TLP:CLEAR

POWER BI

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.0

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

TLP:CLEAR

REVISION HISTORY

Version	Summary of revisions	Edited By	Date
1.0	• Creation	CISA	08/13/2023

CONTENTS

1. CISA M365 SECURITY CONFIGURATION BASELINE FOR POWER BI

Microsoft 365 (M365) Power BI is a software as a service (SaaS) product from Microsoft that facilitates self-service business intelligence dashboards, reports, datasets, and visualizations. Power BI can connect to multiple different data sources, combine and shape data from those connections, then create reports and

dashboards to share with others. This secure configuration baseline (SCB) provides specific policies to strengthen Power BI security.

The Secure Cloud Business Applications (SCuBA) project run by the Cybersecurity and Infrastructure Security Agency (CISA) provides guidance and capabilities to secure federal civilian executive branch (FCEB) agencies' cloud business application environments and protect federal information that is created, accessed, shared, and stored in those environments.

The CISA SCuBA SCBs for Microsoft 365 (M365) help secure federal information assets stored within M365 cloud business application environments through consistent, effective, and manageable security configurations. CISA created baselines tailored to the federal government's threats and risk tolerance with the knowledge that every organization has different threat models and risk tolerance. Non-governmental organizations may also find value in applying these baselines to reduce risks.

The information in this document is being provided "as is" for INFORMATIONAL PURPOSES ONLY. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA. This document does not address, ensure compliance with, or supersede any law, regulation, or other authority. Entities are responsible for complying with any recordkeeping, privacy, and other laws that may apply to the use of technology. This document is not intended to, and does not, create any right or benefit for anyone against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

1.1 LICENSE COMPLIANCE AND COPYRIGHT

Portions of this document are adapted from documents in Microsoft's M365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents are linked throughout this document. The United States government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

1.2 ASSUMPTIONS

The **License Requirements** sections of this document assume the organization is using an M365 E3 or G3 license level at a minimum. Therefore, only licenses not included in E3/G3 are listed.

Agencies using Power BI may have a data classification scheme in place for the data entering Power BI.

- Agencies may connect more than one data source to their Power BI tenant.
- All data sources use a secure connection for data transfer to and from the Power BI tenant; the agency disallows non-secure connections.

1.3 KEY TERMINOLOGY

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Access to Power BI can be controlled by the user type. In this baseline, the types of users are defined as follows:

1. **Internal users**: Members of the agency's M365 tenant.
2. **External users** Members of a different M365 tenant.
3. **Business to business (B2B) guest users:** External users that are formally invited to view and/or edit Power BI workspace content and are added to the agency's Azure Active Directory (Azure AD) as guest users. These users authenticate with their home organization/tenant and are granted access to Power BI content by virtue of being listed as guest users in the tenant's Azure AD..
4. *Note*: These terms vary in use across Microsoft documentation.

2. BASELINE POLICIES

2.1 PUBLISH TO WEB

Power BI has the capability to publish reports and content to the web. This capability creates a publicly accessible web URL that does not require authentication or status as an Azure AD user to view it. While this may be needed for a specific use case or collaboration scenario, it is best practice to keep this setting off by default to prevent unintended and potentially sensitive data exposure.

If it is deemed necessary to make an exception and enable the feature, administrators should limit the ability to publish to the web to only specific security groups, instead of allowing the entire agency to publish data to the web.

2.2 POLICIES

2.2.1 MS.POWERBI.1.1v1

The Publish to Web feature SHOULD be disabled unless the agency mission requires the capability.

- *Rationale:* A publicly accessible web URL can be accessed by everyone, including malicious actors. This policy limits information available on the public web that is not specifically allowed to be published.
- *Last modified:* June 2023

2.3 RESOURCES

- About Power BI tenant settings | Microsoft Learn
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

2.4 LICENSE REQUIREMENTS

- N/A

2.5 IMPLEMENTATION

2.5.1 MS.POWERBI.1.1v1 Instructions

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant Settings**.
3. Scroll to **Export and sharing settings**.
4. Click **Publish to web** and set to **Disabled**.

3. POWER BI GUEST ACCESS

This section provides policies that help reduce guest user access risks related to Power BI data and resources. An agency with externally shareable Power BI resources and data must consider its unique risk tolerance when granting access to guest users.

3.1 POLICIES

3.1.1 MS.POWERBI.2.1v1

Guest user access to the Power BI tenant SHOULD be disabled unless the agency mission requires the capability.

- *Rationale:* Disabling external access to Power BI helps keep guest users from accessing potentially risky data and application programming interfaces (APIs). If an agency needs to allow guest access, this can be limited to users in specific security groups to curb risk.
- *Last modified:* June 2023

3.2 RESOURCES

- About Power BI tenant settings | Microsoft Learn
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

3.3 LICENSE REQUIREMENTS

- N/A

3.4 IMPLEMENTATION

3.4.1 MS.POWERBI.2.1v1 Instructions

To Disable Completely:

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant Settings**.
3. Scroll to **Export and sharing settings**.
4. Click on **Allow Azure Active Directory guest users to edit and manage content in the organization** and set to **Disabled**.

To Enable with Security Group(s):

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant Settings**.
3. Scroll to **Export and sharing settings**.
4. Click on **Allow Azure Active Directory guest users to edit and manage content in the organization** and set to **Enabled**.
5. Select the security group(s) you want to have access to the Power Bi tenant.
   Note: You may need to create a security group for this specific case.

4. POWER BI EXTERNAL INVITATIONS

This section provides policies that help reduce guest user invitation risks related to Power BI data and resources. The settings in this section control whether Power BI allows inviting external users to the agency's

organization through Power BI's sharing workflows and experiences. After an external user accepts the invite, they become an Azure AD B2B guest user in the organization. They will then appear in user pickers throughout the Power BI user experience.

4.1 POLICIES

4.1.1 MS.POWERBI.3.1v1

The Invite external users to your organization feature SHOULD be disabled unless agency mission requires the capability.

- *Rationale:* Disabling this feature prevents internal users from inviting guest users, limiting guest users' access to potentially risky data/APIs. If an agency needs to allow guest access, the invitation feature can be limited to users in specific security groups to minimize risk.
- *Last modified:* June 2023
- *Note:* If this feature is disabled, existing guest users in the tenant continue to have access to the Power BI items they already had access to, and they will continue to be listed in user picker experiences. After it is disabled, an external user who is not already a guest user cannot be added to the tenant through Power BI.

4.2 RESOURCES

- About Power BI Tenant settings | Microsoft Docs
- Distribute Power BI content to external guest users with Azure AD B2B | Microsoft Learn
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

4.3 LICENSE REQUIREMENTS

- N/A

4.4 IMPLEMENTATION

4.4.1 MS.POWERBI.3.1v1 Instructions

To disable completely:

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant Settings**.
3. Scroll to **Export and sharing settings**.
4. Click on **Invite external users to your organization** and set to **Disabled**.

To enable with security groups:

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant Settings**.
3. Scroll to **Export and sharing settings**.
4. Click on **Invite external users to your organization** and set to **Enabled**.
5. Select the security group(s) needed.
   Note: You may need to make a specific security group(s).

5. POWER BI SERVICE PRINCIPALS

Service principals are an authentication method that can be used to let an Azure AD application access Power BI service content and APIs. Power BI supports using service principals to manage application identities. Service principals use APIs to access tenant-level features, controlled by Power BI service administrators and enabled for the entire agency or for agency security groups. Accessing service principals can be controlled by creating dedicated security groups for them and using these groups in any Power BI tenant level-settings. If service principals are employed for Power BI, it is recommended that service principal credentials used for encrypting or accessing Power BI be stored in a key vault, with properly assigned access policies and regularly reviewed access permissions.

Several high-level use cases for service principals:

- Not possible to access a data source using service principals in Power BI (e.g., Azure Table storage).
- A user's service principal for accessing the Power BI service (e.g., app.powerbi.com and app.powerbigov.us).
- Power BI Embedded and other users of the Power BI REST APIs to interact with Power BI content.

5.1 POLICIES

5.1.1 MS.POWERBI.4.1v1

Service principals with access to APIs SHOULD be restricted to specific security groups.

- *Rationale:* With unrestricted service principals, unwanted access to APIs is possible. Allowing service principals through security groups, and only where necessary, mitigates this risk.
- *Last modified:* June 2023

5.1.2 MS.POWERBI.4.2v1

Service principals creating and using profiles SHOULD be restricted to specific security groups.

- *Rationale:* With unrestricted service principals creating/using profiles, there is risk of an unauthorized user using a profile with more permissions than they have. Allowing service principals through security groups will mitigate that risk.
- *Last modified:* June 2023

5.2 RESOURCES

- Automate Premium workspace and dataset tasks with service principal | Microsoft Learn
- Embed Power BI content with service principal and an application secret | Microsoft Learn
- Embed Power BI content with service principal and a certificate | Microsoft Learn
- Enable service principal authentication for read-only admin APIs | Microsoft Learn
- Microsoft Power BI Embedded Developer Code Samples | Microsoft GitHub
- Azure security baseline for Power BI | Microsoft Learn

5.3 LICENSE REQUIREMENTS

- N/A

5.4 IMPLEMENTATION

5.4.1 MS.POWERBI.4.1v1 Instructions

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant settings**.
3. Scroll to **Developer settings**.
4. Click on **Allow Service Principals to use Power BI APIs** set to **Enabled**. Choose a specific security group allowed to use service principles for the APIs.

5.4.2 MS.POWERBI.4.2v1 Instructions

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant settings**.
3. Scroll to **Developer settings**.
4. Then, click on **Allow Service Principals to create and use profiles** and set to **Enabled**. Choose a specific security group allowed to use service principles to create and use profiles.

6. POWER BI RESOURCEKEY AUTHENTICATION

This setting pertains to the security and development of Power BI Embedded content. The Power BI tenant states, "For extra security, block using ResourceKey-based authentication." This baseline statement recommends, but does not mandate, setting ResourceKey-based authentication to the blocked state.

For streaming datasets created using the Power BI service user interface, the dataset owner receives a URL including a resource key. This key authorizes the requestor to push data into the dataset without using an Azure AD OAuth bearer token, so please keep in mind the implications of having a secret key in the URL when working with this type of dataset and method.

This setting applies to streaming and PUSH datasets. If ResourceKey-based authentication is blocked, users with a resource key will not be allowed to send data to stream and PUSH datasets using the API. However, if developers have an approved need to leverage this feature, an exception to the policy can be investigated.

6.1 POLICIES

6.1.1 MS.POWERBI.5.1v1

ResourceKey-based authentication SHOULD be blocked unless a specific use case (e.g., streaming and/or PUSH datasets) merits its use.

- *Rationale:* If resource keys are allowed, someone can move data without Azure AD OAuth bearer token, causing possibly malicious or junk data to be stored. Disabling resource keys reduces risk that an unauthorized individual will make changes.
- *Last modified:* June 2023

6.2 RESOURCES

- Power BI Tenant settings | Microsoft Learn
- Real-time streaming in Power BI | Microsoft Learn

6.3 LICENSE REQUIREMENTS

- N/A

6.4 IMPLEMENTATION

6.4.1 MS.POWERBI.5.1v1 Instructions

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant settings**.
3. Scroll to **Developer settings**.
4. Click on **Block ResourceKey Authentication** and set to **Enabled**.

7. PYTHON AND R VISUAL SHARING HTML

Power BI can interact with Python and R scripts to integrate visualizations from these languages. Python visuals are created from Python scripts, which could contain code with security or privacy risks. When attempting to view or interact with a Python visual for the first time, a user is presented with a security warning message. Python and R visuals should only be enabled if the author and source are trusted, or after a code review of the Python/R script(s) in question is conducted and the scripts are deemed free of security risks.

7.1 POLICIES

7.1.1 MS.POWERBI.6.1v1

Python and R interactions SHOULD be disabled.

- *Rationale:* External code poses a security and privacy risk, as there is no good way to regulate what is done with the data or integrations. Disabling this will reduce the risk of a data leak or malicious actor.
- *Last modified:* June 2023

7.2 RESOURCES

- Create Power BI visuals with Python | Microsoft Learn

7.3 LICENSE REQUIREMENTS

- N/A

7.4 IMPLEMENTATION

7.4.1 MS.POWERBI.6.1v1 Instructions

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant settings**.
3. Scroll to **R and Python Visuals Settings**.
4. Click on **Interact with and share R and Python visuals** and set to **Disabled**.

8. POWER BI SENSITIVE DATA

Use of Microsoft Information Protection sensitivity labels on Power BI reports, dashboards, datasets, and dataflows guards sensitive content against unauthorized data access and leakage. This can also guard against unwanted aggregation and commingling.

Note: At this baseline's time of writing, data loss prevention (DLP) profiles are in preview status for Power BI. Once released for general availability and government, DLP profiles represent another available tool for securing Power BI datasets. Refer to the *Defender for Office 365 Minimum Viable Secure Configuration Baseline* for more on DLP.

8.1 POLICIES

8.1.1 MS.POWERBI.7.1v1

Sensitivity labels SHOULD be enabled for Power BI and employed for sensitive data per enterprise data protection policies.

- *Rationale:* A document without sensitivity labels may be opened unknowingly, potentially exposing data to someone who is not supposed to have access to it. This policy will help organize and classify data, making it easier to keep data out of the wrong hands.
- *Last modified:* June 2023

8.2 RESOURCES

- Enable sensitivity labels in Power BI | Microsoft Learn
- Data loss prevention policies for Power BI | Microsoft Learn
- Data Protection in Power BI | Microsoft Learn
- Power BI Security Baseline v2.0 | Microsoft benchmarks GitHub repo

8.3 LICENSE REQUIREMENTS

- An Azure Information Protection Premium P1 or Premium P2 license is required to apply or view Microsoft Information Protection sensitivity labels in Power BI. Azure Information Protection can be purchased either standalone or through one of the Microsoft licensing suites. See Azure Information Protection service description for details
- Azure Information Protection sensitivity labels need to be migrated to the Microsoft Information Protection Unified Labeling platform to be used in Power BI.
- To apply labels to Power BI content and files, a user must have a Power BI Pro or Premium Per User (PPU) license, in addition to one of the previously mentioned Azure Information Protection licenses.
- Before enabling sensitivity labels on the agency's tenant, ensure sensitivity labels have been defined and published for relevant users and groups. See Create and configure sensitivity labels and their policies for detail.

8.4 IMPLEMENTATION

8.4.1 MS.POWERBI.7.1v1 Instructions

1. Navigate to the **PowerBI Admin Portal**.
2. Click on **Tenant settings**.
3. Scroll to **Information protection**.

4. Click on **Allow users to apply sensitivity labels for content** and set to **Enabled.** Define who can apply and change sensitivity labels in Power BI assets.

APPENDIX A: INFORMATION PROTECTION CONSIDERATIONS

Several best practices and approaches are available to protect sensitive data in Power BI:

- Leverage sensitivity labels via Microsoft Information Protection.
- Power BI allows service users to bring their own key to protect data at rest.
- Customers have the option to keep data sources on premises and leverage Direct Query or Live Connect with an on-premises data gateway to minimize data exposure to the cloud service.
- Implement row-level security in Power BI datasets.

Implementation Steps:

Apply sensitivity labels from data sources to their data in Power BI

When this setting is enabled, Power BI datasets connecting to sensitivity-labeled data in supported data sources can inherit those labels, so the data remains classified and secure when brought into Power BI. For details about sensitivity label inheritance from data sources, see below:

To enable sensitivity label inheritance from data sources:

1. Navigate to the **Power BI tenant settings**.
2. Select **Information protection** -> **Apply sensitivity labels from data sources to their data in Power BI (preview)**.
3. Enable **Restrict content with protected labels from being shared via link with everyone in your agency**.

When this setting is enabled, users cannot generate a sharing link for people in the agency for content with protection settings in the sensitivity label.

Sensitivity labels with protection settings include encryption or content markings. For example, the agency may have a "Highly Confidential" label including encryption and applies a "Highly Confidential" watermark to content with this label. When this tenant setting is enabled and a report has a sensitivity label with protection settings, users cannot create sharing links for people in the agency.

Information Protection Prerequisites Specific to Power BI

- An Azure Information Protection Premium P1 or Premium P2 license is required to apply or view Microsoft Information Protection sensitivity labels in Power BI. Azure Information Protection can be purchased either standalone or through one of the Microsoft licensing suites. See Azure Information Protection service description for details.
- Azure Information Protection sensitivity labels need to be migrated to the Microsoft Information Protection Unified Labeling platform to be used in Power BI.
- To apply labels to Power BI content and files, a user must have a Power BI Pro or PPU license, in addition to one of the previously mentioned Azure Information Protection licenses.
- Before enabling sensitivity labels on the agency's tenant, make sure sensitivity labels have been defined and published for relevant users and groups. See Create and configure sensitivity labels and their policies for detail.

High-Level Steps to Use Bring Your Own Key (BYOK) Feature in Power BI

First, confirm having the latest Power BI Management cmdlet. Install the latest version by running Install-Module -Name MicrosoftPowerBIMgmt. More information about the Power BI cmdlet and its parameters is available in Power BI PowerShell cmdlet module.

Follow steps in Bring Your Own (encryption) Keys for Power BI.

Row-Level Security Implementation

Row-level security (RLS) involves several configuration steps, which should be completed in the following order.

1. Create a report in Microsoft Power BI Desktop.
2. Import the data.
3. Confirm the data model between both tables.
4. Create the report visuals.
5. Create RLS roles in Power BI Desktop by using Data Analysis Expressions (DAX).
6. Test the roles in Power BI Desktop.
7. Deploy the report to Microsoft Power BI service.
8. Add members to the role in Power BI service.
9. Test the roles in Power BI service.

Reference Microsoft Power BI documentation for additional detail on row-level security configuration.

Related Resources

- Sensitivity labels in Power BI | Microsoft Learn
- Bring your own encryption keys for Power BI | Microsoft Learn
- What is an on-premises data gateway? | Microsoft Learn
- Row-level security (RLS) with Power BI | Microsoft Learn
- Power BI PowerShell cmdlets and modules references | Microsoft Learn

APPENDIX B: SOURCE CODE AND CREDENTIAL SECURITY CONSIDERATIONS

Exposing secrets via collaboration spaces is a security concern when using Power BI.

For Power BI embedded applications, it is recommended to implement a source code scanning solution to identify credentials within the code of any app housing embedded Power BI report(s). A source code scanner can encourage moving discovered credentials to more secure locations, such as Azure key vault.

Store encryption keys or service principal credentials used for encrypting or accessing Power BI in a key vault, assign proper access policies to the vault, and regularly review access permissions.

For regulatory or other compliance reasons, some agencies may need to use BYOK, which is supported by Power BI. By default, Power BI uses Microsoft-managed keys to encrypt the data. In Power BI Premium, users can use their own keys for data at-rest imported into a dataset. See Data source and storage considerations for more information.

- For Power BI embedded applications, a best practice is to implement a source code scanning solution to identify credentials within the code of the app housing the embedded Power BI report(s).
- If required under specific regulations, agencies need a strategy for maintaining control and governance of their keys. The BYOK functionality is one option.

Prerequisites

- Implementers must do their own due diligence in selecting a source code scanner that integrates with their specific environment. Microsoft documentation references an Open Web Application Security Project, Source Code Analysis Tools; which is a guide to third-party scanners. This baseline does not endorse or advise on selecting or using any specific third-party tool.
- If BYOK is deemed to be a requirement:
  - Power BI Premium is required for BYOK.
  - To use BYOK, the Power BI tenant admin must upload data to the Power BI service from a Power BI Desktop (PBIX) file.
  - RSA keys must be 4096-bit.
  - Enable BYOK in the tenant.

BYOK Implementation High-Level Steps

Enable BYOK at the tenant level via PowerShell by first introducing the encryption keys created and stored in Azure Key Vault to the Power BI tenant.

Then assign these encryption keys per Premium capacity for encrypting content in the capacity.

To enable bringing the agency's key for Power BI, the high-level configuration steps are as follows:

1. Add the Power BI service as a service principal for the key vault, with wrap and unwrap permissions.
2. Create an RSA key with a 4096-bit length (or use an existing key of this type), with wrap and unwrap permissions.
3. To turn on BYOK, Power BI Tenant administrators must use a set of Power BI Admin PowerShell Cmdlets added to the Power BI Admin Cmdlets.

Follow detailed steps in Microsoft's Bring your own encryption keys for Power BI.

Related Resources

- Bring your own encryption keys for Power BI | Microsoft Learn
- Microsoft Security DevOps Azure DevOps extension
- For GitHub, the agency can use the native secret scanning feature to identify credentials or other form of secrets within code at About secret scanning | GitHub docs
- Announcing General Availability of Bring Your Own Key (BYOK) for Power BI Premium

APPENDIX C: FILE EXPORT AND VISUAL ARTIFACT CONSIDERATIONS

Exporting data from Power BI to image files and comma-separated value (.csv) file format has data security implications. For example, if row-level security (RLS) features are in use in Power BI, an export to image or .csv could allow a user to inadvertently decouple that setting and expose data to a party who does not have permissions or a need to know that previously secured data. A similar scenario applies for information protection sensitivity labels.

A message regarding this condition is provided in the Power BI tenant settings for the types of exports.

In contrast to this, Power BI applies these protection settings (RLS, sensitivity labels) when the report data leaves Power BI via a supported export method, such as export to Excel, PowerPoint, or PDF, download to .pbix, and Save (Desktop). In this case, only authorized users will be able to open protected files.

Copy and Paste Visuals

Power BI can allow users to copy and paste visuals from Power BI reports as static images into external applications. This could represent a data security risk in some contexts. The agency must evaluate whether this represents risk for its data artifacts and whether to turn this off in the Export and Sharing Settings.

Related Resources

- Sensitivity labels in Power BI | Microsoft Learn
- Say No to Export Data, Yes to Analyze in Excel
- Power BI Governance – Why you should consider disabling Export to Excel

Implementation settings

1. In the **Power BI tenant settings**, under **Export and sharing settings**, administrators can opt to toggle off both **Export reports as image files** and **Export to .csv**.
2. In the **Power BI tenant** settings, under **Export and sharing settings**, administrators can opt to toggle off **Copy and paste visuals**.

Establishing Private Network Access Connections Using Azure Private Link

When connecting to Azure services intended to supply Power BI datasets, agencies should consider connecting their Power BI tenant to an Azure Private Link endpoint and disable public internet access.

In this configuration, Azure Private Link and Azure Networking private endpoints are used to send data traffic privately using Microsoft's backbone network infrastructure. The data travels the Microsoft private network backbone, instead of going across the internet.

Using private endpoints with Power BI helps ensure traffic will flow over the Azure backbone to a private endpoint for Azure cloud-based resources.

Within this configuration, there is also the capability to disable public access to Power BI datasets.

High-Level Implementation Steps

Note: It is imperative the VNET and virtual machine (VM) are configured before disabling public internet access.

1. Enable private endpoints for Power BI.
2. Create a Power BI resource in the Azure portal.
3. Create a virtual network.
4. Create a VM.
5. Create a private endpoint.
6. Connect to a VM using Remote Desktop.
7. Access Power BI privately from the virtual machine.
8. Disable public access for Power BI.

Related Resources

- Private endpoints for secure access to Power BI | Microsoft Learn
- Azure security baseline for Power BI

Best Practices for Service Principals

- Evaluate whether certificates or secrets are a more secure option for the implementation.
  Note: Microsoft recommends certificates over secrets.
- Use the principle of least privilege in implementing service principals; only provide the ability to create app registrations to entities requiring it.
- Instead of enabling service principals for the entire agency, implement for a dedicated security group.

Note: This policy is only applicable if the setting **Allow Service Principals to use Power BI APIs** is enabled.