Securing Storage Account in Azure Cloud

Best practices for secure application development

By

SHAILESH GAWANDE

Introduction

Azure Storage account is the most commonly used service on Azure Cloud for variety of Purpose. It may contain huge amount of structured or unstructured data.

We have to note that Azure Storage is a shared service open to public network, so If the security of the storage account is not managed well, it can lead to data theft or leakage, unauthorized access and other risks. So, it's very important to secure the storage account in cloud.

In the context of data integration, Microsoft also offers ADLS (Azure Data Lake Storage) GEN2 besides regular Blog storage OR ADLS Gen1 storage. Which has additional security features.

When application development in cloud happens, security of the application is often ignored or many times given less priority. After the application is developed and goes in to production, security can become a compliance issue under industry standards e.g. ISO27001. It becomes difficult to fix those security issues in later stage as it may even break the application.

There are many other infrastructure items for which security needs to be addressed in advanced stage but here our scope is only storage account.

Here we will discuss various actions can be taken to secure storage account.

Start at Architecture Level

If the application is going to use Highly Restricted or Personal or secret data then complete architecture review focused on security has to be done before application development.

Implement RBAC(Role Based Access Control)

Access management for cloud resources is a critical function for any organization that is using the cloud. Azure role-based access control (Azure RBAC) helps you

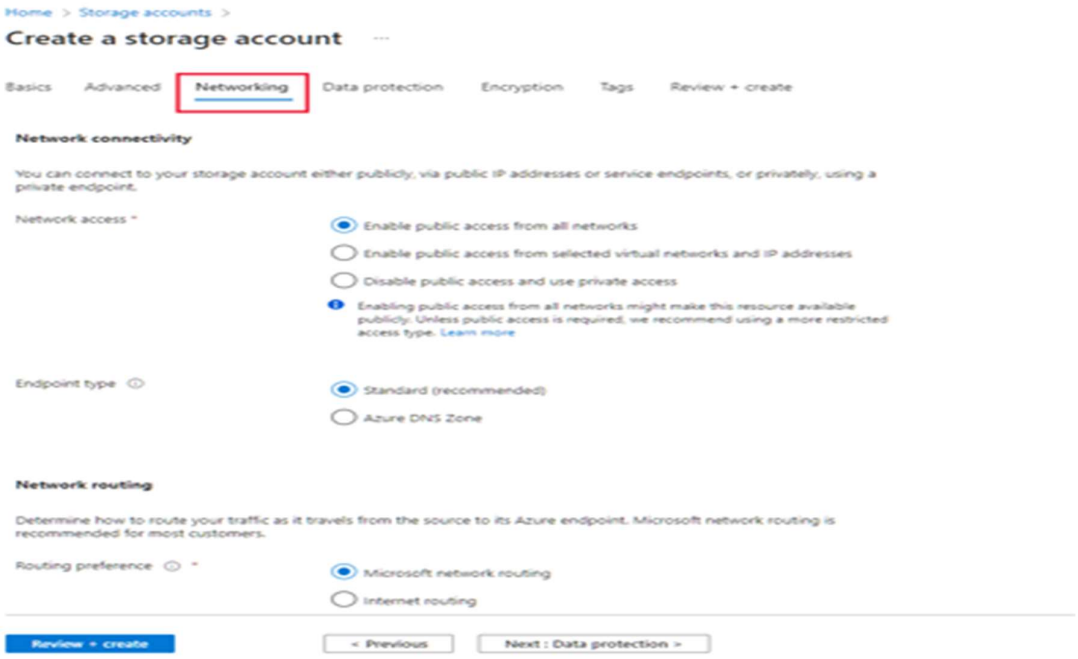
manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Access to the storage account should to be managed by RBAC(Role Based Access Control).

Minimum required access has to be given to the users. System assigned managed identity must be used wherever applicable and must be granted minimum required permissions using RBAC.

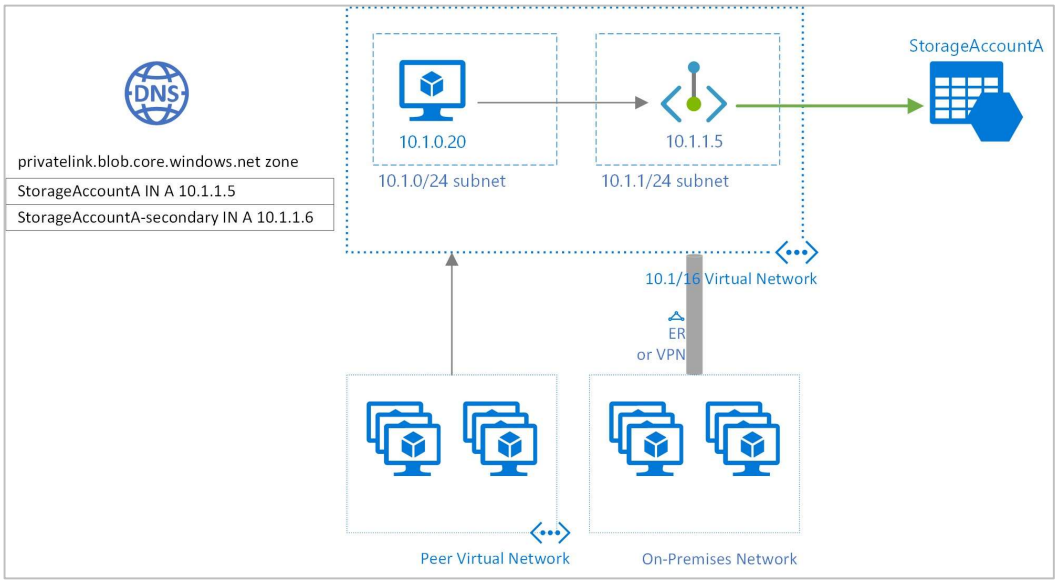
Must consider right networking configuration settings

By Default the storage account is enable for all networks(public access), as a best practice this should be disabled and only access to selected virtual networks or ip addresses should be allowed.

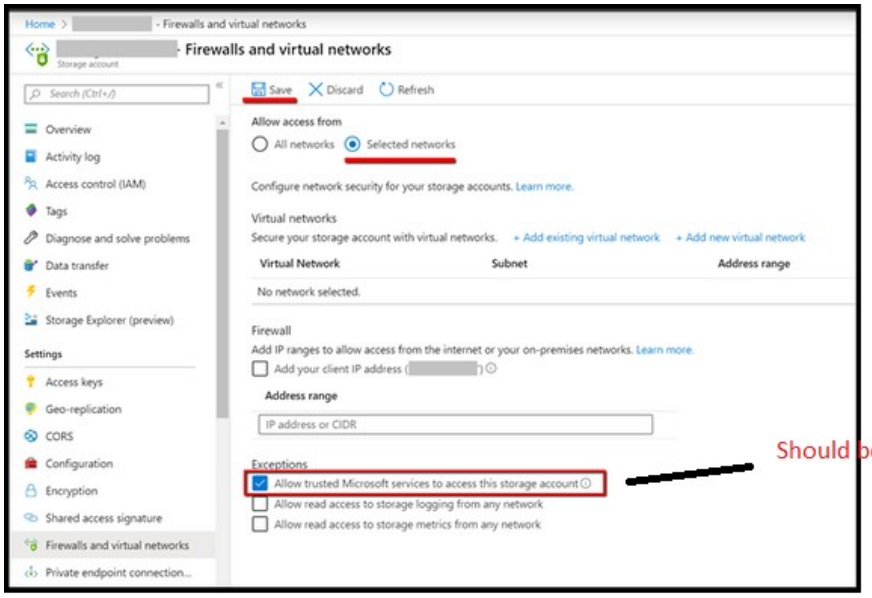


To further restrict the access, disable the public access totally and use private access(**Private Endpoint**). You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet. Please refer to below diagram for understanding.

Private Endpoint Conceptual Overview



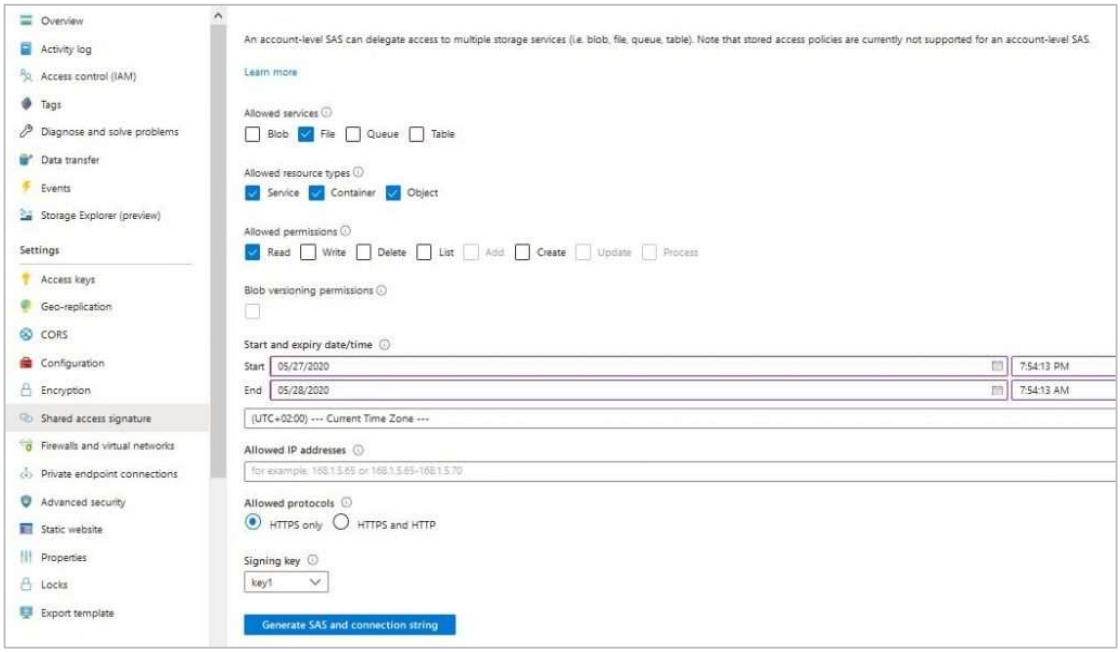
Allow trusted Microsoft services to access this storage account must be disabled. Enabling ‘Allow trusted Microsoft services to access this storage account may be allowed for limited services, please refer to your organizational standards for the same.



Best practice for using SAS (Shared Access Signature)

A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. for Example:

- What resources the client may access.
- What permissions they have to those resources.
- How long the SAS is valid.



As a best practice, SAS keys needs to protect by storing at a secure location like Azure Vault. SAS should be read only access. The keys should be rotated at regular intervals, ideally every 90 days for regular data and every 30 days for Highly Sensitive Data. Only https protocol should be allowed for SAS.

Access type for containers should be anonymous

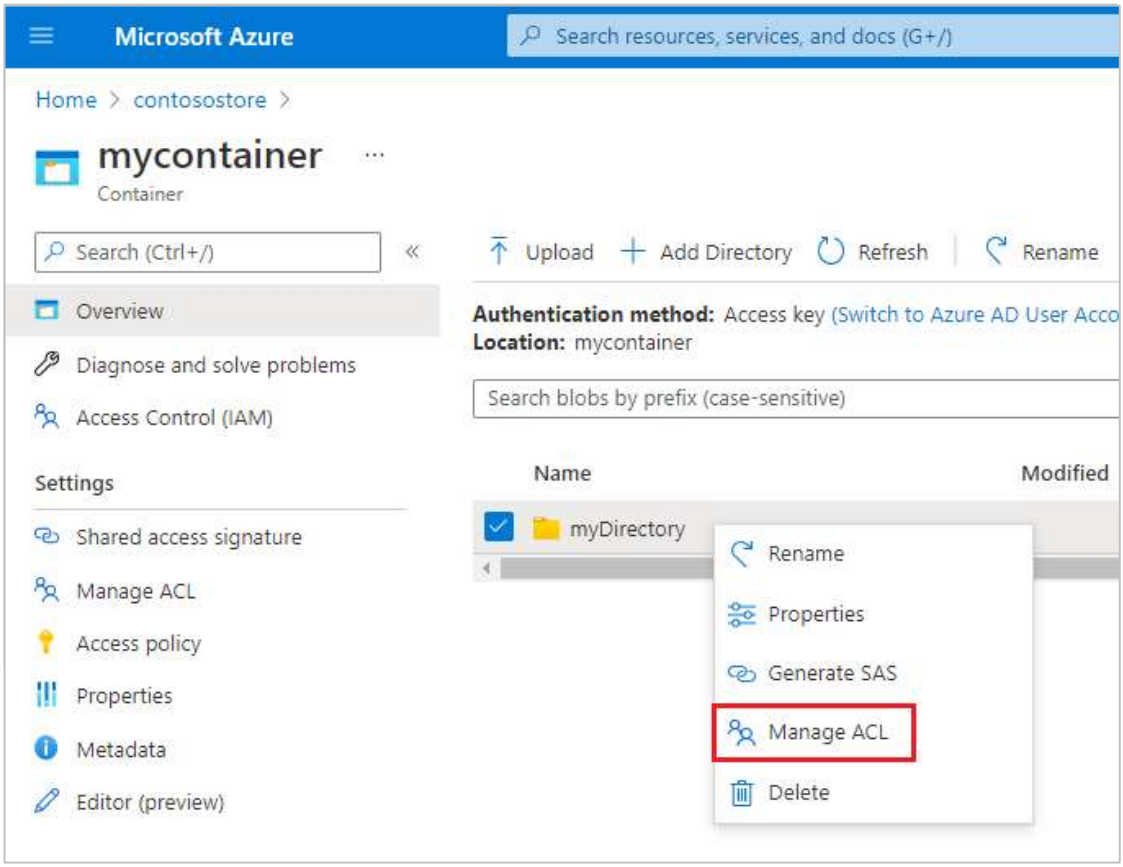
Shared Key authorization: for blobs, files, queues, and tables. A client using Shared Key passes a header with every request that is signed using the storage account access key.

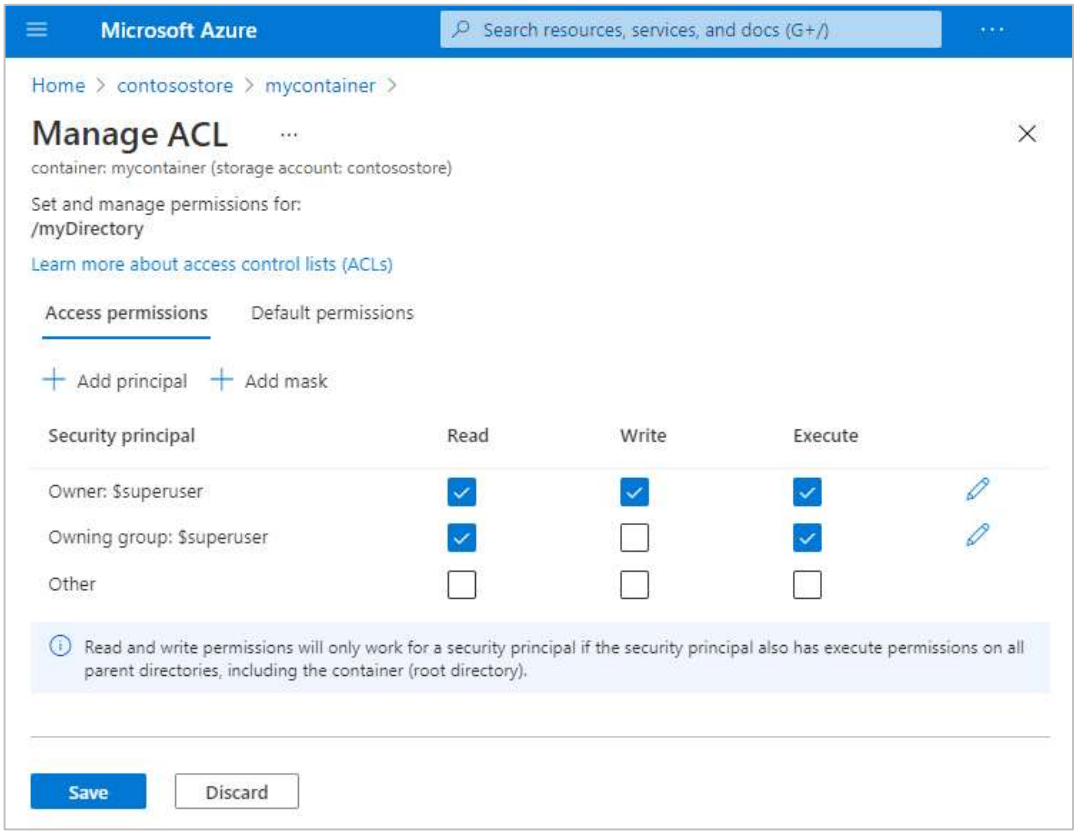
Microsoft recommends that you disallow Shared Key authorization for your storage account. When Shared Key authorization is disallowed, clients must use Azure AD or a user delegation SAS to authorize requests for data in that storage account. For more information, see Prevent Shared Key authorization for an Azure Storage account

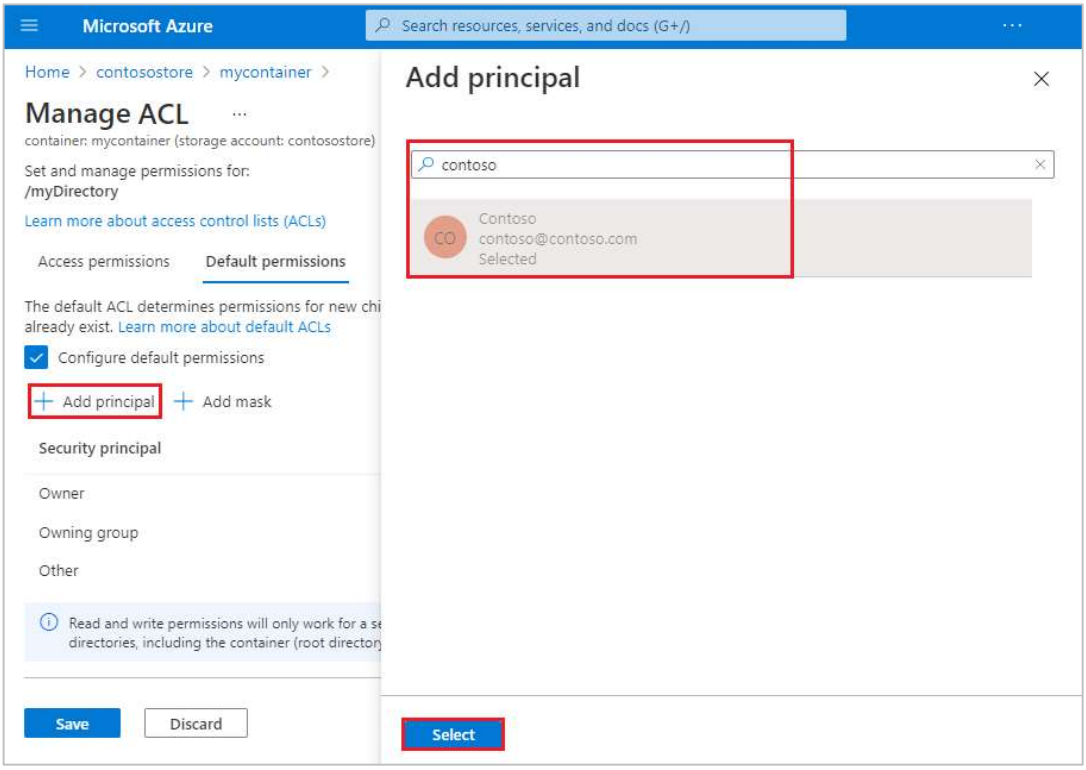
Implement Access Control lists or ACLs

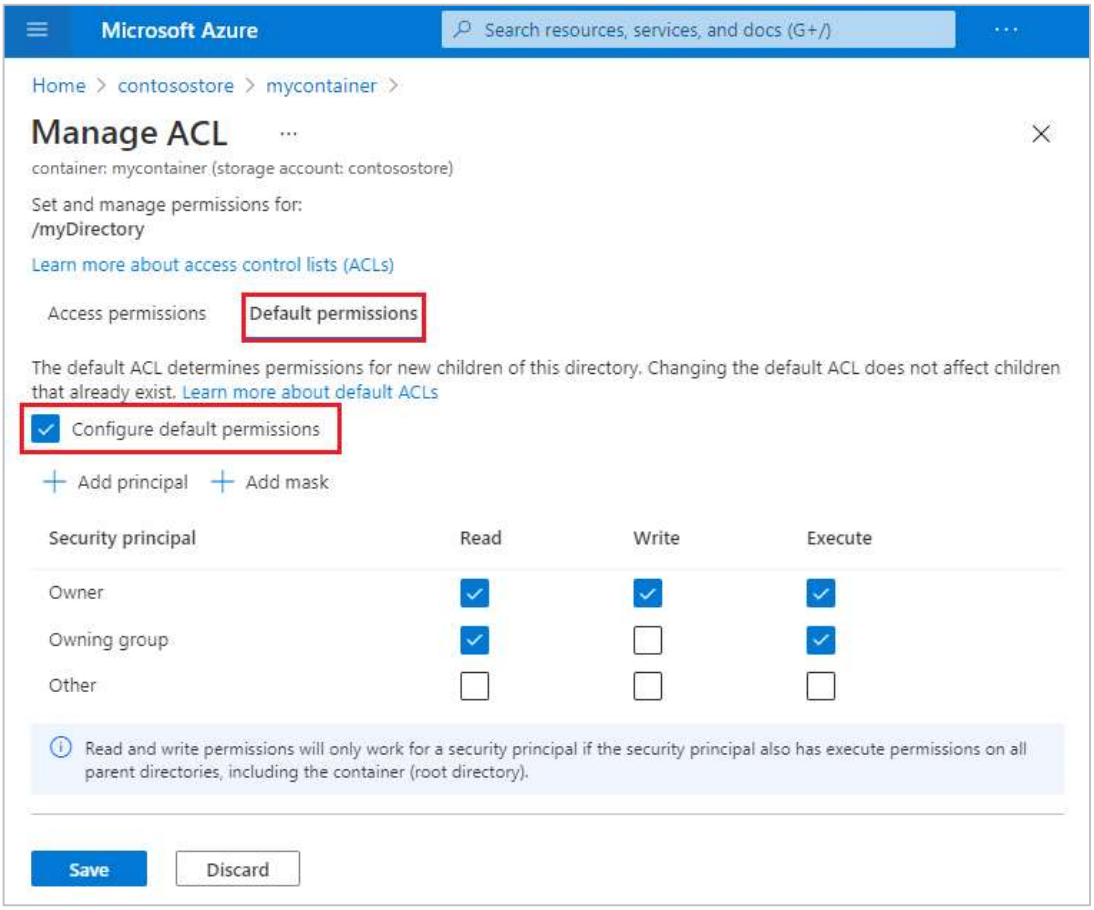
ACLs or access control lists are feature of ADLS Gen 2 along with folder hierarchy. With access control lists the access can be controlled at more granular level like at folder/file level.

This approach is useful when multiple users/developers/apps are trying access the same storage account but the access to be controlled at folder level. Below is how the ACLs are created. The diagrams are select explanatory. Open Azure Portal, navigate to storage account, container and select folder.




Microsoft Azure
Search resources, services, and docs (G+/)
Home > contosostore > mycontainer >
Manage ACL
container: mycontainer (storage account: contosostore)
Set and manage permissions for:
/myDirectory
Learn more about access control lists (ACLs)
Access permissions
Default permissions
Add principal
Add mask
Security principal
Read
Write
Execute
Owner: $superuser
Owning group: $superuser
Other
Read and write permissions will only work for a security principal if the security principal also has execute permissions on all parent directories, including the container (root directory).
Save
Discard


Microsoft Azure
Search resources, services, and docs (G+/)
Home > contosostore > mycontainer >
Manage ACL
container: mycontainer (storage account: contosostore)
Set and manage permissions for:
/myDirectory
Learn more about access control lists (ACLs)
Access permissions
Default permissions
The default ACL determines permissions for new chi
already exist. Learn more about default ACLs
Configure default permissions
Add principal
Add mask
Security principal
Owner
Owning group
Other
Read and write permissions will only work for a se
directories, including the container (root directory
Save
Discard
Add principal
contoso
CO
Contoso
contoso@contoso.com
Selected
Select



Implement Policy Enforcement for proactive and granular level security

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity.

Microsoft provides number of built-in policy definitions for storage accounts. Number of these policies are related to security as well. For example, one of the policies say “Configure secure transfer of data on a storage account”

This will make sure to Disable the public network access property as described in https://aka.ms/storageaccountpublicnetworkaccess. This option disables access from any public address space outside the Azure IP range and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.

There are many other policies like this which can be implemented at subscription level or other granular levels, list is available in azure documentation:

https://learn.microsoft.com/en-us/azure/storage/common/policy-reference

Enable Microsoft Defender for Storage

Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption.

To enable Microsoft defender for Storage

1. **Sign in to the Azure portal.**
2. **Search for and select** Microsoft Defender for Cloud**.**
3. **In the Defender for Cloud menu, select** Environment settings**.**
4. **Select the subscription or workspace that you want to protect.**
5. **Select** on in front of Storage and save.