Microsoft

# Best Security, Compliance, and Privacy Practices

## for the Rapid Deployment of Publicly Facing Microsoft Power Apps Intake Forms

White Paper

# Contents

# Introduction

Have you been tasked with deploying a publicly facing intake form using Microsoft Power Apps? It is a popular way of modernizing legacy form intake, such as having an applicant fill out a paper forms and sending it back to the requesting party via mail to be transcribed or having the applicant stand in line at an agency to submit paper forms.

If the forms require the applicant to provide sensitive personal information, you want to ensure that online forms have the highest level of security, privacy, and comply with best practices for data privacy.

Before getting Started, it is recommended that application support, stakeholders and, if applicable, the Power Apps Center of Excellence established in your organization review "Administering a PowerApps Enterprise Deployment" and the "Power Apps and Power Automate Administration and Governance Whitepaper".

# Security Best Practices Specific to Forms-Level Security

**This section will help organizations plan key aspects of building or updating their enterprise breach response plan across these key functions:**

- Technology
- Operations
- Legal
- Communication

### STEP 1
Configure a contact for use on a portal

After filling out the basic information for a contact, (or having a user fill out the sign-up form in a portal), go to the web authentication tab on the portal contact form to configure a contact by using local authentication. For more information about federated authentication options, see Set authentication identity for a portal.

### STEP 2
Invite contacts to your portals

Use the invitation feature of portals to invite contacts to your portal through automated email(s) created in your Common Data Service. The people you invite receive an email, fully customizable by you, with a link to your portal and an invitation code. This code can be used to gain special access configured by you. With this feature you have the ability to:

- Send Single or Group Invitations
- Specify an expiry date if desired
- Specify a user or portal contact as the inviter if desired
- Automatically assign the invited contact(s) to an account upon invite redemption
- Automatically execute a workflow upon invite redemption
- Automatically assign the invited contact(s) to a Web Role(s) upon redemption

Invitation redemption can be accomplished using any of our many authentication options. For documentation regarding portal authentication, see Set authentication identity for a portal and choose the model applicable to your portal version and configuration. The user will adopt any settings provided by the administrator upon redemption. An Invite Redemption Activity will be created for the Invite and Contact.

Invitations are sent via the **Send Invitation** workflow. By default, the workflow creates an email with a generic message and sends it to the invited Contact's primary email address. The email addresses in the CC and BCC fields are ignored to ensure secure communication. The **Send Invitation** workflow contains an email template that will need to be edited to contain a specific message for your portal and the correct hyperlink to your portal's **Invite Redemption Page**.

To edit the **Send Invitation** workflow email template, locate it and deactivate it. After it is deactivated, edit the email template to send the message you want and provide a link to the **Invite Redemption Page** of your portal.

### STEP 3
Create web roles for portals

After a contact has been configured to use the portal, it must be given one or more web roles to perform any special actions or access any protected content on the portal. For example, to access a restricted page, the contact must be assigned to a role to which read for that page is restricted to. To publish new content, the contact must be placed in a role which is given content publishing permissions.

### STEP 4
Add record-based security by using entity permissions for portals

To apply record-based security in portals to individual records, use entity permissions. You add entity permissions to web roles so you can define roles in your organization that correspond logically to the privileges and concepts of record ownership and access that are introduced by using entity permissions. Remember that a given contact can belong to any number of roles, and a given role can contain any number of entity permissions. More information: Create web roles for portals

Although permissions to change and access URLs in a portal site map is granted via Content Authorization, site managers will also want to secure their custom web applications built with entity forms and entity lists. More information: Define entity forms and Define entity lists

**STEP 5**
[Control webpage access for portals]

Web page access control rules are rules that you create for your site to control both the publishing actions that a web role can perform across the pages of your website and to control which pages are visible by which web roles.

**STEP 6**
[Create website access permissions]

Website Access Permissions is a permission set, associated with a web role, that permits front-side editing of the various content managed elements within the portal other than just web pages. The permission settings determine which components can be managed in the portal.

**STEP 7**
[Add a CAPTCHA helper to any Publicly-facing forms to Reduce Bot Attacks]

Any time you let people register in your site, or even just enter a name and URL (like for a blog comment), you might get a flood of fake names. These are often left by automated programs (bots) that try to leave URLs in every website they can find. (A common motivation is to post the URLs of products for sale.)

You can help make sure that a user is real person and not a computer program by using a CAPTCHA to validate users when they register or otherwise enter their name and site. CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. A CAPTCHA is a *challenge-response* test in which the user is asked to do something that is easy for a person to do but hard for an automated program to do. The most common type of CAPTCHA is one where you see some distorted letters and are asked to type them. (The distortion is supposed to make it hard for bots to decipher the letters.)

# General Security Best Practices for the Power Apps Platform

**STEP 1**
**Understand Power Apps**

Review the Power Apps Platform Overview. This document will help you will better understand the Power Apps Platform and architecture, how to deploy Power Apps, the role of the Power Apps administrator, and checking the health of the Power Apps online service.

**STEP 2**
**Learn How to Manage Power App Environments**

An environment is a space to store, manage, and share your organization's business data, apps, and flows. They also serve as containers to separate apps that may have different roles, security requirements, or target audiences. How you choose to leverage environments depends on your organization and the apps you are trying to build.

**STEP 3**
**Understand How Data is Stored and Processed**

The Common Data Service is a cloud scale database used to securely store data for business applications built on Power Apps. Common Data Service is an abstraction on top of underlying Azure cloud data management services to make it easier to build business applications. Common Data Service provides not just data storage, but a way to implement business logic that enforces business rules and automation against the data. Data in Common Data Service is organized as entities, such as account and contact. These entities can have relationships that define the business connection between the data stored in an entity. For example, John works for Contoso would be expressed as a relationship. The security model of Common Data Service enables data protection down to the field level on individual records.

**STEP 4**
**Review Governance Considerations**

Many customers wonder: How can Power Apps and Power Automate be made available to their broader business and supported by IT? Governance is the answer. It aims to enable business groups to focus on solving business problems efficiently while adhering to IT and business compliance standards. The following content is intended to structure themes often associated with governing software and bring awareness to capabilities available for each theme as it relates to governing Power Apps and Power Automate.

**STEP 5**
**Review Security Concepts in the Common Data Service**

One of the key features of Common Data Service is its rich security model that can adapt to many business usage scenarios. This security model is only in play when there is a Common Data Service database in the environment. As an administrator, you likely won't be building the entire security model yourself but will often be involved in the process of managing users and making sure they have the proper configuration as well as troubleshooting security access related issues.

**STEP 6**
**Configure User Security**

You use the Microsoft 365 admin center to create user accounts for every user who needs access to model-driven apps in Dynamics 365, such as Dynamics 365 Sales and Customer Service. The user account registers the user with Microsoft Online Services environment. In addition to registration with the online service, the user account must be assigned a license for the user to have access to the service. Note that when you assign a user the global administrator or the service administrator role in the Microsoft Online Services environment, it automatically assigns the user the System Administrator security role. More information: Differences between the Microsoft Online services environment administrative roles and security roles.

**STEP 7**
**Implementing Role Based Security In Your PowerApps App**

A very common question our customers ask is, 'how do I implement role-based access control in my app?'. In other words, how do I make certain features or screens of my app available only to the authorized people in my organization? For

example, make Admin screen available only to the users who belong to an Active Directory Group "Administrators" or make management views available only to the users belonging to the Active Directory Group "Managers".

**STEP 8**
Configure Field-level security to control access

Record-level permissions are granted at the entity level, but you may have certain fields associated with an entity that contain data that is more sensitive than the other fields. For these situations, you use field-level security to control access to specific fields.

**STEP 9**
Configure environment security

Common Data Service uses a role-based security model to help secure access to the database. This topic explains how to create the security artifacts that you must have to help secure an app. The user roles control run-time access to data and are separate from the Environment roles that govern environment administrators and environment makers. For an overview of environments, see Environments overview.

**STEP 10**
Control user access to environments: security groups and licenses

If your company has multiple Common Data Service environments, you can use security groups to control which licensed users can be a member of a particular environment.

**STEP 11**
Restrict Cross-Tenant Access

With tenant restrictions, organizations can control access to SaaS cloud applications, based on the Azure AD tenant the applications use for single sign-on. For example, you may want to allow access to your organization's Office 365 applications, while preventing access to other organizations' instances of these same applications.

With tenant restrictions, organizations can specify the list of tenants that their users are permitted to access. Azure AD then only grants access to these permitted tenants.

Restricting outbound cross-tenant connections can be done using tenant restrictions that apply to all Azure AD Cloud SaaS apps, or at the API Hub level which would block outbound connections just for canvas apps and flows.

**STEP 12**
Use Teams to Securely Share Business Objects and Collaborate with Business Units

Using Teams is optional. However, Teams provide an easy way to share business objects and let you collaborate with other people across business units. While a team belongs to one business unit, it can include users from other business units. You can associate a user with more than one team.

**STEP 13**
Collaborate with Team Templates

A team is a group of users. As a group, you will be able to track information about the records and perform assigned tasks in much more efficient and coordinated way.

**STEP 14**
Create a Team Template to control access rights for automatically created Teams

A team template can be used for the entities that are enabled for automatically created access teams. In the team template, you must specify the entity type and the access rights on the entity record. For example, you can create a team template for an account entity and specify the Read, Write, and Share access rights on the account record that the team members are granted when the team is automatically created. After you create a team template, you must customize the entity main form to include the new team template. After you publish customizations, the access team template is added in all record forms for the specified entity in a form of a list. For example, you created a team template called "Sales team" for the account entity. On all account record forms you'll see the list called "Sales team". You can add or remove team members using this list.

**STEP 15**
Implement Azure Security Center

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud, and at the same time, when you move to IaaS (infrastructure as a service) there is more customer responsibility than there was in PaaS (platform as a service), and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services and make sure you're on top of your security posture.

**STEP 16**

**Implement Security Recommendations in Azure Security Center**

Recommendations are actions for you to take in order to secure your resources.

Security Center periodically analyzing the security state of your Azure resources to identify potential security vulnerabilities. It then provides you with recommendations on how to remove them.

Each recommendation provides you with:

- A short description of what is being recommended.
- The remediation steps to carry out in order to implement the recommendation.
- Which resources need you performing the recommended action on them?
- The Secure Score impact, which is the amount that your Secure Score will go up if you implement this recommendation.

# Implementing Compliance and Privacy with Data Loss Prevention

**STEP 1**
Data Loss Prevention Policies

Your organization's data is likely one of the most important assets you are responsible for safeguarding as an administrator. The ability to build apps and automation that uses the data allows your company to be successful. Power Apps and Power Automate allow rapid build and rollout of these high-value applications that allow users to measure and act on the data in real time. Applications and automation are increasingly becoming more connected across multiple data sources and multiple services. Some of these services might be external third-party services and might even include some social networks. Users will often have good intentions but might overlook the potential for exposure from data leakage to services and audiences that shouldn't have access to the data.

Data loss prevention (DLP) policies that help protect organizational data from unintended exposure are available for administrators to create. They can act as guardrails to help prevent users from unintentionally exposing the data. DLP policies can be scoped at the environment and tenant level offering flexibility to craft policies that are sensible and do not block high productivity.

DLP policies enforce rules of what connectors can be used together by classifying connectors as either Business data only or No business data allowed.

**STEP 2**
Create a data loss prevention (DLP) policy

To protect data in your organization, Power Apps lets you create and enforce policies that define with which consumer connectors specific business data can be shared. These policies that define how data can be shared are referred to as data loss prevention (DLP) policies. DLP policies ensure that data is managed in a uniform manner across your organization, and they prevent important business data from being accidentally published to connectors such as social media sites.

In this topic, you'll learn how to create a DLP policy for a single environment that prevents data that's stored in your Common Data Service and SharePoint databases from being published to Twitter.

**STEP 3**
Manage Data Loss Prevention (DLP) Policies

An organization's data is critical to its success. Its data needs to be readily available for decision-making, but it needs to be protected so that it isn't shared with audiences that shouldn't have access to it. For example, an organization that uses Power Apps may not want its business data that's stored in SharePoint to be automatically published to its Twitter feed.

To create, edit, or delete DLP policies, you must have either Environment Admin or Power Platform service admin permissions. For more information, see Environments Administration in Power Apps.

For instructions on how to create a DLP policy, see Create a data loss prevention (DLP) policy.

**STEP 4**
Understand and Implement Data Groups

Data groups are a simple way to categorize services within a data loss prevention (DLP) policy. The two data groups available are the **Business data only** group and the **No business data allowed** group. Organizations are free to determine which services are placed into a particular data group. A good way to categorize services is to place them in groups, based on the impact to the organization. By default, all services are placed into the **No business data allowed** data group. You manage the services in a data group when you create or modify the properties of a DLP policy from the admin center.

# Implementing Compliance with Geolocation and Data Residency

**STEP 1**
Block Access by Location with Azure AD Conditional Access

You can limit access to users with block access by location to reduce unauthorized access. When block access by location restrictions are set in a user's profile and the user tries to log in from a blocked location, access to model-driven apps in Dynamics 365, such as Dynamics 365 Sales and Customer Service, are blocked.

**Requirements**

- A subscription to Azure Active Directory Premium.
- A federated Azure Active Directory tenant. See What is Conditional Access?

# Implementing Compliance with Data Encryption

**STEP 1**
Encrypt Data in Process and at Rest

Model-driven apps in Dynamics 365, such as Dynamics 365 Sales and Customer Service, use standard SQL Server cell level encryption for a set of default entity attributes that contain sensitive information, such as usernames and email passwords. This feature can help organizations meet FIPS 140-2 compliance.

All new and upgraded organizations use data encryption by default. Data encryption can't be turned off.

Users who have the system administrator security role can change the encryption key at any time.

**STEP 2**
Manage the Encryption Key

All environments of Common Data Service use SQL Server Transparent Data Encryption (TDE) to perform real-time encryption of data when written to disk, also known as encryption at rest.

By default, Microsoft stores and manages the database encryption key for your environments, so you don't have to. The manage keys feature in the Power Platform admin center gives administrators the ability to self-manage the database encryption key that is associated with the Common Data Service tenant.

**STEP 3**
Set up Threat Protection for Azure Key Vault

Advanced threat protection for Azure Key Vault provides an additional layer of security intelligence. This tool detects potentially harmful attempts to access or exploit Key Vault accounts. Using the native advanced threat protection in Azure Security Center, you can address threats without being a security expert, and without learning additional security monitoring systems.

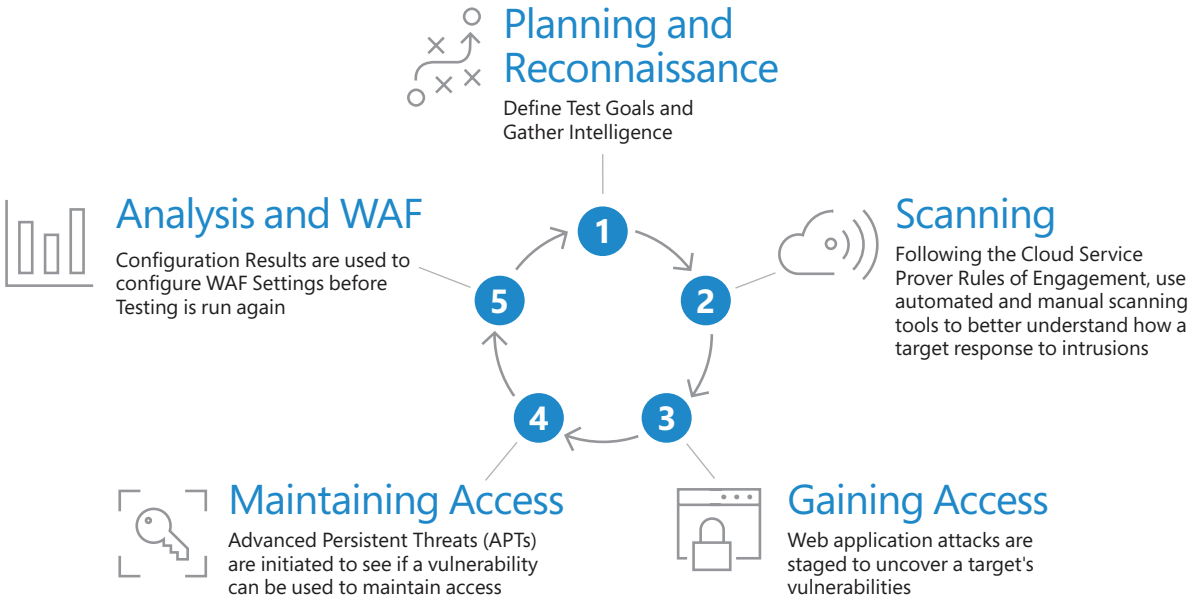
When Security Center detects anomalous activity, it displays alerts. It also emails the subscription administrator with details of the suspicious activity and recommendations for how to investigate and remediate the identified threats.

**STEP 4**
Secure Access and Data in Azure Logic Apps

To control access and protect data in Azure Logic Apps, you can set up security in these areas:

- Access to request-based triggers
- Access to logic app operations
- Access to run history inputs and outputs
- Access to parameter inputs
- Access to services and systems called from logic apps

# Meet Compliance Requirements and Enforce Secure Practices by Managing the Application Lifecycle




**STEP 1**
**Review Microsoft Security Development Lifecycle (SDL) – Process Guidance**

Review Microsoft Cloud Penetration Testing Rules of Engagement

Consider Web Security Testing of Power App Forms or Other Power Apps Objects and Code

**STEP 2**
**Automate application lifecycle management with Power Apps Build Tools**

Use Power Apps Build Tools to automate common build and deployment tasks related to Power Apps. This includes synchronization of solution metadata (solutions) between development environments and source control, generating build artifacts, deploying to downstream environments, provisioning/de-provisioning of environments, and the ability to perform static analysis checks against your solution using the Power Apps checker service.

To learn more, read the following blog post: Automate your application lifecycle management (ALM) with Power Apps Build Tools (Preview).

**STEP 3**
**Perform code reviews**

Before you check in code, conduct code reviews to increase overall code quality and reduce the risk of creating bugs. You can use Visual Studio to manage the code review process.

**STEP 4**
**Perform static code analysis**

Static code analysis (also known as source code analysis) is usually performed as part of a code review. Static code analysis commonly refers to running static code analysis tools to find potential vulnerabilities in non-running code by using techniques like taint checking and data flow analysis. Azure Marketplace offers developer tools that perform static code analysis and assist with code reviews.

**STEP 5**
**Perform Web Application Scanning**

You scan your application and its dependent libraries to identify any known vulnerable components. Products that are available to perform this scan include OWASP Dependency Check, Snyk, and Black Duck.

Vulnerability scanning powered by Tinfoil Security is available for Azure App Service Web Apps. Tinfoil Security scanning through App Service offers developers and administrators a fast, integrated, and economical means of discovering and addressing vulnerabilities before a malicious actor can take advantage of them.

### STEP 6
### Use the Secure DevOps Kit for Azure

The Secure DevOps Kit for Azure (AzSK) was created by the Core Services Engineering & Operations (CSEO) division at Microsoft, to help accelerate Microsoft IT's adoption of Azure. We have shared AzSK and its documentation with the community to provide guidance for rapidly scanning, deploying and operationalizing cloud resources, across the different stages of DevOps, while maintaining controls on security and governance.

### STEP 7
### Implement Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers.

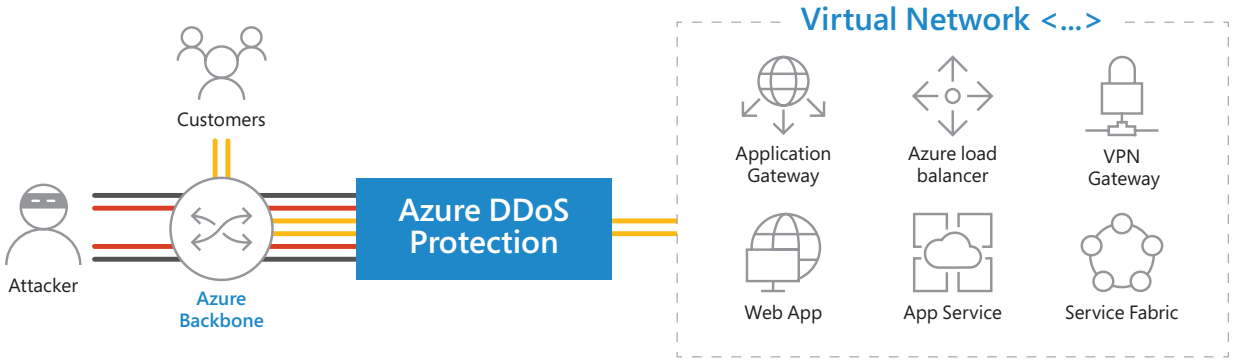
### STEP 8
### Implement Azure DDoS Protection

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns facing customers that are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

Azure DDoS protection, combined with application design best practices, provide defense against DDoS attacks.

### STEP 9
### Implement Azure Web Application Firewall

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.




**Azure DDoS protection, combined with application design best practices, provide defense against DDoS attacks.**

# Monitor and Protect Azure App Services including Power Apps

**STEP 1**
**Protect your Azure App Service web apps and APIs with Azure Security Center**

Azure App Service is a fully managed platform for building and hosting your web apps and APIs without worrying about having to manage the infrastructure. It provides management, monitoring, and operational insights to meet enterprise-grade performance, security, and compliance requirements.

Azure Security Center leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks. Security Center can discover attacks on your applications and identify emerging attacks - even while attackers are in the reconnaissance phase, scanning to identify vulnerabilities across multiple Azure-hosted applications. As an Azure-native service, Security Center is also in a unique position to offer host-based security analytics covering the underlying compute nodes for this PaaS, enabling Security Center to detect attacks against web applications that were already exploited. For more details, see Threat protection for Azure App Service.

**STEP 2**
**Automate Responses to Alerts and Recommendations**

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

**STEP 3**
**Export Security Alerts and Recommendations**

Azure Security Center generates detailed security alerts and recommendations. You can view them in the portal or through programmatic tools. You may also need to export this information or send it to other monitoring tools in your environment.
This article describes the set of tools that allow you to export alerts and recommendations either manually or in an ongoing, continuous fashion.
Using these tools, you can:

- Continuously export to Log Analytics workspaces
- Continuously export to Azure Event Hubs (for integrations with third-party SIEMs)
- Export to CSV (one time)

**STEP 4**
**Setup Email Notifications**

Azure Security Center will recommend that you provide security contact details for your Azure subscription if you haven't already. This information will be used by Microsoft to contact you if the Microsoft Security Response Center (MSRC) discovers that your customer data has been accessed by an unlawful or unauthorized party. MSRC performs select security monitoring of the Azure network and infrastructure and receives threat intelligence and abuse complaints from third parties.

An email notification is sent on the first daily occurrence of an alert and only for high severity alerts. Email preferences can only be configured for subscription policies. Resource groups within a subscription will inherit these settings. Alerts are available only in the Standard tier of Azure Security Center.

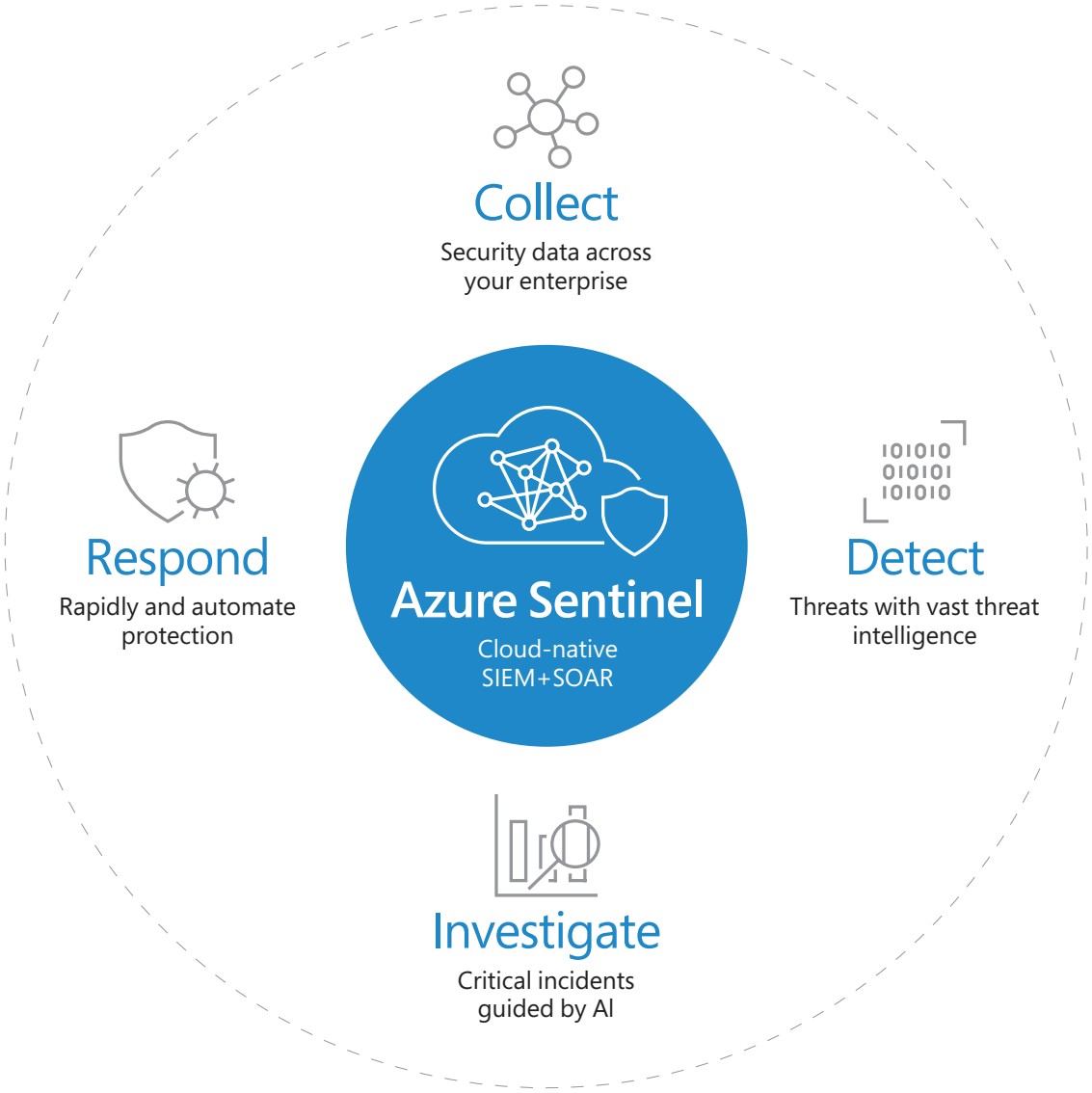
Alert email notifications are sent:

- To a single email recipient per alert type, per day
- No more than 3 email messages are sent to a single recipient in a single day
- Each email message contains a single alert, not an aggregation of alerts
- Only for high severity alerts

**STEP 5**

## Protect and Defend Azure Applications including Power Apps Intake Forms using Azure Sentinel

Azure Sentinel is an enterprise wide solution for threat detection, visibility, hunting and response. In other words, it is a security information event management (SIEM) and security orchestration response system. Azure Sentinel can analyze log data collected into an associated log analytics workspace.



**STEP 6**

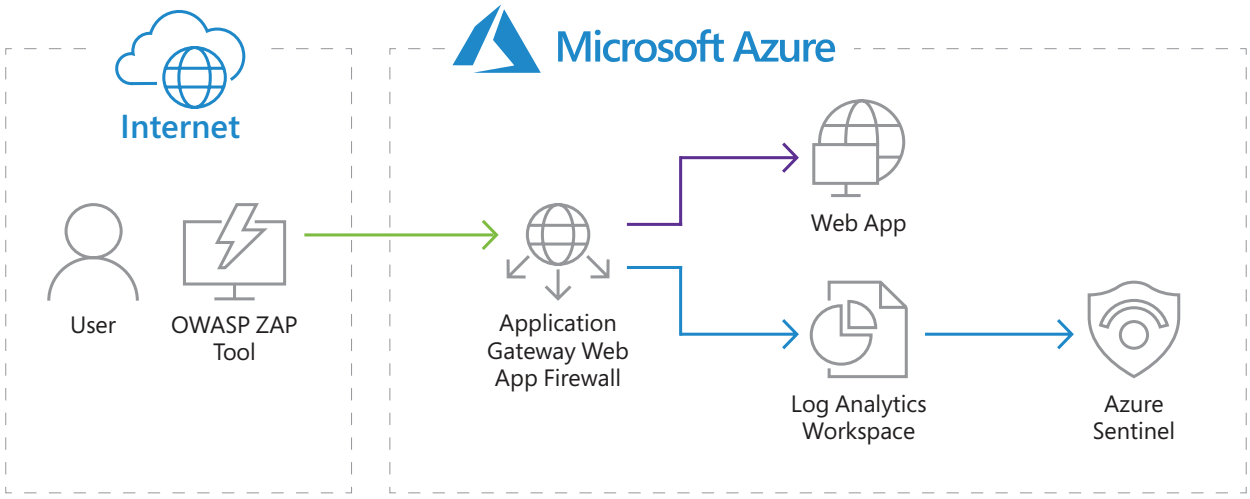
[Using Azure Sentinel with Azure App Gateway to Investigate Web Attacks]

Use Azure Sentinel to monitor and investigate incidents of cyber-attacks on a web application by having a layer of protection by leveraging the Azure Application Gateway's Web Application Firewall.

**STEP 7**

[Monitoring Cloud Security for Zero Trust with Azure Sentinel]

This is the third in a six-part blog series where we will demonstrate the application of Zero Trust concepts for securing federal information systems with Microsoft Azure. In this blog, we will explore how to leverage Azure Sentinel for security monitoring in Zero Trust models. Additional blogs in the series include leveraging policy, investigating insider attacks and monitoring supply chain risk management.



# Implement Data Privacy for Power Apps

**STEP 1**
Track Activity logging for Power Apps

Power Apps activities are now tracked from the Office 365 Security & Compliance Center. Office 365 tenant administrators reach the Security & Compliance Center by navigating to https://protection.office.com. From there, the Audit log search is found under the Search and investigation dropdown.

**STEP 2**
Ensure Data Privacy Compliance in Azure

Microsoft is committed to the highest levels of trust, transparency, standards conformance, and regulatory compliance. Microsoft's broad suite of cloud products and services are all built from the ground up to address the most rigorous security and privacy demands of our customers.

**STEP 3**
Responding to DSR requests for system-generated logs in Power Apps, Power Automate, and Common Data Service

Microsoft gives you the ability to access, export, and delete system-generated logs that may be deemed personal under the European Union (EU) General Data Protection Regulation (GDPR) broad definition of personal data. Examples of system-generated logs that may be deemed personal under GDPR include:

Product and service usage data, such as user activity logs

User search requests and query data
Data generated by product and services as a product of system functionality and interaction by users or other systems

Note that the ability to restrict or rectify data in system-generated logs is not supported. Data in system-generated logs constitutes factual actions conducted within the Microsoft cloud, and diagnostic data—including modifications to such data—would compromise the historical record of actions and increase fraud and security risks.

**STEP 4**
Datacenter Regions and Data Sovereignty - About the Microsoft Cloud Canada Datacenter

Model-driven apps in Dynamics 365, such as Dynamics 365 Sales and Customer Service are currently available and served from the datacenter regions in Toronto and Quebec City, joining Azure and Office 365 in providing the trusted Microsoft Cloud in Canada.

**STEP 5**
Manage Access to Apps by Using Security Roles

You can choose what users see and access from the My Apps page or the Customer Engagement home page by giving app access to specific security roles. Users will have access to apps based on the security roles they're assigned to.

No Best Practice Guide guarantees that your application will be 100% secure, compliant, or following the hundreds of data privacy regulations throughout the world, so it's important to keep up to date with the steps for technology implementation and configurations or any new Microsoft Security services or features outlined above but it is also important to focus on people and process. Ensure the supporting internal or managed service provider is educated and trained, make Secure Application Lifecycle and Change/Release Management a part of your routine process, and ensure continuous monitoring in order to identify, protect, detect, respond and recover.