**AppServices recommendations**

[**API App should only be accessible over HTTPS**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bf82a334-13b6-ca57-ea75-096fc2ffce50)

**Description**: Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. (Related policy: [API App should only be accessible over HTTPS](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fb7ddfbdc-1260-477d-91fd-98bd9be789a6)).

**Severity**: Medium

[**CORS should not allow every resource to access API Apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e40df93c-7a7c-1b0a-c787-9987ceb98e54)

**Description**: Cross-Origin Resource Sharing (CORS) should not allow all domains to access your API app. Allow only required domains to interact with your API app. (Related policy: [CORS should not allow every resource to access your API App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2f358c20a6-3f9e-4f0e-97ff-c6ce485e2aac)).

**Severity**: Low

[**CORS should not allow every resource to access Function Apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/7b3d4796-9400-2904-692b-4a5ede7f0a1e)

**Description**: Cross-Origin Resource Sharing (CORS) should not allow all domains to access your Function app. Allow only required domains to interact with your Function app. (Related policy: [CORS should not allow every resource to access your Function Apps](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2f0820b7b9-23aa-4725-a1ce-ae4558f718e5)).

**Severity**: Low

[**CORS should not allow every resource to access Web Applications**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/df4d1739-47f0-60c7-1706-3731fea6ab03)

**Description**: Cross-Origin Resource Sharing (CORS) should not allow all domains to access your web application. Allow only required domains to interact with your web app. (Related policy: [CORS should not allow every resource to access your Web Applications](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2f5744710e-cc2f-4ee8-8809-3b11e89f4bc9)).

**Severity**: Low

[**Diagnostic logs in App Service should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/40394a2c-60fb-7cc5-1944-065772e94f05)

**Description**: Audit enabling of diagnostic logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised (No related policy).

**Severity**: Medium

[**Ensure API app has Client Certificates Incoming client certificates set to On**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ce2768c3-a7c7-1bbf-22cd-f9db675a9807)

**Description**: Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app. (Related policy: [Ensure API app has 'Client Certificates (Incoming client certificates)' set to 'On'](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0c192fe8-9cbb-4516-85b3-0ade8bd03886)).

**Severity**: Medium

[**FTPS should be required in API apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/67fc622b-4ce6-8c52-08ae-9f830036b757)

**Description**: Enable FTPS enforcement for enhanced security (Related policy: [FTPS only should be required in your API App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f9a1b8c48-453a-4044-86c3-d8bfd823e4f5)).

**Severity**: High

[**FTPS should be required in function apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/972a6579-f38f-c0b9-1b4b-a5bbeba3ab5b)

**Description**: Enable FTPS enforcement for enhanced security (Related policy: [FTPS only should be required in your Function App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f399b2637-a50f-4f95-96f8-3a145476eb15)).

**Severity**: High

[**FTPS should be required in web apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/19beaa2a-a126-b4dd-6d35-617f6cc83fca)

**Description**: Enable FTPS enforcement for enhanced security (Related policy: [FTPS should be required in your Web App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f4d24b6d4-5e53-4a4f-a7f4-618fa573ee4b)).

**Severity**: High

[**Function App should only be accessible over HTTPS**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/cb0acdc6-0846-fd48-debe-9905af151b6d)

**Description**: Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. (Related policy: [Function App should only be accessible over HTTPS](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f6d555dd1-86f2-4f1c-8ed7-5abae7c6cbab)).

**Severity**: Medium

[**Function apps should have Client Certificates (Incoming client certificates) enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c2ab4bea-c663-3259-a4cd-03a8feb02825)

**Description**: Client certificates allow for the app to request a certificate for incoming requests. Only clients with valid certificates will be able to reach the app. (Related policy: [Function apps should have 'Client Certificates (Incoming client certificates)' enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2feaebaea7-8013-4ceb-9d14-7eb32271373c)).

**Severity**: Medium

[**Java should be updated to the latest version for API apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/08a3b009-0178-ee60-e357-e7ee5aea59c7)

**Description**: Periodically, newer versions are released for Java either due to security flaws or to include additional functionality. Using the latest Python version for API apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: [Ensure that 'Java version' is the latest, if used as a part of the API app](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f88999f4c-376a-45c8-bcb3-4058f713cf39)).

**Severity**: Medium

[**Managed identity should be used in API apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/cc6d1865-7617-3cb2-cf7d-4cfc01ece1df)

**Description**: For enhanced authentication security, use a managed identity. On Azure, managed identities eliminate the need for developers to have to manage credentials by providing an identity for the Azure resource in Azure AD and using it to obtain Azure Active Directory (Azure AD) tokens. (Related policy: [Managed identity should be used in your API App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fc4d441f8-f9d9-4a9e-9cef-e82117cb3eef)).

**Severity**: Medium

[**Managed identity should be used in function apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/23aa9cbe-c2fb-6a2f-6c97-885a6d48c4d1)

**Description**: For enhanced authentication security, use a managed identity. On Azure, managed identities eliminate the need for developers to have to manage credentials by providing an identity for the Azure resource in Azure AD and using it to obtain Azure Active Directory (Azure AD) tokens. (Related policy: [Managed identity should be used in your Function App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0da106f2-4ca3-48e8-bc85-c638fe6aea8f)).

**Severity**: Medium

[**Managed identity should be used in web apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/4a3d7cd3-f17c-637a-1ffc-614a01dd03cf)

**Description**: For enhanced authentication security, use a managed identity. On Azure, managed identities eliminate the need for developers to have to manage credentials by providing an identity for the Azure resource in Azure AD and using it to obtain Azure Active Directory (Azure AD) tokens. (Related policy: [Managed identity should be used in your Web App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f2b9ad585-36bc-4615-b300-fd4435808332)).

**Severity**: Medium

[**Microsoft Defender for App Service should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/0876ef51-fee7-449d-ba1e-f2662c7e43c6)

**Description**: Microsoft Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks. Microsoft Defender for App Service can discover attacks on your applications and identify emerging attacks.

Important: Remediating this recommendation will result in charges for protecting your App Service plans. If you don't have any App Service plans in this subscription, no charges will be incurred. If you create any App Service plans on this subscription in the future, they will automatically be protected and charges will begin at that time. Learn more in [Protect your web apps and APIs](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction). (Related policy: [Azure Defender for App Service should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f2913021d-f2fd-4f3d-b958-22354e2bdbcb)).

**Severity**: High

[**PHP should be updated to the latest version for API apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/6b86d069-b3c3-b4d7-47c7-e73ddf786a63)

**Description**: Periodically, newer versions are released for PHP software either due to security flaws or to include additional functionality. Using the latest PHP version for API apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: [Ensure that 'PHP version' is the latest, if used as a part of the API app](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1bc1795e-d44a-4d48-9b3b-6fff0fd5f9ba)).

**Severity**: Medium

[**Python should be updated to the latest version for API apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c2c90d64-38e2-e984-1457-7f4a98168c72)

**Description**: Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest Python version for API apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: [Ensure that 'Python version' is the latest, if used as a part of the API app](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f74c3584d-afae-46f7-a20a-6f8adba71a16)).

**Severity**: Medium

[**Remote debugging should be turned off for API App**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/9172da4e-9571-6e33-2b5b-d742847f3be7)

**Description**: Remote debugging requires inbound ports to be opened on an API app. Remote debugging should be turned off. (Related policy: [Remote debugging should be turned off for API Apps](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2fe9c8d085-d9cc-4b17-9cdc-059f1f01f19e)).

**Severity**: Low

[**Remote debugging should be turned off for Function App**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/093c685b-56dd-13a3-8ed5-887a001837a2)

**Description**: Remote debugging requires inbound ports to be opened on an Azure Function app. Remote debugging should be turned off. (Related policy: [Remote debugging should be turned off for Function Apps](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2f0e60b895-3786-45da-8377-9c6b4b6ac5f9)).

**Severity**: Low

[**Remote debugging should be turned off for Web Applications**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/64b8637e-4e1d-76a9-0fc9-c1e487a97ed8)

**Description**: Remote debugging requires inbound ports to be opened on a web application. Remote debugging is currently enabled. If you no longer need to use remote debugging, it should be turned off. (Related policy: [Remote debugging should be turned off for Web Applications](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2fcb510bfd-1cba-4d9f-a230-cb0976f4bb71)).

**Severity**: Low

[**TLS should be updated to the latest version for API apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/5a659d57-117d-bb18-65f6-54e51da1bb9b)

**Description**: Upgrade to the latest TLS version. (Related policy: [Latest TLS version should be used in your API App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f8cb6aa8b-9e41-4f4e-aa25-089a7ac2581e)).

**Severity**: High

[**TLS should be updated to the latest version for function apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/15be5f3c-e0a4-c0fa-fbff-8e50339b4b22)

**Description**: Upgrade to the latest TLS version. (Related policy: [Latest TLS version should be used in your Function App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ff9d614c5-c173-4d56-95a7-b4437057d193)).

**Severity**: High

[**TLS should be updated to the latest version for web apps**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/2a54c352-7ca4-4bae-ad46-47ecd9595bd2)

**Description**: Upgrade to the latest TLS version. (Related policy: [Latest TLS version should be used in your Web App](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ff0e6e85b-9b9f-4a4b-b67b-f730d42f1b0b)).

**Severity**: High

[**Web Application should only be accessible over HTTPS**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1b351b29-41ca-6df5-946c-c190a56be5fe)

**Description**: Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. (Related policy: [Web Application should only be accessible over HTTPS](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fa4af4a39-4135-47fb-b175-47fbdf85311d)).

**Severity**: Medium

[**Web apps should request an SSL certificate for all incoming requests**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ca4e6a5a-3a9a-bad3-798a-d420a1d9bd6d)

**Description**: Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app. (Related policy: [Ensure WEB app has 'Client Certificates (Incoming client certificates)' set to 'On'](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5bb220d9-2698-4ee4-8404-b9c30c9df609)).

**Severity**: Medium

**Compute recommendations**

[**Adaptive application controls for defining safe applications should be enabled on your machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/35f45c95-27cf-4e52-891f-8390d1de5828)

**Description**: Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Defender for Cloud uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications. (Related policy: [Adaptive application controls for defining safe applications should be enabled on your machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f47a6b606-51aa-4496-8bb7-64b11cf66adc)).

**Severity**: High

[**Allowlist rules in your adaptive application control policy should be updated**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1234abcd-1b53-4fd4-9835-2c2fa3935313)

**Description**: Monitor for changes in behavior on groups of machines configured for auditing by Defender for Cloud's adaptive application controls. Defender for Cloud uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies. (Related policy: [Allowlist rules in your adaptive application control policy should be updated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f123a3936-f020-408a-ba0c-47873faf1534)).

**Severity**: High

[**Authentication to Linux machines should require SSH keys**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/22441184-2f7b-d4a0-e00b-4c5eaef4afc9)

**Description**: Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more in [Detailed steps: Create and manage SSH keys for authentication to a Linux VM in Azure](https://learn.microsoft.com/en-us/azure/virtual-machines/linux/create-ssh-keys-detailed). (Related policy: [Audit Linux machines that are not using SSH key for authentication](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f630c64f9-8b6b-4c64-b511-6544ceff6fd6)).

**Severity**: Medium

[**Automation account variables should be encrypted**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b12bc79e-4f12-44db-acda-571820191ddc)

**Description**: It is important to enable encryption of Automation account variable assets when storing sensitive data. (Related policy: [Automation account variables should be encrypted](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2f3657f5a0-770e-44a3-b44e-9431ba1e9735)).

**Severity**: High

[**Azure Backup should be enabled for virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f2f595ec-5dc6-68b4-82ef-b63563e9c610)

**Description**: Protect the data on your Azure virtual machines with Azure Backup. Azure Backup is an Azure-native, cost-effective, data protection solution. It creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or specific files. (Related policy: [Azure Backup should be enabled for Virtual Machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f013e242c-8828-4970-87b3-ab247555486d)).

**Severity**: Low

[**Container hosts should be configured securely**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/0677209d-e675-2c6f-e91a-54cef2878663)

**Description**: Remediate vulnerabilities in security configuration on machines with Docker installed to protect them from attacks. (Related policy: [Vulnerabilities in container security configurations should be remediated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fe8cbc669-f12d-49eb-93e7-9273119e9933)).

**Severity**: High

[**Diagnostic logs in Azure Stream Analytics should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f11b27f2-8c49-5bb4-eff5-e1e5384bf95e)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Azure Stream Analytics should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ff9be5368-9bf5-4b84-9e0a-7850da98bb46)).

**Severity**: Low

[**Diagnostic logs in Batch accounts should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/32771b45-220c-1a8b-584e-fdd5a2584a66)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Batch accounts should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f428256e6-1fac-4f48-a757-df34c2b3336d)).

**Severity**: Low

[**Diagnostic logs in Event Hubs should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1597605a-0faf-5860-eb74-462ae2e9fc21)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Event Hubs should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f83a214f7-d01a-484b-91a9-ed54470c9a6a)).

**Severity**: Low

[**Diagnostic logs in Logic Apps should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/91387f44-7e43-4ecc-55f0-46f5adee3dd5)

**Description**: To ensure you can recreate activity trails for investigation purposes when a security incident occurs or your network is compromised, enable logging. If your diagnostic logs aren't being sent to a Log Analytics workspace, Azure Storage account, or Azure Event Hubs, ensure you've configured diagnostic settings to send platform metrics and platform logs to the relevant destinations. Learn more in Create diagnostic settings to send platform logs and metrics to different destinations. (Related policy: [Diagnostic logs in Logic Apps should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f34f95f76-5386-4de7-b824-0d8478470c9d)).

**Severity**: Low

[**Diagnostic logs in Service Bus should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f19ab7d9-5ff2-f8fd-ab3b-0bf95dcb6889)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Service Bus should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ff8d36e2f-389b-4ee4-898d-21aeb69a0f45)).

**Severity**: Low

[**Diagnostic logs in Virtual Machine Scale Sets should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/961eb649-3ea9-f8c2-6595-88e9a3aeedeb)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Virtual Machine Scale Sets should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f7c1b1214-f927-48bf-8882-84f0af6588b1)).

**Severity**: High

[**EDR configuration issues should be resolved on virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/dc5357d0-3858-4d17-a1a3-072840bff5be)

**Description**: To protect virtual machines from the latest threats and vulnerabilities, resolve all identified configuration issues with the installed Endpoint Detection and Response (EDR) solution.  
Note: Currently, this recommendation only applies to resources with Microsoft Defender for Endpoint (MDE) enabled.

**Severity**: Low

[**EDR solution should be installed on Virtual Machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/06e3a6db-6c0c-4ad9-943f-31d9d73ecf6c)

**Description**: Installing an Endpoint Detection and Response (EDR) solution on virtual machines is important for protection against advanced threats. EDRs aid in preventing, detecting, investigating, and responding to these threats. Microsoft Defender for Servers can be used to deploy Microsoft Defender for Endpoint. If a resource is classified as "Unhealthy", it indicates the absence of a supported EDR solution. If an EDR solution is installed but not discoverable by this recommendation, it can be exempted. Without an EDR solution, the virtual machines are at risk of advanced threats.

**Severity**: High

[**Endpoint protection health issues on virtual machine scale sets should be resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e71020c2-860c-3235-cd39-04f3f8c936d2)

**Description**: Remediate endpoint protection health failures on your virtual machine scale sets to protect them from threats and vulnerabilities. (Related policy: [Endpoint protection solution should be installed on virtual machine scale sets](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f26a828e1-e88f-464e-bbb3-c134a282b9de)).

**Severity**: Low

[**Endpoint protection should be installed on virtual machine scale sets**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/21300918-b2e3-0346-785f-c77ff57d243b)

**Description**: Install an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities. (Related policy: [Endpoint protection solution should be installed on virtual machine scale sets](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f26a828e1-e88f-464e-bbb3-c134a282b9de)).

**Severity**: High

[**File integrity monitoring should be enabled on machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/9b7d740f-c271-4bfd-88fb-515680c33440)

**Description**: Defender for Cloud has identified machines that are missing a file integrity monitoring solution. To monitor changes to critical files, registry keys, and more on your servers, enable file integrity monitoring. When the file integrity monitoring solution is enabled, create data collection rules to define the files to be monitored. To define rules, or see the files changed on machines with existing rules, go to the [file integrity monitoring management page](https://aka.ms/FimMMA). (No related policy)

**Severity**: High

[**Guest Attestation extension should be installed on supported Linux virtual machine scale sets**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/a9a53f4f-26b6-3d68-33f3-2ec1f2452b5d)

**Description**: Install Guest Attestation extension on supported Linux virtual machine scale sets to allow Microsoft Defender for Cloud to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment only applies to trusted launch enabled Linux virtual machine scale sets.

Important: Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were initially created without it. Learn more about [Trusted launch for Azure virtual machines](https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch). (No related policy)

**Severity**: Low

[**Guest Attestation extension should be installed on supported Linux virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e94a7421-fc27-7a4d-e9ba-2ba01384cacd)

**Description**: Install Guest Attestation extension on supported Linux virtual machines to allow Microsoft Defender for Cloud to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment only applies to trusted launch enabled Linux virtual machines.

Important: Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were initially created without it. Learn more about [Trusted launch for Azure virtual machines](https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch). (No related policy)

**Severity**: Low

[**Guest Attestation extension should be installed on supported Windows virtual machine scale sets**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/02e8ca50-0e7e-cc34-0b91-215af2904248)

**Description**: Install Guest Attestation extension on supported virtual machine scale sets to allow Microsoft Defender for Cloud to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment only applies to trusted launch enabled virtual machine scale sets.

Important: Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were initially created without it. Learn more about [Trusted launch for Azure virtual machines](https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch). (No related policy)

**Severity**: Low

[**Guest Attestation extension should be installed on supported Windows virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/874b14bd-b49e-495a-88c6-46acb89b0a33)

**Description**: Install Guest Attestation extension on supported virtual machines to allow Microsoft Defender for Cloud to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment only applies to trusted launch enabled virtual machines.

Important: Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were initially created without it. Learn more about [Trusted launch for Azure virtual machines](https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch). (No related policy)

**Severity**: Low

[**Guest Configuration extension should be installed on machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/6c99f570-2ce7-46bc-8175-cde013df43bc)

**Description**: To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as [Windows Exploit guard should be enabled](https://aka.ms/gcpol). (Related policy: [Virtual machines should have the Guest Configuration extension](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2fae89ebca-1c92-4898-ac2c-9f63decb045c)).

**Severity**: Medium

[**Install endpoint protection solution on virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/83f577bd-a1b6-b7e1-0891-12ca19d1e6df)

**Description**: Install an endpoint protection solution on your virtual machines, to protect them from threats and vulnerabilities. (Related policy: [Monitor missing Endpoint Protection in Azure Security Center](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2faf6cd1bd-1635-48cb-bde7-5b15693900b9)).

**Severity**: High

[**Linux virtual machines should enforce kernel module signature validation**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e2f798b8-621a-4d46-99d7-1310e09eba26)

**Description**: To help mitigate against the execution of malicious or unauthorized code in kernel mode, enforce kernel module signature validation on supported Linux virtual machines. Kernel module signature validation ensures that only trusted kernel modules will be allowed to run. This assessment only applies to Linux virtual machines that have the Azure Monitor Agent installed. (No related policy)

**Severity**: Low

[**Linux virtual machines should use only signed and trusted boot components**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ad50b498-f90c-451f-886f-d0a169cc5002)

**Description**: With Secure Boot enabled, all OS boot components (boot loader, kernel, kernel drivers) must be signed by trusted publishers. Defender for Cloud has identified untrusted OS boot components on one or more of your Linux machines. To protect your machines from potentially malicious components, add them to your allowlist or remove the identified components. (No related policy)

**Severity**: Low

[**Linux virtual machines should use Secure Boot**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/0396b18c-41aa-489c-affd-4ee5d1714a59)

**Description**: To protect against the installation of malware-based rootkits and boot kits, enable Secure Boot on supported Linux virtual machines. Secure Boot ensures that only signed operating systems and drivers will be allowed to run. This assessment only applies to Linux virtual machines that have the Azure Monitor Agent installed. (No related policy)

**Severity**: Low

[**Log Analytics agent should be installed on Linux-based Azure Arc-enabled machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/720a3e77-0b9a-4fa9-98b6-ddf0fd7e32c1)

**Description**: Defender for Cloud uses the Log Analytics agent (also known as OMS) to collect security events from your Azure Arc machines. To deploy the agent on all your Azure Arc machines, follow the remediation steps. (No related policy)

**Severity**: High

[**Log Analytics agent should be installed on virtual machine scale sets**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/45cfe080-ceb1-a91e-9743-71551ed24e94)

**Description**: Defender for Cloud collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats. Data is collected using the [Log Analytics agent](https://learn.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent), formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. You'll also need to follow that procedure if your VMs are used by an Azure managed service such as Azure Kubernetes Service or Azure Service Fabric. You cannot configure auto-provisioning of the agent for Azure virtual machine scale sets. To deploy the agent on virtual machine scale sets (including those used by Azure managed services such as Azure Kubernetes Service and Azure Service Fabric), follow the procedure in the remediation steps. (Related policy: [Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fa3a6ea0c-e018-4933-9ef0-5aaa1501449b)).

**Severity**: High

[**Log Analytics agent should be installed on virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/d1db3318-01ff-16de-29eb-28b344515626)

**Description**: Defender for Cloud collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats. Data is collected using the [Log Analytics agent](https://learn.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent), formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. This agent is also required if your VMs are used by an Azure managed service such as Azure Kubernetes Service or Azure Service Fabric. We recommend configuring [auto-provisioning](https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection) to automatically deploy the agent. If you choose not to use auto-provisioning, manually deploy the agent to your VMs using the instructions in the remediation steps. (Related policy: [Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fa4fe33eb-e377-4efb-ab31-0784311bc499)).

**Severity**: High

[**Log Analytics agent should be installed on Windows-based Azure Arc-enabled machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/27ac71b1-75c5-41c2-adc2-858f5db45b08)

**Description**: Defender for Cloud uses the Log Analytics agent (also known as MMA) to collect security events from your Azure Arc machines. To deploy the agent on all your Azure Arc machines, follow the remediation steps. (No related policy)

**Severity**: High

[**Machines should be configured securely**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c476dc48-8110-4139-91af-c8d940896b98)

**Description**: Remediate vulnerabilities in security configuration on your machines to protect them from attacks. (Related policy: [Vulnerabilities in security configuration on your machines should be remediated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fe1e5fd5d-3e4c-4ce1-8661-7d1873ae6b15)).

**Severity**: Low

[**Machines should be restarted to apply security configuration updates**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/d79a60ef-d490-484e-91ed-f45ceb0e7cfb)

**Description**: To apply security configuration updates and protect against vulnerabilities, restart your machines. This assessment only applies to Linux virtual machines that have the Azure Monitor Agent installed. (No related policy)

**Severity**: Low

[**Machines should have a vulnerability assessment solution**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ffff0522-1e88-47fc-8382-2a80ba848f5d)

**Description**: Defender for Cloud regularly checks your connected machines to ensure they're running vulnerability assessment tools. Use this recommendation to deploy a vulnerability assessment solution. (Related policy: [A vulnerability assessment solution should be enabled on your virtual machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f501541f7-f7e7-4cd6-868c-4190fdad3ac9)).

**Severity**: Medium

[**Machines should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1195afff-c881-495e-9bc5-1486211ae03f)

**Description**: Resolve the findings from the vulnerability assessment solutions on your virtual machines. (Related policy: [A vulnerability assessment solution should be enabled on your virtual machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f501541f7-f7e7-4cd6-868c-4190fdad3ac9)).

**Severity**: Low

[**Management ports of virtual machines should be protected with just-in-time network access control**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/805651bc-6ecd-4c73-9b55-97a19d0582d0)

**Description**: Defender for Cloud has identified some overly permissive inbound rules for management ports in your Network Security Group. Enable just-in-time access control to protect your VM from internet-based brute-force attacks. Learn more in [Understanding just-in-time (JIT) VM access](https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview). (Related policy: [Management ports of virtual machines should be protected with just-in-time network access control](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fb0f33259-77d7-4c9e-aac6-3aabcfae693c)).

**Severity**: High

[**Microsoft Defender for servers should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/56a6e81f-7413-4f72-9a1b-aaeeaa87c872)

**Description**: Microsoft Defender for servers provides real-time threat protection for your server workloads and generates hardening recommendations as well as alerts about suspicious activities. You can use this information to quickly remediate security issues and improve the security of your servers.

Important: Remediating this recommendation will result in charges for protecting your servers. If you don't have any servers in this subscription, no charges will be incurred. If you create any servers on this subscription in the future, they will automatically be protected and charges will begin at that time. Learn more in [Introduction to Microsoft Defender for servers](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction). (Related policy: [Azure Defender for servers should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f4da35fc9-c9e7-4960-aec9-797fe7d9051d)).

**Severity**: High

[**Microsoft Defender for servers should be enabled on workspaces**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1ce68079-b783-4404-b341-d2851d6f0fa2)

**Description**: Microsoft Defender for servers brings threat detection and advanced defenses for your Windows and Linux machines. With this Defender plan enabled on your subscriptions but not on your workspaces, you're paying for the full capability of Microsoft Defender for servers but missing out on some of the benefits. When you enable Microsoft Defender for servers on a workspace, all machines reporting to that workspace will be billed for Microsoft Defender for servers - even if they're in subscriptions without Defender plans enabled. Unless you also enable Microsoft Defender for servers on the subscription, those machines won't be able to take advantage of just-in-time VM access, adaptive application controls, and network detections for Azure resources. Learn more in [Introduction to Microsoft Defender for servers](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction). (No related policy)

**Severity**: Medium

[**Secure Boot should be enabled on supported Windows virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/69ad830b-d98c-b1cf-2158-9d69d38c7093)

**Description**: Enable Secure Boot on supported Windows virtual machines to mitigate against malicious and unauthorized changes to the boot chain. Once enabled, only trusted bootloaders, kernel, and kernel drivers will be allowed to run. This assessment only applies to trusted launch enabled Windows virtual machines.

Important: Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were initially created without it. Learn more about [Trusted launch for Azure virtual machines](https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch). (No related policy)

**Severity**: Low

[**Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/7f04fc0c-4a3d-5c7e-ce19-666cb871b510)

**Description**: Service Fabric provides three levels of protection (None, Sign, and EncryptAndSign) for node-to-node communication using a primary cluster certificate. Set the protection level to ensure that all node-to-node messages are encrypted and digitally signed. (Related policy: [Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f617c02be-7f02-4efd-8836-3180d47b6c68)).

**Severity**: High

[**Service Fabric clusters should only use Azure Active Directory for client authentication**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/03afeb6f-7634-adb3-0a01-803b0b9cb611)

**Description**: Perform Client authentication only via Azure Active Directory in Service Fabric (Related policy: [Service Fabric clusters should only use Azure Active Directory for client authentication](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fb54ed75b-3e1a-44ac-a333-05ba39b99ff0)).

**Severity**: High

[**System updates on virtual machine scale sets should be installed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bd20bd91-aaf1-7f14-b6e4-866de2f43146)

**Description**: Install missing system security and critical updates to secure your Windows and Linux virtual machine scale sets. (Related policy: [System updates on virtual machine scale sets should be installed](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fc3f317a7-a95c-4547-b7e7-11017ebdf2fe)).

**Severity**: High

[**System updates should be installed on your machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/4ab6e3c5-74dd-8b35-9ab9-f61b30875b27)

**Description**: Install missing system security and critical updates to secure your Windows and Linux virtual machines and computers (Related policy: [System updates should be installed on your machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f86b3d65f-7626-441e-b690-81a8b71cff60)).

**Severity**: High

[**System updates should be installed on your machines (powered by Update Center)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e1145ab1-eb4f-43d8-911b-36ddf771d13f)

**Description**: Your machines are missing system, security, and critical updates. Software updates often include critical patches to security holes. Such holes are frequently exploited in malware attacks so it's vital to keep your software updated. To install all outstanding patches and secure your machines, follow the remediation steps. (No related policy)

**Severity**: High

[**Virtual machine scale sets should be configured securely**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/8941d121-f740-35f6-952c-6561d2b38d36)

**Description**: Remediate vulnerabilities in security configuration on your virtual machine scale sets to protect them from attacks. (Related policy: [Vulnerabilities in security configuration on your virtual machine scale sets should be remediated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f3c735d8a-a4ba-4a3a-b7cf-db7754cf57f4)).

**Severity**: High

[**Virtual machines guest attestation status should be healthy**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b7604066-ed76-45f9-a5c1-c97e4812dc55)

**Description**: Guest attestation is performed by sending a trusted log (TCGLog) to an attestation server. The server uses these logs to determine whether boot components are trustworthy. This assessment is intended to detect compromises of the boot chain, which might be the result of a bootkit or rootkit infection. This assessment only applies to Trusted Launch enabled virtual machines that have the Guest Attestation extension installed. (No related policy)

**Severity**: Medium

[**Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/69133b6b-695a-43eb-a763-221e19556755)

**Description**: The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. [Learn more](https://aka.ms/gcpol) (Related policy: [Guest Configuration extension should be deployed to Azure virtual machines with system assigned managed identity](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fd26f7642-7545-4e18-9b75-8c9bbdee3a9a)).

**Severity**: Medium

[**Virtual machines should be migrated to new Azure Resource Manager resources**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/12018f4f-3d10-999b-e4c4-86ec25be08a1)

**Description**: Virtual Machines (classic) was deprecated and these VMs should be migrated to Azure Resource Manager. Because Azure Resource Manager now has full IaaS capabilities and other advancements, we deprecated the management of IaaS virtual machines (VMs) through Azure Service Manager (ASM) on February 28, 2020. This functionality will be fully retired on March 1, 2023.

To view all affected classic VMs make sure to select all your Azure subscriptions under 'directories + subscriptions' tab.

Available resources and information about this tool & migration: [Overview of Virtual machines (classic) deprecation, step by step process for migration & available Microsoft resources.](https://learn.microsoft.com/en-us/azure/virtual-machines/classic-vm-deprecation?toc=/azure/virtual-machines/windows/toc.json&bc=/azure/virtual-machines/windows/breadcrumb/toc.json) [Details about Migrate to Azure Resource Manager migration tool.](https://learn.microsoft.com/en-us/azure/virtual-machines/migration-classic-resource-manager-deep-dive?toc=/azure/virtual-machines/windows/toc.json&bc=/azure/virtual-machines/windows/breadcrumb/toc.json) [Migrate to Azure Resource Manager migration tool using PowerShell.](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/migration-classic-resource-manager-ps) (Related policy: [Virtual machines should be migrated to new Azure Resource Manager resources](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1d84d5fb-01f6-4d12-ba4f-4a26081d403d)).

**Severity**: High

[**Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/d57a4221-a804-52ca-3dea-768284f06bb7)

**Description**: By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys; temp disks and data caches aren't encrypted, and data isn't encrypted when flowing between compute and storage resources. For a comparison of different disk encryption technologies in Azure, see <https://aka.ms/diskencryptioncomparison>. Use Azure Disk Encryption to encrypt all this data. Disregard this recommendation if:

1. You're using the encryption-at-host feature, or 2. Server-side encryption on Managed Disks meets your security requirements. Learn more in [Server-side encryption of Azure Disk Storage](https://aka.ms/disksse). (Related policy: [Disk encryption should be applied on virtual machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0961003e-5a0a-4549-abde-af6a37f2724d))

**Severity**: High

[**vTPM should be enabled on supported virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/861bbc73-0a55-8d1d-efc6-e92d9e1176e0)

**Description**: Enable virtual TPM device on supported virtual machines to facilitate Measured Boot and other OS security features that require a TPM. Once enabled, vTPM can be used to attest boot integrity. This assessment only applies to trusted launch enabled virtual machines.

Important: Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were initially created without it. Learn more about [Trusted launch for Azure virtual machines](https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch). (No related policy)

**Severity**: Low

[**Vulnerabilities in security configuration on your Linux machines should be remediated (powered by Guest Configuration)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1f655fb7-63ca-4980-91a3-56dbc2b715c6)

**Description**: Remediate vulnerabilities in security configuration on your Linux machines to protect them from attacks. (Related policy: [Linux machines should meet requirements for the Azure security baseline](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ffc9b3da7-8347-4380-8e70-0a0361d8dedd)).

**Severity**: Low

[**Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/8c3d9ad0-3639-4686-9cd2-2b2ab2609bda)

**Description**: Remediate vulnerabilities in security configuration on your Windows machines to protect them from attacks. (No related policy)

**Severity**: Low

[**Windows Defender Exploit Guard should be enabled on machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/22489c48-27d1-4e40-9420-4303ad9cffef)

**Description**: Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only). (Related policy: [Audit Windows machines on which Windows Defender Exploit Guard is not enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2fbed48b13-6647-468e-aa2f-1af1d3f4dd40)).

**Severity**: Medium

[**Windows web servers should be configured to use secure communication protocols**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/87448ec1-55f6-3746-3f79-0f35beee76b4)

**Description**: To protect the privacy of information communicated over the Internet, your web servers should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by using security certificates to encrypt a connection between machines. (Related policy: [Audit Windows web servers that are not using secure communication protocols](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5752e6d6-1206-46d8-8ab1-ecc2f71a8112)).

**Severity**: High

[**Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/a40cc620-e72c-fdf4-c554-c6ca2cd705c0)

**Description**: By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys; temp disks and data caches aren't encrypted, and data isn't encrypted when flowing between compute and storage resources. Use Azure Disk Encryption or EncryptionAtHost to encrypt all this data. Visit <https://aka.ms/diskencryptioncomparison> to compare encryption offerings. This policy requires two prerequisites to be deployed to the policy assignment scope. For details, visit <https://aka.ms/gcpol>. (Related policy: [Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2fca88aadc-6e2b-416c-9de2-5a0f01d1693f)).

**Severity**: High

[**Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/0cb5f317-a94b-6b80-7212-13a9cc8826af)

**Description**: By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys; temp disks and data caches aren't encrypted, and data isn't encrypted when flowing between compute and storage resources. Use Azure Disk Encryption or EncryptionAtHost to encrypt all this data. Visit <https://aka.ms/diskencryptioncomparison> to compare encryption offerings. This policy requires two prerequisites to be deployed to the policy assignment scope. For details, visit <https://aka.ms/gcpol>. (Related policy: [Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f3dc5edcd-002d-444c-b216-e123bbfa37c0)).

**Severity**: High

[**Virtual machines and virtual machine scale sets should have encryption at host enabled**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/efbbd784-656d-473a-9863-ea7693bfcd2a)

**Description**: Use encryption at host to get end-to-end encryption for your virtual machine and virtual machine scale set data. Encryption at host enables encryption at rest for your temporary disk and OS/data disk caches. Temporary and ephemeral OS disks are encrypted with platform-managed keys when encryption at host is enabled. OS/data disk caches are encrypted at rest with either customer-managed or platform-managed key, depending on the encryption type selected on the disk. Learn more at [Use the Azure portal to enable end-to-end encryption using encryption at host](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal). (Related policy: [Virtual machines and virtual machine scale sets should have encryption at host enabled](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ffc4d8e41-e223-45ea-9bf5-eada37891d87)).

**Severity**: Medium

[**[Preview] Azure Stack HCI servers should meet Secured-core requirements**](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2Fmicrosoft.authorization%2Fpolicydefinitions%2F5e6bf724-0154-49bc-985f-27b2e07e636b)

**Description**: Ensure that all Azure Stack HCI servers meet the Secured-core requirements. (Related policy: [Guest Configuration extension should be installed on machines - Microsoft Azure](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/6c99f570-2ce7-46bc-8175-cde013df43bc)).

**Severity**: Low

[**[Preview] Azure Stack HCI servers should have consistently enforced application control policies**](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2Fmicrosoft.authorization%2Fpolicydefinitions%2Fdad3a6b9-4451-492f-a95c-69efc6f3fada)

**Description**: At a minimum, apply the Microsoft WDAC base policy in enforced mode on all Azure Stack HCI servers. Applied Windows Defender Application Control (WDAC) policies must be consistent across servers in the same cluster. (Related policy: [Guest Configuration extension should be installed on machines - Microsoft Azure](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/6c99f570-2ce7-46bc-8175-cde013df43bc)).

**Severity**: High

[**[Preview] Azure Stack HCI systems should have encrypted volumes**](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2Fmicrosoft.authorization%2Fpolicydefinitions%2Fee8ca833-1583-4d24-837e-96c2af9488a4)

**Description**: Use BitLocker to encrypt the OS and data volumes on Azure Stack HCI systems. (Related policy: [Guest Configuration extension should be installed on machines - Microsoft Azure](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/6c99f570-2ce7-46bc-8175-cde013df43bc)).

**Severity**: High

[**[Preview] Host and VM networking should be protected on Azure Stack HCI systems**](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2Fmicrosoft.authorization%2Fpolicydefinitions%2F36f0d6bc-a253-4df8-b25b-c3a5023ff443)

**Description**: Protect data on the Azure Stack HCI host's network and on virtual machine network connections. (Related policy: [Guest Configuration extension should be installed on machines - Microsoft Azure](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/6c99f570-2ce7-46bc-8175-cde013df43bc)).

**Severity**: Low

**Container recommendations**

[**[Preview] Container images in Azure registry should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/33422d8f-ab1e-42be-bc9a-38685bb567b9)

**Description**: Defender for Cloud scans your registry images for known vulnerabilities (CVEs) and provides detailed findings for each scanned image. Scanning and remediating vulnerabilities for container images in the registry helps maintain a secure and reliable software supply chain, reduces the risk of security incidents, and ensures compliance with industry standards.

**Severity**: High

**Type**: Vulnerability Assessment

[**[Preview] Containers running in Azure should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e9acaf48-d2cf-45a3-a6e7-3caa2ef769e0)

**Description**: Defender for Cloud creates an inventory of all container workloads currently running in your Kubernetes clusters and provides vulnerability reports for those workloads by matching the images being used and the vulnerability reports created for the registry images. Scanning and remediating vulnerabilities of container workloads is critical to ensure a robust and secure software supply chain, reduce the risk of security incidents, and ensures compliance with industry standards.

**Severity**: High

**Type**: Vulnerability Assessment

[**(Enable if required) Container registries should be encrypted with a customer-managed key (CMK)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/af560c4d-9c05-e073-b9f1-f7a94958ff25)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Use customer-managed keys to manage the encryption at rest of the contents of your registries. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys (CMK) are commonly required to meet regulatory compliance standards. CMKs enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more about CMK encryption at <https://aka.ms/acr/CMK>. (Related policy: [Container registries should be encrypted with a customer-managed key (CMK)](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5b9159ae-1701-4a6f-9a7a-aa9c8ddd0580)).

**Severity**: Low

**Type**: Control plane

[**Azure Arc-enabled Kubernetes clusters should have the Azure Policy extension installed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/0642d770-b189-42ef-a2ce-9dcc3ec6c169)

**Description**: Azure Policy extension for Kubernetes extends [Gatekeeper](https://github.com/open-policy-agent/gatekeeper) v3, an admission controller webhook for [Open Policy Agent](https://www.openpolicyagent.org/) (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner. (No related policy)

**Severity**: High

**Type**: Control plane

[**Azure Arc-enabled Kubernetes clusters should have the Defender extension installed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/3ef9848c-c2c8-4ff3-8b9c-4c8eb8ddfce6)

**Description**: Defender's extension for Azure Arc provides threat protection for your Arc-enabled Kubernetes clusters. The extension collects data from all control plane (master) nodes in the cluster and sends it to the [Microsoft Defender for Kubernetes backend](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc&tabs=aks-deploy-portal) in the cloud for further analysis. (No related policy)

**Severity**: High

**Type**: Control plane

[**Azure Kubernetes Service clusters should have Defender profile enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/56a83a6e-c417-42ec-b567-1e6fcb3d09a9)

**Description**: Microsoft Defender for Containers provides cloud-native Kubernetes security capabilities including environment hardening, workload protection, and run-time protection. When you enable the SecurityProfile.AzureDefender profile on your Azure Kubernetes Service cluster, an agent is deployed to your cluster to collect security event data. Learn more in [Introduction to Microsoft Defender for Containers](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction). (No related policy)

**Severity**: High

**Type**: Control plane

[**Azure Kubernetes Service clusters should have the Azure Policy add-on for Kubernetes installed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/08e628db-e2ed-4793-bc91-d13e684401c3)

**Description**: Azure Policy add-on for Kubernetes extends [Gatekeeper](https://github.com/open-policy-agent/gatekeeper) v3, an admission controller webhook for [Open Policy Agent](https://www.openpolicyagent.org/) (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner. Defender for Cloud requires the Add-on to audit and enforce security capabilities and compliance inside your clusters. [Learn more](https://learn.microsoft.com/en-us/azure/governance/policy/concepts/policy-for-kubernetes). Requires Kubernetes v1.14.0 or later. (Related policy: [Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0a15ec92-a229-4763-bb14-0ea34a568f8d)).

**Severity**: High

**Type**: Control plane

[**Container registries should not allow unrestricted network access**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/9b828565-a0ed-61c2-6bf3-1afc99a9b2ca)

**Description**: Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific public IP addresses or address ranges. If your registry doesn't have an IP/firewall rule or a configured virtual network, it will appear in the unhealthy resources. Learn more about Container Registry network rules here: <https://aka.ms/acr/portal/public-network> and here <https://aka.ms/acr/vnet>. (Related policy: [Container registries should not allow unrestricted network access](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fd0793b48-0edc-4296-a390-4c75d1bdfd71)).

**Severity**: Medium

**Type**: Control plane

[**Container registries should use private link**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/13e7d036-6903-821c-6018-962938929bf0)

**Description**: Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <https://aka.ms/acr/private-link>. (Related policy: [Container registries should use private link](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fe8eef0a8-67cf-4eb4-9386-14b0e78733d4)).

**Severity**: Medium

**Type**: Control plane

[**Diagnostic logs in Kubernetes services should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bb318338-de6a-42ff-8428-8274c897d564)

**Description**: Enable diagnostic logs in your Kubernetes services and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs. (No related policy)

**Severity**: Low

**Type**: Control plane

[**Kubernetes API server should be configured with restricted access**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1a2b5b4c-f80d-46e7-ac81-b51a9fb363de)

**Description**: To ensure that only applications from allowed networks, machines, or subnets can access your cluster, restrict access to your Kubernetes API server. You can restrict access by defining authorized IP ranges, or by setting up your API servers as private clusters as explained in [Create a private Azure Kubernetes Service cluster](https://learn.microsoft.com/en-us/azure/aks/private-clusters). (Related policy: [Authorized IP ranges should be defined on Kubernetes Services](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0e246bcf-5f6f-4f87-bc6f-775d4712c7ea)).

**Severity**: High

**Type**: Control plane

[**Role-Based Access Control should be used on Kubernetes Services**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b0fdc63a-38e7-4bab-a7c4-2c2665abbaa9)

**Description**: To provide granular filtering on the actions that users can perform, use [Role-Based Access Control (RBAC)](https://learn.microsoft.com/en-us/azure/aks/concepts-identity#azure-role-based-access-control) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies. (Related policy: [Role-Based Access Control (RBAC) should be used on Kubernetes Services](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fac4a19c2-fa67-49b4-8ae5-0b2e78c49457)).

**Severity**: High

**Type**: Control plane

[**Microsoft Defender for Containers should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e599a9fe-30e3-47c6-a173-8b4b6d9d3255)

**Description**: Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multicloud Kubernetes environments. You can use this information to quickly remediate security issues and improve the security of your containers.

Important: Remediating this recommendation will result in charges for protecting your Kubernetes clusters. If you don't have any Kubernetes clusters in this subscription, no charges will be incurred. If you create any Kubernetes clusters on this subscription in the future, they'll automatically be protected and charges will begin at that time. Learn more in [Introduction to Microsoft Defender for Containers](https://learn.microsoft.com/en-us/azure/defender-for-cloud/container-security). (No related policy)

**Severity**: High

**Type**: Control plane

[**Container CPU and memory limits should be enforced**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/405c9ae6-49f9-46c4-8873-a86690f27818)

**Description**: Enforcing CPU and memory limits prevents resource exhaustion attacks (a form of denial of service attack).

We recommend setting limits for containers to ensure the runtime prevents the container from using more than the configured resource limit.

(Related policy: [Ensure container CPU and memory resource limits do not exceed the specified limits in Kubernetes cluster](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fe345eecc-fa47-480f-9e88-67dcc122b164)).

**Severity**: Medium

**Type**: Kubernetes Data plane

[**Container images should be deployed from trusted registries only**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/8d244d29-fa00-4332-b935-c3a51d525417)

**Description**: Images running on your Kubernetes cluster should come from known and monitored container image registries. Trusted registries reduce your cluster's exposure risk by limiting the potential for the introduction of unknown vulnerabilities, security issues, and malicious images.

(Related policy: [Ensure only allowed container images in Kubernetes cluster](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ffebd0533-8e55-448f-b837-bd0e06f16469)).

**Severity**: High

**Type**: Kubernetes Data plane

[**Container with privilege escalation should be avoided**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/43dc2a2e-ce69-4d42-923e-ab7d136f2cfe)

**Description**: Containers shouldn't run with privilege escalation to root in your Kubernetes cluster. The AllowPrivilegeEscalation attribute controls whether a process can gain more privileges than its parent process. (Related policy: [Kubernetes clusters should not allow container privilege escalation](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1c6e92c9-99f0-4e55-9cf2-0c234dc48f99)).

**Severity**: Medium

**Type**: Kubernetes data plane

[**Containers sharing sensitive host namespaces should be avoided**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/802c0637-5a8c-4c98-abd7-7c96d89d6010)

**Description**: To protect against privilege escalation outside the container, avoid pod access to sensitive host namespaces (host process ID and host IPC) in a Kubernetes cluster. (Related policy: [Kubernetes cluster containers should not share host process ID or host IPC namespace](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f47a1ee2f-2a2a-4576-bf2a-e0e36709c2b8)).

**Severity**: Medium

**Type**: Kubernetes data plane

[**Containers should only use allowed AppArmor profiles**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/86f91051-9d6a-47c3-a07f-bd14cb214b45)

**Description**: Containers running on Kubernetes clusters should be limited to allowed AppArmor profiles only. ;AppArmor (Application Armor) is a Linux security module that protects an operating system and its applications from security threats. To use it, a system administrator associates an AppArmor security profile with each program. (Related policy: [Kubernetes cluster containers should only use allowed AppArmor profiles](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f511f5417-5d12-434d-ab2e-816901e72a5e)).

**Severity**: High

**Type**: Kubernetes data plane

[**Immutable (read-only) root filesystem should be enforced for containers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/27d6f0e9-b4d5-468b-ae7e-03d5473fd864)

**Description**: Containers should run with a read only root file system in your Kubernetes cluster. Immutable filesystem protects containers from changes at run-time with malicious binaries being added to PATH. (Related policy: [Kubernetes cluster containers should run with a read only root file system](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fdf49d893-a74c-421d-bc95-c663042e5b80)).

**Severity**: Medium

**Type**: Kubernetes data plane

[**Kubernetes clusters should be accessible only over HTTPS**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c6d87087-9ebe-b31f-b452-0bf3bbbaccd2)

**Description**: Use of HTTPS ensures authentication and protects data in transit from network layer eavesdropping attacks. This capability is currently generally available for Kubernetes Service (AKS), and in preview for AKS Engine and Azure Arc-enabled Kubernetes. For more info, visit <https://aka.ms/kubepolicydoc> (Related policy: [Enforce HTTPS ingress in Kubernetes cluster](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1a5b4dca-0b6f-4cf5-907c-56316bc1bf3d)).

**Severity**: High

**Type**: Kubernetes Data plane

[**Kubernetes clusters should disable automounting API credentials**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/32060ac3-f17f-4848-db8e-e7cf2c9a53eb)

**Description**: Disable automounting API credentials to prevent a potentially compromised Pod resource to run API commands against Kubernetes clusters. For more information, see <https://aka.ms/kubepolicydoc>. (Related policy: [Kubernetes clusters should disable automounting API credentials](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f423dd1ba-798e-40e4-9c4d-b6902674b423)).

**Severity**: High

**Type**: Kubernetes Data plane

[**Kubernetes clusters should not grant CAPSYSADMIN security capabilities**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/aba14f78-27c5-af84-848e-9105d18dfd92)

**Description**: To reduce the attack surface of your containers, restrict CAP\_SYS\_ADMIN Linux capabilities. For more information, see <https://aka.ms/kubepolicydoc>. (No related policy)

**Severity**: High

**Type**: Kubernetes data plane

[**Kubernetes clusters should not use the default namespace**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ff87e0b4-17df-d338-5b19-80e71e0dcc9d)

**Description**: Prevent usage of the default namespace in Kubernetes clusters to protect against unauthorized access for ConfigMap, Pod, Secret, Service, and ServiceAccount resource types. For more information, see <https://aka.ms/kubepolicydoc>. (Related policy: [Kubernetes clusters should not use the default namespace](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f9f061a12-e40d-4183-a00e-171812443373)).

**Severity**: Low

**Type**: Kubernetes data plane

[**Least privileged Linux capabilities should be enforced for containers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/11c95609-3553-430d-b788-fd41cde8b2db)

**Description**: To reduce attack surface of your container, restrict Linux capabilities and grant specific privileges to containers without granting all the privileges of the root user. We recommend dropping all capabilities, then adding those that are required (Related policy: [Kubernetes cluster containers should only use allowed capabilities](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fc26596ff-4d70-4e6a-9a30-c2506bd2f80c)).

**Severity**: Medium

**Type**: Kubernetes data plane

[**Privileged containers should be avoided**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/5d90913f-a1c5-4429-ad54-2c6c17fb3c73)

**Description**: To prevent unrestricted host access, avoid privileged containers whenever possible.

Privileged containers have all of the root capabilities of a host machine. They can be used as entry points for attacks and to spread malicious code or malware to compromised applications, hosts, and networks. (Related policy: [Do not allow privileged containers in Kubernetes cluster](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f95edb821-ddaf-4404-9732-666045e056b4)).

**Severity**: Medium

**Type**: Kubernetes data plane

[**Running containers as root user should be avoided**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/9b795646-9130-41a4-90b7-df9eae2437c8)

**Description**: Containers shouldn't run as root users in your Kubernetes cluster. Running a process as the root user inside a container runs it as root on the host. If there's a compromise, an attacker has root in the container, and any misconfigurations become easier to exploit. (Related policy: [Kubernetes cluster pods and containers should only run with approved user and group IDs](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ff06ddb64-5fa3-4b77-b166-acb36f7f6042)).

**Severity**: High

**Type**: Kubernetes Data plane

[**Services should listen on allowed ports only**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/add45209-73f6-4fa5-a5a5-74a451b07fbe)

**Description**: To reduce the attack surface of your Kubernetes cluster, restrict access to the cluster by limiting services access to the configured ports. (Related policy: [Ensure services listen only on allowed ports in Kubernetes cluster](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f233a2a17-77ca-4fb1-9b6b-69223d272a44)).

**Severity**: Medium

**Type**: Kubernetes data plane

[**Usage of host networking and ports should be restricted**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ebc68898-5c0f-4353-a426-4a5f1e737b12)

**Description**: Restrict pod access to the host network and the allowable host port range in a Kubernetes cluster. Pods created with the hostNetwork attribute enabled will share the node's network space. To avoid compromised container from sniffing network traffic, we recommend not putting your pods on the host network. If you need to expose a container port on the node's network, and using a Kubernetes Service node port does not meet your needs, another possibility is to specify a hostPort for the container in the pod spec. (Related policy: [Kubernetes cluster pods should only use approved host network and port range](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f82985f06-dc18-4a48-bc1c-b9f4f0098cfe)).

**Severity**: Medium

**Type**: Kubernetes data plane

[**Usage of pod HostPath volume mounts should be restricted to a known list to restrict node access from compromised containers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f0debc84-981c-4a0d-924d-aa4bd7d55fef)

**Description**: We recommend limiting pod HostPath volume mounts in your Kubernetes cluster to the configured allowed host paths. If there's a compromise, the container node access from the containers should be restricted. (Related policy: [Kubernetes cluster pod hostPath volumes should only use allowed host paths](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f098fc59e-46c7-4d99-9b16-64990e543d75)).

**Severity**: Medium

**Type**: Kubernetes Data plane

[**Azure registry container images should have vulnerabilities resolved (powered by Qualys)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/dbd0cb49-b563-45e7-9724-889e799fa648)

**Description**: Container image vulnerability assessment scans your registry for security vulnerabilities and exposes detailed findings for each image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks. (Related policy: [Vulnerabilities in Azure Container Registry images should be remediated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5f0f936f-2f01-4bf5-b6be-d423792fa562)).

**Severity**: High

**Type**: Vulnerability Assessment

[**Azure registry container images should have vulnerabilities resolved (powered by Microsoft Defender Vulnerability Management)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c0b7cfc6-3172-465a-b378-53c7ff2cc0d5)

**Important**

This recommendation is on a retirement path. It is being replaced by the recommendation [[**[Preview] Container images in Azure registry should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/33422d8f-ab1e-42be-bc9a-38685bb567b9)](#preview-container-images-in-azure-registry-should-have-vulnerability-findings-resolvedhttpsportalazurecomblademicrosoft\_azure\_securityrecommendationsbladeassessmentkey33422d8f-ab1e-42be-bc9a-38685bb567b9).

**Description**: Container image vulnerability assessment scans your registry for commonly known vulnerabilities (CVEs) and provides a detailed vulnerability report for each image. Resolving vulnerabilities can greatly improve your security posture, ensuring images are safe to use prior to deployment. (Related policy: [Vulnerabilities in Azure Container Registry images should be remediated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5f0f936f-2f01-4bf5-b6be-d423792fa562)).

**Severity**: High

**Type**: Vulnerability Assessment

[**Azure running container images should have vulnerabilities resolved (powered by Microsoft Defender Vulnerability Management)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c609cf0f-71ab-41e9-a3c6-9a1f7fe1b8d5)

**Important**

This recommendation is on a retirement path. It is being replaced by the recommendation [[**[Preview] Containers running in Azure should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e9acaf48-d2cf-45a3-a6e7-3caa2ef769e0)](#preview-containers-running-in-azure-should-have-vulnerability-findings-resolvedhttpsportalazurecomblademicrosoft\_azure\_securityrecommendationsbladeassessmentkeye9acaf48-d2cf-45a3-a6e7-3caa2ef769e0).

**Description**: Container image vulnerability assessment scans your registry for commonly known vulnerabilities (CVEs) and provides a detailed vulnerability report for each image. This recommendation provides visibility to vulnerable images currently running in your Kubernetes clusters. Remediating vulnerabilities in container images that are currently running is key to improving your security posture, significantly reducing the attack surface for your containerized workloads.

**Severity**: High

**Type**: Vulnerability Assessment

**Data recommendations**

[**(Enable if required) Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/814df446-7128-eff0-9177-fa52ac035b74)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Use customer-managed keys to manage the encryption at rest of your Azure Cosmos DB. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys (CMK) are commonly required to meet regulatory compliance standards. CMKs enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more about CMK encryption at <https://aka.ms/cosmosdb-cmk>. (Related policy: [Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1f905d99-2ab7-462c-a6b0-f709acca6c8f)).

**Severity**: Low

[**(Enable if required) Azure Machine Learning workspaces should be encrypted with a customer-managed key (CMK)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bbd14f11-6228-4588-82a4-517b8d77b23f)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Manage encryption at rest of your Azure Machine Learning workspace data with customer-managed keys (CMK). By default, customer data is encrypted with service-managed keys, but CMKs are commonly required to meet regulatory compliance standards. CMKs enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more about CMK encryption at <https://aka.ms/azureml-workspaces-cmk>. (Related policy: [Azure Machine Learning workspaces should be encrypted with a customer-managed key (CMK)](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fba769a63-b8cc-4b2d-abf6-ac33c7204be8)).

**Severity**: Low

[**(Enable if required) Cognitive Services accounts should enable data encryption with a customer-managed key (CMK)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/18bf29b3-a844-e170-2826-4e95d0ba4dc9)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Customer-managed keys (CMK) are commonly required to meet regulatory compliance standards. CMKs enable the data stored in Cognitive Services to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more about CMK encryption at <https://aka.ms/cosmosdb-cmk>. (Related policy: [Cognitive Services accounts should enable data encryption with a customer-managed key?(CMK)](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f67121cc7-ff39-4ab8-b7e3-95b84dab487d))

**Severity**: Low

[**(Enable if required) MySQL servers should use customer-managed keys to encrypt data at rest**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/6b51b7f7-cbed-75bf-8a02-43384bf47562)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Use customer-managed keys to manage the encryption at rest of your MySQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys (CMK) are commonly required to meet regulatory compliance standards. CMKs enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. (Related policy: [Bring your own key data protection should be enabled for MySQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f83cef61d-dbd1-4b20-a4fc-5fbc7da10833)).

**Severity**: Low

[**(Enable if required) PostgreSQL servers should use customer-managed keys to encrypt data at rest**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/19d45f8f-245c-852e-dbf9-d4aab4758b1f)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Use customer-managed keys to manage the encryption at rest of your PostgreSQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys (CMK) are commonly required to meet regulatory compliance standards. CMKs enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. (Related policy: [Bring your own key data protection should be enabled for PostgreSQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f18adea5e-f416-4d0f-8aa8-d24321e3e274)).

**Severity**: Low

[**(Enable if required) SQL managed instances should use customer-managed keys to encrypt data at rest**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/06ac6ef4-1e66-1334-5418-6e79ab444ce0)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Implementing Transparent Data Encryption (TDE) with your own key provides you with increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement. (Related policy: [SQL managed instances should use customer-managed keys to encrypt data at rest](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f048248b0-55cd-46da-b1ff-39efd52db260)).

**Severity**: Low

[**(Enable if required) SQL servers should use customer-managed keys to encrypt data at rest**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1a93e945-3675-aef6-075d-c661498e1046)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Implementing Transparent Data Encryption (TDE) with your own key provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement. (Related policy: [SQL servers should use customer-managed keys to encrypt data at rest](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0d134df8-db83-46fb-ad72-fe0c9428c8dd)).

**Severity**: Low

[**(Enable if required) Storage accounts should use customer-managed key (CMK) for encryption**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ca98bba7-719e-48ee-e193-0b76766cdb07)

**Description**: Recommendations to use customer-managed keys for encryption of data at rest are not assessed by default, but are available to enable for applicable scenarios. Data is encrypted automatically using platform-managed keys, so the use of customer-managed keys should only be applied when obligated by compliance or restrictive policy requirements. To enable this recommendation, navigate to your Security Policy for the applicable scope, and update the *Effect* parameter for the corresponding policy to audit or enforce the use of customer-managed keys. Learn more in [Manage security policies](https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy). Secure your storage account with greater flexibility using customer-managed keys (CMKs). When you specify a CMK, that key is used to protect and control access to the key that encrypts your data. Using CMKs provides additional capabilities to control rotation of the key encryption key or cryptographically erase data. (Related policy: [Storage accounts should use customer-managed key (CMK) for encryption](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f6fac406b-40ca-413b-bf8e-0bf964659c25)).

**Severity**: Low

[**All advanced threat protection types should be enabled in SQL managed instance advanced data security settings**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ebe970fe-9c27-4dd7-a165-1e943d565e10)

**Description**: It is recommended to enable all advanced threat protection types on your SQL managed instances. Enabling all types protects against SQL injection, database vulnerabilities, and any other anomalous activities. (No related policy)

**Severity**: Medium

[**All advanced threat protection types should be enabled in SQL server advanced data security settings**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f7010359-8d21-4598-a9f2-c3e81a17141e)

**Description**: It is recommended to enable all advanced threat protection types on your SQL servers. Enabling all types protects against SQL injection, database vulnerabilities, and any other anomalous activities. (No related policy)

**Severity**: Medium

[**API Management services should use a virtual network**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/74e7dcff-317f-9635-41d2-ead5019acc99)

**Description**: Azure Virtual Network deployment provides enhanced security, isolation, and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway can be configured to be accessible either from the Internet or only within the virtual network. (Related policy: [API Management services should use a virtual network](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fef619a2c-cc4d-4d03-b2ba-8c94a834d85b)).

**Severity**: Medium

[**App Configuration should use private link**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/8318c3a1-fcac-2e1d-9582-50912e5578e5)

**Description**: Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <https://aka.ms/appconfig/private-endpoint>. (Related policy: [App Configuration should use private link](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fca610c1d-041c-4332-9d88-7ed3094967c7)).

**Severity**: Medium

[**Audit retention for SQL servers should be set to at least 90 days**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/620671b8-6661-273a-38ac-4574967750ec)

**Description**: Audit SQL servers configured with an auditing retention period of less than 90 days. (Related policy: [SQL servers should be configured with 90 days auditing retention or higher.](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f89099bee-89e0-4b26-a5f4-165451757743))

**Severity**: Low

[**Auditing on SQL server should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/94208a8b-16e8-4e5b-abbd-4e81c9d02bee)

**Description**: Enable auditing on your SQL Server to track database activities across all databases on the server and save them in an audit log. (Related policy: [Auditing on SQL server should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fa6fb4358-5bf4-4ad7-ba82-2cd2f41ce5e9)).

**Severity**: Low

[**Auto provisioning of the Log Analytics agent should be enabled on subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/af849052-4299-0692-acc0-bffcbe9e440c)

**Description**: To monitor for security vulnerabilities and threats, Microsoft Defender for Cloud collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created. (Related policy: [Auto provisioning of the Log Analytics agent should be enabled on your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f475aae12-b88a-4572-8b36-9b712b2b3a17)).

**Severity**: Low

[**Azure Cache for Redis should reside within a virtual network**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/be264018-593c-1162-bd5e-b74a39396652)

**Description**: Azure Virtual Network (VNet) deployment provides enhanced security and isolation for your Azure Cache for Redis, as well as subnets, access control policies, and other features to further restrict access. When an Azure Cache for Redis instance is configured with a VNet, it is not publicly addressable and can only be accessed from virtual machines and applications within the VNet. (Related policy: [Azure Cache for Redis should reside within a virtual network](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f7d092e0a-7acd-40d2-a975-dca21cae48c4)).

**Severity**: Medium

[**Azure Database for MySQL should have an Azure Active Directory administrator provisioned**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/8af8a87b-7aa6-4c83-b22b-36801896177b/)

**Description**: Provision an Azure AD administrator for your Azure Database for MySQL to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services (Related policy: [An Azure Active Directory administrator should be provisioned for MySQL servers](https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f146412e9-005c-472b-9e48-c87b72ac229e)).

**Severity**: Medium

[**Azure Database for PostgreSQL should have an Azure Active Directory administrator provisioned**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b20d1b00-11a8-4ce7-b477-4ea6e147c345)

**Description**: Provision an Azure AD administrator for your Azure Database for PostgreSQL to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services  
(Related policy: [An Azure Active Directory administrator should be provisioned for PostgreSQL servers](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fb4dec045-250a-48c2-b5cc-e0c4eec8b5b4)).

**Severity**: Medium

[**Azure Cosmos DB accounts should have firewall rules**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/276b1952-c364-852b-11e5-657f0fa34dc6)

**Description**: Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources. Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant. (Related policy: [Azure Cosmos DB accounts should have firewall rules](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f862e97cf-49fc-4a5c-9de4-40d4e2e7c8eb)).

**Severity**: Medium

[**Azure Event Grid domains should use private link**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bef092f5-bea7-3df3-1ee8-4376dd9c111e)

**Description**: Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domains instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <https://aka.ms/privateendpoints>. (Related policy: [Azure Event Grid domains should use private link](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f9830b652-8523-49cc-b1b3-e17dce1127ca)).

**Severity**: Medium

[**Azure Event Grid topics should use private link**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bdac9c7b-b9b8-f572-0450-f161c430861c)

**Description**: Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your topics instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <https://aka.ms/privateendpoints>. (Related policy: [Azure Event Grid topics should use private link](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f4b90e17e-8448-49db-875e-bd83fb6f804f)).

**Severity**: Medium

[**Azure Machine Learning workspaces should use private link**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/692343df-7e70-b082-7b0e-67f97146cea3)

**Description**: Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Machine Learning workspaces instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <https://aka.ms/azureml-workspaces-privatelink>. (Related policy: [Azure Machine Learning workspaces should use private link](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f40cec1dd-a100-4920-b15b-3024fe8901ab)).

**Severity**: Medium

[**Azure SignalR Service should use private link**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b6f84d18-0137-3176-6aa1-f4d9ac95155c)

**Description**: Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your SignalR resources instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <https://aka.ms/asrs/privatelink>. (Related policy: [Azure SignalR Service should use private link](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f53503636-bcc9-4748-9663-5348217f160f)).

**Severity**: Medium

[**Azure Spring Cloud should use network injection**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/4c768356-5ad2-e3cc-c799-252b27d3865a)

**Description**: Azure Spring Cloud instances should use virtual network injection for the following purposes: 1. Isolate Azure Spring Cloud from Internet. 2. Enable Azure Spring Cloud to interact with systems in either on premises data centers or Azure service in other virtual networks. 3. Empower customers to control inbound and outbound network communications for Azure Spring Cloud. (Related policy: [Azure Spring Cloud should use network injection](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2faf35e2a4-ef96-44e7-a9ae-853dd97032c4)).

**Severity**: Medium

[**SQL servers should have an Azure Active Directory administrator provisioned**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f0553104-cfdb-65e6-759c-002812e38500)

**Description**: Provision an Azure AD administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. (Related policy: [An Azure Active Directory administrator should be provisioned for SQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1f314764-cb73-4fc9-b863-8eca98ac36e9)).

**Severity**: High

[**Azure Synapse Workspace authentication mode should be Azure Active Directory Only**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/3320d1ac-0ebe-41ab-b96c-96fb91214c5c)

**Description**: Azure Synapse Workspace authentication mode should be Azure Active Directory Only Azure Active Directory only authentication methods improves security by ensuring that Synapse Workspaces exclusively require Azure AD identities for authentication. [Learn more](https://aka.ms/Synapse). (Related policy: [Synapse Workspaces should use only Azure Active Directory identities for authentication](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f2158ddbe-fefa-408e-b43f-d4faef8ff3b8)).

**Severity**: Medium

[**Cognitive Services accounts should enable data encryption**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/cdcf4f71-60d3-540b-91e3-aa19792da364)

**Description**: This policy audits any Cognitive Services account not using data encryption. For each Cognitive Services account with storage, should enable data encryption with either customer managed or Microsoft managed key. (Related policy: [Cognitive Services accounts should enable data encryption](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f2bdd0062-9d75-436e-89df-487dd8e4b3c7)).

**Severity**: Low

[**Cognitive Services accounts should use customer owned storage or enable data encryption**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/aa395469-1687-78a7-bf76-f4614ef72977)

**Description**: This policy audits any Cognitive Services account not using customer owned storage nor data encryption. For each Cognitive Services account with storage, use either customer owned storage or enable data encryption. (Related policy: [Cognitive Services accounts should use customer owned storage or enable data encryption.](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f11566b39-f7f7-4b82-ab06-68d8700eb0a4))

**Severity**: Low

[**Diagnostic logs in Azure Data Lake Store should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ad5bbaeb-7632-5edf-f1c2-752075831ce8)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Azure Data Lake Store should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f057ef27e-665e-4328-8ea3-04b3122bd9fb)).

**Severity**: Low

[**Diagnostic logs in Data Lake Analytics should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c6dad669-efd7-cd72-61c5-289935607791)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Data Lake Analytics should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fc95c74d9-38fe-4f0d-af86-0c7d626a315c)).

**Severity**: Low

[**Email notification for high severity alerts should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/3869fbd7-5d90-84e4-37bd-d9a7f4ce9a24)

**Description**: To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Defender for Cloud. (Related policy: [Email notification for high severity alerts should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f6e2593d9-add6-4083-9c9b-4b7d2188c899)).

**Severity**: Low

[**Email notification to subscription owner for high severity alerts should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/9f97e78d-88ee-a48d-abe2-5ef12954e7ea)

**Description**: To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Defender for Cloud. (Related policy: [Email notification to subscription owner for high severity alerts should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0b15565f-aa9e-48ba-8619-45960f2c314d)).

**Severity**: Medium

[**Enforce SSL connection should be enabled for MySQL database servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1f6d29f6-4edb-ea39-042b-de8f123ddd39)

**Description**: Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server. (Related policy: [Enforce SSL connection should be enabled for MySQL database servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fe802a67a-daf5-4436-9ea6-f6d821dd0c5d)).

**Severity**: Medium

[**Enforce SSL connection should be enabled for PostgreSQL database servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1fde2073-a488-17e9-9534-5a3b23379b4b)

**Description**: Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server. (Related policy: [Enforce SSL connection should be enabled for PostgreSQL database servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fd158790f-bfb0-486c-8631-2dc6b4e8e6af)).

**Severity**: Medium

[**Function apps should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/afd071f0-ebaa-422b-bb2f-8a772a31db75)

**Description**: Runtime vulnerability scanning for functions scans your function apps for security vulnerabilities and exposes detailed findings. Resolving the vulnerabilities can greatly improve your serverless applications security posture and protect them from attacks. (No related policy)

**Severity**: High

[**Geo-redundant backup should be enabled for Azure Database for MariaDB**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/2ce368b5-7882-89fd-6645-885b071a2409)

**Description**: Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery options in case of a region failure. Configuring geo-redundant storage for backup is only allowed when creating a server. (Related policy: [Geo-redundant backup should be enabled for Azure Database for MariaDB](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0ec47710-77ff-4a3d-9181-6aa50af424d0)).

**Severity**: Low

[**Geo-redundant backup should be enabled for Azure Database for MySQL**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/8ad68a2f-c6b1-97b5-41b5-174359a33688)

**Description**: Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery options in case of a region failure. Configuring geo-redundant storage for backup is only allowed when creating a server. (Related policy: [Geo-redundant backup should be enabled for Azure Database for MySQL](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f82339799-d096-41ae-8538-b108becf0970)).

**Severity**: Low

[**Geo-redundant backup should be enabled for Azure Database for PostgreSQL**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/95592ab0-ddc8-660d-67f3-6df1fadfe7ec)

**Description**: Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery options in case of a region failure. Configuring geo-redundant storage for backup is only allowed when creating a server. (Related policy: [Geo-redundant backup should be enabled for Azure Database for PostgreSQL](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f48af4db5-9b8b-401c-8e74-076be876a430)).

**Severity**: Low

[**GitHub repositories should have Code scanning enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/6672df26-ff2e-4282-83c3-e2f20571bd11)

**Description**: GitHub uses code scanning to analyze code in order to find security vulnerabilities and errors in code. Code scanning can be used to find, triage, and prioritize fixes for existing problems in your code. Code scanning can also prevent developers from introducing new problems. Scans can be scheduled for specific days and times, or scans can be triggered when a specific event occurs in the repository, such as a push. If code scanning finds a potential vulnerability or error in code, GitHub displays an alert in the repository. A vulnerability is a problem in a project's code that could be exploited to damage the confidentiality, integrity, or availability of the project. (No related policy)

**Severity**: Medium

[**GitHub repositories should have Dependabot scanning enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/92643c1f-1a95-4b68-bbd2-5117f92d6e35)

**Description**: GitHub sends Dependabot alerts when it detects vulnerabilities in code dependencies that affect repositories. A vulnerability is a problem in a project's code that could be exploited to damage the confidentiality, integrity, or availability of the project or other projects that use its code. Vulnerabilities vary in type, severity, and method of attack. When code depends on a package that has a security vulnerability, this vulnerable dependency can cause a range of problems. (No related policy)

**Severity**: Medium

[**GitHub repositories should have Secret scanning enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1a600c61-6443-4ab4-bd28-7a6b6fb4691d)

**Description**: GitHub scans repositories for known types of secrets, to prevent fraudulent use of secrets that were accidentally committed to repositories. Secret scanning will scan the entire Git history on all branches present in the GitHub repository for any secrets. Examples of secrets are tokens and private keys that a service provider can issue for authentication. If a secret is checked into a repository, anyone who has read access to the repository can use the secret to access the external service with those privileges. Secrets should be stored in a dedicated, secure location outside the repository for the project. (No related policy)

**Severity**: High

[**Microsoft Defender for Azure SQL Database servers should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/58d72d9d-0310-4792-9a3b-6dd111093cdb)

**Description**: Microsoft Defender for SQL is a unified package that provides advanced SQL security capabilities. It includes functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate a threat to your database, and discovering and classifying sensitive data. Important: Protections from this plan are charged as shown on the [Defender plans](https://aka.ms/pricing-security-center) page. If you don't have any Azure SQL Database servers in this subscription, you won't be charged. If you later create Azure SQL Database servers on this subscription, they'll automatically be protected and charges will begin. Learn about the [pricing details per region](https://aka.ms/pricing-security-center). Learn more in [Introduction to Microsoft Defender for SQL](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction). (Related policy: [Azure Defender for Azure SQL Database servers should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f7fe3b40f-802b-4cdd-8bd4-fd799c948cc2)).

**Severity**: High

[**Microsoft Defender for DNS should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/aae10e53-8403-3576-5d97-3b00f97332b2)

**Description**: Microsoft Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Defender for DNS alerts you about suspicious activity at the DNS layer. Learn more in [Introduction to Microsoft Defender for DNS](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-dns-introduction). Enabling this Defender plan results in charges. Learn about the pricing details per region on Defender for Cloud's pricing page: [Defender for Cloud Pricing](https://azure.microsoft.com/services/defender-for-cloud/#pricing). (No related policy)

**Severity**: High

[**Microsoft Defender for open-source relational databases should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b6a28450-dd5d-4ba4-8806-245e20ef6632)

**Description**: Microsoft Defender for open-source relational databases detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. Learn more in [Introduction to Microsoft Defender for open-source relational databases](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-databases-introduction).

Important: Enabling this plan will result in charges for protecting your open-source relational databases. If you don't have any open-source relational databases in this subscription, no charges will be incurred. If you create any open-source relational databases on this subscription in the future, they will automatically be protected and charges will begin at that time. (No related policy)

**Severity**: High

[**Microsoft Defender for Resource Manager should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f0fb2a7e-16d5-849f-be57-86db712e9bd0)

**Description**: Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization. Defender for Cloud detects threats and alerts you about suspicious activity. Learn more in [Introduction to Microsoft Defender for Resource Manager](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-resource-manager-introduction). Enabling this Defender plan results in charges. Learn about the pricing details per region on Defender for Cloud's pricing page: [Defender for Cloud Pricing](https://azure.microsoft.com/services/defender-for-cloud/#pricing). (No related policy)

**Severity**: High

[**Microsoft Defender for SQL on machines should be enabled on workspaces**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e9c320f1-03a0-4d2b-9a37-84b3bdc2e281)

**Description**: Microsoft Defender for servers brings threat detection and advanced defenses for your Windows and Linux machines. With this Defender plan enabled on your subscriptions but not on your workspaces, you're paying for the full capability of Microsoft Defender for servers but missing out on some of the benefits. When you enable Microsoft Defender for servers on a workspace, all machines reporting to that workspace will be billed for Microsoft Defender for servers - even if they're in subscriptions without Defender plans enabled. Unless you also enable Microsoft Defender for servers on the subscription, those machines won't be able to take advantage of just-in-time VM access, adaptive application controls, and network detections for Azure resources. Learn more in [Introduction to Microsoft Defender for servers](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction). (No related policy)

**Severity**: Medium

[**Microsoft Defender for SQL servers on machines should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/6ac66a74-761f-4a59-928a-d373eea3f028)

**Description**: Microsoft Defender for SQL is a unified package that provides advanced SQL security capabilities. It includes functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate a threat to your database, and discovering and classifying sensitive data.

Important: Remediating this recommendation will result in charges for protecting your SQL servers on machines. If you don't have any SQL servers on machines in this subscription, no charges will be incurred. If you create any SQL servers on machines on this subscription in the future, they will automatically be protected and charges will begin at that time. [Learn more about Microsoft Defender for SQL servers on machines.](https://learn.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security) (Related policy: [Azure Defender for SQL servers on machines should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f6581d072-105e-4418-827f-bd446d56421b)).

**Severity**: High

[**Microsoft Defender for SQL should be enabled for unprotected Azure SQL servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/400a6682-992c-4726-9549-629fbc3b988f)

**Description**: Microsoft Defender for SQL is a unified package that provides advanced SQL security capabilities. It surfaces and mitigates potential database vulnerabilities, and detects anomalous activities that could indicate a threat to your database. Microsoft Defender for SQL is billed as shown on [pricing details per region](https://aka.ms/pricing-security-center). (Related policy: [Advanced data security should be enabled on your SQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2fabfb4388-5bf4-4ad7-ba82-2cd2f41ceae9)).

**Severity**: High

[**Microsoft Defender for SQL should be enabled for unprotected SQL Managed Instances**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ff6dbca8-d93c-49fc-92af-dc25da7faccd)

**Description**: Microsoft Defender for SQL is a unified package that provides advanced SQL security capabilities. It surfaces and mitigates potential database vulnerabilities, and detects anomalous activities that could indicate a threat to your database. Microsoft Defender for SQL is billed as shown on [pricing details per region](https://aka.ms/pricing-security-center). (Related policy: [Advanced data security should be enabled on SQL Managed Instance](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fabfb7388-5bf4-4ad7-ba99-2cd2f41cebb9)).

**Severity**: High

[**Microsoft Defender for Storage should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1be22853-8ed1-4005-9907-ddad64cb1417)

**Description**: Microsoft Defender for storage detects unusual and potentially harmful attempts to access or exploit storage accounts. Important: Protections from this plan are charged as shown on the **Defender plans** page. If you don't have any Azure Storage accounts in this subscription, you won't be charged. If you later create Azure Storage accounts on this subscription, they'll automatically be protected and charges will begin. Learn about the [pricing details per region](https://aka.ms/pricing-security-center). Learn more in [Introduction to Microsoft Defender for Storage](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction). (Related policy: [Azure Defender for Storage should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f308fbb08-4ab8-4e67-9b29-592e93fb94fa)).

**Severity**: High

[**Network Watcher should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f1f2f7dc-7bd5-18bf-c403-cbbdb7ec3d68)

**Description**: Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end-to-end network level view. Network diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your network in Azure. (Related policy: [Network Watcher should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fb6e2945c-0b7b-40f5-9233-7a5323b5cdc6)).

**Severity**: Low

[**Over-provisioned identities in subscriptions should be investigated to reduce the Permission Creep Index (PCI)**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/d103537b-9f3d-4658-a568-31dd66eb05cb)

**Description**: Over-provisioned identities in subscription should be investigated to reduce the Permission Creep Index (PCI) and to safeguard your infrastructure. Reduce the PCI by removing the unused high risk permission assignments. High PCI reflects risk associated with the identities with permissions that exceed their normal or required usage (No related policy).

**Severity**: Medium

[**Private endpoint connections on Azure SQL Database should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/75396512-3323-9be4-059d-32ecb113c3de)

**Description**: Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database. (Related policy: [Private endpoint connections on Azure SQL Database should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f7698e800-9299-47a6-b3b6-5a0fee576eed)).

**Severity**: Medium

[**Private endpoint should be enabled for MariaDB servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ca9b93fe-6f1f-676c-2f31-d20f88fdbe56)

**Description**: Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure. (Related policy: [Private endpoint should be enabled for MariaDB servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0a1302fb-a631-4106-9753-f3d494733990)).

**Severity**: Medium

[**Private endpoint should be enabled for MySQL servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/cec4922b-1eb3-cb74-660b-ffad9b9ac642)

**Description**: Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure. (Related policy: [Private endpoint should be enabled for MySQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f7595c971-233d-4bcf-bd18-596129188c49)).

**Severity**: Medium

[**Private endpoint should be enabled for PostgreSQL servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c5b83aed-f53d-5201-8ffb-1f9938de410a)

**Description**: Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure. (Related policy: [Private endpoint should be enabled for PostgreSQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0564d078-92f5-4f97-8398-b9f58a51f70b)).

**Severity**: Medium

[**Public network access on Azure SQL Database should be disabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/22e93e92-4a31-b4cd-d640-3ef908430aa6)

**Description**: Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules. (Related policy: [Public network access on Azure SQL Database should be disabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1b8ca024-1d5c-4dec-8995-b1a932b41780)).

**Severity**: Medium

[**Public network access should be disabled for MariaDB servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ab153e43-2fb5-0670-2117-70340851ea9b)

**Description**: Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. (Related policy: [Public network access should be disabled for MariaDB servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ffdccbe47-f3e3-4213-ad5d-ea459b2fa077)).

**Severity**: Medium

[**Public network access should be disabled for MySQL servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/d5d090f1-7d5c-9b38-7344-0ede8343276d)

**Description**: Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. (Related policy: [Public network access should be disabled for MySQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fd9844e8a-1437-4aeb-a32c-0c992f056095)).

**Severity**: Medium

[**Public network access should be disabled for PostgreSQL servers**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b34f9fe7-80cd-6fb3-2c5b-951993746ca8)

**Description**: Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. (Related policy: [Public network access should be disabled for PostgreSQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fb52376f7-9612-48a1-81cd-1ffe4b61032c)).

**Severity**: Medium

[**Redis Cache should allow access only via SSL**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/35b25be2-d08a-e340-45ed-f08a95d804fc)

**Description**: Enable only connections via SSL to Redis Cache. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking. (Related policy: [Only secure connections to your Azure Cache for Redis should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f22bee202-a82f-4305-9a2a-6d7f44d4dedb)).

**Severity**: High

[**SQL databases should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/82e20e14-edc5-4373-bfc4-f13121257c37)

**Description**: SQL Vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture. [Learn more](https://aka.ms/SQL-Vulnerability-Assessment/) (Related policy: [Vulnerabilities on your SQL databases should be remediated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2ffeedbf84-6b99-488c-acc2-71c829aa5ffc)).

**Severity**: High

[**SQL managed instances should have vulnerability assessment configured**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c42fc28d-1703-45fc-aaa5-39797f570513)

**Description**: Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities. (Related policy: [Vulnerability assessment should be enabled on SQL Managed Instance](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1b7aa243-30e4-4c9e-bca8-d0d3022b634a)).

**Severity**: High

[**SQL servers on machines should have vulnerability findings resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f97aa83c-9b63-4f9a-99f6-b22c4398f936)

**Description**: SQL Vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture. [Learn more](https://aka.ms/explore-vulnerability-assessment-reports/) (Related policy: [Vulnerabilities on your SQL servers on machine should be remediated](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicydefinitions%2f6ba6d016-e7c3-4842-b8f2-4992ebc0d72d)).

**Severity**: High

[**SQL servers should have an Azure Active Directory administrator provisioned**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f0553104-cfdb-65e6-759c-002812e38500)

**Description**: Provision an Azure AD administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services. (Related policy: [An Azure Active Directory administrator should be provisioned for SQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1f314764-cb73-4fc9-b863-8eca98ac36e9)).

**Severity**: High

[**SQL servers should have vulnerability assessment configured**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1db4f204-cb5a-4c9c-9254-7556403ce51c)

**Description**: Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities. (Related policy: [Vulnerability assessment should be enabled on your SQL servers](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fef2a8f2a-b3d9-49cd-a8a8-9a3aaaf647d9)).

**Severity**: High

[**Storage account should use a private link connection**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/cdc78c07-02b0-4af0-1cb2-cb7c672a8b0a)

**Description**: Private links enforce secure communication, by providing private connectivity to the storage account (Related policy: [Storage account should use a private link connection](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f6edd7eda-6dd8-40f7-810d-67160c639cd9)).

**Severity**: Medium

[**Storage accounts should be migrated to new Azure Resource Manager resources**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/47bb383c-8e25-95f0-c2aa-437add1d87d3)

**Description**: To benefit from new capabilities in Azure Resource Manager, you can migrate existing deployments from the Classic deployment model. Resource Manager enables security enhancements such as: stronger access control (RBAC), better auditing, ARM-based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication, and support for tags and resource groups for easier security management. [Learn more](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/migration-classic-resource-manager-overview) (Related policy: [Storage accounts should be migrated to new Azure Resource Manager resources](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f37e0d2fe-28a5-43d6-a273-67d37d1f5606)).

**Severity**: Low

[**Storage accounts should restrict network access using virtual network rules**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/ad4f3ff1-30eb-5042-16ed-27198f640b8d)

**Description**: Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts. (Related policy: [Storage accounts should restrict network access using virtual network rules](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f2a1a9cdf-e04d-429a-8416-3bfb72a1b26f)).

**Severity**: Medium

[**Subscriptions should have a contact email address for security issues**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/77758c9d-8a56-5f54-6ff7-69a762ca6004)

**Description**: To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Defender for Cloud. (Related policy: [Subscriptions should have a contact email address for security issues](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f4f4f78b8-e367-4b10-a341-d9a4ad5cf1c7))

**Severity**: Low

[**Transparent Data Encryption on SQL databases should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/651967bf-044e-4bde-8376-3e08e0600105)

**Description**: Enable transparent data encryption to protect data-at-rest and meet compliance requirements (Related policy: [Transparent Data Encryption on SQL databases should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f17k78e20-9358-41c9-923c-fb736d382a12)).

**Severity**: Low

[**VM Image Builder templates should use private link**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f6b0e473-eb23-c3be-fe61-2ae3e8309530)

**Description**: Audit VM Image Builder templates that do not have a virtual network configured. When a virtual network is not configured, a public IP is created and used instead, which might directly expose resources to the internet and increase the potential attack surface. (Related policy: [VM Image Builder templates should use private link](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f2154edb9-244f-4741-9970-660785bccdaa)).

**Severity**: Medium

[**Web Application Firewall (WAF) should be enabled for Application Gateway**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/efe75f01-6fff-5d9d-08e6-092b98d3fb3f)

**Description**: Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries/regions, IP address ranges, and other http(s) parameters via custom rules. (Related policy: [Web Application Firewall (WAF) should be enabled for Application Gateway](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f564feb30-bf6a-4854-b4bb-0d2d2d1e6c66)).

**Severity**: Low

[**Web Application Firewall (WAF) should be enabled for Azure Front Door Service service**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/0c02a769-03f1-c4d7-85a5-db5dca505c49)

**Description**: Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries/regions, IP address ranges, and other http(s) parameters via custom rules. (Related policy: [Web Application Firewall (WAF) should be enabled for Azure Front Door Service?service](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f055aa869-bc98-4af8-bafc-23f1ab6ffe2c))

**Severity**: Low

[**Cognitive Services should use private link**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/54f53ddf-6ebd-461e-a247-394c542bc5d1)

**Description**: Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage. Learn more about [private links](https://go.microsoft.com/fwlink/?linkid=2129800). (Related policy: [Cognitive Services should use private link](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fcddd188c-4b82-4c48-a19d-ddf74ee66a01)).

**Severity**: Medium

[**Azure Cosmos DB should disable public network access**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/334a182c-7c2c-41bc-ae1e-55327891ab50)

**Description**: Disabling public network access improves security by ensuring that your Cosmos DB account isn't exposed on the public internet. Creating private endpoints can limit exposure of your Cosmos DB account. [Learn more](https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints#blocking-public-network-access-during-account-creation). (Related policy: [Azure Cosmos DB should disable public network access](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f797b37f7-06b8-444c-b1ad-fc62867f335a)).

**Severity**: Medium

[**Cosmos DB accounts should use private link**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/80dc29d6-9887-4071-a66c-e763376c2de3)

**Description**: Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Cosmos DB account, data leakage risks are reduced. Learn more about [private links](https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints). (Related policy: [Cosmos DB accounts should use private link](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f58440f8a-10c5-4151-bdce-dfbaad4a20b7)).

**Severity**: Medium

[**Azure SQL Database should be running TLS version 1.2 or newer**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/8e9a37b9-2828-4c8f-a24e-7b0ab0e89c78)

**Description**: Setting TLS version to 1.2 or newer improves security by ensuring your Azure SQL Database can only be accessed from clients using TLS 1.2 or newer. Using versions of TLS less than 1.2 is not recommended since they have well documented security vulnerabilities. (Related policy: [Azure SQL Database should be running TLS version 1.2 or newer](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f32e6bbec-16b6-44c2-be37-c5b672d103cf)).

**Severity**: Medium

[**Azure SQL Managed Instances should disable public network access**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/a2624c52-2937-400c-af9d-3bf2d97382bf)

**Description**: Disabling public network access (public endpoint) on Azure SQL Managed Instances improves security by ensuring that they can only be accessed from inside their virtual networks or via Private Endpoints. Learn more about [public network access](https://aka.ms/mi-public-endpoint). (Related policy: [Azure SQL Managed Instances should disable public network access](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f9dfea752-dd46-4766-aed1-c355fa93fb91)).

**Severity**: Medium

[**Storage accounts should prevent shared key access**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/3b363842-30f5-4056-980d-3a40fa5de8b3)

**Description**: Audit requirement of Azure Active Directory (Azure AD) to authorize requests for your storage account. By default, requests can be authorized with either Azure Active Directory credentials, or by using the account access key for Shared Key authorization. Of these two types of authorization, Azure AD provides superior security and ease of use over shared Key, and is recommended by Microsoft. (Related policy: [policy](https://ms.portal.azure.com/#view/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%8c6a50c6-9ffd-4ae7-986f-5fa6111f9a54))

**Severity**: Medium

**Identity and access recommendations**

[**A maximum of 3 owners should be designated for subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/6f90a6d6-d4d6-0794-0ec1-98fa77878c2e)

**Description**: To reduce the potential for breaches by compromised owner accounts, we recommend limiting the number of owner accounts to a maximum of 3 (Related policy: [A maximum of 3 owners should be designated for your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f4f11b553-d42e-4e3a-89be-32ca364cad4c)).

**Severity**: High

[**Accounts with owner permissions on Azure resources should be MFA enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/6240402e-f77c-46fa-9060-a7ce53997754)

**Description**: If you only use passwords to authenticate your users, you're leaving an attack vector open. Users often use weak passwords for multiple services. By enabling [multifactor authentication](https://learn.microsoft.com/en-us/azure/defender-for-cloud/multi-factor-authentication-enforcement) (MFA), you provide better security for your accounts, while still allowing your users to authenticate to almost any application with single sign-on (SSO). Multifactor authentication is a process by which users are prompted, during the sign-in process, for another form of identification. For example, a code might be sent to their cellphone, or they might be asked for a fingerprint scan. We recommend you to enable MFA for all accounts that have [owner permissions](https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner) on Azure resources, to prevent breach and attacks. More details and frequently asked questions are available here: [Manage multifactor authentication (MFA) enforcement on your subscriptions](https://learn.microsoft.com/en-us/azure/defender-for-cloud/multi-factor-authentication-enforcement) (No related policy).

**Severity**: High

[**Accounts with read permissions on Azure resources should be MFA enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/dabc9bc4-b8a8-45bd-9a5a-43000df8aa1c)

**Description**: If you only use passwords to authenticate your users, you're leaving an attack vector open. Users often use weak passwords for multiple services. By enabling [multifactor authentication](https://learn.microsoft.com/en-us/azure/defender-for-cloud/multi-factor-authentication-enforcement) (MFA), you provide better security for your accounts, while still allowing your users to authenticate to almost any application with single sign-on (SSO). Multifactor authentication is a process by which users are prompted, during the sign-in process, for an additional form of identification. For example, a code might be sent to their cellphone, or they might be asked for a fingerprint scan. We recommend you to enable MFA for all accounts that have [read permissions](https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner) on Azure resources, to prevent breach and attacks. More details and frequently asked questions are available [here](https://learn.microsoft.com/en-us/azure/defender-for-cloud/multi-factor-authentication-enforcement). (No related policy)

**Severity**: High

[**Accounts with write permissions on Azure resources should be MFA enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c0cb17b2-0607-48a7-b0e0-903ed22de39b)

**Description**: If you only use passwords to authenticate your users, you are leaving an attack vector open. Users often use weak passwords for multiple services. By enabling [multifactor authentication](https://learn.microsoft.com/en-us/azure/defender-for-cloud/multi-factor-authentication-enforcement) (MFA), you provide better security for your accounts, while still allowing your users to authenticate to almost any application with single sign-on (SSO). Multifactor authentication is a process by which users are prompted, during the sign-in process, for an additional form of identification. For example, a code might be sent to their cellphone, or they might be asked for a fingerprint scan. We recommend you to enable MFA for all accounts that have [write permissions](https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner) on Azure resources, to prevent breach and attacks. More details and frequently asked questions are available here: [Manage multifactor authentication (MFA) enforcement on your subscriptions](https://learn.microsoft.com/en-us/azure/defender-for-cloud/multi-factor-authentication-enforcement) (No related policy).

**Severity**: High

[**Azure Cosmos DB accounts should use Azure Active Directory as the only authentication method**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/14acab4e-ad95-11ec-b909-0242ac120002)

**Description**: The best way to authenticate to Azure services is by using Role-Based Access Control (RBAC). RBAC allows you to maintain the minimum privilege principle and supports the ability to revoke permissions as an effective method of response when compromised. You can configure your Azure Cosmos DB account to enforce RBAC as the only authentication method. When the enforcement is configured, all other methods of access will be denied (primary/secondary keys and access tokens). (No related policy)

**Severity**: Medium

[**Blocked accounts with owner permissions on Azure resources should be removed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/050ac097-3dda-4d24-ab6d-82568e7a50cf)

**Description**: Accounts that have been blocked from signing in on Active Directory, should be removed from your Azure resources. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (No related policy)

**Severity**: High

[**Blocked accounts with read and write permissions on Azure resources should be remove**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1ff0b4c9-ed56-4de6-be9c-d7ab39645926)

**Description**: Accounts that have been blocked from signing in on Active Directory, should be removed from your Azure resources. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (No related policy)

**Severity**: High

[**Deprecated accounts should be removed from subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/00c6d40b-e990-6acf-d4f3-471e747a27c4)

**Description**: User accounts that have been blocked from signing in, should be removed from your subscriptions. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (Related policy: [Deprecated accounts should be removed from your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f6b1cbf55-e8b6-442f-ba4c-7246b6381474)).

**Severity**: High

[**Deprecated accounts with owner permissions should be removed from subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e52064aa-6853-e252-a11e-dffc675689c2)

**Description**: User accounts that have been blocked from signing in, should be removed from your subscriptions. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (Related policy: [Deprecated accounts with owner permissions should be removed from your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2febb62a0c-3560-49e1-89ed-27e074e9f8ad)).

**Severity**: High

[**Diagnostic logs in Key Vault should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/88bbc99c-e5af-ddd7-6105-6150b2bfa519)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in Key Vault should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fcf820ca0-f99e-4f3e-84fb-66e913812d21)).

**Severity**: Low

[**External accounts with owner permissions should be removed from subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c3b6ae71-f1f0-31b4-e6c1-d5951285d03d)

**Description**: Accounts with owner permissions that have different domain names (external accounts), should be removed from your subscription. This prevents unmonitored access. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (Related policy: [External accounts with owner permissions should be removed from your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ff8456c1c-aa66-4dfb-861a-25d127b775c9)).

**Severity**: High

[**External accounts with read permissions should be removed from subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/a8c6a4ad-d51e-88fe-2979-d3ee3c864f8b)

**Description**: Accounts with read permissions that have different domain names (external accounts), should be removed from your subscription. This prevents unmonitored access. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (Related policy: [External accounts with read permissions should be removed from your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5f76cf89-fbf2-47fd-a3f4-b891fa780b60)).

**Severity**: High

[**External accounts with write permissions should be removed from subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/04e7147b-0deb-9796-2e5c-0336343ceb3d)

**Description**: Accounts with write permissions that have different domain names (external accounts), should be removed from your subscription. This prevents unmonitored access. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (Related policy: [External accounts with write permissions should be removed from your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5c607a2e-c700-4744-8254-d77e7c9eb5e4)).

**Severity**: High

[**Firewall should be enabled on Key Vault**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/52f7826a-ace7-3107-dd0d-4875853c1576)

**Description**: Key vault's firewall prevents unauthorized traffic from reaching your key vault and provides an additional layer of protection for your secrets. Enable the firewall to make sure that only traffic from allowed networks can access your key vault. (Related policy: [Firewall should be enabled on Key Vault](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f55615ac9-af46-4a59-874e-391cc3dfb490)).

**Severity**: Medium

[**Guest accounts with owner permissions on Azure resources should be removed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/20606e75-05c4-48c0-9d97-add6daa2109a)

**Description**: Accounts with owner permissions that have been provisioned outside of the Azure Active Directory tenant (different domain names), should be removed from your Azure resources. Guest accounts aren't managed to the same standards as enterprise tenant identities. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (No related policy)

**Severity**: High

[**Guest accounts with read permissions on Azure resources should be removed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/fde1c0c9-0fd2-4ecc-87b5-98956cbc1095)

**Description**: Accounts with read permissions that have been provisioned outside of the Azure Active Directory tenant (different domain names), should be removed from your Azure resources. Guest accounts aren't managed to the same standards as enterprise tenant identities. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (No related policy)

**Severity**: High

[**Guest accounts with write permissions on Azure resources should be removed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/0354476c-a12a-4fcc-a79d-f0ab7ffffdbb)

**Description**: Accounts with write permissions that have been provisioned outside of the Azure Active Directory tenant (different domain names), should be removed from your Azure resources. Guest accounts aren't managed to the same standards as enterprise tenant identities. These accounts can be targets for attackers looking to find ways to access your data without being noticed. (No related policy)

**Severity**: High

[**Key Vault keys should have an expiration date**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1aabfa0d-7585-f9f5-1d92-ecb40291d9f2)

**Description**: Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It's a recommended security practice to set expiration dates on cryptographic keys. (Related policy: [Key Vault keys should have an expiration date](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f152b15f7-8e1f-4c1f-ab71-8c010ba5dbc0)).

**Severity**: High

[**Key Vault secrets should have an expiration date**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/14257785-9437-97fa-11ae-898cfb24302b)

**Description**: Secrets should have a defined expiration date and not be permanent. Secrets that are valid forever provide a potential attacker with more time to compromise them. It's a recommended security practice to set expiration dates on secrets. (Related policy: [Key Vault secrets should have an expiration date](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f98728c90-32c7-4049-8429-847dc0f4fe37)).

**Severity**: High

[**Key vaults should have purge protection enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/4ed62ae4-5072-f9e7-8d94-51c76c48159a)

**Description**: Malicious deletion of a key vault can lead to permanent data loss. A malicious insider in your organization can potentially delete and purge key vaults. Purge protection protects you from insider attacks by enforcing a mandatory retention period for soft deleted key vaults. No one inside your organization or Microsoft will be able to purge your key vaults during the soft delete retention period. (Related policy: [Key vaults should have purge protection enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0b60c0b2-2dc2-4e1c-b5c9-abbed971de53)).

**Severity**: Medium

[**Key vaults should have soft delete enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/78211c00-15a9-336e-17c4-0b48613dadf4)

**Description**: Deleting a key vault without soft delete enabled permanently deletes all secrets, keys, and certificates stored in the key vault. Accidental deletion of a key vault can lead to permanent data loss. Soft delete allows you to recover an accidentally deleted key vault for a configurable retention period. (Related policy: [Key vaults should have soft delete enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f1e66c121-a66a-4b1f-9b83-0fd99bf0fc2d)).

**Severity**: High

[**MFA should be enabled on accounts with owner permissions on subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/94290b00-4d0c-d7b4-7cea-064a9554e681)

**Description**: Multifactor authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources. (Related policy: [MFA should be enabled on accounts with owner permissions on your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2faa633080-8b72-40c4-a2d7-d00c03e80bed)).

**Severity**: High

[**MFA should be enabled on accounts with read permissions on subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/151e82c5-5341-a74b-1eb0-bc38d2c84bb5)

**Description**: Multifactor authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources. (Related policy: [MFA should be enabled on accounts with read permissions on your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fe3576e28-8b17-4677-84c3-db2990658d64)).

**Severity**: High

[**MFA should be enabled on accounts with write permissions on subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/57e98606-6b1e-6193-0e3d-fe621387c16b)

**Description**: Multifactor authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources. (Related policy: [MFA should be enabled accounts with write permissions on your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f9297c21d-2ed6-4474-b48f-163f75654ce3)).

**Severity**: High

[**Microsoft Defender for Key Vault should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/b1af52e4-e968-4e2b-b6d0-6736c9651f0a)

**Description**: Microsoft Defender for Cloud includes Microsoft Defender for Key Vault, providing an additional layer of security intelligence. Microsoft Defender for Key Vault detects unusual and potentially harmful attempts to access or exploit Key Vault accounts. Important: Protections from this plan are charged as shown on the **Defender plans** page. If you don't have any key vaults in this subscription, you won't be charged. If you later create key vaults on this subscription, they'll automatically be protected and charges will begin. Learn about the [pricing details per region](https://aka.ms/pricing-security-center). Learn more in [Introduction to Microsoft Defender for Key Vault](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-key-vault-introduction). (Related policy: [Azure Defender for Key Vault should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f0e6763cc-5078-4e64-889d-ff4d9a839047)).

**Severity**: High

[**Private endpoint should be configured for Key Vault**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/2e96bc2f-1972-e471-9e70-ae58d41e9d2a)

**Description**: Private link provides a way to connect Key Vault to your Azure resources without sending traffic over the public internet. Private link provides defense in depth protection against data exfiltration. (Related policy: [Private endpoint should be configured for Key Vault](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f5f0bc445-3935-4915-9981-011aa2b46147)).

**Severity**: Medium

[**Storage account public access should be disallowed**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/51fd8bb1-0db4-bbf1-7e2b-cfcba7eb66a6)

**Description**: Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it. (Related policy: [Storage account public access should be disallowed](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fmicrosoft.authorization%2fpolicyDefinitions%2f4fa4b6c0-31ca-4c0d-b10d-24b96f62a751)).

**Severity**: Medium

[**There should be more than one owner assigned to subscriptions**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/2c79b4af-f830-b61e-92b9-63dfa30f16e4)

**Description**: Designate more than one subscription owner in order to have administrator access redundancy. (Related policy: [There should be more than one owner assigned to your subscription](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f09024ccc-0c5f-475e-9457-b7c0d9ed487b)).

**Severity**: High

[**Validity period of certificates stored in Azure Key Vault should not exceed 12 months**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/fc84abc0-eee6-4758-8372-a7681965ca44)

**Description**: Ensure your certificates do not have a validity period that exceeds 12 months. (Related policy: [Certificates should have the specified maximum validity period](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0a075868-4c26-42ef-914c-5bc007359560)).

**Severity**: Medium

[**Azure overprovisioned identities should have only the necessary permissions (Preview)**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/dcedec72-5b25-45b3-b8b9-0ed9219f8f29)

**Description**: Overprovisioned identities, or over permissioned identities, don't use many of their granted permissions. Regularly right-size permissions of these identities to reduce the risk of permissions misuse, either accidental or malicious. This action decreases the potential blast radius during a security incident.

**Severity**: Medium

[**Super identities in your Azure environment should be removed (Preview)**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/fe7d5a87-36fc-4530-99b5-1848512a3209)

**Description**: Super Identity is any human or workload identity such as users, Service Principals, and serverless functions that have admin permissions and can perform any action on any resource across the infrastructure. Super Identities are extremely high risk, as any malicious or accidental permissions misuse can result in catastrophic service disruption, service degradation, or data leakage. Super Identities pose a huge threat to cloud infrastructure. Too many super identities can create excessive risks and increase the blast radius during a breach.

**Severity**: Medium

[**Permissions of inactive identities in your Azure subscription should be revoked**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/7af29efb-41cc-47b6-81b8-800a0888f9a2)

**Description**: Microsoft Defender for Cloud discovered an identity that has not performed any action on any resource within your Azure subscription in the past 45 days. It is recommended to revoke permissions of inactive identities, in order to reduce the attack surface of your cloud environment.

**Severity**: Medium

**IoT recommendations**

[**Default IP Filter Policy should be Deny**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/5a3d6cdd-8eb3-46d2-ba11-d24a0d47fe65)

**Description**: IP Filter Configuration should have rules defined for allowed traffic and should deny all other traffic by default (No related policy).

**Severity**: Medium

[**Diagnostic logs in IoT Hub should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/77785808-ce86-4e40-b45f-19110a547397)

**Description**: Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: [Diagnostic logs in IoT Hub should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f383856f8-de7f-44a2-81fc-e5135b5c2aa4)).

**Severity**: Low

[**Identical Authentication Credentials**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/9d07b7e6-2986-4964-a76c-b2689604e212)

**Description**: Identical authentication credentials to the IoT Hub used by multiple devices. This could indicate an illegitimate device impersonating a legitimate device. It also exposes the risk of device impersonation by an attacker (No related policy).

**Severity**: High

[**IP Filter rule large IP range**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/d8326952-60bb-40fb-b33f-51e662708a88)

**Description**: An Allow IP Filter rule's source IP range is too large. Overly permissive rules might expose your IoT hub to malicious intenders (No related policy).

**Severity**: Medium

**Networking recommendations**

[**Access to storage accounts with firewall and virtual network configurations should be restricted**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/45d313c3-3fca-5040-035f-d61928366d31)

**Description**: Review the settings of network access in your storage account firewall settings. We recommended configuring network rules so that only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges. (Related policy: [Storage accounts should restrict network access](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f34c877ad-507e-4c82-993e-3452a6e0ad3c)).

**Severity**: Low

[**Adaptive network hardening recommendations should be applied on internet facing virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f9f0eed0-f143-47bf-b856-671ea2eeed62)

**Description**: Defender for Cloud has analyzed the internet traffic communication patterns of the virtual machines listed below, and determined that the existing rules in the NSGs associated to them are overly permissive, resulting in an increased potential attack surface. This typically occurs when this IP address doesn't communicate regularly with this resource. Alternatively, the IP address has been flagged as malicious by Defender for Cloud's threat intelligence sources. Learn more in [Improve your network security posture with adaptive network hardening](https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-network-hardening). (Related policy: [Adaptive network hardening recommendations should be applied on internet facing virtual machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f08e6af2d-db70-460a-bfe9-d5bd474ba9d6)).

**Severity**: High

[**All network ports should be restricted on network security groups associated to your virtual machine**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/3b20e985-f71f-483b-b078-f30d73936d43)

**Description**: Defender for Cloud has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources. (Related policy: [All network ports should be restricted on network security groups associated to your virtual machine](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f9daedab3-fb2d-461e-b861-71790eead4f6)).

**Severity**: High

[**Azure DDoS Protection Standard should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/e3de1cc0-f4dd-3b34-e496-8b5381ba2d70)

**Description**: Defender for Cloud has discovered virtual networks with Application Gateway resources unprotected by the DDoS protection service. These resources contain public IPs. Enable mitigation of network volumetric and protocol attacks. (Related policy: [Azure DDoS Protection Standard should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fa7aca53f-2ed4-4466-a25e-0b45ade68efd)).

**Severity**: Medium

[**Internet-facing virtual machines should be protected with network security groups**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/483f12ed-ae23-447e-a2de-a67a10db4353)

**Description**: Protect your VM from potential threats by restricting access to it with a network security group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your VM from other instances, in or outside the same subnet. To keep your machine as secure as possible, the VM access to the internet must be restricted and an NSG should be enabled on the subnet. VMs with 'High' severity are internet-facing VMs. (Related policy: [Internet-facing virtual machines should be protected with network security groups](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ff6de0be7-9a8a-4b8a-b349-43cf02d22f7c)).

**Severity**: High

[**IP forwarding on your virtual machine should be disabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/c3b51c94-588b-426b-a892-24696f9e54cc)

**Description**: Defender for Cloud has discovered that IP forwarding is enabled on some of your virtual machines. Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team. (Related policy: [IP Forwarding on your virtual machine should be disabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fbd352bd5-2853-4985-bf0d-73806b4a5744)).

**Severity**: Medium

[**Machines should have ports closed that might expose attack vectors**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bbff27d2-73db-4c2d-8b1a-5f20b1f1da7e)

**Description**: [Azure's terms of use](https://www.microsoft.com/legal/terms-of-use) prohibit the use of Azure services in ways that could damage, disable, overburden, or impair any Microsoft server or the network. This recommendation lists exposed ports that need to be closed for your continued security. It also illustrates the potential threat to each port. (No related policy)

**Severity**: High

[**Management ports of virtual machines should be protected with just-in-time network access control**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/805651bc-6ecd-4c73-9b55-97a19d0582d0)

**Description**: Defender for Cloud has identified some overly permissive inbound rules for management ports in your Network Security Group. Enable just-in-time access control to protect your VM from internet-based brute-force attacks. Learn more in [Understanding just-in-time (JIT) VM access](https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview). (Related policy: [Management ports of virtual machines should be protected with just-in-time network access control](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fb0f33259-77d7-4c9e-aac6-3aabcfae693c)).

**Severity**: High

[**Management ports should be closed on your virtual machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/bc303248-3d14-44c2-96a0-55f5c326b5fe)

**Description**: Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine. (Related policy: [Management ports should be closed on your virtual machines](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f22730e10-96f6-4aac-ad84-9383d35b5917)).

**Severity**: Medium

[**Non-internet-facing virtual machines should be protected with network security groups**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/a9341235-9389-42f0-a0bf-9bfb57960d44)

**Description**: Protect your non-internet-facing virtual machine from potential threats by restricting access to it with a network security group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your VM from other instances, whether or not they're on the same subnet. Note that to keep your machine as secure as possible, the VM's access to the internet must be restricted and an NSG should be enabled on the subnet. (Related policy: [Non-internet-facing virtual machines should be protected with network security groups](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fbb91dfba-c30d-4263-9add-9c2384e659a6)).

**Severity**: Low

[**Secure transfer to storage accounts should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/1c5de8e1-f68d-6a17-e0d2-ec259c42768c)

**Description**: Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking. (Related policy: [Secure transfer to storage accounts should be enabled](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f404c3081-a854-4457-ae30-26a93ef643f9)).

**Severity**: High

[**Subnets should be associated with a network security group**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/eade5b56-eefd-444f-95c8-23f29e5d93cb)

**Description**: Protect your subnet from potential threats by restricting access to it with a network security group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VM instances and integrated services in that subnet, but don't apply to internal traffic inside the subnet. To secure resources in the same subnet from one another, enable NSG directly on the resources as well. Note that the following subnet types will be listed as not applicable: GatewaySubnet, AzureFirewallSubnet, AzureBastionSubnet. (Related policy: [Subnets should be associated with a Network Security Group](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2fe71308d3-144b-4262-b144-efdc3cc90517)).

**Severity**: Low

[**Virtual networks should be protected by Azure Firewall**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f67fb4ed-d481-44d7-91e5-efadf504f74a)

**Description**: Some of your virtual networks aren't protected with a firewall. Use [Azure Firewall](https://azure.microsoft.com/pricing/details/azure-firewall) to restrict access to your virtual networks and prevent potential threats. (Related policy: [All Internet traffic should be routed via your deployed Azure Firewall](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2ffc5e4038-4584-4632-8c85-c0448d374b2c)).

**Severity**: Low

**API recommendations**

**Microsoft Defender for APIs should be enabled**

**Description & related policy**: Enable the Defender for APIs plan to discover and protect API resources against attacks and security misconfigurations. [Learn more](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-apis-deploy)

**Severity**: High

**Azure API Management APIs should be onboarded to Defender for APIs**

**Description & related policy**: Onboarding APIs to Defender for APIs requires compute and memory utilization on the Azure API Management service. Monitor performance of your Azure API Management service while onboarding APIs, and scale out your Azure API Management resources as needed.

**Severity**: High

**API endpoints that are unused should be disabled and removed from the Azure API Management service**

**Description & related policy**: As a security best practice, API endpoints that haven't received traffic for 30 days are considered unused, and should be removed from the Azure API Management service. Keeping unused API endpoints might pose a security risk. These might be APIs that should have been deprecated from the Azure API Management service, but have accidentally been left active. Such APIs typically do not receive the most up-to-date security coverage.

**Severity**: Low

**API endpoints in Azure API Management should be authenticated**

**Description & related policy**: API endpoints published within Azure API Management should enforce authentication to help minimize security risk. Authentication mechanisms are sometimes implemented incorrectly or are missing. This allows attackers to exploit implementation flaws and to access data. For APIs published in Azure API Management, this recommendation assesses authentication through verifying the presence of Azure API Management subscription keys for APIs or products where subscription is required, and the execution of policies for validating [JWT](https://learn.microsoft.com/en-us/azure/api-management/validate-jwt-policy), [client certificates](https://learn.microsoft.com/en-us/azure/api-management/validate-client-certificate-policy), and [Microsoft Entra](https://learn.microsoft.com/en-us/azure/api-management/validate-azure-ad-token-policy) tokens. If none of these authentication mechanisms are executed during the API call, the API will receive this recommendation.

**Severity**: High

**API management recommendations**

**API Management subscriptions should not be scoped to all APIs**

**Description & related policy**: API Management subscriptions should be scoped to a product or an individual API instead of all APIs, which could result in excessive data exposure.

**Severity**: Medium

**API Management calls to API backends should not bypass certificate thumbprint or name validation**

**Description & related policy**: API Management should validate the backend server certificate for all API calls. Enable SSL certificate thumbprint and name validation to improve the API security.

**Severity**: Medium

**API Management direct management endpoint should not be enabled**

**Description & related policy**: The direct management REST API in Azure API Management bypasses Azure Resource Manager role-based access control, authorization, and throttling mechanisms, thus increasing the vulnerability of your service.

**Severity**: Low

**API Management APIs should use only encrypted protocols**

**Description & related policy**: APIs should be available only through encrypted protocols, like HTTPS or WSS. Avoid using unsecured protocols, such as HTTP or WS to ensure security of data in transit.

**Severity**: High

**API Management secret named values should be stored in Azure Key Vault**

**Description & related policy**: Named values are a collection of name and value pairs in each API Management service. Secret values can be stored either as encrypted text in API Management (custom secrets) or by referencing secrets in Azure Key Vault. Reference secret named values from Azure Key Vault to improve security of API Management and secrets. Azure Key Vault supports granular access management and secret rotation policies.

**Severity**: Medium

**API Management should disable public network access to the service configuration endpoints**

**Description & related policy**: To improve the security of API Management services, restrict connectivity to service configuration endpoints, like direct access management API, Git configuration management endpoint, or self-hosted gateways configuration endpoint.

**Severity**: Medium

**API Management minimum API version should be set to 2019-12-01 or higher**

**Description & related policy**: To prevent service secrets from being shared with read-only users, the minimum API version should be set to 2019-12-01 or higher.

**Severity**: Medium

**API Management calls to API backends should be authenticated**

**Description & related policy**: Calls from API Management to backends should use some form of authentication, whether via certificates or credentials. Does not apply to Service Fabric backends.

**Severity**: Medium

**AI recommendations**

**Resource logs in Azure Machine Learning Workspaces should be enabled (Preview)**

**Description & related policy**: Resource logs enable recreating activity trails to use for investigation purposes when a security incident occurs or when your network is compromised.

**Severity**: Medium

**Azure Machine Learning Workspaces should disable public network access (Preview)**

**Description & related policy**: Disabling public network access improves security by ensuring that the Machine Learning Workspaces aren't exposed on the public internet. You can control exposure of your workspaces by creating private endpoints instead. For more information, see [Configure a private endpoint for an Azure Machine Learning workspace](https://learn.microsoft.com/en-us/azure/machine-learning/how-to-configure-private-link).

**Severity**: Medium

**Azure Machine Learning Computes should be in a virtual network (Preview)**

**Description & related policy**: Azure Virtual Networks provide enhanced security and isolation for your Azure Machine Learning Compute Clusters and Instances, as well as subnets, access control policies, and other features to further restrict access. When a compute is configured with a virtual network, it is not publicly addressable and can only be accessed from virtual machines and applications within the virtual network.

**Severity**: Medium

**Azure Machine Learning Computes should have local authentication methods disabled (Preview)**

**Description & related policy**: Disabling local authentication methods improves security by ensuring that Machine Learning Computes require Azure Active Directory identities exclusively for authentication. For more information, see [Azure Policy Regulatory Compliance controls for Azure Machine Learning](https://learn.microsoft.com/en-us/azure/machine-learning/security-controls-policy).

**Severity**: Medium

**Azure Machine Learning compute instances should be recreated to get the latest software updates (Preview)**

**Description & related policy**: Ensure Azure Machine Learning compute instances run on the latest available operating system. Security is improved and vulnerabilities reduced by running with the latest security patches. For more information, see [Vulnerability management for Azure Machine Learning](https://learn.microsoft.com/en-us/azure/machine-learning/concept-vulnerability-management#compute-instance).

**Severity**: Medium

**Resource logs in Azure Databricks Workspaces should be enabled (Preview)**

**Description & related policy**: Resource logs enable recreating activity trails to use for investigation purposes when a security incident occurs or when your network is compromised.

**Severity**: Medium

**Azure Databricks Workspaces should disable public network access (Preview)**

**Description & related policy**: Disabling public network access improves security by ensuring that the resource isn't exposed on the public internet. You can control exposure of your resources by creating private endpoints instead. For more information, see [Enable Azure Private Link](https://learn.microsoft.com/en-us/azure/databricks/administration-guide/cloud-configurations/azure/private-link).

**Severity**: Medium

**Azure Databricks Clusters should disable public IP (Preview)**

**Description & related policy**: Disabling public IP of clusters in Azure Databricks Workspaces improves security by ensuring that the clusters aren't exposed on the public internet. For more information, see [Secure cluster connectivity](https://learn.microsoft.com/en-us/azure/databricks/security/network/secure-cluster-connectivity).

**Severity**: Medium

**Azure Databricks Workspaces should be in a virtual network (Preview)**

**Description & related policy**: Azure Virtual Networks provide enhanced security and isolation for your Azure Databricks Workspaces, as well as subnets, access control policies, and other features to further restrict access. For more information, see [Deploy Azure Databricks in your Azure virtual network](https://learn.microsoft.com/en-us/azure/databricks/administration-guide/cloud-configurations/azure/vnet-inject).

**Severity**: Medium

**Azure Databricks Workspaces should use private link (Preview)**

**Description & related policy**: Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Databricks workspaces, you can reduce data leakage risks. For more information, see [Create the workspace and private endpoints in the Azure portal UI](https://learn.microsoft.com/en-us/azure/databricks/administration-guide/cloud-configurations/azure/private-link-standard#create-the-workspace-and-private-endpoints-in-the-azure-portal-ui).

**Severity**: Medium

[**Azure AI Services resources should restrict network access**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/f738efb8-005f-680d-3d43-b3db762d6243)

**Description**: By restricting network access, you can ensure that only allowed networks can access the service. This can be achieved by configuring network rules so that only applications from allowed networks can access the Azure AI service resource.

**Severity**: Medium

[**Azure AI Services resources should have key access disabled (disable local authentication)**](https://ms.portal.azure.com/#view/Microsoft_Azure_Security/GenericRecommendationDetailsBlade/assessmentKey/13b10b36-aa99-4db6-b00c-dcf87c4761e6)

**Description**: Key access (local authentication) is recommended to be disabled for security. Azure OpenAI Studio, typically used in development/testing, requires key access and will not function if key access is disabled. After disabling, Microsoft Entra ID becomes the only access method, which allows maintaining minimum privilege principle and granular control. [Learn more](https://aka.ms/AI/auth).

**Severity**: Medium

[**Diagnostic logs in Azure AI services resources should be enabled**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/dea5192e-1bb3-101b-b70c-4646546f5e1e)

**Description**: Enable logs for Azure AI services resources. This enables you to recreate activity trails for investigation purposes, when a security incident occurs or your network is compromised.

**Severity**: Low

**Deprecated recommendations**

**Access to App Services should be restricted**

**Description & related policy**: Restrict access to your App Services by changing the networking configuration, to deny inbound traffic from ranges that are too broad. (Related policy: [Preview]: Access to App Services should be restricted).

**Severity**: High

**The rules for web applications on IaaS NSGs should be hardened**

**Description & related policy**: Harden the network security group (NSG) of your virtual machines that are running web applications, with NSG rules that are overly permissive with regard to web application ports. (Related policy: The NSGs rules for web applications on IaaS should be hardened).

**Severity**: High

**Pod Security Policies should be defined to reduce the attack vector by removing unnecessary application privileges (Preview)**

**Description & related policy**: Define Pod Security Policies to reduce the attack vector by removing unnecessary application privileges. It is recommended to configure pod security policies so pods can only access resources which they are allowed to access. (Related policy: [Preview]: Pod Security Policies should be defined on Kubernetes Services).

**Severity**: Medium

**Install Azure Security Center for IoT security module to get more visibility into your IoT devices**

**Description & related policy**: Install Azure Security Center for IoT security module to get more visibility into your IoT devices.

**Severity**: Low

**Your machines should be restarted to apply system updates**

**Description & related policy**: Restart your machines to apply the system updates and secure the machine from vulnerabilities. (Related policy: System updates should be installed on your machines).

**Severity**: Medium

**Monitoring agent should be installed on your machines**

**Description & related policy**: This action installs a monitoring agent on the selected virtual machines. Select a workspace for the agent to report to. (No related policy)

**Severity**: High

**Java should be updated to the latest version for web apps**

**Description & related policy**: Periodically, newer versions are released for Java software either due to security flaws or to include additional functionality. Using the latest Java version for web apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: Ensure that 'Java version' is the latest, if used as a part of the Web app).

**Severity**: Medium

**Python should be updated to the latest version for function apps**

**Description & related policy**: Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest Python version for function apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: Ensure that 'Python version' is the latest, if used as a part of the Function app).

**Severity**: Medium

**Python should be updated to the latest version for web apps**

**Description & related policy**: Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest Python version for web apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: Ensure that 'Python version' is the latest, if used as a part of the Web app).

**Severity**: Medium

**Java should be updated to the latest version for function apps**

**Description & related policy**: Periodically, newer versions are released for Java software either due to security flaws or to include additional functionality. Using the latest Java version for function apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: Ensure that 'Java version' is the latest, if used as a part of the Function app).

**Severity**: Medium

**PHP should be updated to the latest version for web apps**

**Description & related policy**: Periodically, newer versions are released for PHP software either due to security flaws or to include additional functionality. Using the latest PHP version for web apps is recommended to benefit from security fixes, if any, and/or new functionalities of the latest version. (Related policy: Ensure that 'PHP version' is the latest, if used as a part of the WEB app).

**Severity**: Medium

[**Endpoint protection health issues on machines should be resolved**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/37a3689a-818e-4a0e-82ac-b1392b9bb000)

**Description**: Resolve endpoint protection health issues on your virtual machines to protect them from latest threats and vulnerabilities. See the documentation for the [endpoint protection solutions supported by Defender for Cloud](https://learn.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds#supported-endpoint-protection-solutions-) and the [endpoint protection assessments](https://learn.microsoft.com/en-us/azure/defender-for-cloud/endpoint-protection-recommendations-technical). (No related policy)

**Severity**: Medium

[**Endpoint protection should be installed on machines**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/4fb67663-9ab9-475d-b026-8c544cced439)

**Description**: To protect machines from threats and vulnerabilities, install a supported endpoint protection solution. Learn more about how endpoint protection for machines is evaluated in [Endpoint protection assessment and recommendations in Microsoft Defender for Cloud](https://learn.microsoft.com/en-us/azure/defender-for-cloud/endpoint-protection-recommendations-technical). (No related policy)

**Severity**: High

[**Public network access should be disabled for Cognitive Services accounts**](https://portal.azure.com/#blade/Microsoft_Azure_Security/RecommendationsBlade/assessmentKey/684a5b6d-a270-61ce-306e-5cea400dc3a7)

**Description**: This policy audits any Cognitive Services account in your environment with public network access enabled. Public network access should be disabled so that only connections from private endpoints are allowed. (Related policy: [Public network access should be disabled for Cognitive Services accounts](https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2fproviders%2fMicrosoft.Authorization%2fpolicyDefinitions%2f0725b4dd-7e76-479c-a735-68e7ee23d5ca)).

**Severity**: Medium