 365 services like Teams.

Because some Power Platform services are part of Microsoft 365, they need some shared services, such as the admin portal and authentication. You can't protect all these services with ExpressRoute. For example, the Microsoft 365 admin center doesn't use ExpressRoute. ExpressRoute also doesn't work between Power Platform and Azure services.

You might still need the on-premises data gateway to connect to on-premises systems with ExpressRoute. The gateway has features that change the data format. For example, with SQL Server, the on-premises data gateway converts OData requests to SQL statements.

Power Platform uses Azure Content Delivery Network to improve performance and user experience for static content like images and icons. This content doesn't use ExpressRoute, so it goes over the public Internet. But this content doesn't have any customer data, so you don't need to protect it with private networks like ExpressRoute. For canvas apps, you can turn off Content Delivery Network with a setting called *Load default static content* if you have firewall or IP list issues. This setting doesn't apply to model-driven apps because they don't use Content Delivery Network.

Data protection

Your business application data is one of your most valuable and vulnerable business assets. You need to protect it from threats inside and outside your organization. You need to secure it when it's stored and when it moves. You need to control who can access it. Power Platform has features that you can set up to help prevent data leaks and protect data at rest.

To protect your data, you need to know what data you have. Keep a list of your sensitive data. You can use tools like Microsoft Purview to scan, classify, and label sensitive data. Microsoft Dataverse has built-in integration with Microsoft Purview.

With Microsoft Purview, you can create an up-to-date view of all your data sources, including the data in your Power Platform Dataverse environments. Microsoft Purview can sort your data assets by built-in or custom categories to help you understand what data your makers have in their Dataverse environments. For example, Microsoft Purview could tell you if a maker has added sensitive data like government IDs or credit card numbers. Then you can either tell the maker how to change the data to follow your policies or use safeguards to secure it.

In this section of the paper, we'll explore how Power Platform protects your data and help you understand your options for protecting the data that Power Platform services and solutions use.

Data loss prevention policies

Data that doesn't reside in a Power Platform data store like Dataverse flows in and out of apps and automations using a Power Platform connector. Connectors are essentially proxies for the application programming interfaces (APIs) of other services that allow Power Automate, Power Apps, and Logic Apps to interact with them. Connectors can be public or custom. Anyone can use more than a thousand public connectors, such as Microsoft 365 (formerly Office 365), SharePoint, Salesforce, and SAP. Microsoft, a verified publisher, or an independent publisher can create public connectors. Public connectors must pass Microsoft certification.

For APIs that don't have public connectors, you can create custom connectors. Custom connectors can work with internal or external APIs.

By default, makers can use any connector in their apps and automations. You can set up data loss prevention (DLP) policies to help makers follow your guidelines for using connectors. DLP policies act as guardrails to help prevent users from exposing data by mistake.

You can use DLP policies to make rules for using a connector or a connector's actions in a Power Platform environment. DLP policies can apply to the entire tenant or to specific environments. In your

DLP policies, you can classify connectors as business data only, no business data, or blocked. If you place a connector in the business data-only group, makers can only use it with other connectors in that group in the same app or flow. Makers can't use a blocked connector in any app or flow.

DLP policies work at design time to prevent makers from building an app or flow that breaks the rules. If you activate a DLP policy after a connector is already in use, the app or flow can't use the connector or connector action. DLP policies only affect how Power Platform resources use the connector. They don't block programmatic access directly to the API. To block the API completely, you need to use traditional network security techniques like blocking it at your firewall.

DLP policies can't block some connectors that support core Power Platform functionality or Office features, like Dataverse, approvals, and notifications. You can put them in business or non-business groups to control how makers use them with other connectors.

New connectors are added to Power Platform all the time. When they're added, they're placed in the default data group. If you don't change it, the non-business data group is the default group for new connectors. You can change the default group to business or blocked.

More granular control through connector actions and endpoint filtering

You can achieve more granular control by choosing which actions on a connector are allowed or not allowed. This option is for blockable connectors that you have added to a DLP policy's non-business or business data group. Using it, you might let makers use the "read" actions but not the "modify" actions on the connector. Connectors can get new actions when they're updated. You can set whether to allow or block new actions.

Another way to get more granular control is to use connector endpoint filtering to make rules about which endpoint values makers can use. Connector endpoint filtering applies to six connectors (HTTP, HTTP with Microsoft Entra ID, HTTP Webhook, SQL Server, Azure Blob Storage, and SMTP). The rules only apply when a maker uses a static value to specify an endpoint. For example, you could specify that in the test environment, the SQL Server endpoint can only be contosodev.database.windows.net*.

If you want to lock down an environment but exclude some resources, you can use PowerShell cmdlets to add them as resource exemptions. The DLP policy doesn't affect exempted resources. But be careful not to exempt too many resources, especially in environments where general users can change them. They could change them to use any connector.

Desktop flow policies

Power Automate has both cloud flows and desktop flows. By default, you won't see desktop flow actions in DLP policies. You can change this in the tenant settings in the admin portal. Effective January 2024, DLP policies for desktop flows apply only to Managed Environments.

You can create and enforce DLP policies to classify desktop flow modules and individual module actions as business, non-business, or blocked. This prevents makers from combining modules and actions from different groups in a desktop flow or between a cloud flow and the desktop flows it uses. For example, if you mark the Azure module as business and the AWS module as non-business, they can't be used together in a desktop flow.

In addition to DLP policies, you can use local Windows registry settings to make restrictions for desktop flows. Learn more about governance in Power Automate for desktop.

Effect of multiple DLP policies

Most organizations use both tenant and environment DLP policies. Policies are checked when you create and run resources and consider all the policies together. For tenant-level policies, you can choose which environments to include or exclude. If a policy blocks a connector and others don't, the connector is blocked. If you put a connector in business data only in one policy and non-business in another, which one it's treated as depends on what other connectors you use with it. The most restrictive grouping is when all the policies that apply to an environment are checked together.

The more policies that apply to an environment, the harder it is to understand why a connector isn't allowed. You should plan to have as few policies as possible that can apply to an environment.

You also need to think about how new policies affect existing resources. The new policy will be combined with the other policies, and resources will be checked again. Use some general policies for your organization and then deal with exceptions to reduce the impact.

Strategies for initial DLP policies

DLP policies should be one of the first things you set up when you take over an environment or start to support Power Platform. This way, you have a basic set of policies and then you can work on creating DLP policies for exceptions.

We recommend following these steps:

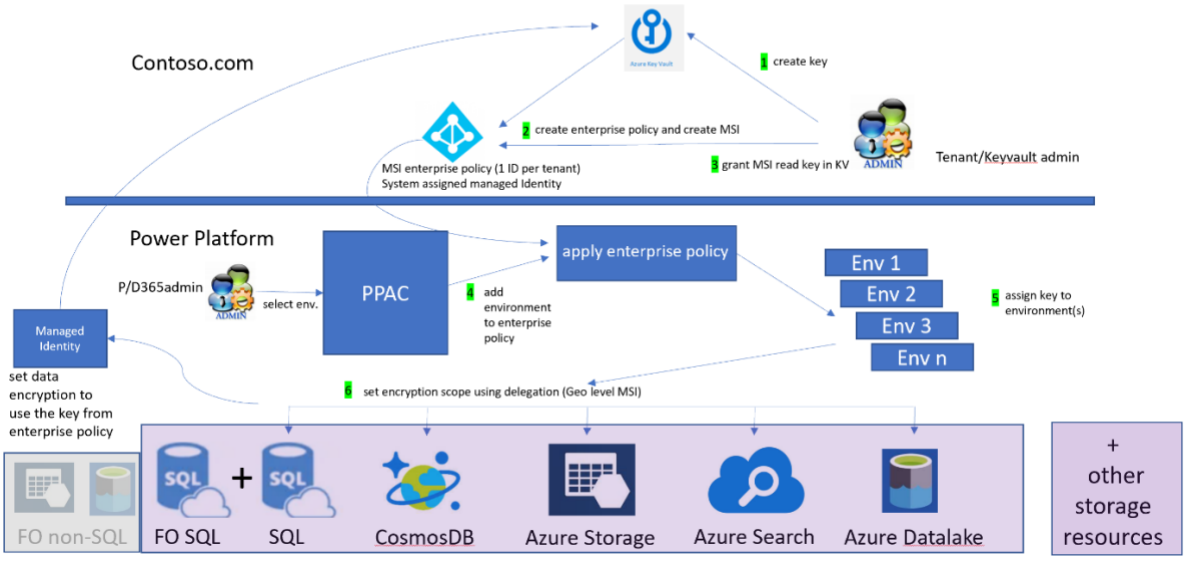
1. Create a policy for all environments that blocks all unsupported non-Microsoft connectors and classifies all Microsoft connectors as business data.
2. Create a policy for the default environment (and other training environments) that limits which Microsoft connectors are classified as business data.
3. Create more policies or exclude some environments from policies #1 and #2 that let certain connectors or connector combinations be used for certain environments.
4. In each policy, choose the default group for new connectors. In the custom connector section, choose any custom connector patterns that you want to allow or block.

Customer-managed encryption keys

Power Platform encrypts data both at rest and in transit with a strong Microsoft-managed key by default. Some organizations need more control over their data security and compliance, however, so we offer the ability to manage the encryption key yourself. The customer-managed key capability lets you use your own data encryption keys for your Dataverse environment. You can change or replace your keys whenever you want. You can prevent Microsoft from being able to access your data by removing the keys from the service at any time.

The following diagram illustrates the customer-managed encryption key process with Azure services and resources:

Customer Managed Key (CMK)



You can provide your own encryption keys from your Azure Key Vault. Microsoft doesn't have direct access to your Azure Key Vault. To let Power Platform services use your encryption keys, you need to create a Power Platform enterprise policy that allows Power Platform to read them from your Azure Key Vault.

You decide which Power Platform environments that have Dataverse you want to encrypt with your own keys. You need to enable them as Managed Environments first, then add them to the enterprise policy that references your encryption keys. If you want to change your encryption key, you need to create another enterprise policy and move the environments from the old policy to the new one. If you remove an environment from all enterprise policies, it goes back to using Microsoft-managed keys for encryption.

You can use different encryption keys for different Dataverse environments to separate your data more securely.

Customer-managed key rotation

If you use your own encryption keys for Power Platform data, you need to rotate them regularly to prevent service interruptions if the key version expires. To rotate your encryption keys, use a new key version and set a rotation policy. Rotating the key version doesn't affect performance or cause downtime. It might take up to 24 hours for all the resource providers to apply the new key version. Don’t disable or delete the previous key version for at least 28 days. The service needs it to re-encrypt the data and to support database restoration.

Lock and unlock Power Platform environments

You can revoke Power Platform’s access to your encryption keys at any time. Microsoft services immediately lose access to your customer data. Since you can use separate keys to encrypt different Dataverse environments, you can lock environments separately by revoking access to the appropriate enterprise policy. Only the Azure Key Vault admin can revoke key access and lock an environment.

Any one of several actions will revoke key access, such as disabling the encryption key or deleting the key vault. You should only take these actions if you intend to lock your environments. Don't revoke key access as part of your normal business process. When you revoke key access, all environments that are associated with the enterprise policy are taken offline immediately. Any users who were working in the environment will lose data.

If you decide to leave the service, locking your environments makes sure that no one, including Microsoft, can ever access your data again.

To unlock your environments, you need to restore the key access permissions for the original encryption key. Then, send a Microsoft Support request to unlock and enable the environments. The environments can only be enabled if you have the original key that encrypted your data.

Reduce the risk of managing your own encryption keys

Using your own encryption keys for your Power Platform data gives you more control over your data security. But you should understand the risk of managing your own keys. For example, a malicious administrator in your organization could use the key management feature to lock your environments and harm your business. Azure Key Vault has built-in safeguards to help prevent this risk. These include soft delete and purge protection settings, which, if you've enabled them, can restore the key. Another safeguard is to separate the tasks of the Azure Key Vault admin and the Power Platform admin, so that the person who manages the key vault can't access the Power Platform admin center.

Manage Microsoft access to customer data with Customer Lockbox

Microsoft personnel (including vendors) usually don't require access to your data for operations, support, and troubleshooting. But sometimes they might need to access it to be more effective in resolving a problem if Microsoft detects one or you ask for support. Power Platform's Customer Lockbox lets your global admins or Power Platform admins review and approve any requests from Microsoft personnel to access your data. You can also track and audit all the requests. The lockbox policy doesn't apply in certain situations, such as emergencies or legal demands.

Turn on the lockbox feature at the tenant level in the Power Platform admin center. The Customer Lockbox policy applies to any Managed Environments. Power Platform and Dynamics 365 services use different Azure storage technologies to store your data. When you turn on the Customer Lockbox for an environment, the lockbox policy protects your data regardless of the storage type.

For support requests where Microsoft makes a copy of your environment in a special support environment, the lockbox policy applies just as it would in the original environment. Microsoft personnel need your approval to access the data in the support environment.

Role-based security in Dataverse

One of the key features of Dataverse is its flexible security model that can adapt to many business needs. The Dataverse security model is only available when you have a Dataverse database in your environment. As a security professional, you might create the entire security model yourself, but you might need to check that it meets your organization's data security requirements.

Dataverse uses security roles to group privileges. You can assign these roles to users or to Dataverse teams and business units. Users who belong to a team or a business unit inherit the role of that group. A key concept of Dataverse security is that privileges are cumulative and additive. This means that if you grant broad access to some data, you can't restrict access to a specific part of it later.

Dataverse teams can be associated with either Microsoft Entra ID security groups or Microsoft 365 groups. When the association is established, the system automatically manages the members of the Dataverse team. The first time a user uses an app that depends on this security, the system adds them to the Dataverse team.

Also, Dataverse security roles can act as if they were assigned directly to the user. This gives the user user-level privileges through their membership in a Dataverse team.

To make this easier to set up, when you share a canvas app with a Microsoft Entra ID security group, you can select the Dataverse security roles that are needed to use the app. The system creates a Dataverse team for you and associates it with the Microsoft Entra ID security group. The new team also gets the Dataverse security roles that you selected. This simplifies the admin experience and helps you manage user security with less manual work.

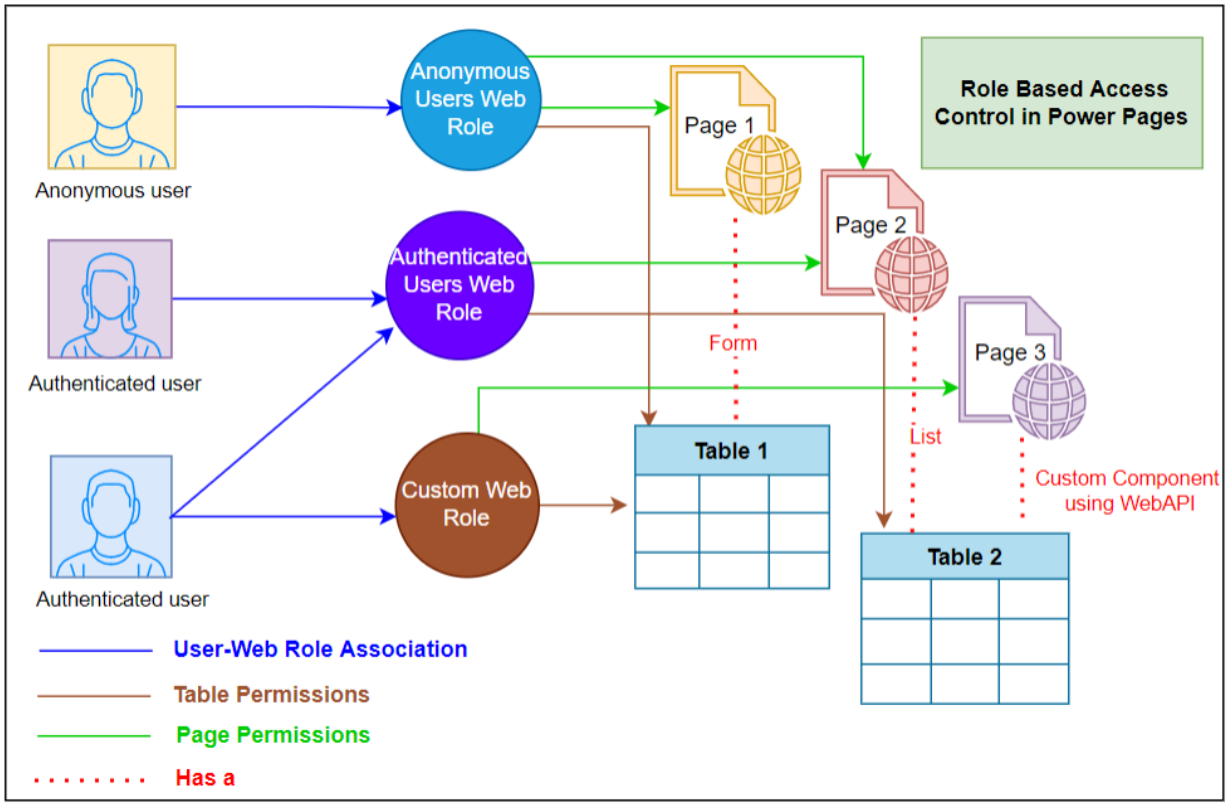
Security is a complex topic and requires collaboration between the application makers, the security team, and the user admin team. You should plan and communicate any major changes before you apply them to your environment.

Protect Dataverse data used by Power Pages

With Power Pages, you can create websites where customers or other external users can access and manage their own data from a Dataverse environment. Power Pages has a different security model from the Dataverse security model we described earlier. The Power Pages security model uses web roles to allow website users, both anonymous and authenticated, to access Dataverse data from the site. You can assign web roles to groups of users. The web roles are associated with one or more page permissions and table permissions.

Page permissions let you control who can access pages in a Power Pages site. Table permissions let you control who can access data in your Dataverse tables. Column-level permissions give more granular control over table data. You can combine these permissions in a web role that you give to users to allow them to use the Power Pages site for a business purpose. For example, they could send a request, monitor its progress, and see the response from your internal team. In this scenario, you would create a web role that gives them only the permissions they need for this task.

The following diagram illustrates how web roles and permissions work together:



User management

Power Platform empowers users to build solutions with low code and be more productive. From a security perspective, user management is a balance of giving users enough access to do their tasks while protecting your assets and data.

As we mentioned earlier, all internal users are Microsoft Entra ID users in your Microsoft Entra ID tenant. External users can use Power Platform apps and automations if you invite them as guests with the B2B collaboration feature of Microsoft Entra ID. You can manage the basic user settings in the Microsoft Entra admin center, Microsoft admin center, or the Azure portal.

Users who have a Power Platform admin, Dynamics 365 admin, or any global admin role can manage user access to resources in a Power Platform environment. They do this by setting up security groups in the environment, assigning Dataverse security roles, and sharing resources like apps and automations. Users who are environment admins or environment makers in a Power Platform environment can share resources like apps and automations with users who have access to the environment.

Microsoft Entra ID security groups

Power Platform lets you allow both users and groups to access environments and their resources. Groups are useful for managing large numbers of users of Power Platform resources. Individual user sharing and assignment of privileges are better for handling exceptions and small-scale user management.

You can use both Microsoft 365 groups and security groups to group users who need access to Power Platform environments and their resources. Security-enabled Power Apps canvas apps can be shared with security groups, but not with other types of Microsoft 365 groups.

Groups aren't just convenient. They should play an essential part in your security plans. The groups you create for Power Platform resources should reflect your security and administrative needs. A good group strategy helps you minimize the administrative work of managing users. It also helps you make sure that users are in the right groups and don't have access to things they don't need.

Security groups fall into two categories, those that control environment access and those that control access to apps.

- **Environment access**: This is the group of all users who are admins, makers, or users of the environment.
- **Application access**: These are one or more groups that let users use the Power Platform resources in the environment.

Environment access

You can create environments with or without a Dataverse database. If you create an environment without Dataverse, is has simple security permissions with two built-in roles, environment admin and environment maker. If you add Dataverse to an environment, it has a more complex security model. In the rest of this section, we'll assume that you have Dataverse in your environment.

You can use security groups to control who can access resources in Power Platform environments other than the default environment or developer environments. Link one security group to each environment that has at least one user or nested security group. Using a security group for each environment helps you make sure that only the right users have access to each one. If you automate your environment creation process, you can also automate creating the security group and make sure that your admins have access to any new environment.

Global admins and Power Platform admins have access to all environments, even if they aren't in the security group for the environment. Dynamics 365 admins need to be in the security group to access the environment. You might also have environment admins who don't have service-level access to admin roles. If you don't want to manage each admin for each environment individually, create a security group with all the admins that you want to manage environments. You could then add this group as a nested group to each environment-specific security group. Only admins and makers need access to the environment for development environments.

For example, to set up the dev environment for the Kudos app that Contoso is building, you could create an environment security group called Env_Kudos_Dev_SG that contains two nested security groups, Power_Platform_Admins_SG (six users) and Makers_Kudos_App_SG (three users).

The test environment might be dedicated to the Kudos app or it might support testing multiple apps. To make sure that the right testers have access in either case, you could create an environment security group called Env_Contoso_Test_SG that contains three nested security groups, Power_Platform_Admins_SG (six users), Testers_Kudos_App_SG (three users), and Testers_TimeOff_App_SG (three users).

Notice that in this example, makers and users who aren't testers don't have access to the test environment.

The production environment, like the test environment, can support a single app or multiple apps. You could create an environment security group called Env_Contoso_Prod_SG that contains three nested security groups, Power_Platform_Admins_SG (six users), App_Kudos_SG (5,000 users), and App_TimeOff_SG (7,000 users).

For simple individual productivity, users can build apps in the default environment. When power users need more access, you can create a shared environment with a security group that has fewer restrictions. For example, you could create an environment security group called Env_PowerUsers_SG that contains two nested security groups, Power_Platform_Admins_SG (six users) and Makers_PowerUsers_SG (100 users).

Not all makers need a dedicated environment to build an app. For training and learning, they can use developer environments, which allow access to a single user by default. Environment routing is a governance feature that lets you direct new makers to their own personal development environments instead of building in the default environment. You can turn on environment routing in the Power Platform tenant settings.

Application access

Users who have access to an environment need more permissions to access resources like apps, flows, and data in the environment. Sharing is how users get access to apps and flows. Access to Dataverse table data depends on the Dataverse security roles and their privileges that you set up. You can assign security roles to users directly or through a team.

You should create security roles when you build an application and give users only the privileges they need to use the app. Security teams should check the permissions for security roles, especially if the role will be used in a shared environment, to make sure that the role doesn't give access to data that users don't need.

When you share an app with a security group, a Dataverse team is automatically created so that the security group can be associated with it. You can also share or add Dataverse security roles to the Dataverse teams to give security role privileges to the members of the security group. The first time a user uses Dataverse, they're added to the Dataverse team members list. Users have all the privileges of their directly associated security roles and those that are assigned through the Dataverse teams they belong to.

As we saw with environment access, using security groups to give access to an app for a large number of users is easier than using direct assignment of security roles. For example, let's return to the Time Off app from our environment access example and look at how application access would work.

First, the maker team would create a Dataverse security role called Time Off User in their development environment. When they moved the app to test and production, the security role would go with it. A security group called App_TimeOff_SG would be created, and all users who need to use the Time Off app would be added to it. In the production environment, the admin would share the Time Off app with the App_TimeOff_SG security group and select the Time Off User security role on the sharing page.

Sharing would create a Dataverse team called App_TimeOff_SG, and the Time Off User security role would be associated with the new team:

App_TimeOff_SG (security group) ↔ App_TimeOff_SG (Dataverse group) ↔ Time Off User (Dataverse security role)

Limit app sharing

By default, anyone who has an environment maker security role can share a Power Apps canvas app with everyone in the organization. You can change this in the tenant app-sharing settings. When app sharing to everyone is turned off, only admin roles or service admins can share with everyone in the organization.

You can set other limits on sharing Power Apps canvas apps in environments that are set up as Managed Environments:

- Turn on **Exclude sharing with security groups** to allow users in the environment to share canvas apps directly with other users, but not with security groups.
- When **Exclude sharing with security groups** is turned on, you can also turn on **Limit total individuals** to restrict the number of people the user can share a canvas app with.

These limits affect only new shares and don't affect apps that have already been shared.

Learn more about the sharing limits you could configure for each type of environment.

Guest users

You might need to let guest users access environments and Power Platform resources. Set up their access to environments and apps as described earlier. As with internal users, you can use Microsoft Entra ID conditional access and continuous access evaluation to ensure that guest users are held to an elevated level of security. For example, you could use a conditional access policy to require multifactor authentication for all guest users who access Power Platform resources.

When you share Power Platform resources in an environment, sharing with everyone includes *everyone* in the tenant, even guests. To prevent this, you can create security groups for the environment and add everyone except guests. You can also limit sharing with everyone, so that only admins can share an application with everyone.

System and application users

When you add Dataverse to an environment, special application users and a system user are created automatically. The application users are created to support Dataverse functions. For example, the Power Apps checker application user is used to check solutions for errors. Learn more about application users and what each one does.

You can create your own application users to run automation or integration without an interactive user. For example, an Azure Function could use the Dataverse APIs and authenticate and perform operations as an application user. To create an application user:

1. Register a Microsoft Entra ID service principle.
2. Create an application user in Dataverse for the registered Microsoft Entra ID application.
3. Assign one or more Dataverse security roles to the application user to define its permissions.

Non-interactive application users can sign in with a client ID and secret or client assertion. Then they can use the app to access Dataverse data and features with the privileges that are assigned to the application user's role in the Dataverse environment.

The system user is a special account for plug-ins that need elevated permissions. Users can't sign in with this account, but custom plug-ins can use it to do any Dataverse action. The system user has all the privileges that normally come with security roles. If you turn on auditing for a table, it records any changes that the system user makes to the data in the table. You can use the system user for custom code scenarios where the plug-in runs when a record is created, for example, and needs to do something that the record creator can't. The plug-in runs as the system user and uses that access to perform the operation without granting access to the original user.

SecOps with Power Platform

Monitoring should be part of your Power Platform security operations (SecOps) strategy. You need to monitor your platform to collect the right data for threat detection and incident response. Power Platform services offer basic monitoring by default, and you can customize it to fit your needs.

You should connect your Power Platform monitoring to the tools that your organization uses to analyze and act on the signals and data from monitoring. For example, Power Platform has built-in integration with Microsoft Sentinel, or you can integrate with your own security information and event management (SIEM) service. You can also use Power Platform's integration with Microsoft Purview to view and manage activity logs. Data export and admin connectors allow you to use your own data stores and build your own custom processes.

Collect data and activity logs

To monitor your Power Platform usage effectively, you need to collect the right data and logs. Some logging happens automatically, such as Power Automate flow run history, which is stored for 28 days. You can use the following capabilities to collect and log more activity:

- **Activity logging**: Track and view Power Apps, Power Automate, connectors, and data loss prevention activities from the Microsoft Purview compliance portal.
- **Dataverse auditing**: Log changes to customer records and user access in an environment with a Dataverse database. Turn on auditing at the environment level and set it up as needed for specific tables and columns.
- **Export Power Platform inventory and usage data**: Export Power Platform inventory and usage data directly to Azure Data Lake Storage. You can use it for custom analysis based on your requirements.

- **Export to Application Insights**: Subscribe to data about operations that applications perform in your Dataverse environment to get deep insights into the apps' performance and behavior. Applications can log custom telemetry that you can include in your export. This level of detail helps you investigate the cause or impact of an incident.

Microsoft Sentinel

Microsoft Sentinel is a comprehensive security information and event management (SIEM) solution that helps you detect, investigate, and respond to threats. Power Platform and Dynamics 365 solutions have built-in integration with Microsoft Sentinel to enable the following key SIEM activities:

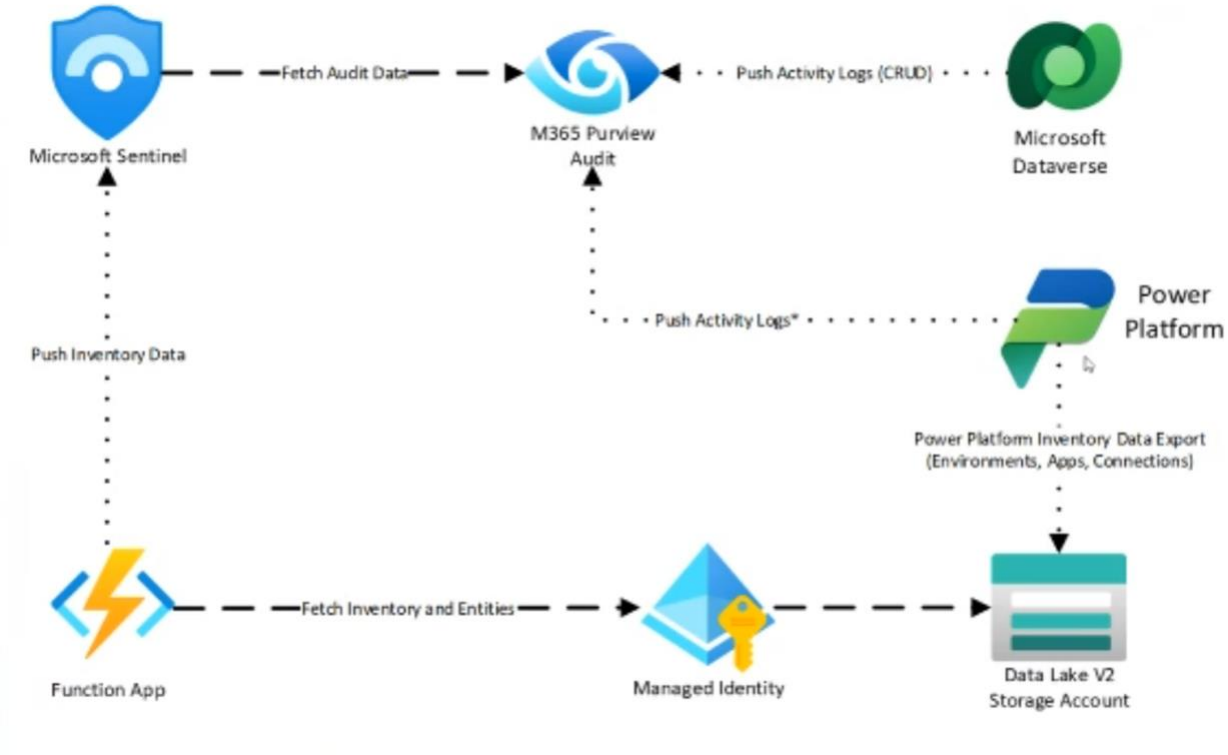
- **Collect** data at cloud scale from all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. This includes business applications that are often left out of SIEM data collection.
- **Detect** new threats and minimize false positives with analytics and unparalleled threat intelligence from Microsoft. Detect specific business application threats like data exfiltration.
- **Investigate** threats with AI and hunt for suspicious activities at scale, tapping into decades of Microsoft's cybersecurity experience.
- **Respond** to incidents quickly with built-in orchestration and automation of common tasks.

Microsoft Sentinel has more than 300 solutions that extend its capabilities for specific domains or vertical scenarios. Each solution understands how to ingest data, monitor, alert, hunt, investigate, and respond.

Power Platform, Dynamics 365 Customer Engagement, and Dynamics 365 Finance and Operations have their own individual Microsoft Sentinel solutions.

The Power Platform solution monitors and detects suspicious or malicious activity in Power Platform environments. It collects data from all the activity logging that we discussed earlier, including the Power Platform inventory. ~~This will include Power Platform admin activities soon.~~

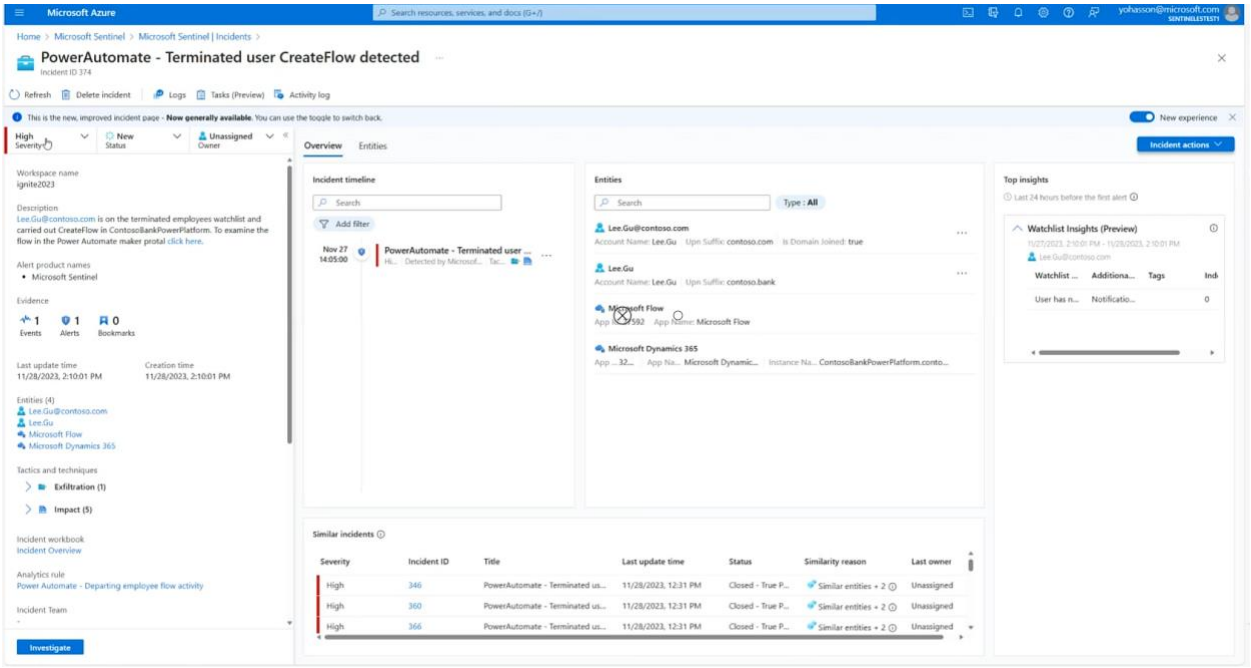
he following diagram illustrates the architecture for the data connectors:



The solution includes built-in threat coverage for the following scenarios that customers commonly encounter in their business applications:

- Power Apps activity from an unauthorized geographic location
- Access to malicious links through Power Apps
- Bulk deletion of Power Apps data
- Destruction of Power Apps data in Dataverse
- A new Power Platform connector in a sensitive environment
- Automated Power Automate activity by departing employees
- Change or removal of a Power Platform DLP policy

The SecOps team can use the Microsoft Sentinel tools to investigate and respond to these incidents. The following screenshot shows an example of such an incident, a Power Automate flow that was created by a fired employee:



The goal of Microsoft Sentinel solutions that are focused on business applications is to offer robust capabilities to detect, investigate, and disrupt threats.

To **detect** threats and malicious activities, the solutions check for signals such as data leaving the system, strange changes, data access without permission, threats from inside the organization, fraud, and odd activity.

These signals trigger **investigations** that help SecOps teams understand the threats better with guided steps, information enriched with context, master data integration, threat hunting, cross-correlation, and data integrity impact.

Based on the investigation findings, the solutions help SecOps teams **disrupt** and respond to legitimate threats by taking actions like blocking sensitive activities, limiting user or endpoint access, changing permissions, alerting managers, running scanning tools, or running a data restore.

Not all capabilities to achieve these goals have been implemented in each Microsoft Sentinel solution yet. The plan is to bring the solutions together as they mature into a unified solution that can cross-correlate data from different workloads. The unified solution is intended to be more than a SIEM add-on. It's envisioned as a complete threat detection solution and platform for Microsoft business applications and will be a premium offering when it's generally available.

CoE Starter Kit

If you want to build your own tools, Power Platform has a wealth of capabilities, including connectors, APIs, and PowerShell modules that are focused on security and administrative tasks.

Microsoft has a Center of Excellence (CoE) starter kit to help you govern your Power Platform environments and jump-start solutions that support your unique security, governance, and

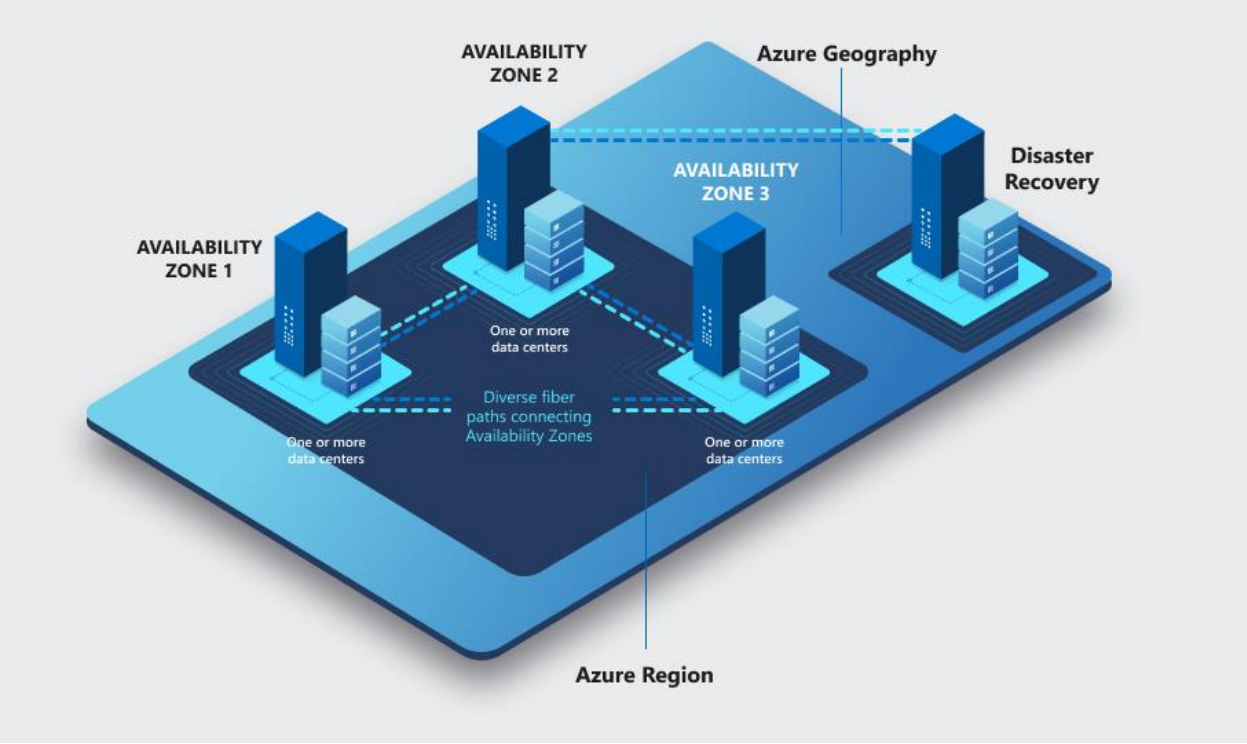
administration needs. Watch a quick video overview of the CoE starter kit to see if it could be a good fit for your organization. Learn more about the Center of Excellence starter kit.

Disaster recovery and business continuity

Business-critical applications need high availability and business continuity and disaster recovery (BCDR) plans. If you use Power Platform services, you should consider how they fit into your BCDR strategy.

Power Platform services depend on Azure reliability services, such as availability zones, to remain available. An availability zone is a physically and logically separated Azure datacenter that has its own independent power source, network, and cooling. Azure availability zones are connected with low-latency networks to deliver high-availability applications and ensure that if an event affects a datacenter, your data is protected.

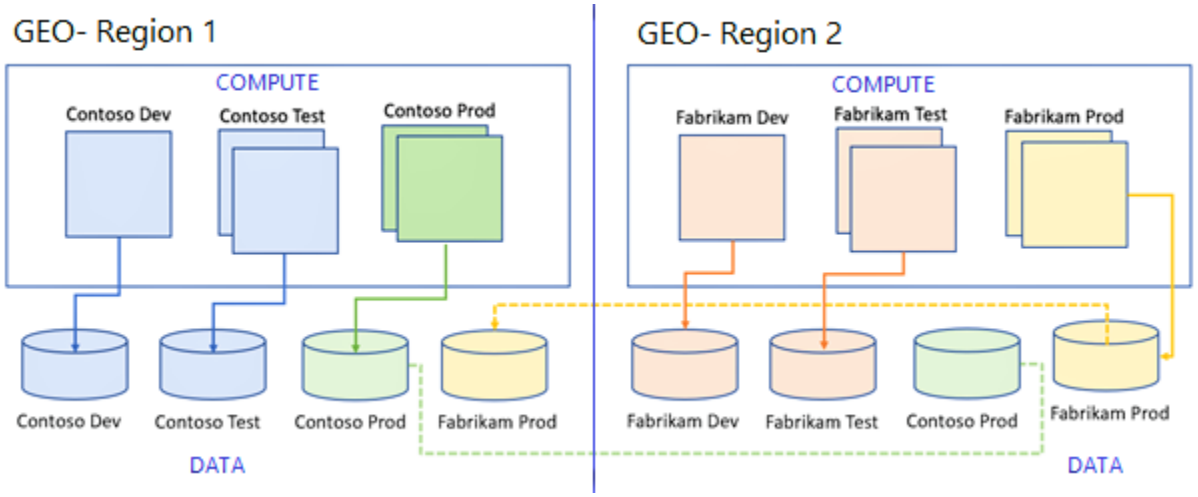
In the following illustration, an Azure region contains three availability zones, each with one or more Azure datacenters. Fiber connections link the availability zones, giving the data a variety of paths to travel:



High-availability failovers happen within an Azure region. They're guaranteed not to lose any data, whether they're planned or unplanned. They use synchronous replication, meaning that any changes to the primary replica are also made to the secondary replica at the same time to keep the data consistent and up to date on both. A fabric layer, software that manages communication and coordination between the replicas and can detect when the primary fails, switches from the primary replica to a secondary replica quickly and correctly. These failovers typically happen in seconds and are rarely noticed by users.

In contrast, disaster recovery failovers happen across two Azure regions and use asynchronous replication to keep a disaster recovery copy ready for production instances. With asynchronous replication, changes to the primary replica are made to the secondary replica after a delay to reduce the impact on performance and bandwidth, enabling faster failover with minimal data loss. Planned failovers don't lose any data and, for production environments, can be completed in several seconds to a few minutes.

In the following diagram, a Contoso production environment has a primary replica in Azure region 1 and a secondary replica in Azure region 2. Similarly, a Fabrikam production environment has a primary replica in Azure region 2 and a secondary replica in Azure region 1:



What about an unanticipated region-wide outage, such as a natural disaster that affects the entire Azure region? If Microsoft determines the region will take too long to recover, it notifies customers and switches the traffic to the secondary environments. Customers might lose up to 15 minutes of data, depending on when and how the outage happened. When the primary region is back online, a switchback happens with no loss of data.

Besides the technical implementation of high availability and BCDR, the operations team regularly tests their readiness to respond to different types of events. Power Platform services follow the Microsoft BCDR standard, which requires that each online service has a BCDR plan reviewed, updated, and tested at least annually. The Microsoft Cloud Business Continuity and Disaster Recovery Plan Validation Report is available for download on Service Trust Portal.

Recovery and environment strategy

The platform does much of the work, but you should think about how your organization uses the services and the integrations they depend on. Consider the following areas:

- **Environments**: Use production environments for all business-critical Power Platform environments. Use Managed Environments if you need to keep backups longer.
- **Connectors:** Power Platform connectors let apps and automations use services that aren't part of Power Platform high availability. You might need to do more work to make sure these services meet your desired level of availability.

- **User-initiated incidents:** Not all BCDR incidents come from service outages or problems. Sometimes, users cause them. For example, a user with access might delete all the rows from a Dataverse table. You must handle these types of incidents with environment backups.

All environments except trial environments (standard and subscription-based) are backed up. The system makes backups automatically and continuously. You can also make backups manually when you need to, such as before making significant customizations or major data modifications in an environment.

The default backup retention period is seven days for production environments that don't have Dynamics 365 apps. You can keep backups of Managed Environments for 7, 14, 21, or 28 days.

You can restore the original environment or another sandbox environment in the same region. If the original was a production environment and you want to replace it, you must change it to a sandbox environment first. Restoring an environment overwrites all the data in it and returns it to a specific point in time (when the backup was made). If you want to restore only some of the data, it's better to restore to a different environment and use the Power Platform data tools to get the data you want.

Important: Changing an environment to a sandbox reduces the backup retention to seven days immediately. If you might need older backups, you should keep the environment as production and consider restoring it to a different sandbox environment.

If you encrypt your environments using your own customer-managed key, you can only restore a backup to the same environment or to another environment that's encrypted with the same key.

After you restore an environment, you might need to change some security settings. Apps that are shared with everyone in a backed-up environment aren't shared with everyone in the restored environment. Or, a canvas app can be shared with a security group, and the app in the restored environment is shared with that group.

Power Platform apps, automations, and other components that you customize are backed up with the environment. Power Apps canvas or model-driven apps and Power Automate flows that aren't in a Dataverse solution are not. You should have an application lifecycle management (ALM) process for the apps and automations you build that includes storing them in a source control tool or keeping backups of Dataverse solution exports. This helps you recover an app or automation without restoring the environment.

Compliance

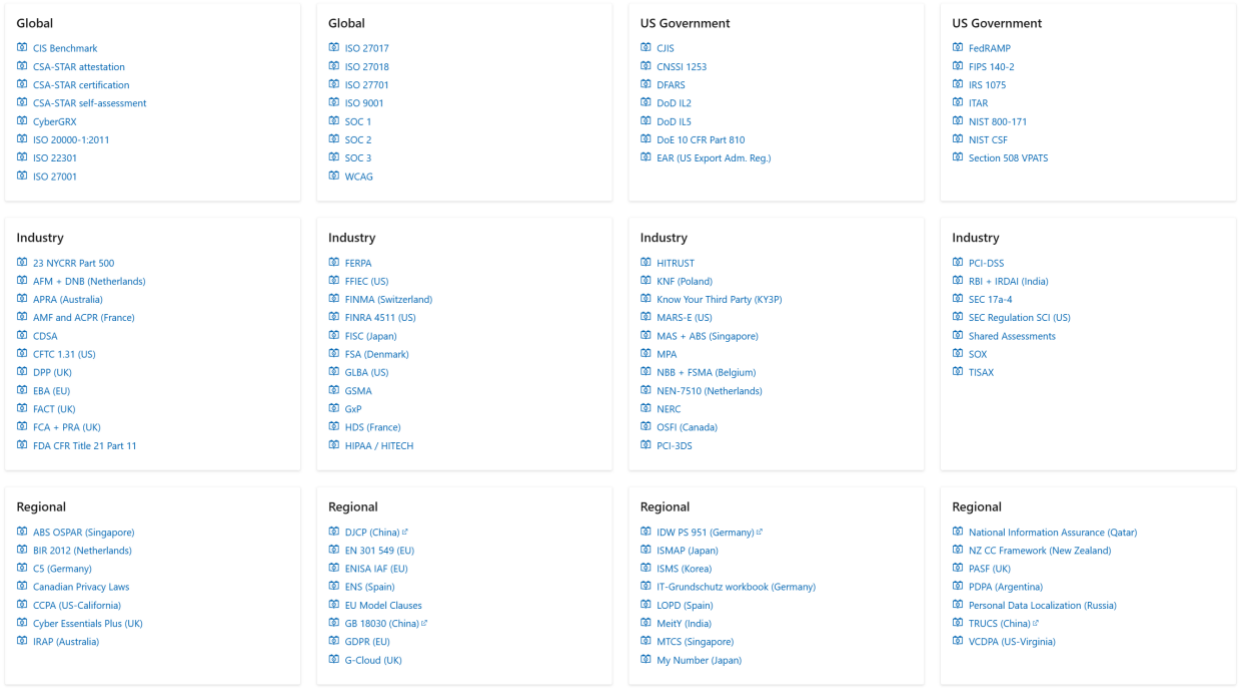
Microsoft is committed to the highest levels of trust, transparency, standards conformance, and regulatory compliance. Our cloud products and services are designed to meet our customers' most rigorous security and privacy demands.

The **Microsoft Trust Center** (https://www.microsoft.com/trustcenter) is a centralized source of publicly available information about the security, privacy, compliance, and transparency of Microsoft products. Although this paper might have some of this information for Power Platform, you should always refer to the Microsoft Trust Center for the most up to date authoritative information.

The **Microsoft Service Trust portal** (https://servicetrust.microsoft.com) is a centralized resource for learning how Microsoft cloud services protect your data and how you can manage your cloud data security and compliance. Along with resources specific to your organization based on your subscription and permissions, the portal has private materials, such as audit reports from other parties for current and potential customers who are testing Microsoft cloud computing services. You can save reports, white papers, and other resources to your Library for easy access in the future.

Certifications and regulatory compliance standards

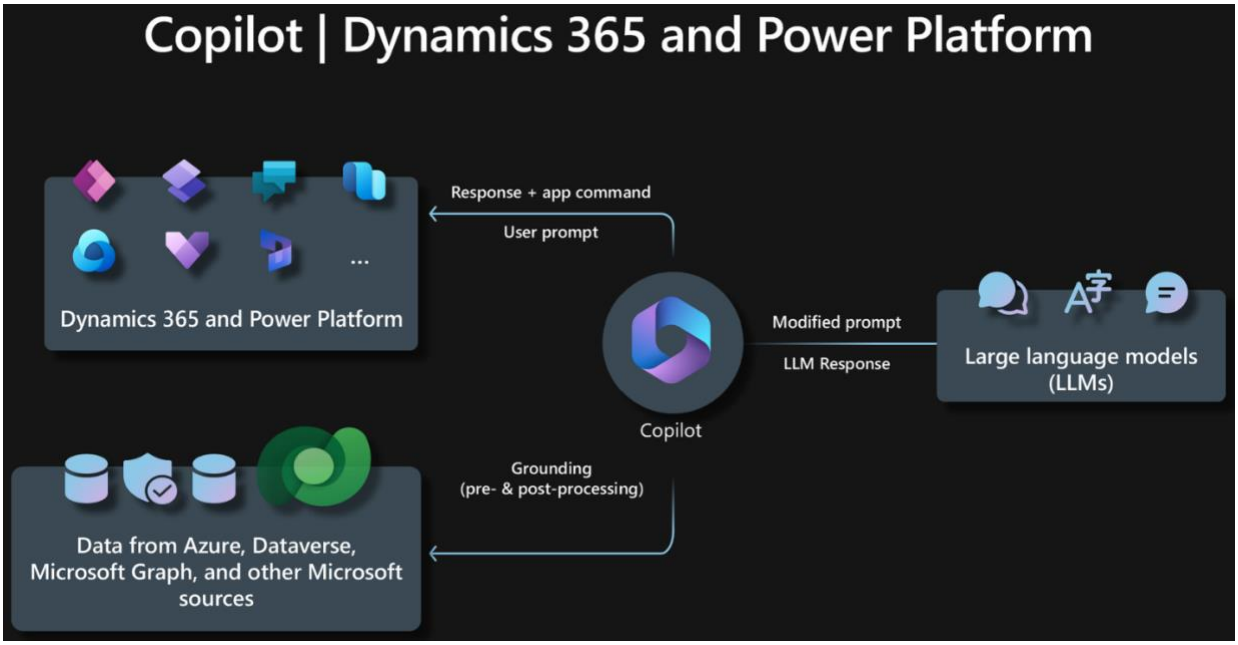
Azure, Dynamics 365, and Power Platform all have a number of certifications to help your organization meet national, regional, and industry-specific regulations for collecting and using data, as shown in the following lists. You can find details in the Microsoft Trust Center.



Responsible AI

Microsoft is committed to the advancement of ethical AI that's guided by our responsible AI principles and approach. Our commitment applies to all Microsoft AI capabilities and products that use AI and includes publishing the Microsoft Responsible AI Standard, internal guidance we follow when we design, build, and test AI products and systems. Microsoft expects customers that use AI to follow responsible AI practices as they adopt these capabilities in their organizations.

Copilot in Microsoft apps enables users to be more productive. Copilot is available in Dynamics 365 and Power Platform business applications as a new way to generate ideas, draft content, and access and organize information across the business. In Power Platform products like Power Automate, Copilot is also helping makers build flows just by describing what they want to happen.



Copilot can unlock business value by connecting language models with your business data securely, compliantly, and privately. With your approval, which you can revoke at any time, Copilot can access your content and context in Microsoft 365 Graph and Dataverse in real time to generate answers grounded in your business content. Copilot also uses your working context, such as email or chat conversations, to make its answers more relevant. Microsoft doesn't use your data to train language models. We don't use prompts, responses, or data from Microsoft 365 Graph and Microsoft services to train Copilot capabilities in Dynamics 365 and Power Platform for other customers. Copilot shows you data that only you can access, using the same technology that has secured your data for years. Learn more in the Copilot data security and privacy FAQ.

You can opt in to share your data with us to help improve the quality of Copilot AI features. When you share your data, Microsoft can capture and manually review data such as users' natural language inputs, outputs, and related telemetry to help build, improve, and validate the service. Sharing your data doesn't allow us to use it to train the foundational models. We strictly control access to your data. Only authorized Microsoft employees can view your data. Learn more in the Copilot data sharing FAQ.

Penetration testing

We test Microsoft Cloud services thoroughly and publish the results on the Service Trust Portal for your review. Our tests include penetration testing, evaluating the security of our services by simulating an attack to identify and exploit vulnerabilities so that we can fix them.

You can do your own penetration tests on Power Platform and Dynamics 365 services. You must follow the Microsoft Cloud Penetration Testing Rules of Engagement. Remember that the Microsoft Cloud hosts your assets and assets belonging to other customers on shared infrastructure. Make sure that your penetration tests affect only your assets and don't harm other customers.

Conclusion

In this white paper, we explored the comprehensive suite of tools and technologies that help your security team manage your Power Platform use securely. You learned how to include Power Platform in your security architecture.

Security threats and business needs change fast. You need an agile approach to security that can keep up and fit your organization. Power Platform builds on Microsoft's security capabilities. You can integrate Power Platform into the protection and operations aspects of your organization's security efforts. Its flexible security models can help you meet the requirements for your Power Platform solutions and create a secure and productive workplace for your users.

A key factor for success with low code approaches is training. Make sure that the people who build low-code applications and automations know how to follow your organization's security guidelines. Low code allows a broader set of people to build applications, such as business users. These people are often closer to the business problem than purely technical resources are. This has a lot of benefits, but these users might not understand the security risks well. You can help them by setting up security rules and guidelines.

This white paper gave you the map. The next step is yours. Here are some next steps you can take:

- Find out what your organization is already doing with low code. You might be surprised!
- Learn how to integrate Power Platform into your security architecture and operations.
- Prioritize securing your existing Power Platform applications.
- Assign and train security professionals who will work with low-code users in your organization.
- Make sure that the users who are building Power Platform solutions have the security training they need to succeed.

Every organization's journey to integrating Power Platform into their security practices is unique. These are some ideas to help you start on the right foot. Your Microsoft account team or Power Platform partner can help you create a more customized roadmap for your organization.

Resources

https://learn.microsoft.com/en-us/power-platform/admin/security

https://learn.microsoft.com/en-us/power-platform/admin/content-security-policy

https://learn.microsoft.com/en-us/power-platform/admin/security/faqs

https://learn.microsoft.com/en-us/power-platform/admin/block-forwarded-email-from-power-automate

https://learn.microsoft.com/en-us/power-platform/admin/security/data-storage#sas-ip-binding

https://learn.microsoft.com/en-us/power-platform/admin/support-environment

AI-assisted content. This article was partially edited with the help of AI. An editor reviewed and revised the content as needed. Learn more about our principles for using AI-generated content.