



# Nebezpečné nastavení Azure: Jak z malých chyb vznikají velké průšvihy

Lubomír Ošmera

Microsoft Security trainer, consultant and  
red teamer

(MCT, MCSE, CEI, CEH, CND, CARTE,  
CAWASP, CRTE)

[https://www.linkedin.com/in/lubomirosm  
era/](https://www.linkedin.com/in/lubomirosm<br/>era/)

[lubomir@osmera.tech](mailto:lubomir@osmera.tech)

# Kontakt, další spolupráce

**Healtchecky, konzultace, pentesty, red teaming, security tuning:**

Emailem na: [lubomir@osmera.tech](mailto:lubomir@osmera.tech)

<https://www.lubomirosmerna.cz/securitytuning/>

**Kurzy:**

Zabezpečení cloudového prostředí Microsoft – 2 dny intenzivní praktický workshop dotovaný z 82 % přes MPSV. **Nutnost přihlášení nejpozději do 3. 7. 2025**  
<https://www.uradprace.cz/vyhledani-rekvalifikacniho-kurzu#/rekvalifikacni-kurz-detail/15843>

Hacking and pentesting Azure – 5 denní kurz obsahující ukázky útoků na MS cloud a obranu proti nim  
[https://www.gopas.cz/microsoft-azure-hacking-a-penetracni-testovani\\_goc238](https://www.gopas.cz/microsoft-azure-hacking-a-penetracni-testovani_goc238)

Bezpečnost hybridního prostředí Microsoft – 5 denní komplexní kurz zaměřený na zabezpečení MS hybridního prostředí  
[https://www.gopas.cz/microsoft-365-bezpecnost-hybridniho-prostredi\\_goc215](https://www.gopas.cz/microsoft-365-bezpecnost-hybridniho-prostredi_goc215)



Azure  
misconfigurations  
and mistakes

Entra  
misconfigurations  
and mistakes

Microsoft 365  
misconfigurations  
and mistakes



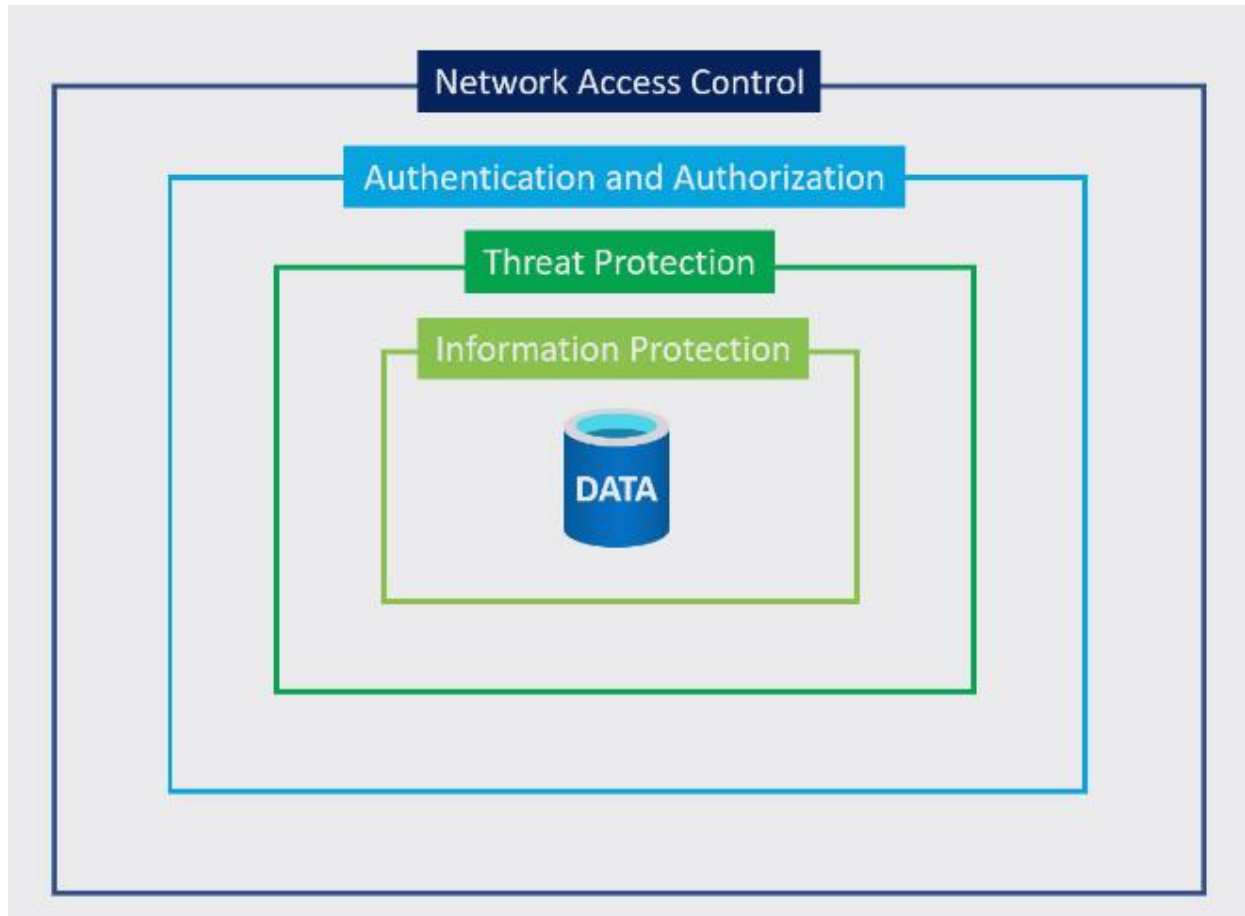
# MICROSOFT AZURE MISCONFIGURATIONS AND MISTAKES



# Why this topic is important

Source (Year)	Supporting statistic or quote
WatchTowr research – TechTarget news (Feb 4 2025)	Researchers found 150 abandoned Amazon S3 buckets that ‘received more than 8 million HTTP requests in two months,’ proving how quickly neglected cloud resources become an active attack surface. <a href="#">Informa TechTarget</a>
Wiz Research – <i>Cloud Data Security Snapshot</i> (May 7 2025)	“54 % of cloud environments have VMs or serverless instances exposed to the public internet while containing sensitive data such as PII or payment information.” <a href="#">wiz.io</a>
Gartner forecast (quoted in Spacelift “100+ Cloud Security Statistics 2025”)	“By 2025, 99 % of cloud-security failures will be the customer’s fault, primarily due to misconfigurations.” <a href="#">Spacelift</a>
SentinelOne <i>Cloud Misconfigurations Statistics</i> (Apr 3 2025)	“82 % of cloud misconfigurations stem from human error rather than software defects.” <a href="#">SentinelOne IT</a>
CybersecurityCloud (2025)	“31 % of cloud data leaks originate from simple configuration blunders that leave sensitive data publicly accessible.” <a href="#">cybersecuritycloud.com</a>
StrongDM – Cloud Security Stats (2025)	“Cloud misconfiguration is the third-most common initial attack vector—accounting for 15 % of all recorded breaches.” <a href="#">strongdm.com</a>
Wiz Academy (2024)	“20 % of organizations have at least one application misconfigured in a way that allows remote code execution or data leakage.” <a href="#">wiz.io</a>
Expert Insights (2025)	“Orphaned resources represent 15 % of detection priorities for advanced cloud-security teams.” <a href="#">Expert Insights</a>
The Record (2025)	“Abandoned S3 containers received more than eight million HTTP requests within two months, proving they remain ‘alive’ and susceptible to takeover by attackers.” <a href="#">Record 2025</a>
PDF Infographic – “Cloud Zombies”	“The most common cause of cloud breaches is misconfiguration; zombie assets are neither scanned nor managed.” <a href="#">HubSpot</a>

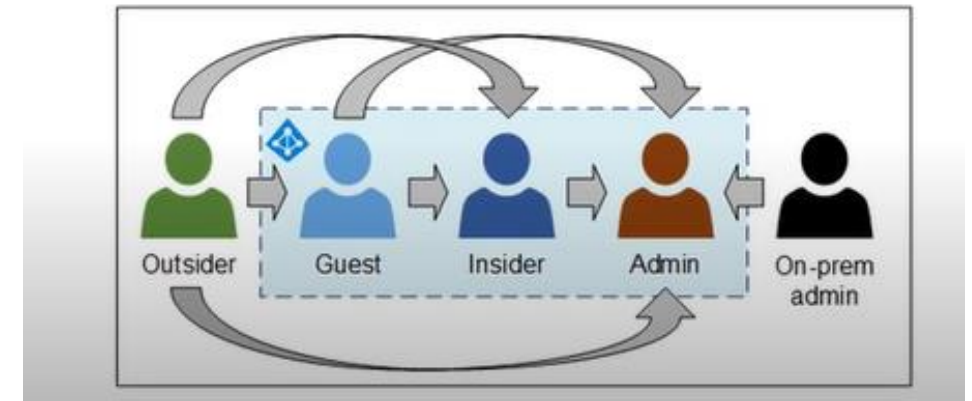
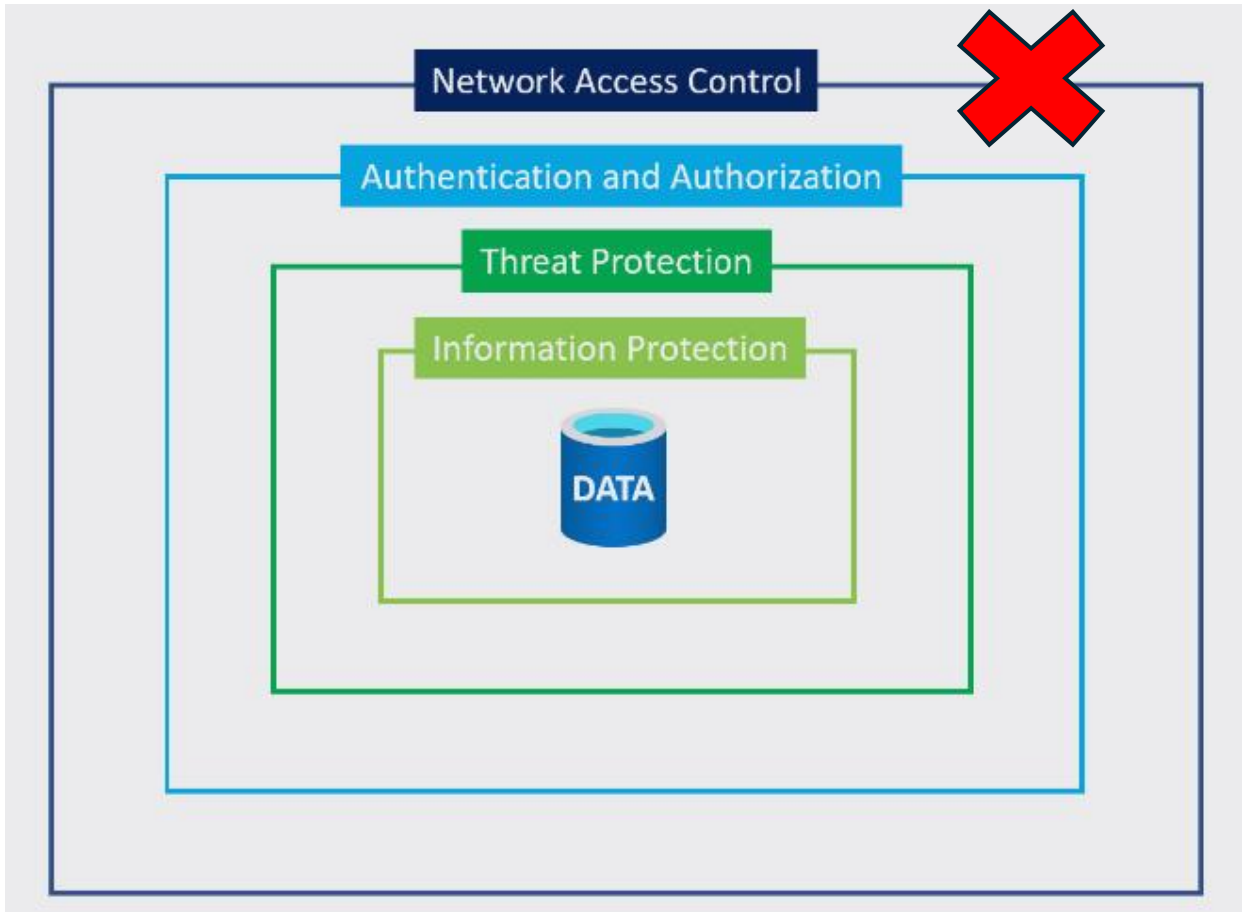
# Azure resource multi layered approach



Publicly exposed? Oh, this is common only for temporary resources....or?




# Security hole



<https://my.ine.com/Cloud/courses/75c31e17/azure-pentesting>



 Add inbound security rule

VM-tools-nsg

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges \* ⓘ

3389

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMPv4

☐ ICMPv6

Action

☒ Allow

☐ Deny


Priority \* ⓘ

330

Name \*


AllowAnyCustom3389Inbound

Description

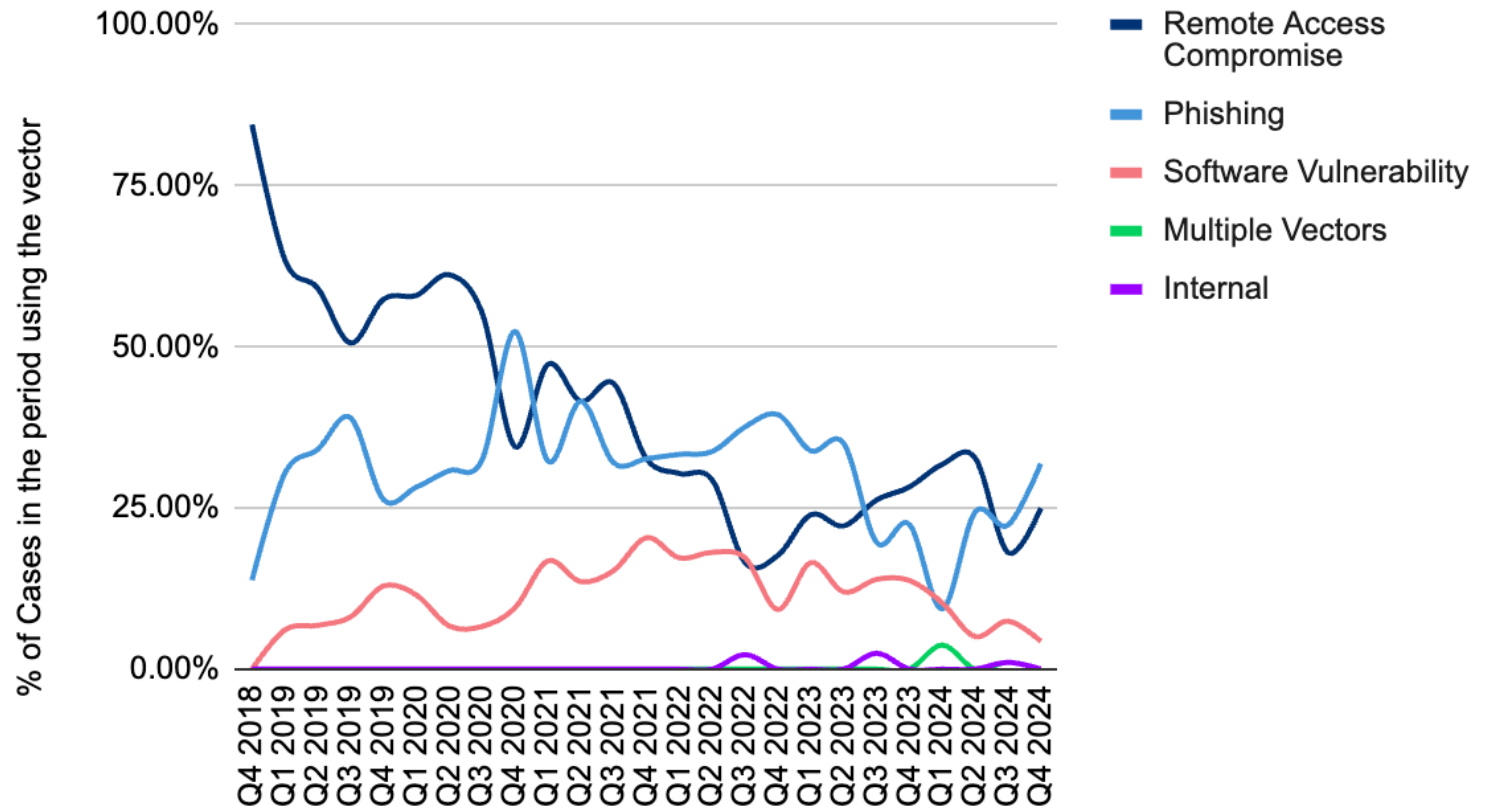
 RDP port 3389 is exposed to the Internet. This is only recommended for testing. For production environments, we recommend using a VPN or private connection.

Add

Cancel

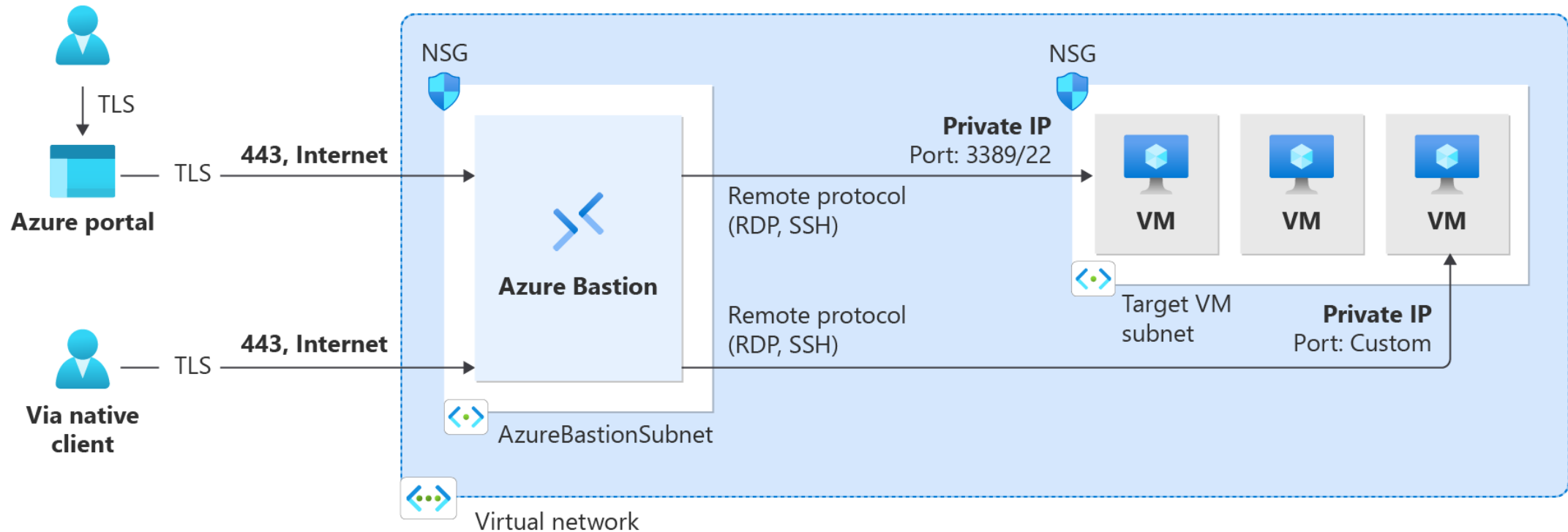
 Give feedback

## Ransomware Attack Vectors



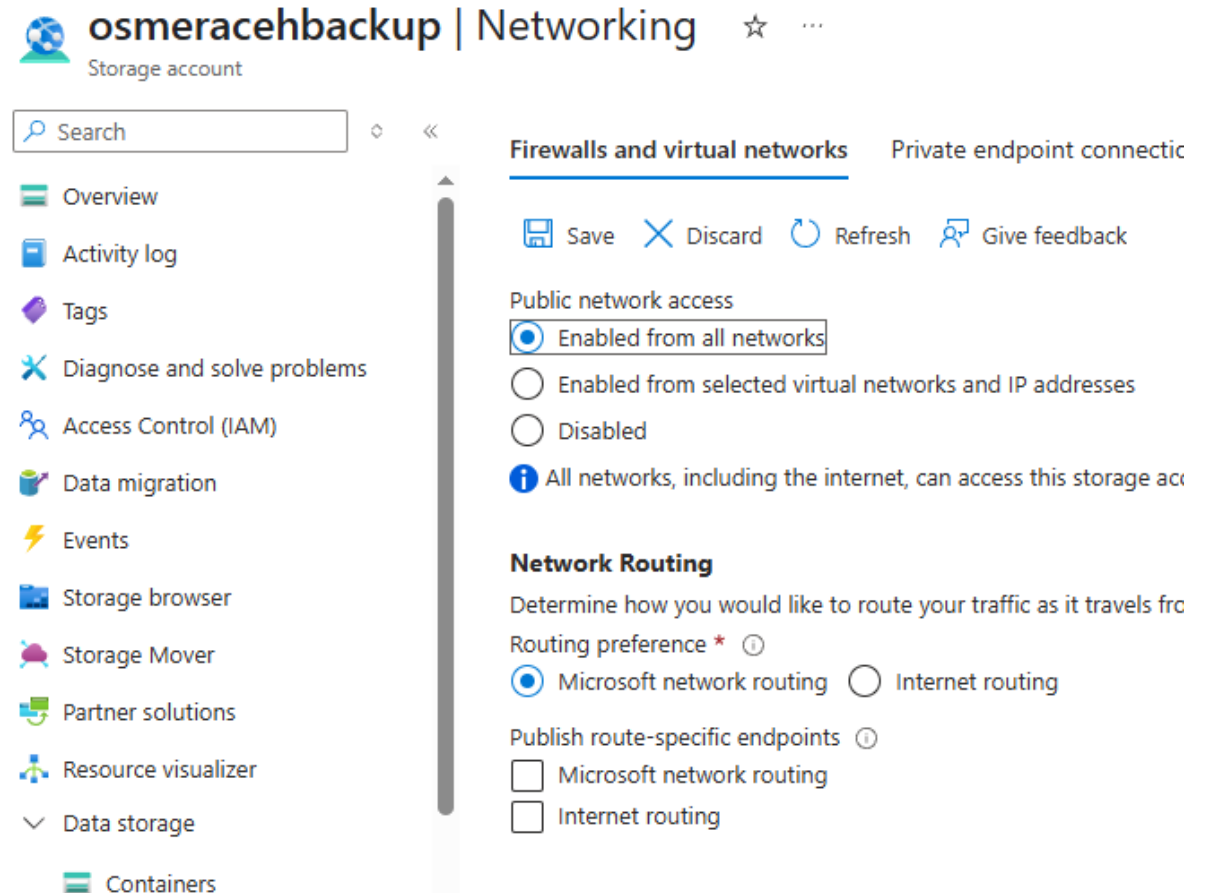
# Security measures

- S2S VPN
- Azure bastion
- Azure JIT
- NSG of VM - allowing only specific ip ranges



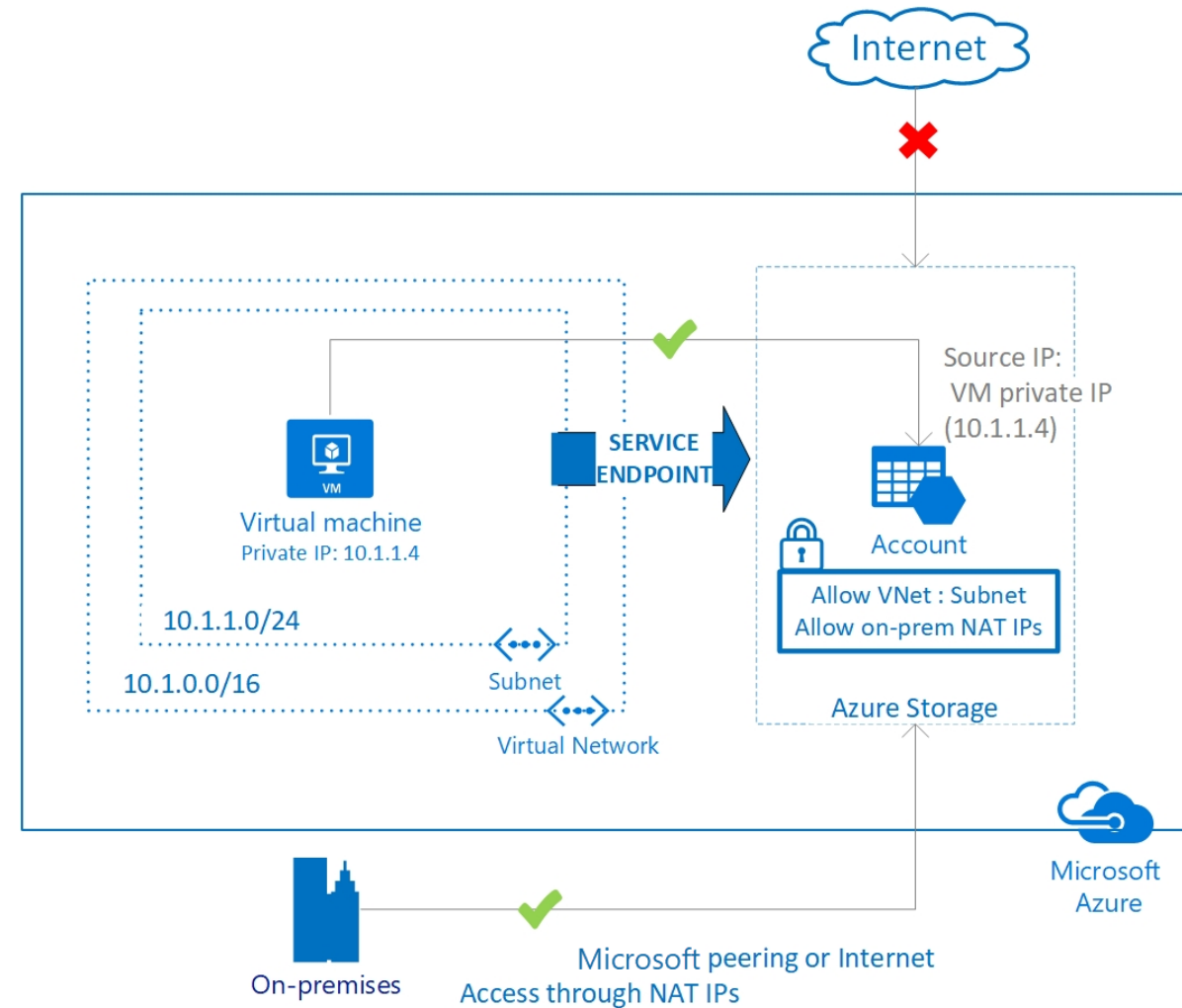
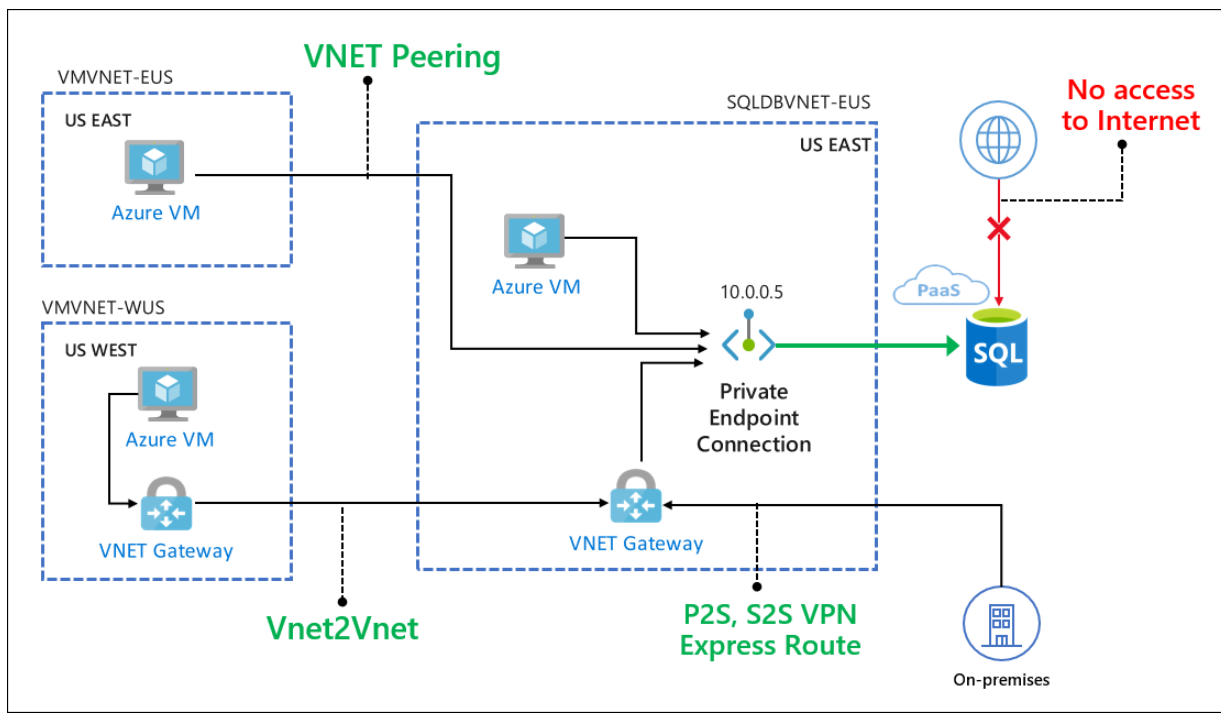
# What about platform as a service

- Mostly – publicly exposed
- There are often no restrictions in default configuration



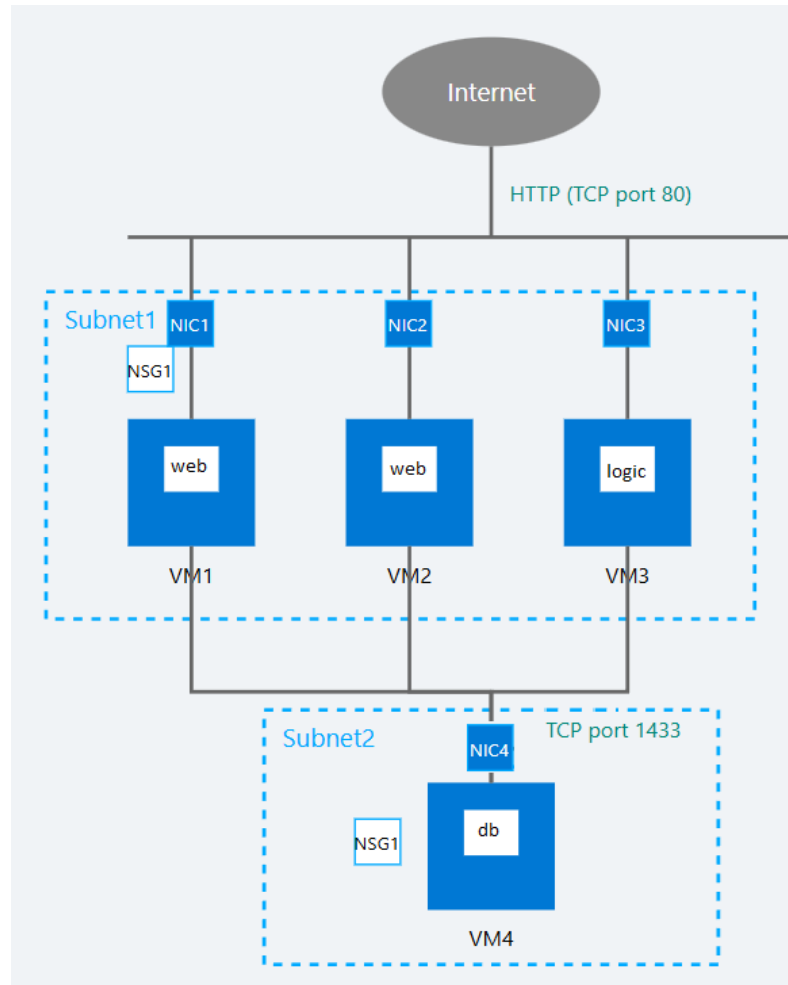
The screenshot displays the Azure portal interface for a storage account named 'osmeracehbackup'. The left-hand navigation pane lists various management tools: Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, Resource visualizer, Data storage, and Containers. The main content area is titled 'Networking' and features a search bar and a set of action buttons: Save, Discard, Refresh, and Give feedback. Under the 'Firewalls and virtual networks' section, the 'Public network access' is configured to 'Enabled from all networks', which is highlighted by a red box. Below this, a blue information icon indicates that 'All networks, including the internet, can access this storage account'. The 'Network Routing' section provides instructions on how to route traffic and offers two routing preferences: 'Microsoft network routing' (selected) and 'Internet routing'. At the bottom, there is a section for 'Publish route-specific endpoints' with checkboxes for 'Microsoft network routing' and 'Internet routing', both of which are currently unchecked.

# Service endpoint and private endpoint





# NSG leaved in default configuration



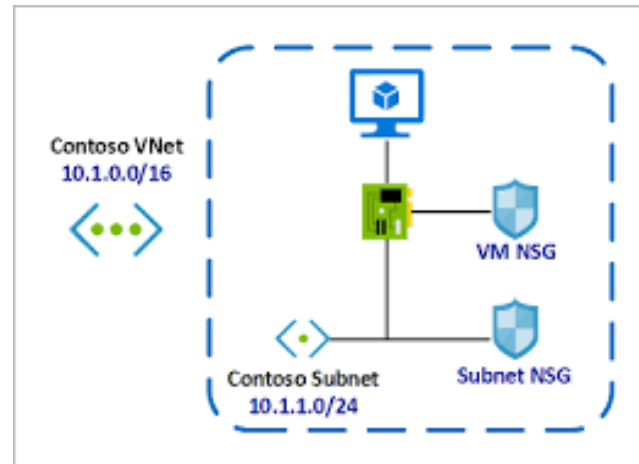
## ▼ Inbound Security Rules

65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

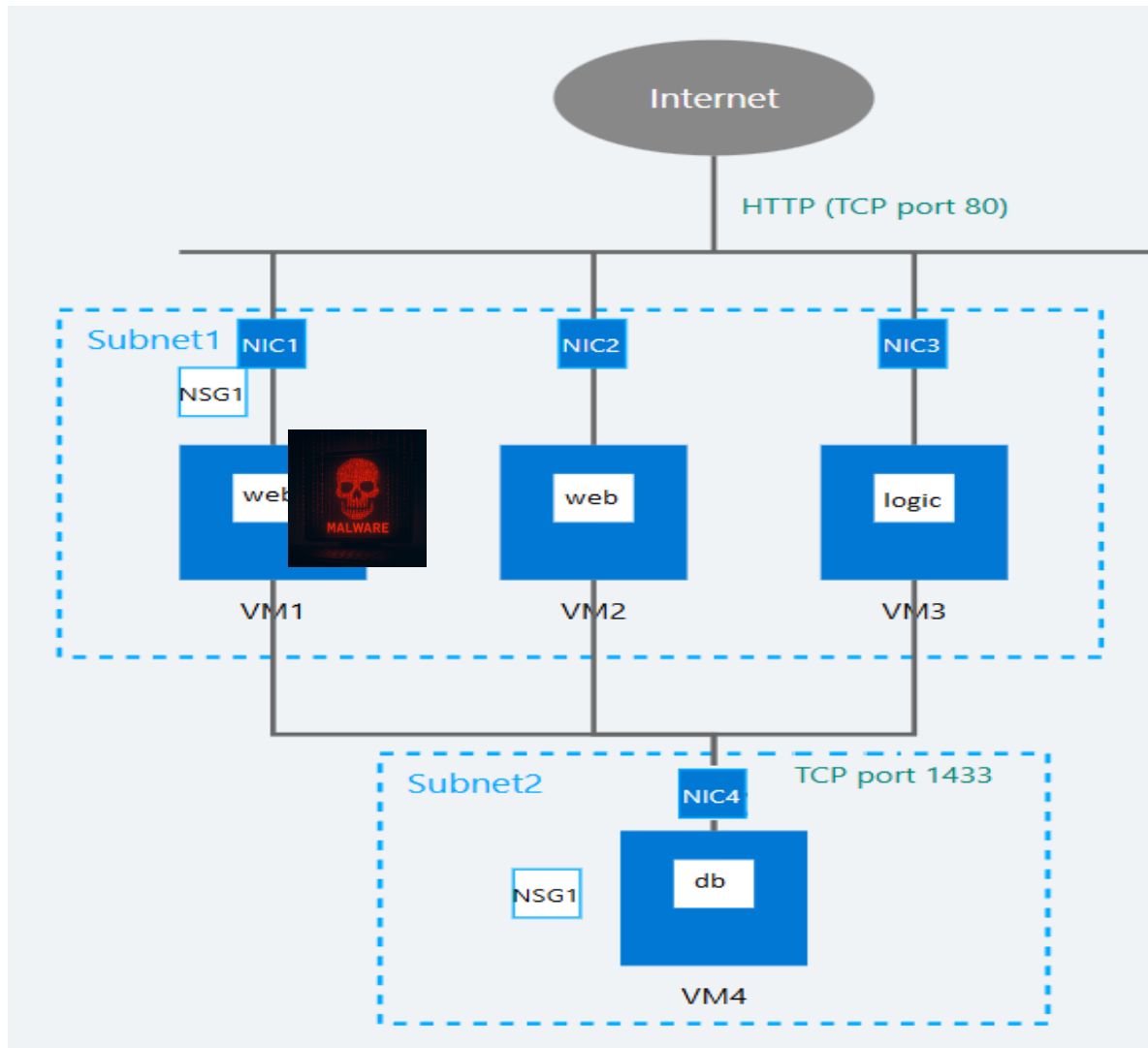
## ▼ Outbound Security Rules

65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

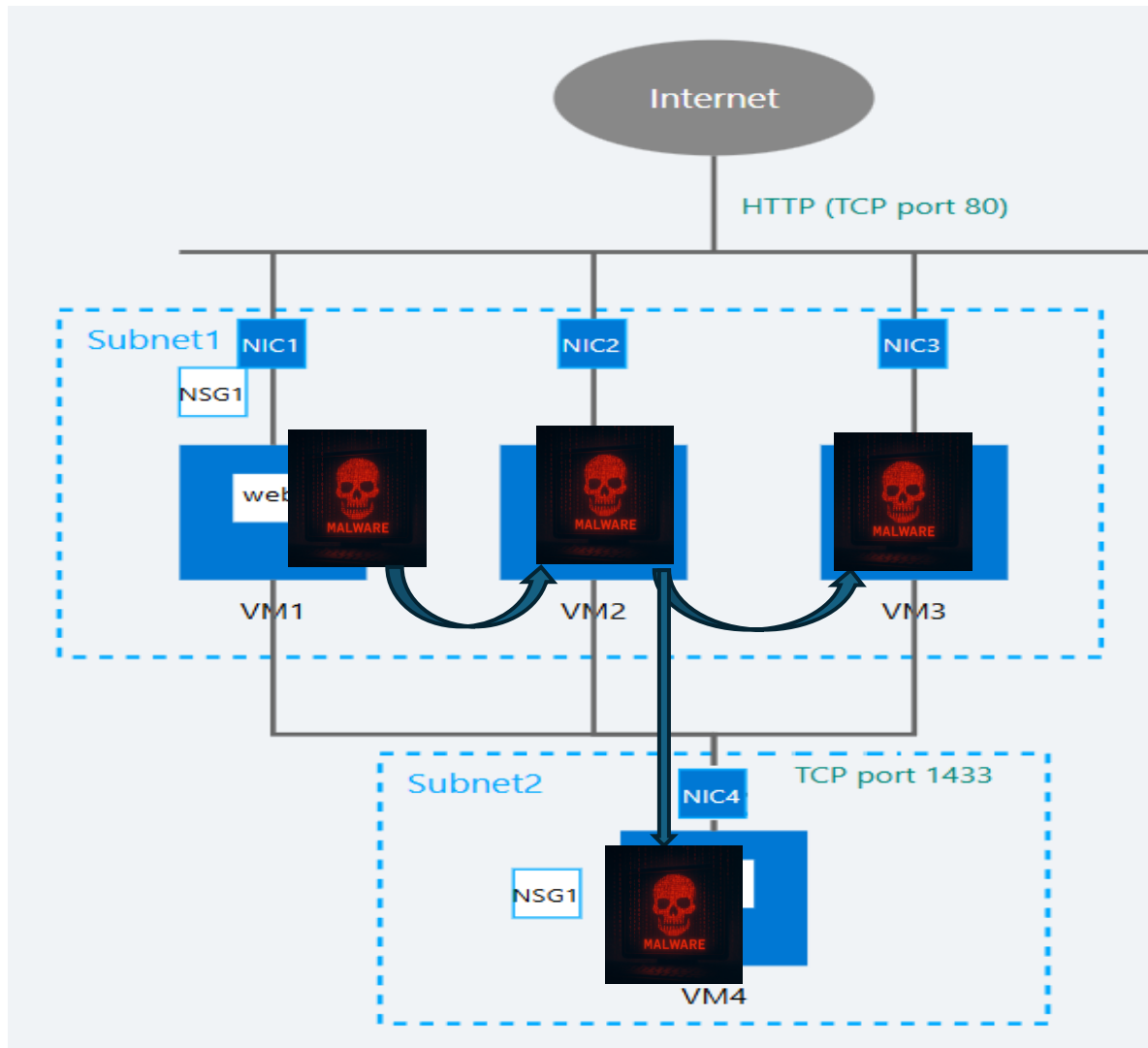
<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>



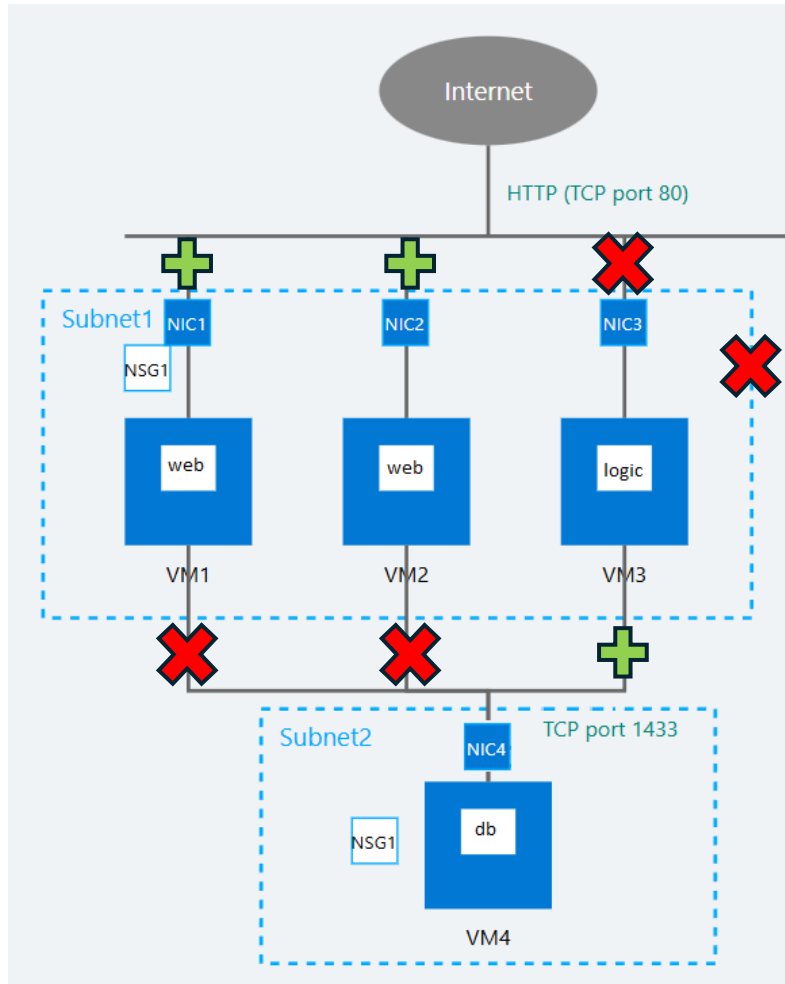
# Potential lateral movement



# Potential lateral movement



# NSG leaved in default configuration



Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
100	Internet	*	AsgWeb	80	TCP	Allow

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
120	*	*	AsgDb	1433	Any	Deny

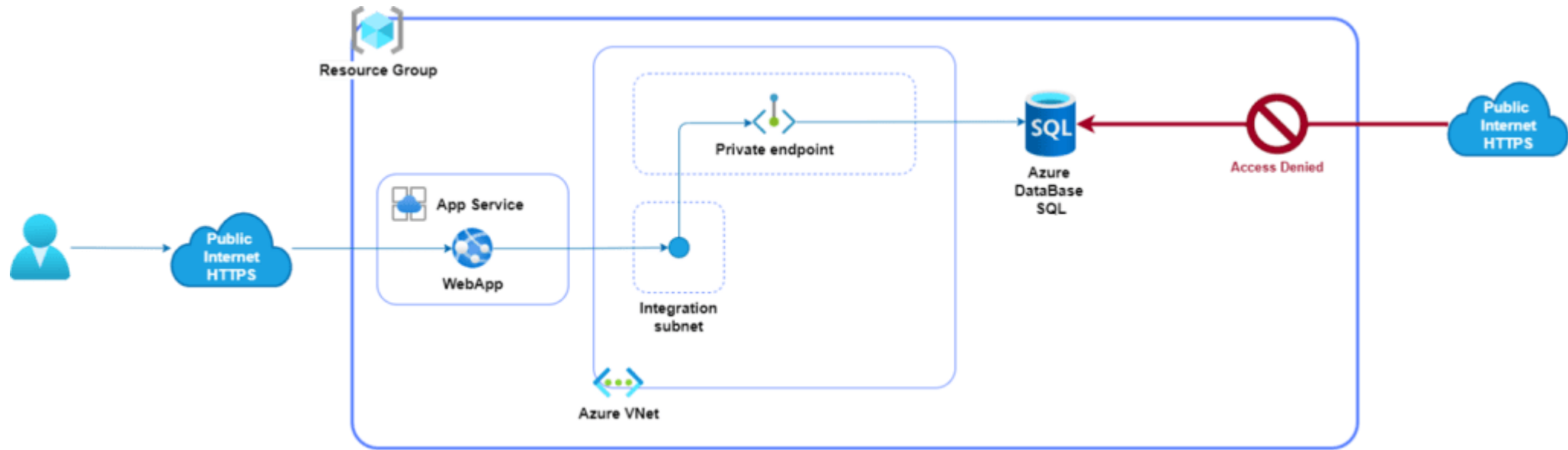
Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
110	AsgLogic	*	AsgDb	1433	TCP	Allow



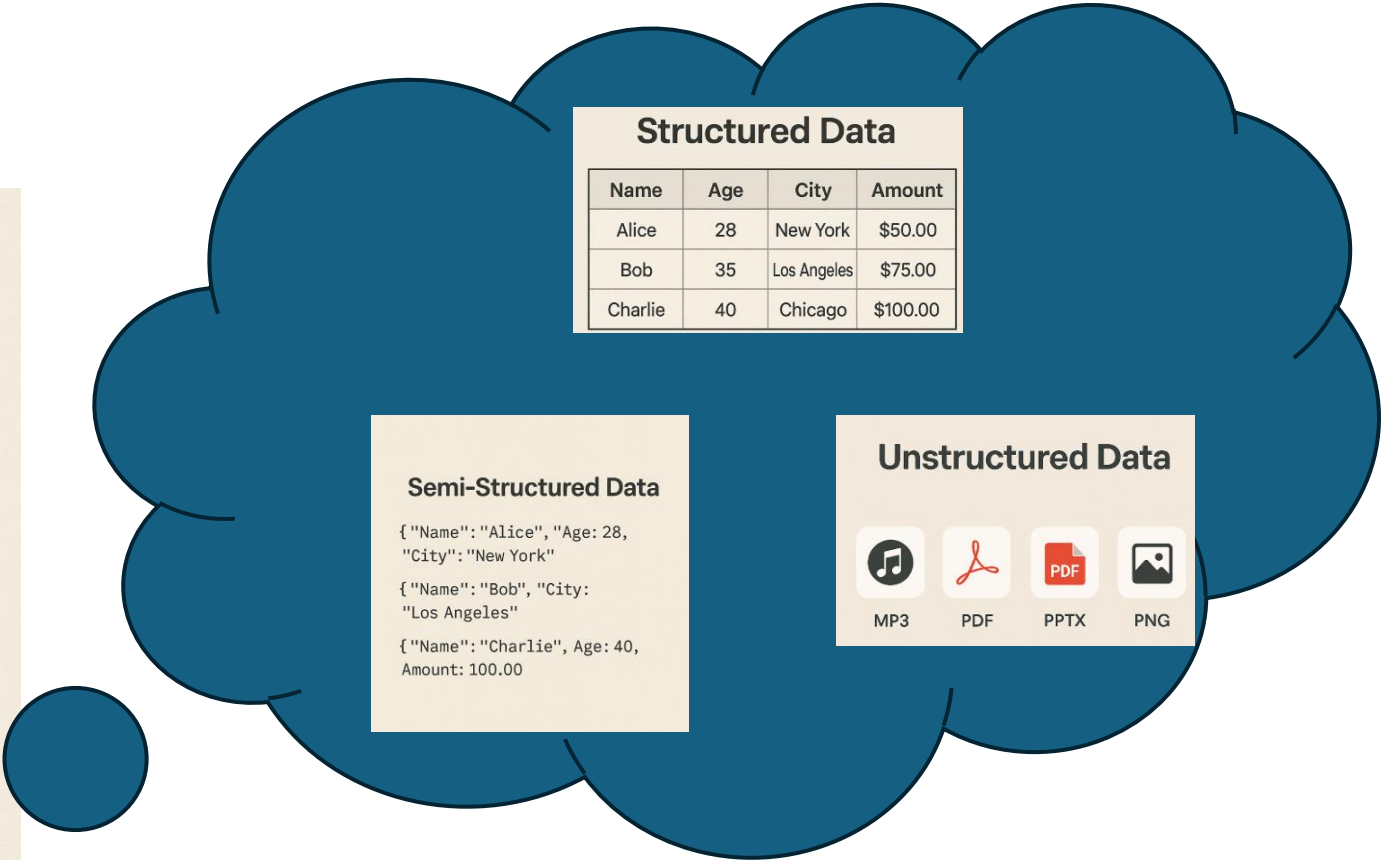
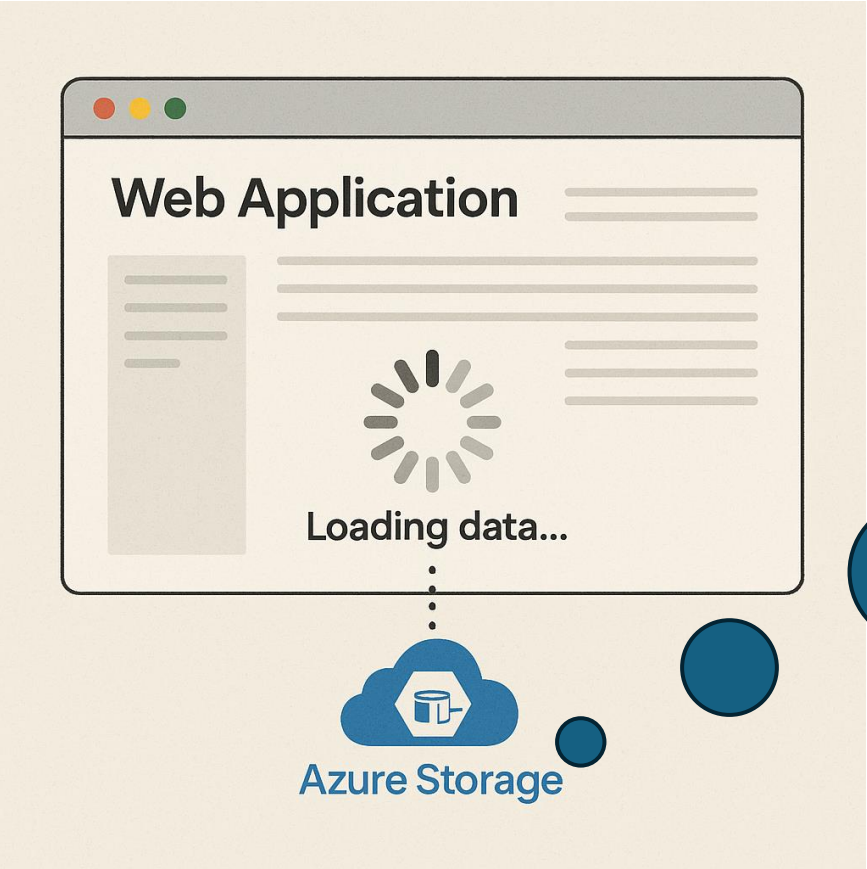
# Multilayered approach



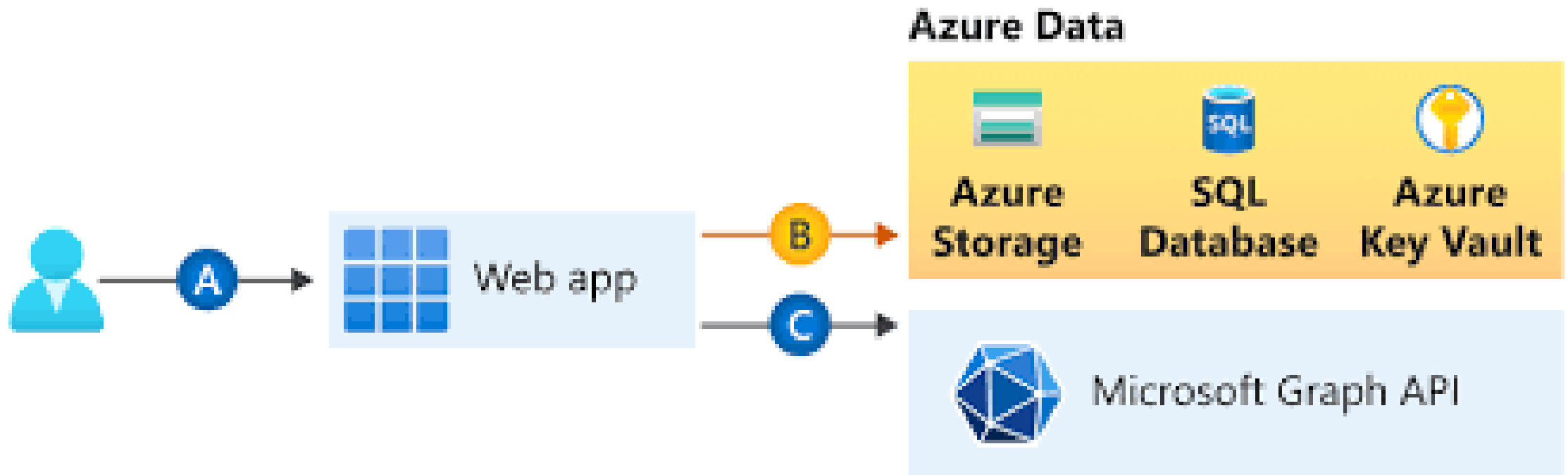
# Secure access to SQL



# Azure storage

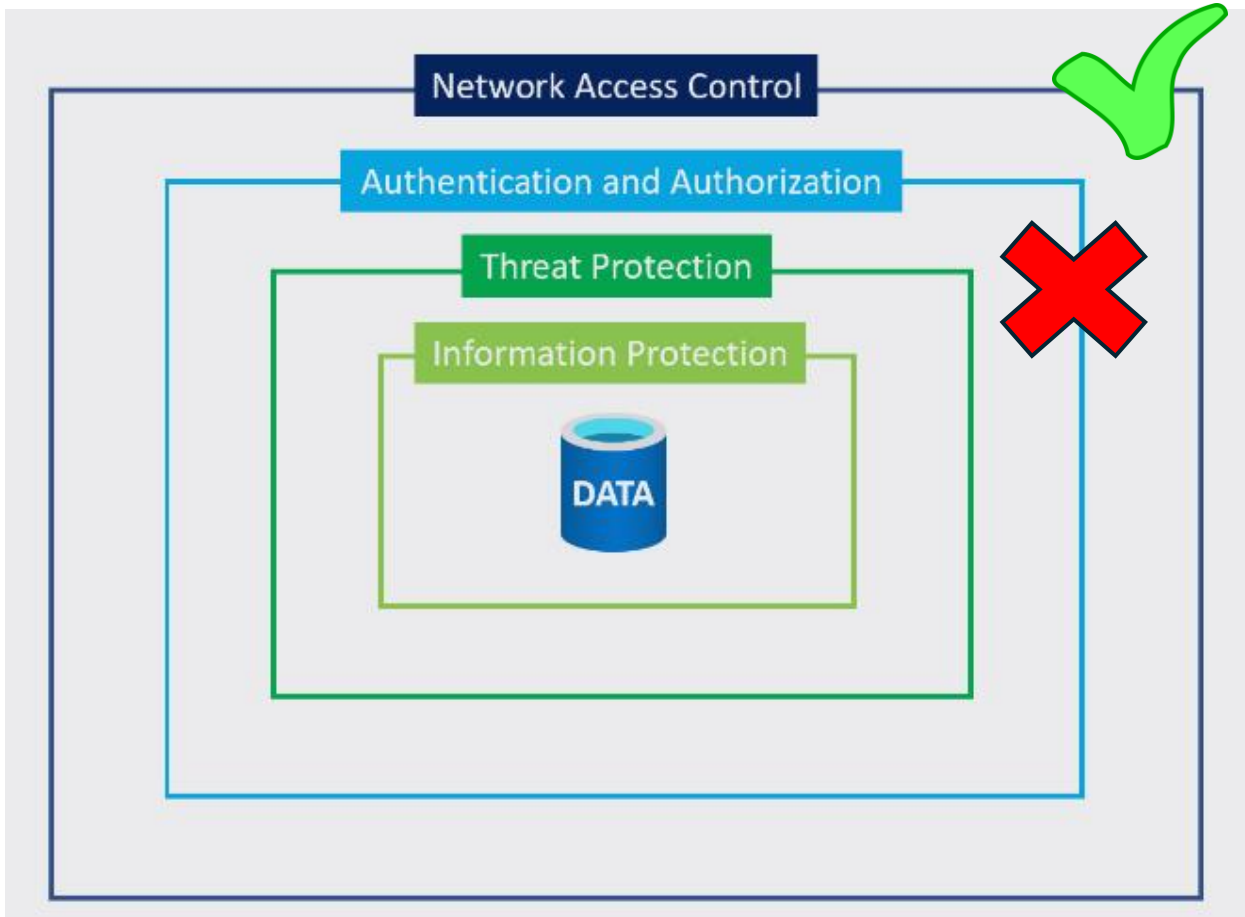


# Storage using example



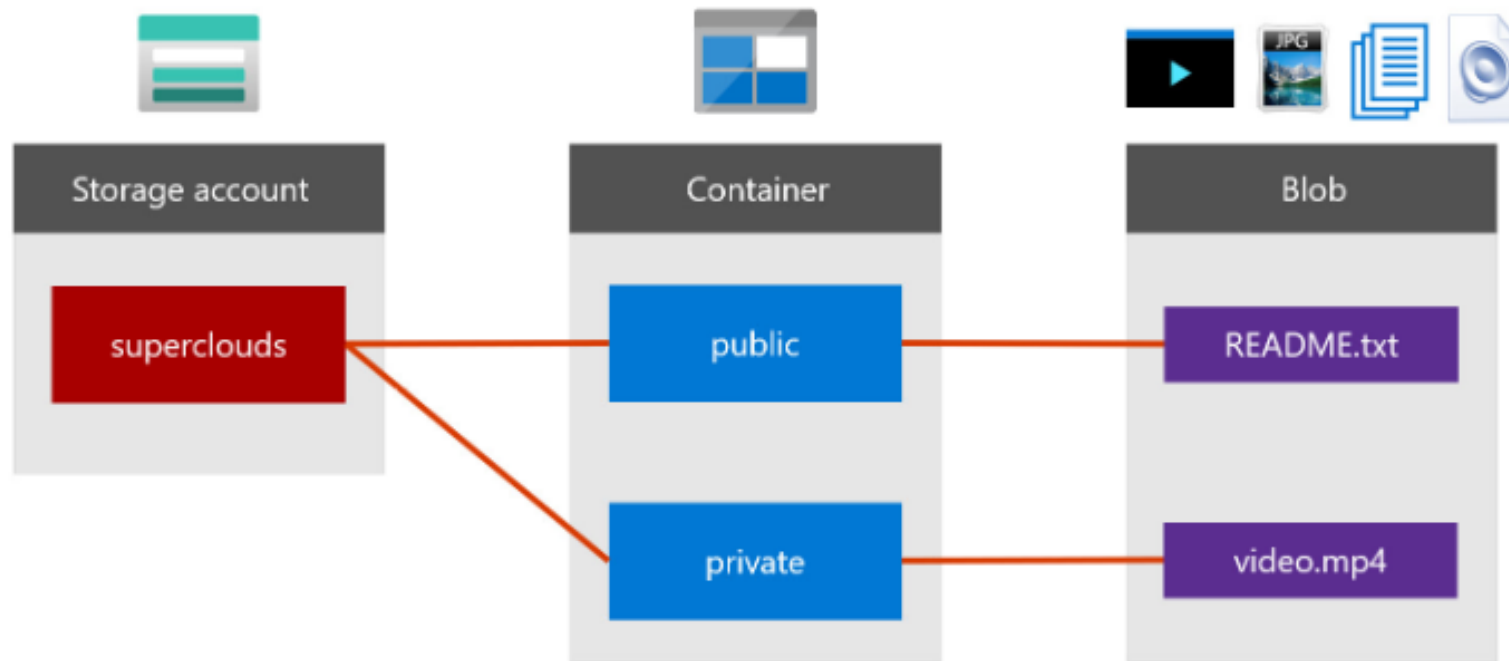


# Multi-layered approach



# Azure blob storage

[https://<STORAGE\\_ACCOUNT\\_NAME>.blob.core.windows.net/<CONTAINER\\_NAME>/<BLOB\\_NAME>](https://<STORAGE_ACCOUNT_NAME>.blob.core.windows.net/<CONTAINER_NAME>/<BLOB_NAME>)



Anonymous access to some containers –  
there are not important data. Or?





```
img src="https://osmeracehbackun.blob.core.windows.net/obrazky/azuresec.png" />
```



Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

KOOPday1.ps1 Untitled1.ps1\*

```
1 Import-Module "C:\Users\lubos\OneDrive - Lubomír Ošmera - IT consulting\digisecurity\Teched2025\MicroBurst\MicroBurst.psm1" -verbose
2
3 Invoke-EnumerateAzureBlobs -base osmeracehbackup
4
5
6 https://osmeracehbackup.blob.core.windows.net/obrazky
```

VERBOSE: Importing function 'Get-AzStorageKeysREST'.  
VERBOSE: Importing function 'Get-AzureADDomainInfo'.  
VERBOSE: Importing function 'Get-MSOLDomainInfo'.  
VERBOSE: Importing function 'Invoke-AzVMBulkCMD'.  
VERBOSE: Importing function 'Invoke-EnumerateAzureBlobs'.  
VERBOSE: Importing function 'Invoke-EnumerateAzureSubDomains'.  
WARNING: The names of some imported commands from the module 'MicroBurst' include unapproved verbs that might make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.  
VERBOSE: The 'Run-AZRunbook' command in the MicroBurst' module was imported, but because its name does not include an approved verb, it might be difficult to find. The suggested alternative verbs are "Invoke,Start".  
VERBOSE: Importing function 'Run-AZRunbook'.  
VERBOSE: Importing alias 'Get-AzureADApplicationProxyConnectorGroupMembers'.

Completed

Ln 6 Col 54

175%

# Consider these settings!

The screenshot displays the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a Copilot button. The user's profile is visible in the top right corner.

The left sidebar shows the 'Storage accounts' section, with a list of storage accounts. The 'osmeracehbackup' account is selected and highlighted.

The main content area shows the 'Configuration' settings for the 'osmeracehbackup' storage account. The settings are organized into sections:

- Account kind:** StorageV2 (general purpose v2)
- Performance:** Standard (selected), Premium
- Secure transfer required:** Disabled (selected), Enabled
- Allow Blob anonymous access:** Disabled, Enabled (selected) - This setting is highlighted with a red box.
- Allow storage account key access:** Disabled, Enabled (selected)
- Allow recommended upper limit for shared access signature (SAS) expiry interval:** Disabled (selected), Enabled
- Default to Microsoft Entra authorization in the Azure portal:** Disabled (selected), Enabled
- Minimum TLS version:** Version 1.2
- Permitted scope for copy operations (preview):** From any storage account
- Blob access tier (default):** Hot (selected), Cool, Cold
- Large file shares:** Disabled, Enabled (selected)

The bottom of the page shows a pagination bar indicating 'Showing 1 - 4 of 4. Display count: auto'.

# Storage account is correct place for credentials?

Location / Artifact	Typical Credential Leak
Terraform / Bicep / CloudFormation	Hard-coded provider credentials or sensitive outputs not flagged as sensitive = true.
.env, appsettings.json, local.settings.json, secrets.yml	Stored unencrypted on laptops or accidentally checked into the repository.
Shared Dropbox / OneDrive (secrets.xlsx)	File publicly accessible because the share link is open to anyone with the URL.
Wiki / Confluence	Documentation includes full connection strings “for quick setup.”
Email threads	Credentials shared during incident response and later forgotten.
VM / AMI golden images	SSH keys or cloud-init scripts with passwords baked into the image.
Inline code (app.py, index.js)	Keys or passwords hard-coded for quick tests that never got removed.
Config constants (config.js, settings.py)	“Temporary” values that silently ship to production.
Commit history (old commits, abandoned branches, Git tags)	Credentials removed in a later commit but still retrievable via git log, reflog, or GitHub’s web UI.

"Anonymous access is strictly prohibited  
all operations are performed securely."



# Accidental data exposing

---

## 38TB of data accidentally exposed by Microsoft AI researchers

Wiz Research found a data exposure incident on Microsoft's AI GitHub repository, including over 30,000 internal Microsoft Teams messages – all caused by one misconfigured SAS token



Hillai Ben-Sasson, Ronny Greenberg  
September 18, 2023

10 minutes read



<https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers>

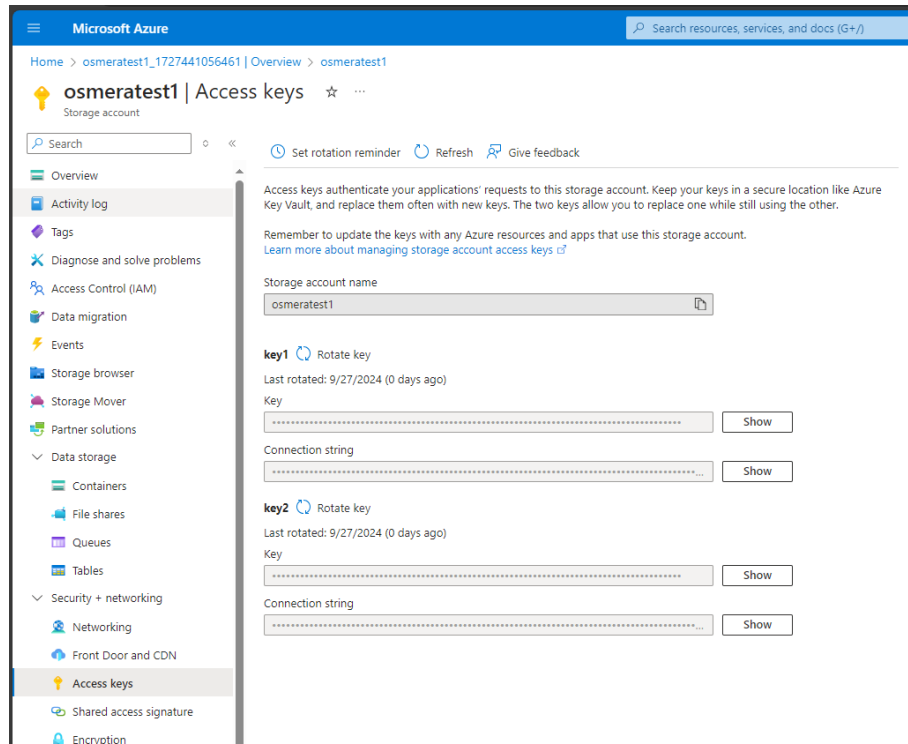
# How access to storage?



- Access keys
- SAS
- RBAC



# Access keys



**FULL CONTROL TO WHOLE  
STORAGE ACCOUNT!**

# SAS tokens

- <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
- Container:  
<https://backupstoragehackerfest.blob.core.windows.net/backupdata>
- SAS URL:  
<https://backupstoragehackerfest.blob.core.windows.net/backupdata?sp=racw&st=2023-11-02T22:07:45Z&se=2023-11-03T06:07:45Z&spr=https&sv=2022-11-02&sr=c&sig=gpvaL04CmnUMup%2FOp1As6KtTM%2FaYe1iJayvf8sbQcV4%3D>

# SAS scopes - demo

# Potential persistence

## How a shared access signature works

A shared access signature is a token that is appended to the URI for an Azure Storage resource. The token contains a special set of query parameters that indicate how the resources may be accessed by the client. One of the query parameters, the signature, is constructed from the SAS parameters and signed with the key that was used to create the SAS. This signature is used by Azure Storage to authorize access to the storage resource.

### ⓘ Note

It's not possible to audit the generation of SAS tokens. Any user that has privileges to generate a SAS token, either by using the account key, or via an Azure role assignment, can do so without the knowledge of the owner of the storage account. Be careful to restrict permissions that allow users to generate SAS tokens. To prevent users from generating a SAS that is signed with the account key for blob and queue workloads, you can disallow Shared Key access to the storage account. For more information, see [Prevent authorization with Shared Key](#).

# Consider these settings!

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'lubomir@osmera.tech'. The left sidebar shows the 'Storage accounts' section with a list of accounts: 'cnapptest', 'csb10030000a88ddf51', 'osmeracehbackup' (selected), and 'veambackupstorage2'. The main content area is titled 'osmeracehbackup | Configuration'. It features a left-hand menu with categories like 'Queues', 'Tables', 'Security + networking', 'Data management', and 'Settings'. The 'Settings' category is expanded, and the 'Configuration' option is selected. The configuration page lists various settings for the storage account, including 'Account kind' (StorageV2), 'Performance' (Standard), 'Secure transfer required' (Disabled), 'Allow Blob anonymous access' (Enabled), and 'Allow storage account key access' (Enabled). The 'Allow storage account key access' setting is highlighted with a red rectangular box. Other settings include 'Allow recommended upper limit for shared access signature (SAS) expiry interval' (Enabled), 'Default to Microsoft Entra authorization in the Azure portal' (Disabled), 'Minimum TLS version' (Version 1.2), 'Permitted scope for copy operations (preview)' (From any storage account), 'Blob access tier (default)' (Hot), and 'Large file shares' (Enabled).

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

lubomir@osmera.tech  
LUBOMIR OSMERA (OSMERA.ON...)

Dashboard > Storage accounts > osmeracehbackup

Storage accounts  
Lubomír Ošmera (osmera.onmicrosoft.com)

+ Create ... Group by none

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Name ↑

- cnapptest
- csb10030000a88ddf51
- osmeracehbackup
- veambackupstorage2

osmeracehbackup | Configuration

Search

Save Discard Refresh Give feedback

The cost of your storage account depends on the usage and the options you choose below. [Learn more about storage pricing](#)

Account kind  
StorageV2 (general purpose v2)

Performance  
☒ Standard ☐ Premium

This setting cannot be changed after the storage account is created.

Secure transfer required  
☒ Disabled ☐ Enabled

Allow Blob anonymous access  
☐ Disabled ☒ Enabled

Allow storage account key access  
☐ Disabled ☒ Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval  
☒ Disabled ☐ Enabled

Default to Microsoft Entra authorization in the Azure portal  
☒ Disabled ☐ Enabled

Minimum TLS version  
Version 1.2

Permitted scope for copy operations (preview)  
From any storage account

Blob access tier (default)  
☒ Hot ☐ Cool ☐ Cold

Large file shares  
☐ Disabled ☒ Enabled

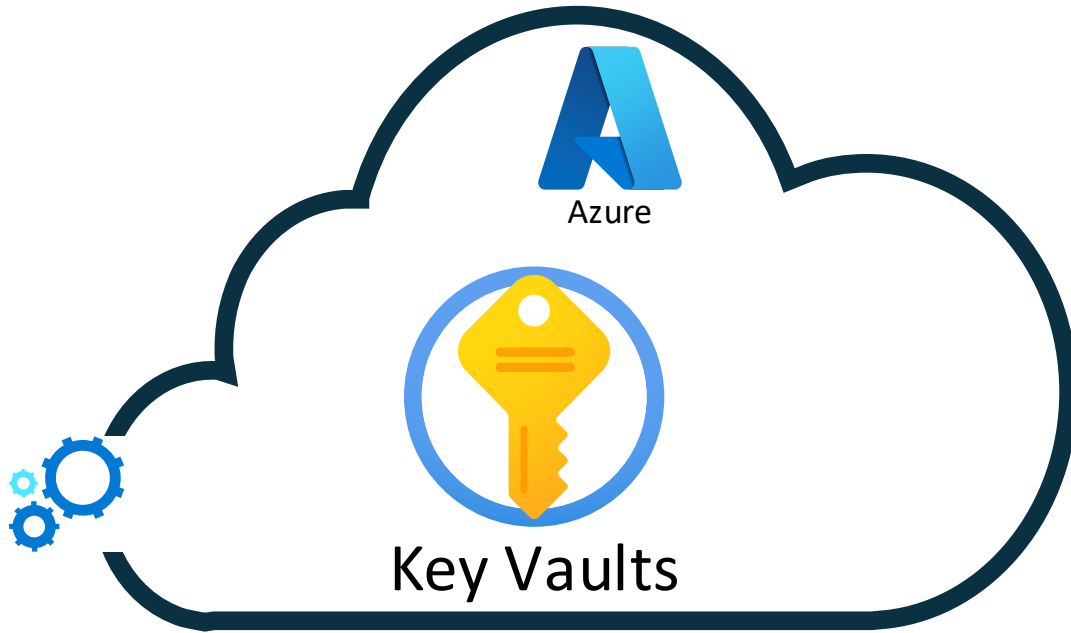
Showing 1 - 4 of 4. Display count: auto

"For storing secrets, a vault is a better option."



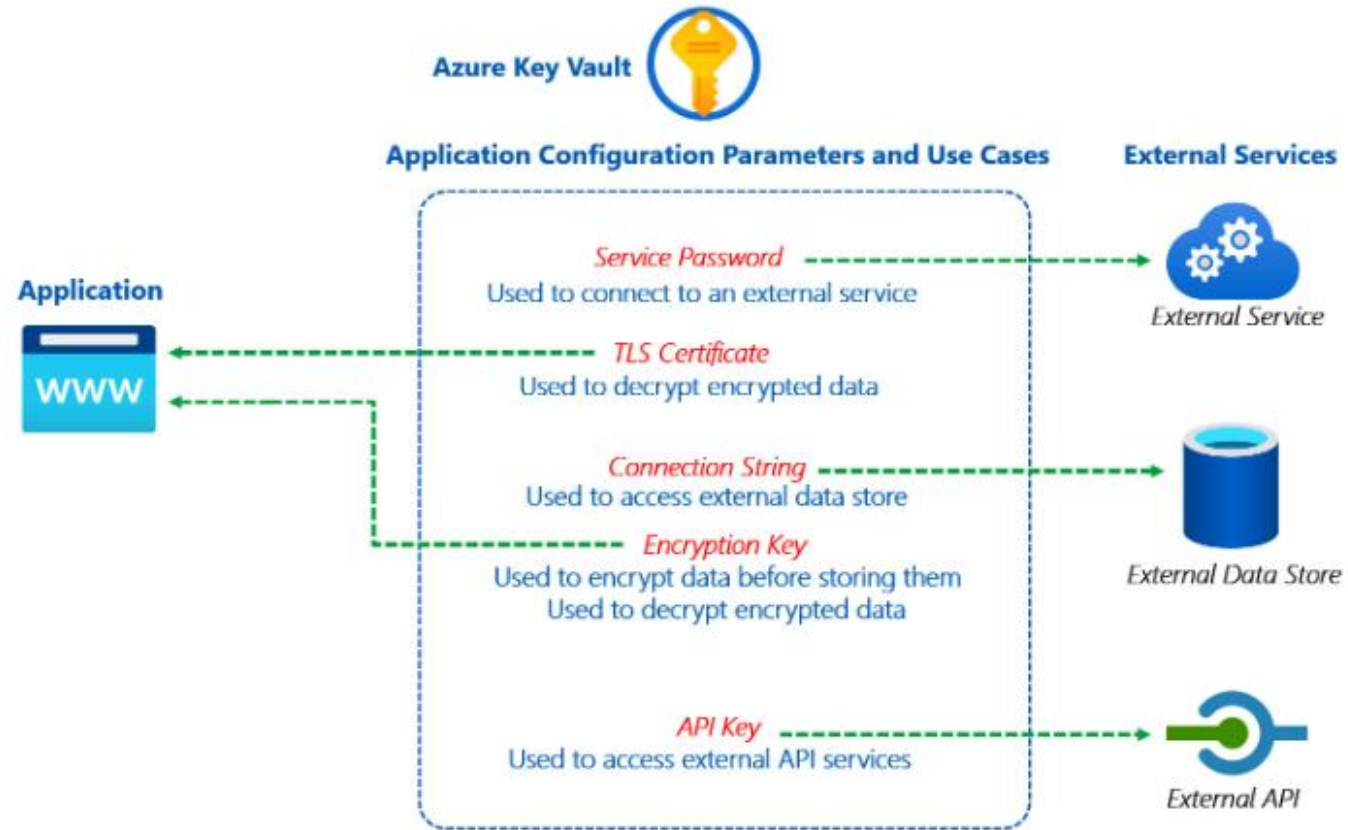


# Azure Key Vault

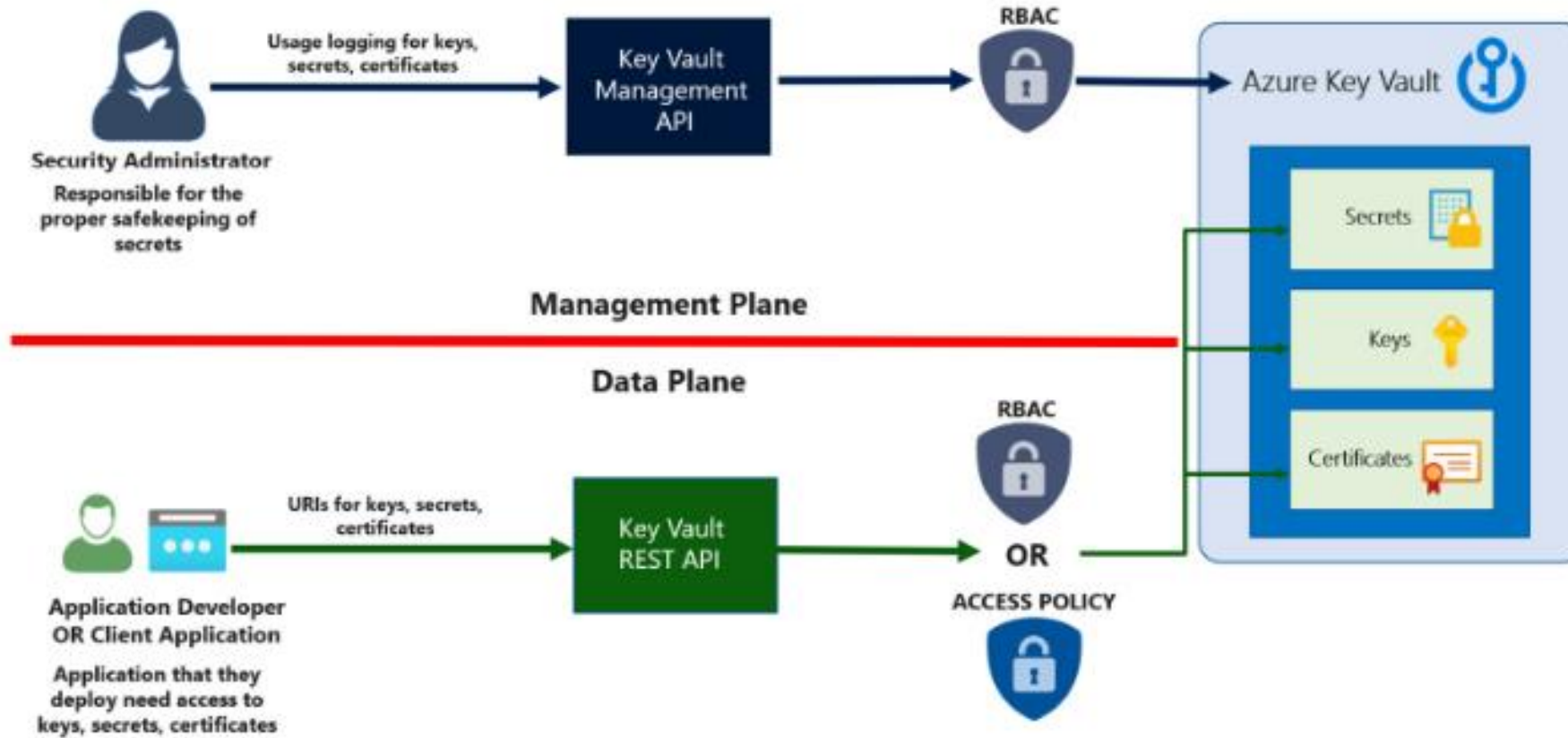


Azure Key Vault is a cloud service for securely storing and accessing secrets.

# Use cases



# Management plane vs data plane



# Demo: dangerous app



# How long is infinity?



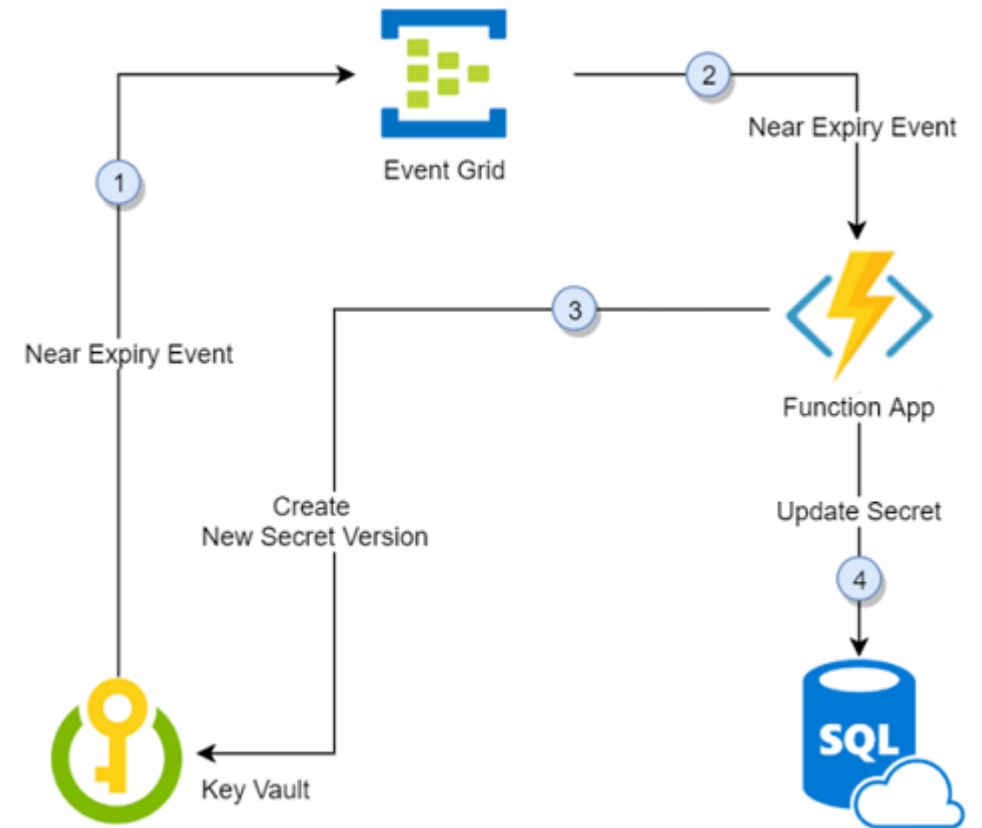
```
$sp = New-AzADServicePrincipal -DisplayName  
"LegacyApp"  
$credential = New-AzADSpCredential -ObjectId $sp.Id -  
EndDate "2099-12-31"
```

# Key and Secret Rotation

Update keys and secrets without affecting your application

Rotate keys and secrets in several ways:

- As part of a manual process
- Programmatically with the REST API
- With an Azure Automation script

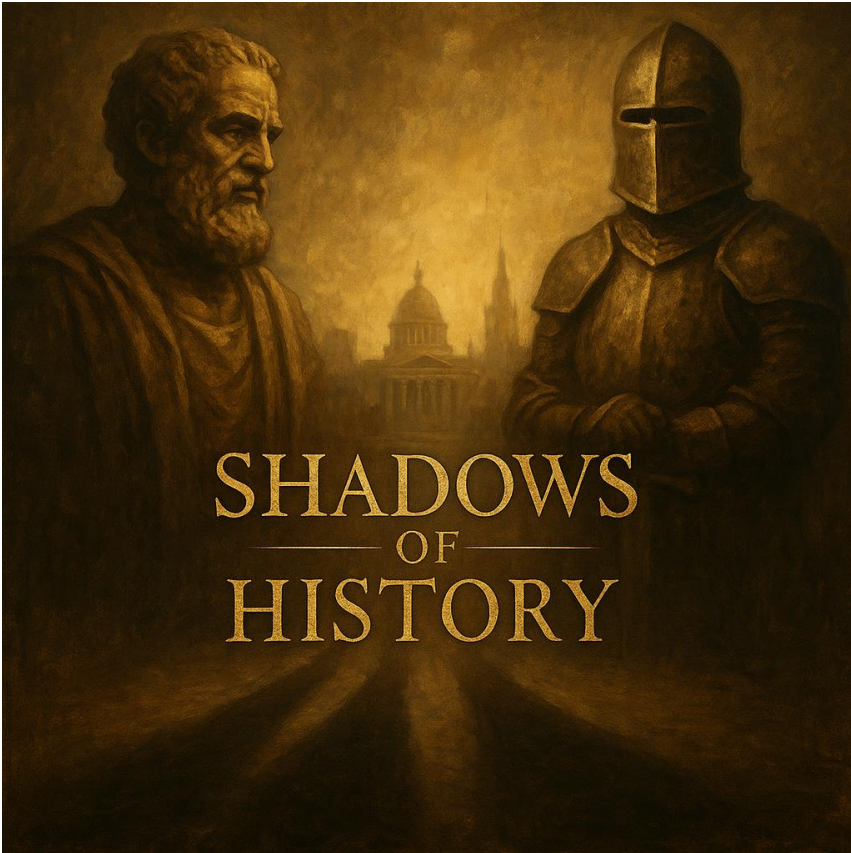




# Some recommendations about expiration

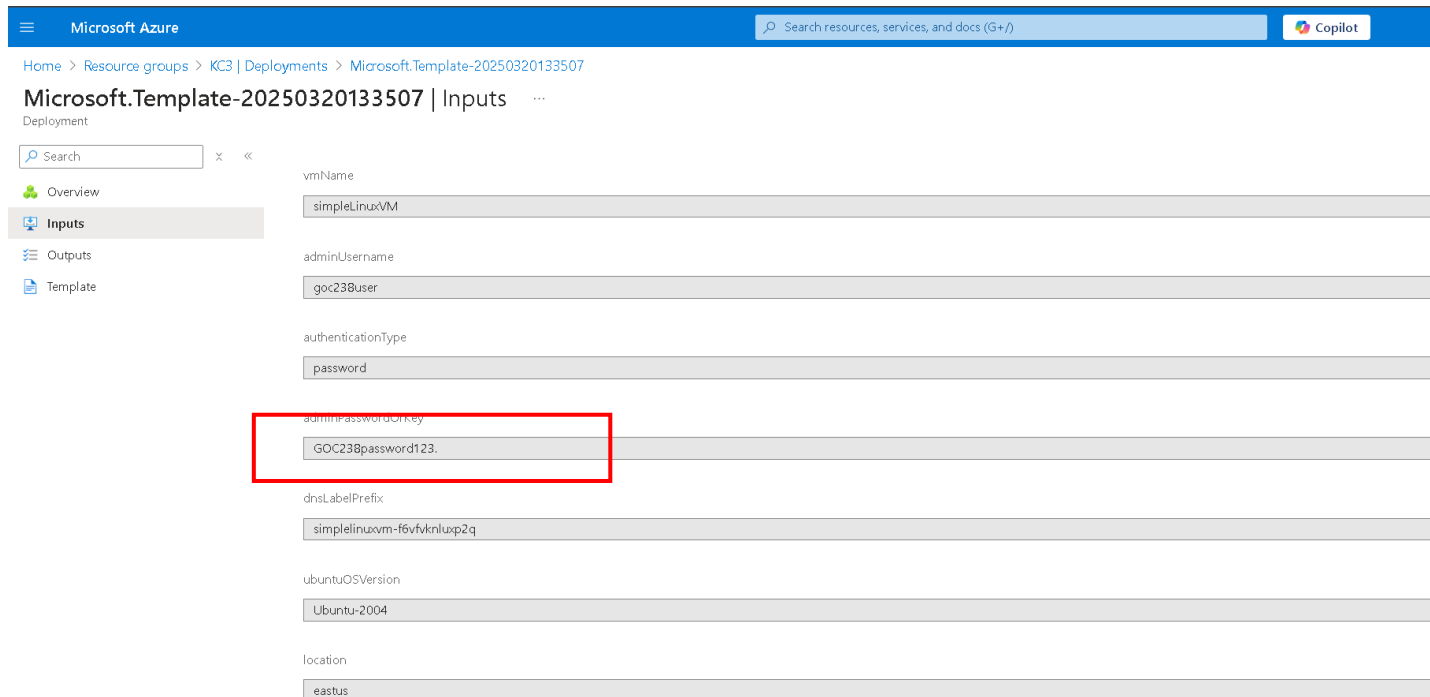
Secret / Credential Type	Max. Recommended Lifetime <sup>(1)</sup>	Typical “Safe” Rotation Interval	Notes & Key References <sup>(2)</sup>
<b>App Registration — Client Secret</b>	6 months (Microsoft strongly recommends this limit)	90 – 180 days	Azure AD best practices: shorter is safer; many orgs enforce 90 days.
<b>Key Vault Secrets</b> (passwords, connection strings, API keys)	No hard limit, but frequent rotation is advised	≤ 60 days	CIS Benchmark & NIST SP-800-63 recommend 60 days or less for high-value secrets.
<b>Storage Account Access Keys</b>	Two 512-bit keys; rotate without downtime	≤ 90 days	Azure storage guidance: use key-pair model for seamless rollover.
<b>SAS (Shared Access Signature)</b>	Intended for short-lived sharing	Hours – a few days at most	Generate per operation, with minimal scope and TTL.
<b>Encryption Keys</b> (Key Vault or Managed HSM)	Up to 2 years	≤ 24 months	NIST SP-800-57 recommends < 2 years for symmetric data-encryption keys.
<b>TLS / SSL Certificates</b> (e.g., App Service managed certs)	Auto-renew every 6 months	6 – 12 months	Let’s Encrypt & ACM issue 90-day or 12-month certs; Azure managed certs renew automatically.

# What is dangerous of template deployment history?



# Template deployment history properties

- By default, Azure retains the last 800 deployments per resource group.
- Older deployments beyond this limit are automatically deleted



The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header with the Microsoft Azure logo, a search bar, and a Copilot button. Below the header, the breadcrumb navigation shows 'Home > Resource groups > KC3 | Deployments > Microsoft.Template-20250320133507'. The main title is 'Microsoft.Template-20250320133507 | Inputs'. Below the title, there's a 'Deployment' section with a search bar and a list of tabs: 'Overview', 'Inputs' (selected), 'Outputs', and 'Template'. The 'Inputs' tab displays a list of input parameters for the deployment. The parameters are: 'vmName' (simpleLinuxVM), 'adminUsername' (goc238user), 'authenticationType' (password), 'adminPasswordOnKey' (GOC238password123), 'dnsLabelPrefix' (simplelinuxvm-f6vfuknluxp2q), 'ubuntuOSVersion' (Ubuntu-2004), and 'location' (eastus). The 'adminPasswordOnKey' input field is highlighted with a red box.

Parameter	Value
vmName	simpleLinuxVM
adminUsername	goc238user
authenticationType	password
adminPasswordOnKey	GOC238password123
dnsLabelPrefix	simplelinuxvm-f6vfuknluxp2q
ubuntuOSVersion	Ubuntu-2004
location	eastus

# RBAC mistakes

"There are not really only four roles in Azure, and there is no reason to assign the Contributor role to every IT person."

<https://learn.microsoft.com/en-us/azure/role-based-access->

## Add role assignment ...

[Role](#) [Members](#) [Conditions](#) [Review + assign](#)

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles [Privileged administrator roles](#)

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠ Can a job function role with less access be used instead?

🔍 Search by role name, description, permission, or ID

Type : **All**

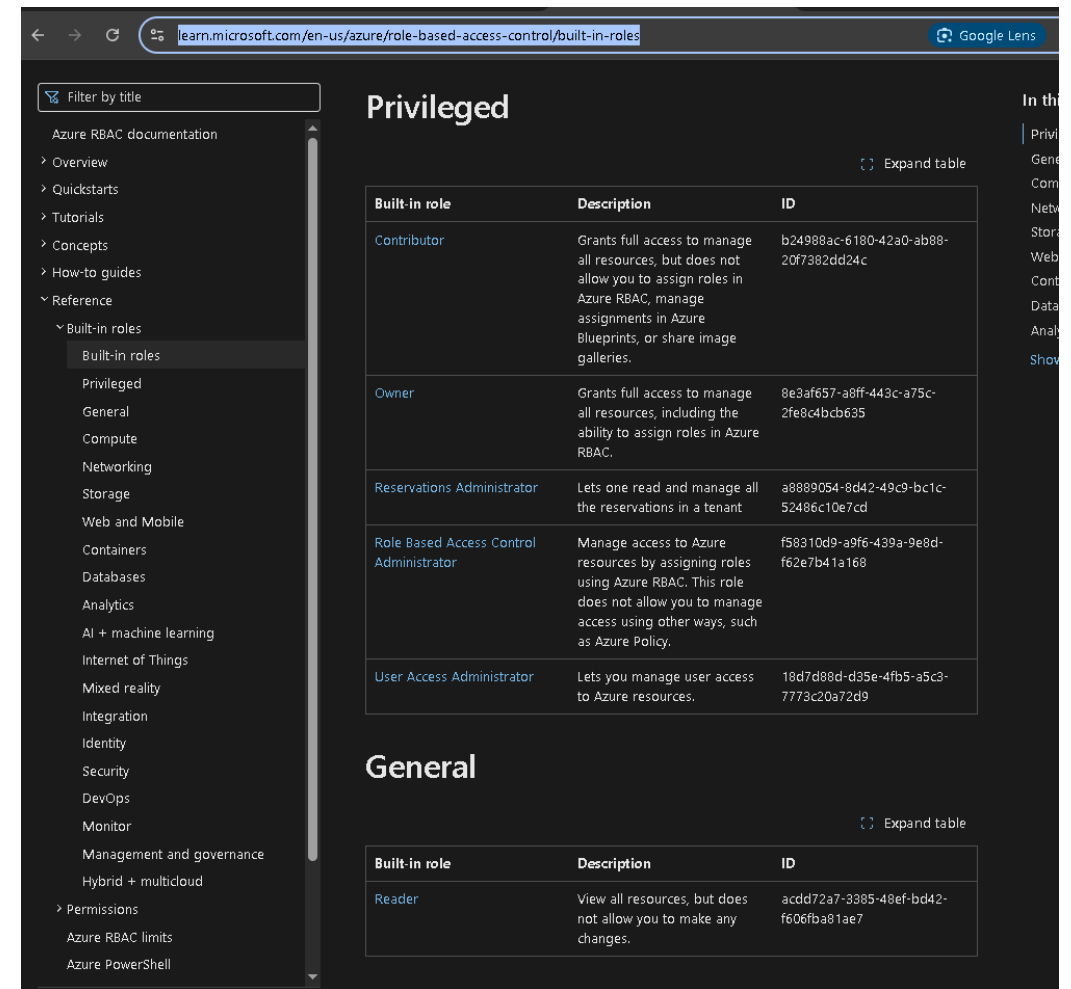
Category : **All**

Name ↑↓	Description ↑↓	Type ↑↓
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image gal...	BuiltInRole
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure Policy.	BuiltInRole
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole

Showing 1 - 4 of 4 results.

# Which RBAC role I should use?

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>



The screenshot shows the Microsoft Learn page for Azure RBAC built-in roles. The page is titled "Privileged" and "General". The left sidebar contains a navigation menu with categories like "Azure RBAC documentation", "Overview", "Quickstarts", "Tutorials", "Concepts", "How-to guides", and "Reference". Under "Reference", there is a sub-menu for "Built-in roles" which is currently selected. The main content area displays two tables: "Privileged" and "General". Each table lists built-in roles with their descriptions and IDs. The "Privileged" table includes roles like Contributor, Owner, Reservations Administrator, Role Based Access Control Administrator, and User Access Administrator. The "General" table includes the Reader role.

Filter by title

- Azure RBAC documentation
- > Overview
- > Quickstarts
- > Tutorials
- > Concepts
- > How-to guides
- > Reference
  - > Built-in roles
    - Built-in roles**
    - Privileged
    - General
    - Compute
    - Networking
    - Storage
    - Web and Mobile
    - Containers
    - Databases
    - Analytics
    - AI + machine learning
    - Internet of Things
    - Mixed reality
    - Integration
    - Identity
    - Security
    - DevOps
    - Monitor
    - Management and governance
    - Hybrid + multcloud
  - > Permissions
  - Azure RBAC limits
  - Azure PowerShell

## Privileged

Expand table

Built-in role	Description	ID
<a href="#">Contributor</a>	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.	b24988ac-6180-42a0-ab88-20f7382dd24c
<a href="#">Owner</a>	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	8e3af657-a8ff-443c-a75c-2fe8c4bcb635
<a href="#">Reservations Administrator</a>	Lets one read and manage all the reservations in a tenant	a8889054-8d42-49c9-bc1c-52486c10e7cd
<a href="#">Role Based Access Control Administrator</a>	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure Policy.	f58310d9-a9f6-439a-9e8d-f62e7b41a168
<a href="#">User Access Administrator</a>	Lets you manage user access to Azure resources.	18d7d88d-d35e-4fb5-a5c3-7773c20a72d9

## General

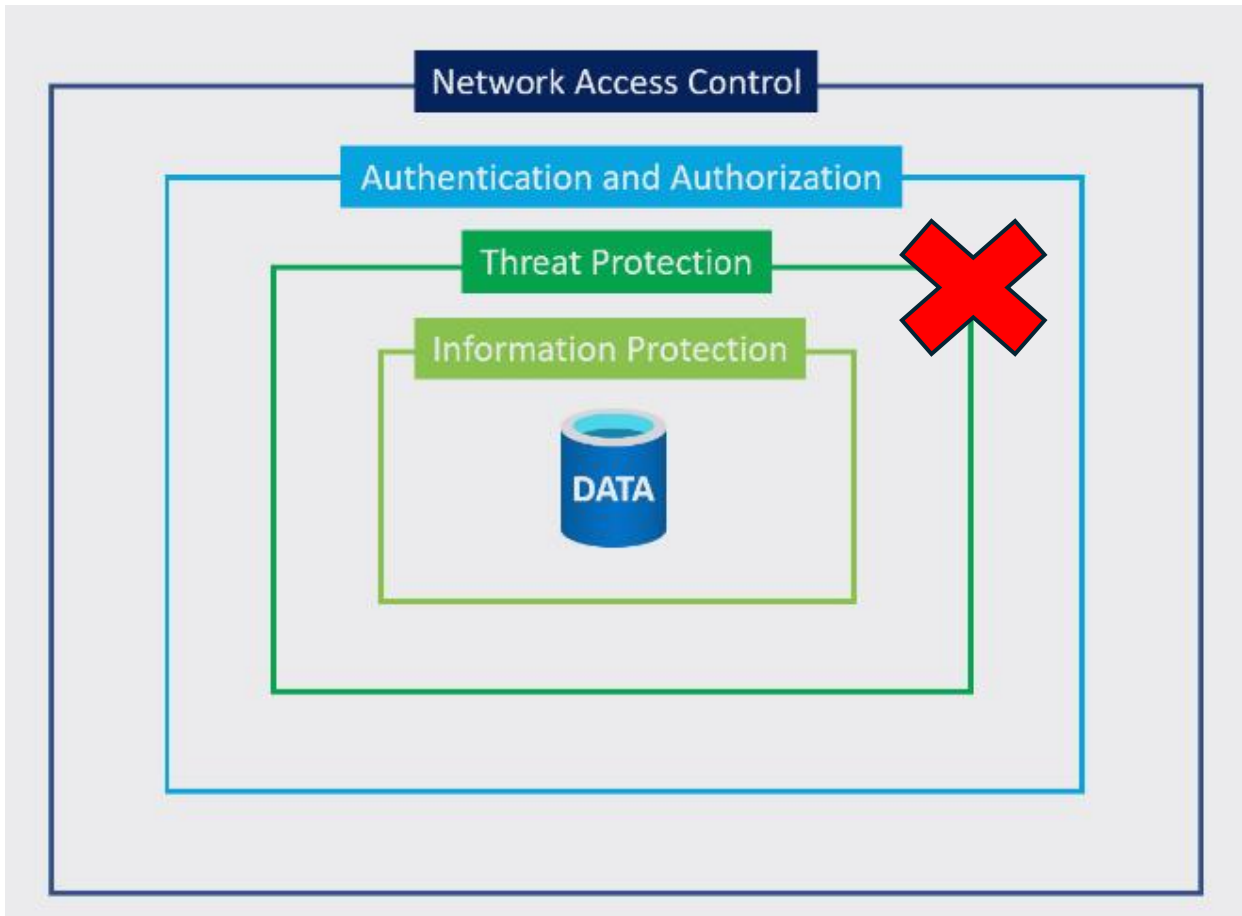
Expand table

Built-in role	Description	ID
<a href="#">Reader</a>	View all resources, but does not allow you to make any changes.	acdd72a7-3385-48ef-bd42-f606fba81ae7

# Optional demo

- Run command demo on adminVM
- <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/run-command>

# Azure resource multi layered approach

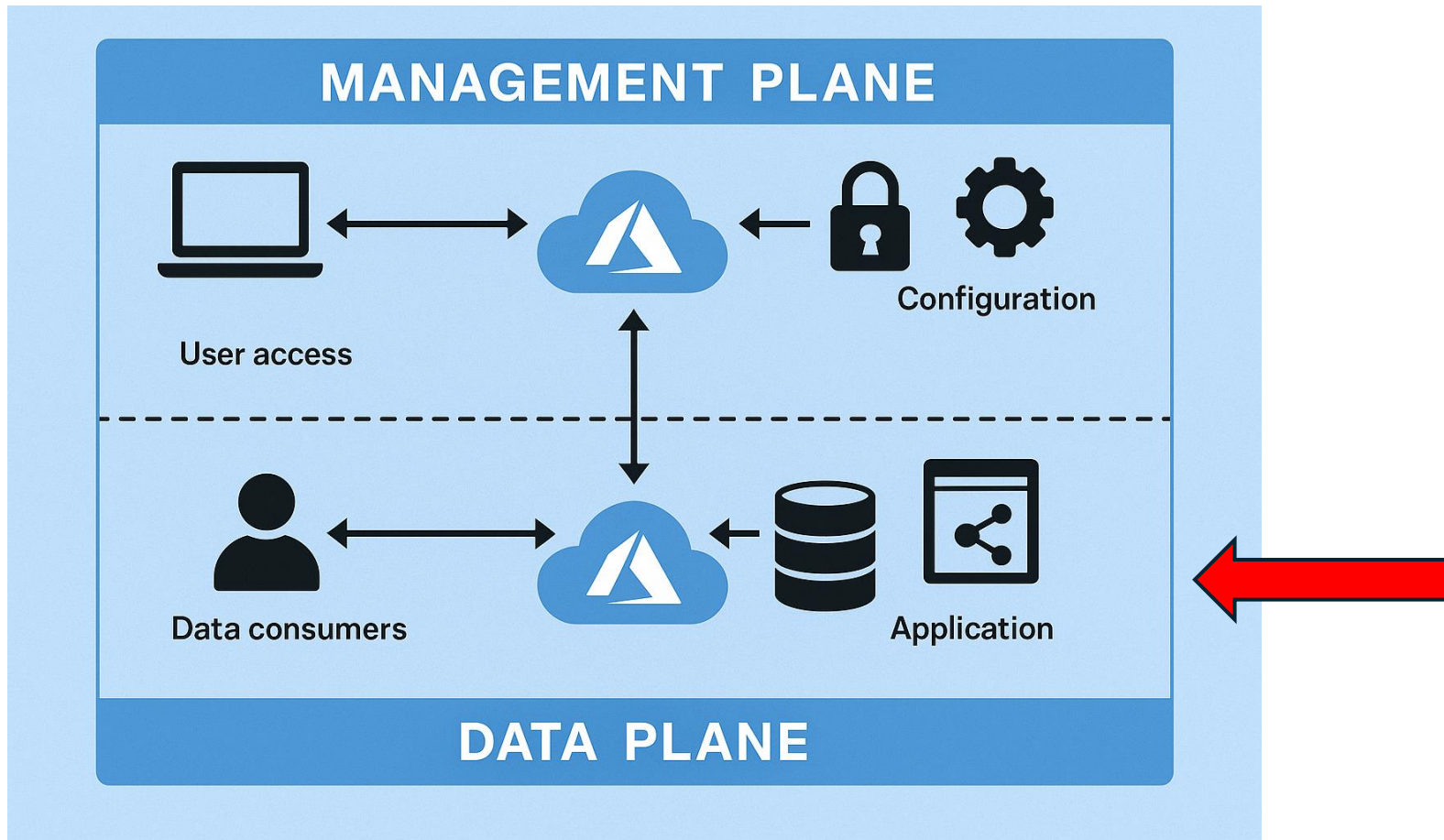




# Yes, also in cloud be attention!

- Missing Web Application Protection (WAF and Updates)
- OWASP check
- Not applying critical security patches regularly
- Missing OS hardening, Implement security software
- Missing backups
- SQL sysadmin is used for access to db
- AKS - Insufficient security of stored container images
- Logic app security

# Monitoring and alerting



# SQL auditing

sqlsrv5e35jyex5eyrg | Auditing ...  
SQL server

Search (Ctrl+ /)

Backups  
Deleted databases  
Failover groups  
Import/Export history

Security

**Auditing**

Firewalls and virtual networks  
Private endpoint connections

Save Discard Feedback

## Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure account, Log Analytics workspace or Event Hub. [Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing ⓘ

Audit log destination (choose at least one):

- ☐ Storage
- ☐ Log Analytics
- ☐ Event Hub

## Auditing of Microsoft support operations

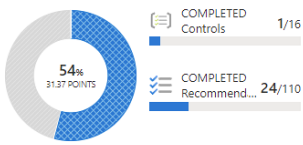
73 Azure subscriptions 4 AWS accounts 4 GCP projects 5984 Assessed resources 209 Active recommendations 7336 Security alerts



### Secure score

**Unhealthy resources**  
4101 To harden these resources and improve your score, follow the security recommendations

Current secure score



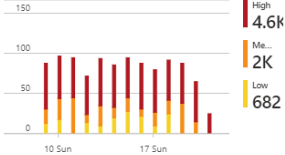
[Improve your secure score >](#)



### Workload protections

**Resource coverage**  
98% For full protection, enable 11 resource plans

Alerts by severity



[Enhance your threat protection capabilities >](#)



### Regulatory compliance

**Azure Security Benchmark**  
1 of 40 passed controls

Lowest compliance regulatory standards by passed controls

CMMC Level 3	0/55
NIST SP 800 53 R5	2/55
ISO 27001	1/20

[Improve your compliance >](#)

### Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	1025
Append a tag and its value to resou...	549
Storage account should use a privat...	447
Storage accounts should restrict net...	446

### New security alerts

145 new alerts were detected by Defender for Cloud in the last 48 hours.

[View full alerts list >](#) 5

[Microsoft Defender for SQL on machine...](#) 7

### Controls with the highest potential increase

Remediate vulnerabilities	+10% (6pt)
Remediate security configurations	+6% (4pt)
Enable MFA	+6% (10pt)

[View controls >](#)



### Firewall Manager

5 Firewalls 3 Firewall policies 4 Regions with firewalls

Network protection status by resource

Virtual hubs 0/0

Virtual networks 8/249

[Improve your network security >](#)



### Inventory

**Unmonitored VMs**  
134 To better protect your organization, we recommend installing agents

Total Resources

5984

Unhealthy (4101)

Healthy (1435) Not applicable (448)

[Explore your resources >](#)



### Information protection Preview

**Resource scan coverage**  
1% For full coverage scan additional resources

Recommendations & Alerts by classified resources



[View classified resources in inventory >](#)

# Defender for cloud



## Continuously Assess

Know your security posture.  
Identify and track vulnerabilities.



## Secure

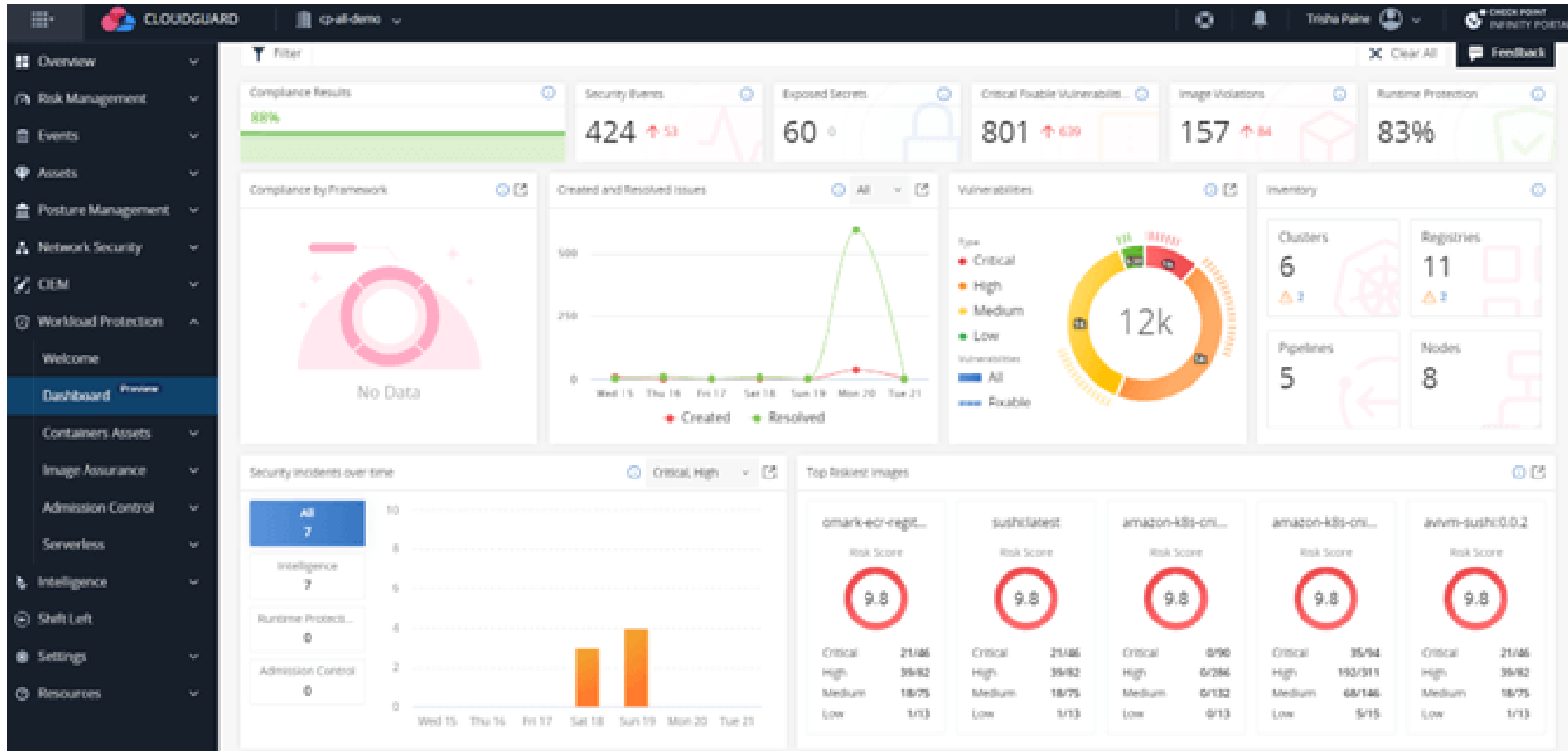
Harden resources and services with  
Azure Security Benchmark and  
AWS Security Best Practices standard



## Defend

Detect and resolve threats to  
resources and services.

# CheckPoint CNAPP



# MICROSOFT ENTRA MISCONFIGURATIONS AND MISTAKES



#	Statistic (what it tells us)	Misconfiguration theme	Year / report
1	Only <b>38 %</b> of Entra ID monthly active users authenticate with MFA.	MFA not enforced for most users	2024 – Practical365 article ( <a href="https://practical365.com">practical365.com</a> )
2	<b>99.9 %</b> of compromised accounts had <b>no MFA</b> enabled.	Absent MFA leaves accounts wide-open	2025 – Microsoft security stats page ( <a href="https://learn.microsoft.com">learn.microsoft.com</a> )
3	Microsoft testing shows MFA can <b>block 99.2 %</b> of account-compromise attacks.	Ignoring MFA wastes a near-perfect defence	2024 – Entra mandatory-MFA announcement ( <a href="https://learn.microsoft.com">learn.microsoft.com</a> )
4	<b>&gt; 99 %</b> of password-spray attacks use <b>legacy (basic) authentication</b> .	Legacy protocols still enabled	2025 – MSCA block-legacy-auth guidance ( <a href="https://learn.microsoft.com">learn.microsoft.com</a> )
5	<b>97 %</b> of credential-stuffing attacks also rely on legacy auth.	Same as above – disable it!	2025 – same Microsoft analysis ( <a href="https://learn.microsoft.com">learn.microsoft.com</a> )
6	Tenants that disabled legacy auth have <b>67 % fewer compromises</b> than those that keep it enabled.	Tangible payoff for blocking legacy protocols	2024 – PracticeProtect advisory ( <a href="https://support.practiceprotect.com">support.practiceprotect.com</a> )
7	Tenants that leave <b>Security Defaults</b> enabled suffer <b>80 % fewer compromises</b> ; over <b>7 million</b> tenants now have the defaults, but many later turn them off.	Disabling built-in baselines	2024 – Tommi Hovi security-defaults analysis ( <a href="https://tommihoivi.com">tommihoivi.com</a> )
8	Roughly <b>58 %</b> of an organisation's sensitive cloud data lives in Teams & Microsoft 365, multiplying exposure when sharing settings are lax.	Over-permissive data-sharing / Teams	2025 – CoreView governance brief ( <a href="https://coreview.com">coreview.com</a> )
9	<b>99 %</b> of cloud breaches are traced to preventable misconfigurations, according to Gartner (quoted in M365 context).	Misconfiguration as leading root cause	2024 – CoreView security-risks post ( <a href="https://coreview.com">coreview.com</a> )



HACKED AGAIN —

# Microsoft network breached through password-spraying by Russia-state hackers

Senior execs' emails accessed in network breach that wasn't caught for 2 months.

DAN GOODIN · 1/20/2024, 2:41 AM



Enlarge

117

Russia-state hackers exploited a weak password to compromise Microsoft's corporate network and accessed emails and documents that belonged to senior executives and employees working in security and legal teams, Microsoft said late Friday.

The attack, which Microsoft attributed to a Kremlin-backed hacking group it tracks as Midnight Blizzard, is at least the second time in as many years that failures to follow basic security hygiene have resulted in a breach that has the potential to harm customers. One paragraph in [Friday's disclosure](#), filed with the Securities and Exchange Commission, was gobsmacking:

“

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents. The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in

[Home](#) > Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network

Storm · October 31, 2024 · 8 min read


## Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network

By [Microsoft Threat Intelligence](#)

Listen to this post



0:00 / 0:00 1X

 Powered by Microsoft Copilot



<https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/>



INNOVATION > CYBERSECURITY

# Microsoft Password Spray And Pray Attack Targets Accounts Without 2FA

By **Davey Winder**, Senior Contributor. Davey Win... [Follow Aut](#)

Published Feb 25, 2025, 06:18am EST, Updated Feb 26, 2025, 10:20pm EST

[https://www.forbes.com/sites/daveywinder/2025/02/25/microsoft-password-spray-and-pray-attack-targets-accounts-without-2fa/?utm\\_source=chatgpt.com](https://www.forbes.com/sites/daveywinder/2025/02/25/microsoft-password-spray-and-pray-attack-targets-accounts-without-2fa/?utm_source=chatgpt.com)

DIVE BRIEF

## Attackers wield password-spray attacks to zero-in on targets, research finds

The highly effective brute-force attack method requires little effort, Trellix said. Organizations with weak password policies or no MFA are especially at risk.

[https://www.cybersecuritydive.com/news/password-spray-attacks-targeted/733460/?utm\\_source=chatgpt.com](https://www.cybersecuritydive.com/news/password-spray-attacks-targeted/733460/?utm_source=chatgpt.com)  
Published Nov. 20, 2024



Portnox

<https://www.portnox.com/blog> · Přeložit tuto stránku

### Spray and Pray: Botnet Takes Aim at Microsoft 365

27. 2. 2025 — Researchers at SecurityScoreCard recently discovered a botnet of over 130,000 devices is conducting **password spray** attacks against **Microsoft 365**.

<https://www.portnox.com/blog/cyber-attacks/spray-and-pray-botnet-takes-aim-at-microsoft-365/>

# Dangerous

- **Attacker know what is the correct password!**
- Probably MFA is not everywhere – consider RD gateway, VPN, onprem AD, Citrix, ERP systems
- MFA really for “All cloud apps”?  
<https://github.com/d>
- Maybe user use sam personal purposes



of passwords  
are duplicates



of breaches are caused  
by credential theft

```
\Desktop> Invoke-MFASweep -Username smonkey@glitchcloud.com -Password 
----- MFASweep -----

Microsoft Services Recon
This script can attempt to determine if ADFS is configured for the domain you submitted. Would
you like to do this now?
[Y] Yes [N] No [?] Help (default is "Y"): y
----- Running recon checks -----
[*] Checking if ADFS configured...
[*] ADFS does not appear to be in use. Authentication appears to be managed by Microsoft.

Confirm MFA Sweep
[*] WARNING: This script is about to attempt logging into the smonkey@glitchcloud.com account
SIX (6) different times
(7 if you included ADFS). If you entered an incorrect password this may lock the account out.
Are you sure you want to
continue?
[Y] Yes [N] No [?] Help (default is "Y"): y

----- Microsoft Graph API -----
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft Graph API - NOT
E: The response indicates MFA (Microsoft) is in use.

----- Azure Service Management API -----
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Azure Service Management
API - NOTE: The response indicates MFA (Microsoft) is in use.

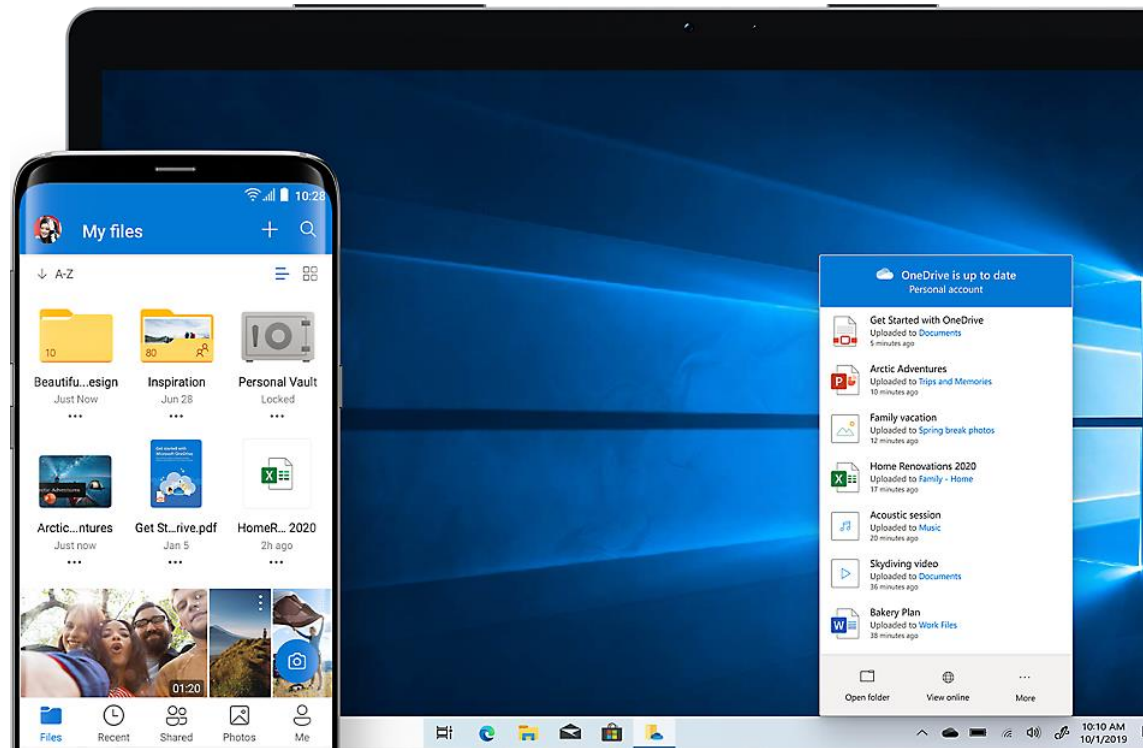
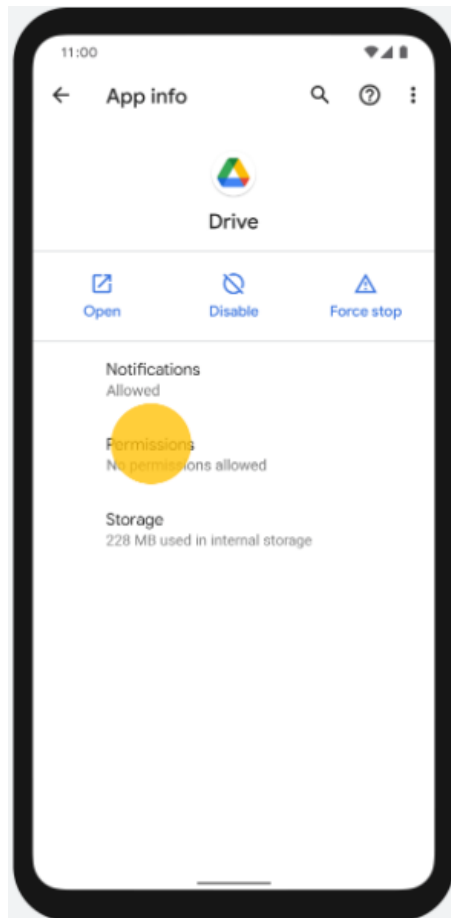
----- Microsoft 365 Exchange Web Services -----
[*] Authenticating to Microsoft 365 Exchange Web Services (EWS)...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to Microsoft 365 EWS!
[***] NOTE: MailSniper should work here.

----- Microsoft 365 Web Portal -----
[*] Authenticating to Microsoft 365 Web Portal...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft 365 Web Portal.
Checking MFA now...
[**] It appears MFA is setup for this account to access Microsoft 365 via the web portal.

----- Microsoft 365 Web Portal w/ Mobile User Agent (Android) -----
[*] Authenticating to Microsoft 365 Web Portal using a mobile user agent...
[*] SUCCESS! smonkey@glitchcloud.com was able to authenticate to the Microsoft 365 Web Portal.
Checking MFA now...
[**] It appears there is no MFA for this account.
[***] NOTE: Login with a web browser to https://outlook.office365.com using a mobile user agen
t.

----- Microsoft 365 ActiveSync -----
[*] Authenticating to Microsoft 365 Active Sync...
[*] SUCCESS! smonkey@glitchcloud.com successfully authenticated to O365 ActiveSync.
[***] NOTE: The Windows 10 Mail app can connect to ActiveSync.
PS C:\Users\beau\Desktop>
```

# Synchronized data on devices



Name	Status	Date modified	Type	Size
1-MB-Test.docx	✓	3/11/2021 12:13 PM	Microsoft Word D...	1,022 KB
10-MB-Test.docx	✓	3/11/2021 12:13 PM	Microsoft Word D...	10,473 KB
10-MB-Test.xlsx	✓	3/11/2021 12:13 PM	Microsoft Excel W...	9,343 KB
creditcards.docx	✓	7/22/2022 10:40 AM	Microsoft Word D...	15 KB
creditcardtest.docx	✓ ⚠	5/4/2023 9:27 PM	Microsoft Word D...	14 KB



# Valid account can access to some data in the cloud



Jannovak@domena.cz

Password:SuperTajne123



Jannovak@domena.cz

Password:SuperTajne123



Jannovak@domena.cz

Password:SuperTajne123

CLOUD DATA



# Weak Password Policies and No Banned Passwords

## **Key Point**

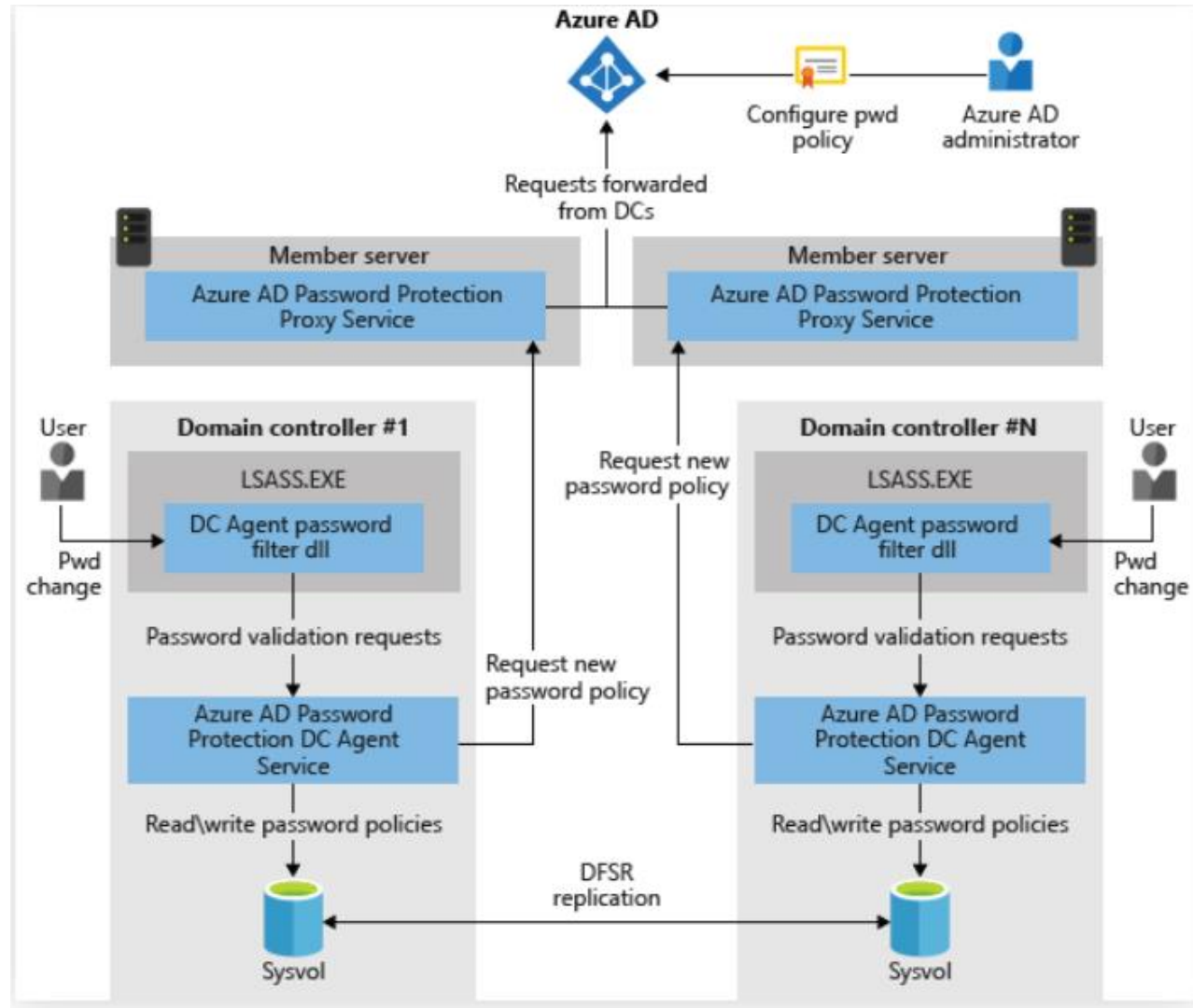
- Simple passwords (e.g., “Welcome2025!”) are easily guessable.
- Attackers rely on common password lists and previous breaches.

## **Mitigation**

- Enforce Azure AD Password Protection and a banned password list.
- Implement passphrases or passwordless sign-in.
- Monitor for leaked credentials and train users on strong password habits.

# Azure AD password protection

<https://download.manageengine.com/products/self-service-password/azure-ad-password-protection.pdf>





# Leaked passwords

## Auditing Active Directory Password Quality

📅 Aug 7, 2016 👤 [Michael Grafnetter](#)

### Overview

The latest version of the [DSInternals PowerShell Module](#) contains a new cmdlet called `Test-PasswordQuality`, which is a powerful yet easy to use tool for Active Directory password auditing. It can detect **weak, duplicate, default, non-expiring or empty passwords** and find accounts that are violating **security best practices**. All domain administrators can now audit Active Directory passwords on a regular basis, without any special knowledge.

### Usage

The `Test-PasswordQuality` cmdlet accepts output of the `Get-ADDBAccount` and `Get-ADRepAccount` cmdlets, so both **offline** (ntds.dit) and **online** (DCSync) analysis can be done:

```
Get-ADRepAccount -All -Server LON-DC1 -NamingContext "dc=adatum,dc=com" |  
    Test-PasswordQuality -WeakPasswordHashesFile .\pwned-passwords-ntlm-ordered-by-count.txt -IncludeDisabledAccounts
```

<https://www.dsinternals.com/en/auditing-active-directory-password-quality/>

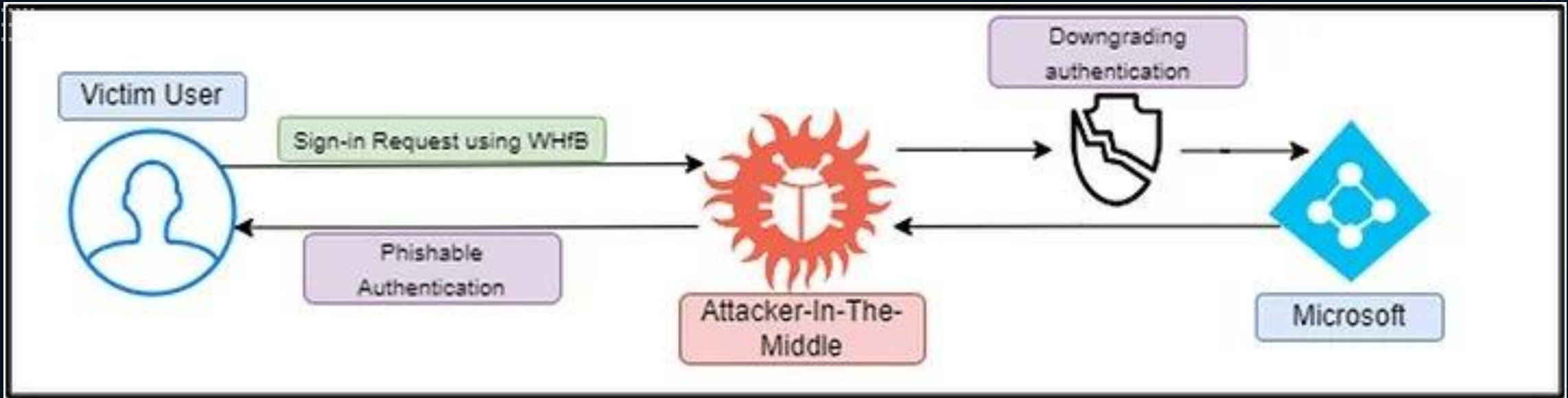
# Not Enforcing Multi-Factor Authentication (MFA) for All Users

## Key Point

- Single-factor (password-only) authentication is highly vulnerable to stolen or guessed credentials.
- MFA blocks over 99.9% of account compromise attempts.

## Mitigation

- Require MFA for **all** user accounts, not just administrators.
- Use Conditional Access to enforce MFA or enable Security Defaults.
- Prefer stronger methods (FIDO2 keys, Authenticator app) over SMS.



Strong authentication  
for admin is not  
enforced

# Emergency account

You should carefully review the (now updated) Microsoft guidance on [managing emergency access](#). It suggests both that at least one emergency access account should be excluded from all CA policies *and* that these policies will be overridden when accessing certain admin portals (MFA will be required). These two things don't necessarily contradict each other (you'll need MFA to access some admin portals, but your break glass account won't be dependent on your Conditional Access architecture), but I can understand why people are so confused by this.

Here's how we've decided to handle this, for what it's worth:

- Our break glass account is excluded from all MFA policies.
- The account has a very long passphrase stored in separate parts and in secure locations [per Microsoft's guidance](#).
- We set up multiple FIDO2 keys, which are stored in secure locations. We will try to use these keys to log in to the break glass account and only fall back to the password if necessary.
- We test both authentication methods for the account every 90 days.
- [We have Azure alerts set up to notify all admins whenever the account is used](#) via email and text message.

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication?tabs=dotnet#request-more-time-to-prepare-for-enforcement>

## Scope of enforcement

The scope of enforcement includes which applications plan to enforce MFA, applications that are out of scope, when enforcement is planned to occur, and which accounts have a mandatory MFA requirement.



## Applications

### Note

The date of enforcement for Phase 2 has changed to July 1, 2025.

The following table lists affected apps, app IDs, and URLs for Azure.

[Expand table](#)

Application Name	App ID	Enforcement starts
<a href="#">Azure portal</a>	c44b4083-3bb0-49c1-b47d-974e53cbdf3c	Second half of 2024
<a href="#">Microsoft Entra admin center</a> 	c44b4083-3bb0-49c1-b47d-974e53cbdf3c	Second half of 2024
<a href="#">Microsoft Intune admin center</a> 	c44b4083-3bb0-49c1-b47d-974e53cbdf3c	Second half of 2024
<a href="#">Azure command-line interface (Azure CLI)</a>	04b07795-8ddb-461a-bbee-02f9e1bf7b46	July 1, 2025
<a href="#">Azure PowerShell</a>	1950a258-227b-4e31-a9cf-717495945fc2	July 1, 2025
<a href="#">Azure mobile app</a>	0c1307d4-29d6-4389-a11c-5cbe7f65d7fa	July 1, 2025
<a href="#">Infrastructure as Code (IaC) tools</a>	Use Azure CLI or Azure PowerShell IDs	July 1, 2025

# Entra ID default configuration

- User settings:  
[Users - Microsoft Entra admin center](#)
- External collaboration:  
[https://entra.microsoft.com/#view/Microsoft\\_AAD\\_IAM/AllowlistPolicyBlade](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AllowlistPolicyBlade)
- Groups:  
[Groups - Microsoft Entra admin center](#)
- Devices  
[Devices - Microsoft Entra admin center](#)
  - Warning – autopilot: <https://learn.microsoft.com/en-us/autopilot/tutorial/user-driven/azure-ad-join-allow-users-to-join>

The screenshot displays the Microsoft Azure portal interface for the 'osmerait365' subscription. The left-hand navigation pane lists various administrative tools, with 'User settings' currently selected. The main content area is titled 'osmerait365 | User settings' and includes a 'Save' button, a 'Discard' button, and a 'Got feedback?' link. The settings are organized into several sections: 'Enterprise applications' (with a link to manage end users), 'App registrations' (with a toggle for 'Users can register applications' set to 'Yes'), 'Tenant creation' (with a toggle for 'Restrict non-admin users from creating tenants' set to 'No'), 'Administration portal' (with a toggle for 'Restrict access to Azure AD administration portal' set to 'No'), 'LinkedIn account connections' (with a toggle for 'Allow users to connect their work or school account' set to 'Yes' and a 'Selected group' dropdown), 'Show keep user signed in' (with a toggle set to 'Yes'), and 'External users' (with a link to manage external collaboration settings). The bottom of the page features a 'Troubleshooting + Support' link.

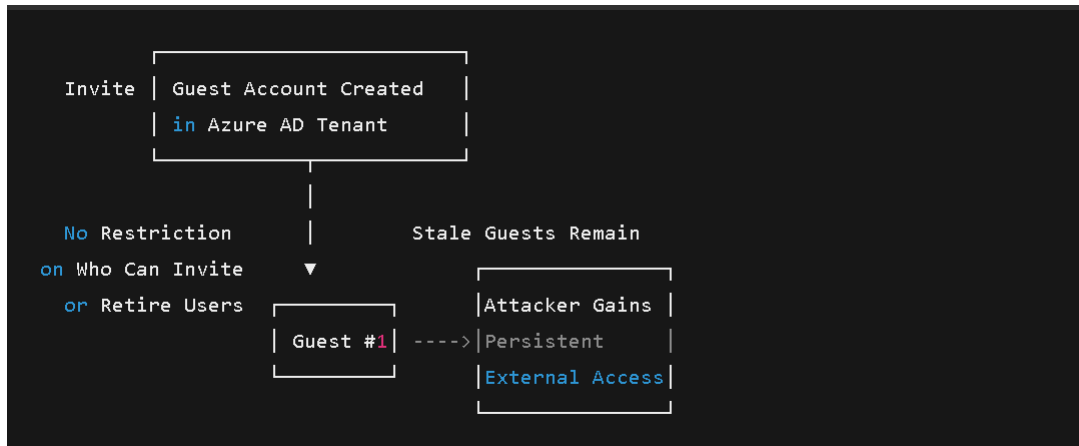
# Inadequate Guest User Access Controls

Who can be invited?

Who can access to your organization from outside?

- Possible reasons for guest cleaning

- A guest account is used to review a shared document and is not needed thereafter.
- External people leave a team (or teams) and their guest account remains in Entra ID.
- People leave their employer and move on to new challenges. Their guest account is invalid because they can no longer authenticate using the Entra ID instance for the tenant of their old employer.



[Home](#) > [Sign-in events](#) > [Users](#) >

## Invite external user

Invite an external user to collaborate with your organization

[Basics](#) [Properties](#) [Assignments](#) [Review + invite](#)

### Basics

Email	luba585@seznam.cz
Display name	kala
Send invite message	Yes
Message	
Cc recipient	
Invite redirect URL	https://myapplications.microsoft.com/?tenantid=0442af0e-caec-48c3-96b7-68b280ef2316

### Properties

User type	Guest
-----------	-------

### Assignments

[Groups](#)[Roles](#)

#### User invitation failed

The invited user already exists in the directory as object ID: 845eb78c-e55d-41c8-b904-420e3b387abb, but the account is blocked from signing in. If the account is unblocked, they can use that account to sign in to shared apps and resources.

[Help me troubleshoot](#)



# Dangerous dynamic groups



Medium · Ahmad Mansour  
50+ lajků



## Absuing Dynamic groups for Entra ID privileg escalation

In Azure, misconfigured dynamic groups can open doors for privilege escalation attacks, allowing attackers to exploit automated membership changes for ...



Tenable

<https://www.tenable.com> > entra · Přeložit tuto stránku



## Dynamic Group Featuring an Exploitable Rule

13. 12. 2024 — This misconfiguration can result in **unauthorized access or privilege escalation** if the group grants access to sensitive resources. While many attributes in a ...



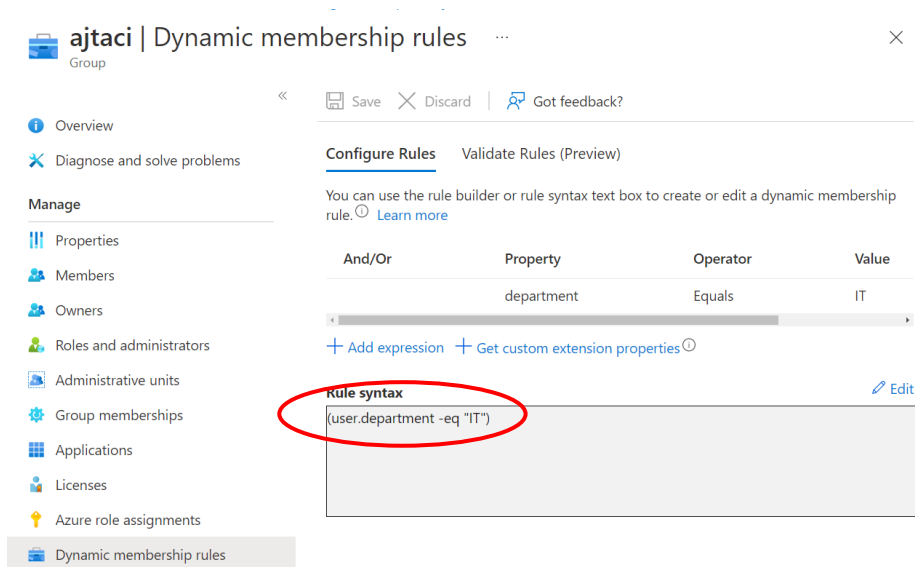
Medium · Albert Glenn  
20+ lajků



## Abuse Dynamic Groups in Entra ID for Privilege Escalation

This role allows role members to manage all aspects of users and groups, including resetting passwords for limited admins.

# Example



**ajtací | Dynamic membership rules**

Overview  
Diagnose and solve problems

**Manage**

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments
- Dynamic membership rules**

Configure Rules | Validate Rules (Preview)

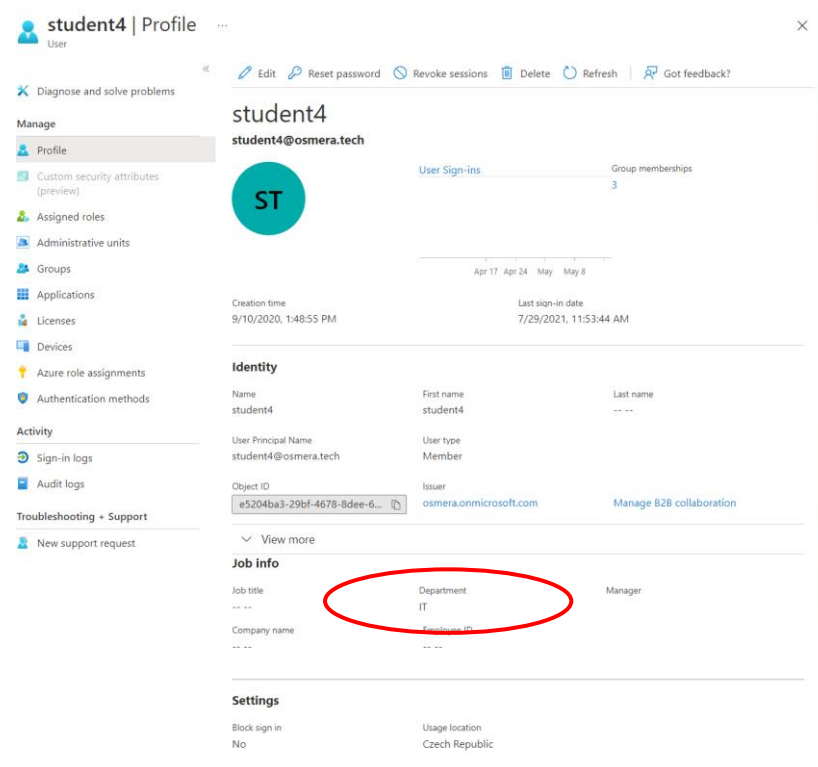
You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
	department	Equals	IT

[+ Add expression](#) [+ Get custom extension properties](#)

**Rule syntax** [Edit](#)

(user.department -eq "IT")



**student4 | Profile**

student4  
student4@osmera.tech

User Sign-ins | Group memberships

Creation time: 9/10/2020, 1:48:55 PM | Last sign-in date: 7/29/2021, 11:53:44 AM

**Identity**

Name	First name	Last name
student4	student4	...

User Principal Name: student4@osmera.tech | User type: Member

Object ID: e5204ba3-29bf-4678-8dee-6... | Issuer: osmera.onmicrosoft.com | Manage B2B collaboration

**Job info**

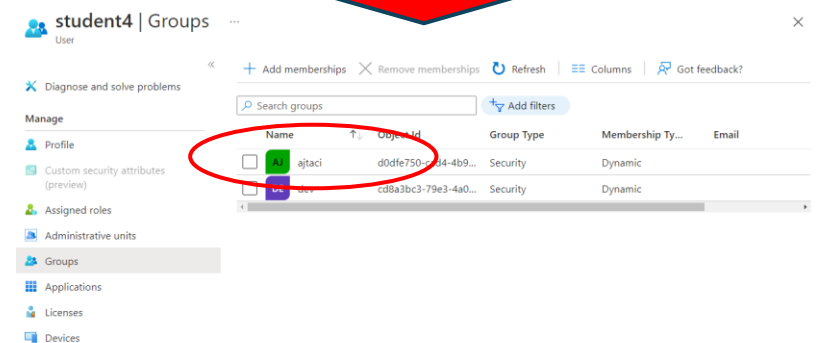
Job title	Department	Manager
...	IT	...

Company name: ...

**Settings**

Block sign in	Usage location
No	Czech Republic

Po několika minutách



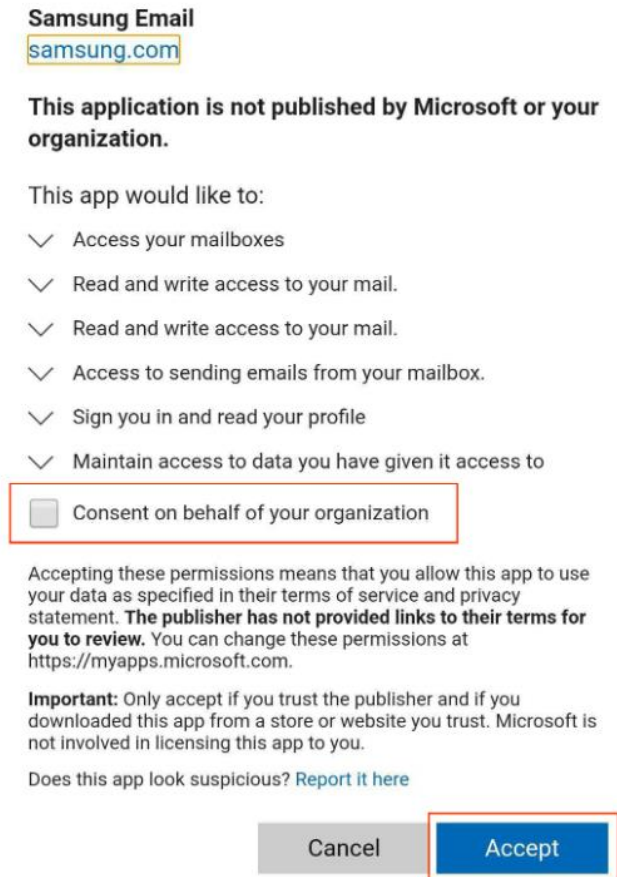
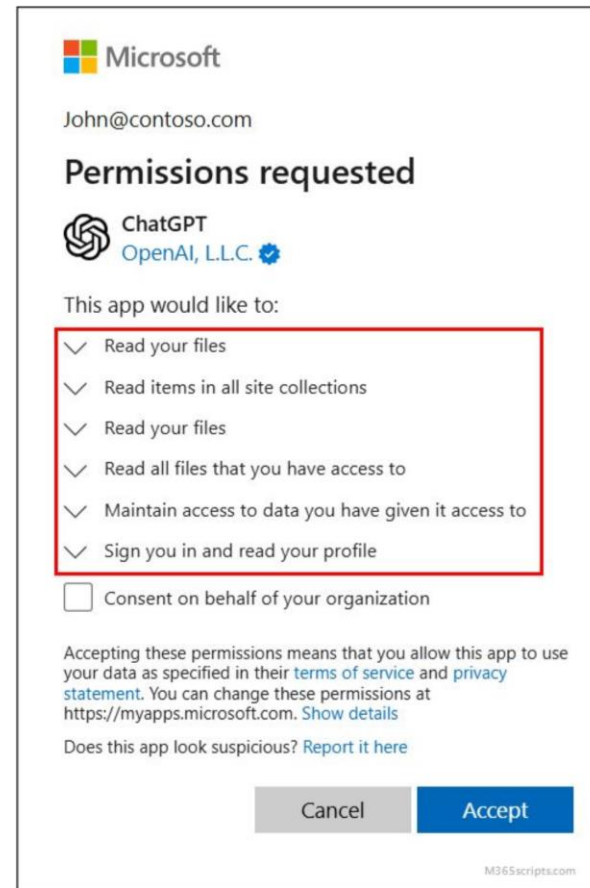
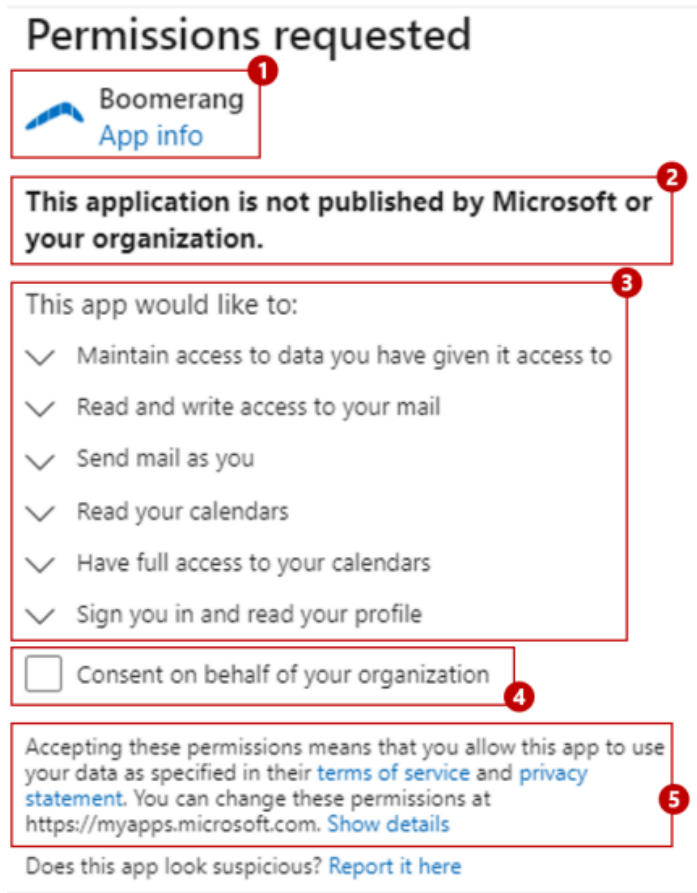
**student4 | Groups**

+ Add memberships | Remove memberships | Refresh | Columns | [Got feedback?](#)

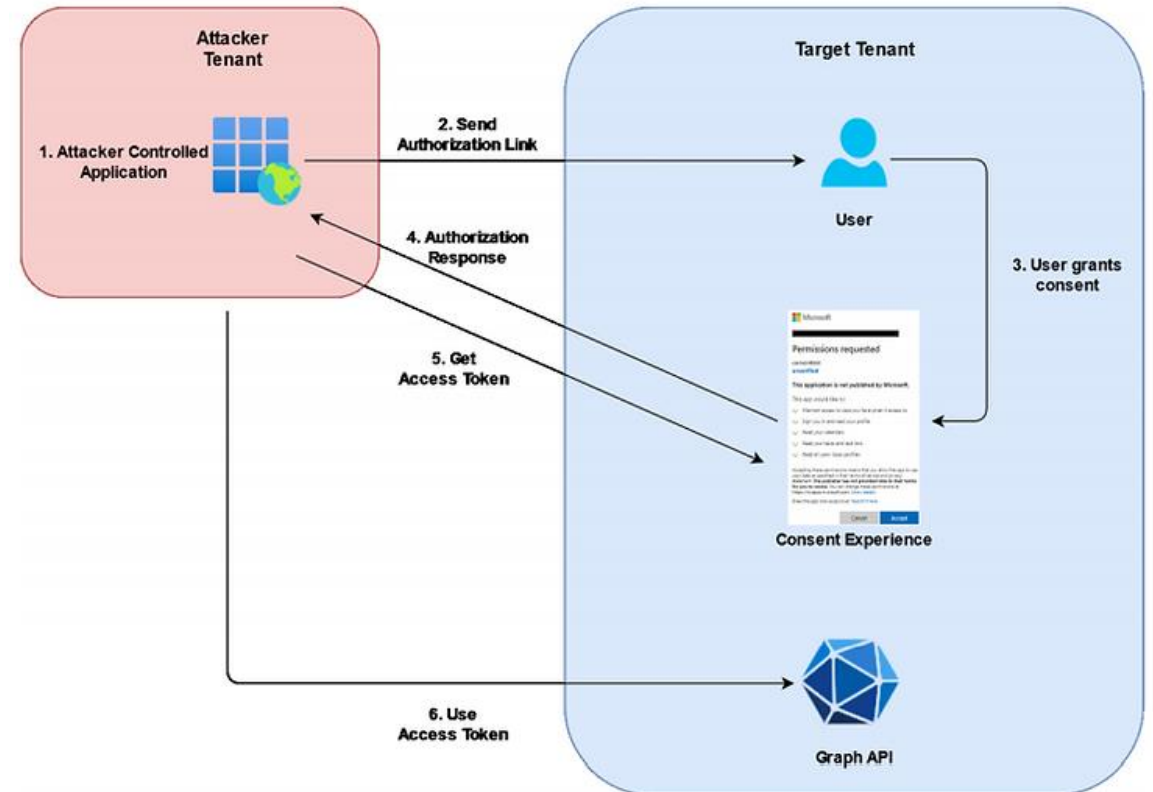
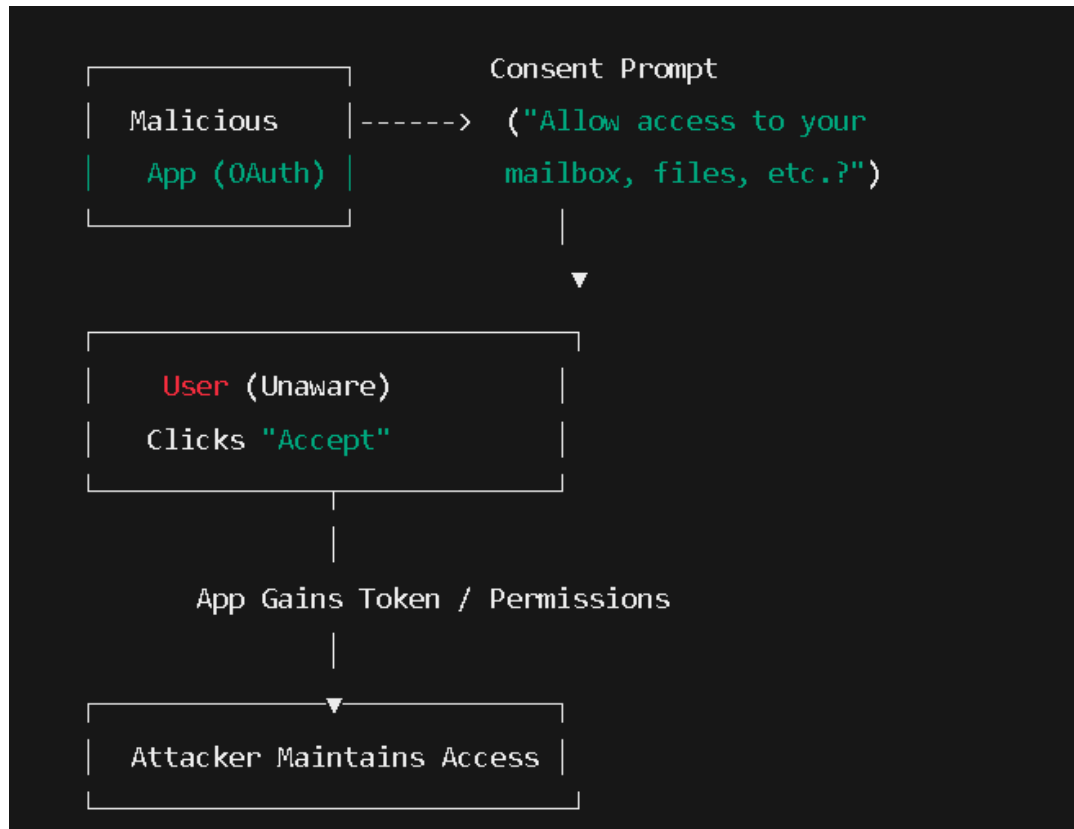
Search groups | Add filters

Name	Object ID	Group Type	Membership Ty...	Email
ajtací	d0dfe750-...4-4b9...	Security	Dynamic	
dev	cd8a3bc3-79e3-4a0...	Security	Dynamic	

# Permission dialog window



# Unregulated Application Registrations and OAuth Consent



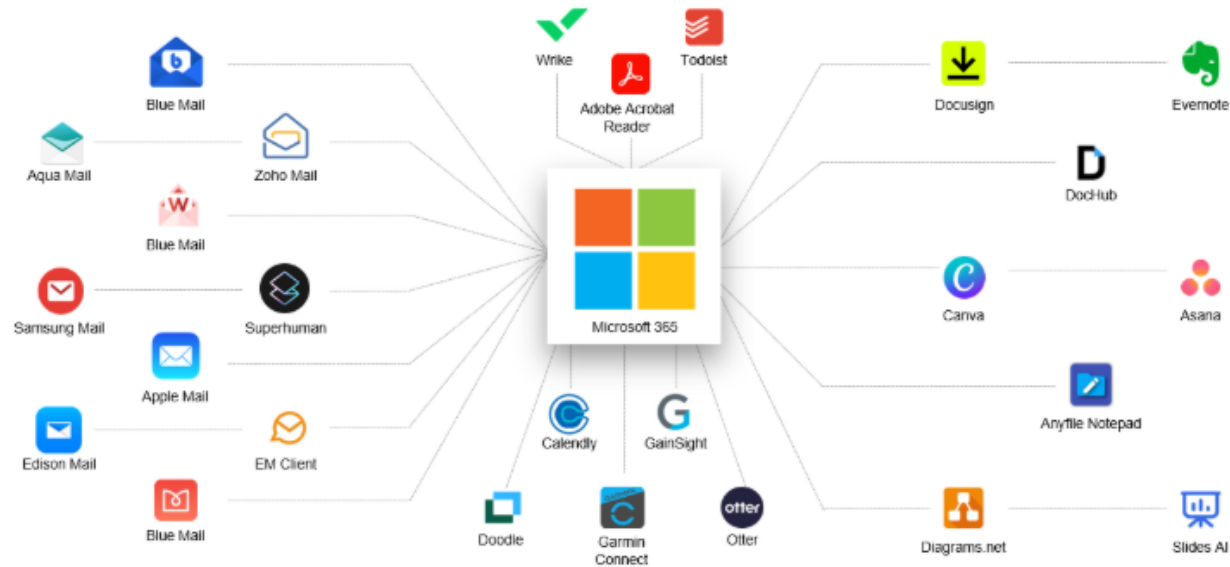
# Harmony SaaS

## How It Works

### 1. SaaS Discovery

Harmony SaaS discovers SaaS applications using these methods:

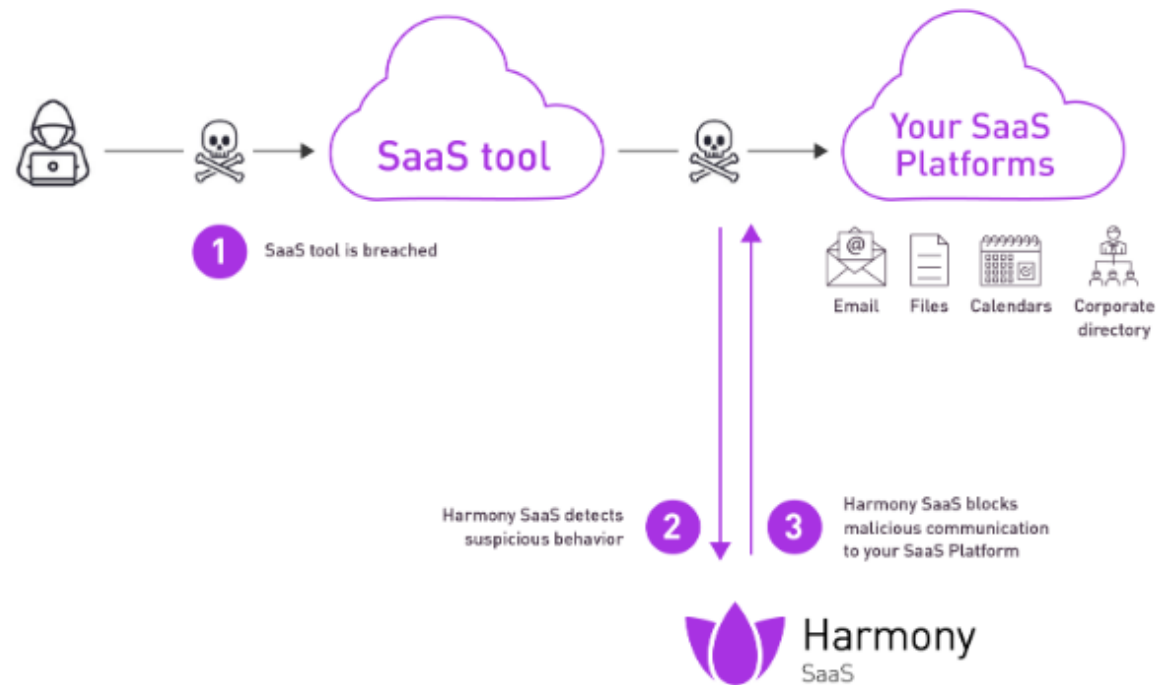
- **API** - If you use any of the supported SaaS applications, then Harmony SaaS uses API to discover all the plug-ins, applications, services, users, accounts and tokens associated with it.
- **Check Point Quantum Gateway** - If you use a Check Point Quantum Gateway, then Harmony SaaS uses its logs to discover the SaaS applications in your organization.



# Harmony SaaS

## 2. Threat Prevention

Harmony SaaS uses Machine Learning (ML) to detect threats and recommends corrective actions, such as blocking connection with malicious applications, revoking the token and so on.



# Entra links

- [https://entra.microsoft.com/#view/Microsoft\\_AAD\\_IAM/ConsentPoliciesMenuBlade/~/UserSettings](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings)
- [https://entra.microsoft.com/#view/Microsoft\\_AAD\\_IAM/ConsentPoliciesMenuBlade/~/UserSettings](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings)
- <https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-app-consent>

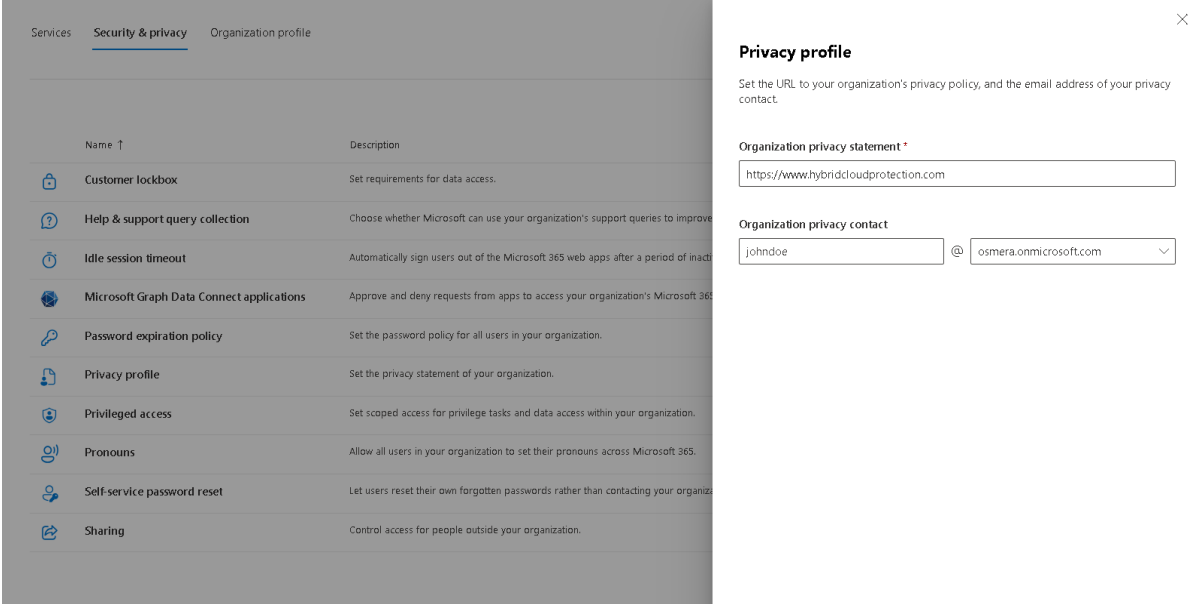
What I mustn't forget













# MICROSOFT 365 MISCONFIGURATIONS AND MISTAKES



# Privacy information missing



The screenshot shows the Microsoft 365 Admin Center interface. The top navigation bar includes 'Services', 'Security & privacy' (which is selected), and 'Organization profile'. Below this is a table of settings. The 'Privacy profile' setting is highlighted. To the right, a detailed view of the 'Privacy profile' is shown, including a description, a field for the 'Organization privacy statement' URL, and a field for the 'Organization privacy contact' email address.

Name ↑	Description
 Customer lockbox	Set requirements for data access.
 Help & support query collection	Choose whether Microsoft can use your organization's support queries to improve
 Idle session timeout	Automatically sign users out of the Microsoft 365 web apps after a period of inacti
 Microsoft Graph Data Connect applications	Approve and deny requests from apps to access your organization's Microsoft 365
 Password expiration policy	Set the password policy for all users in your organization.
 Privacy profile	Set the privacy statement of your organization.
 Privileged access	Set scoped access for privilege tasks and data access within your organization.
 Pronouns	Allow all users in your organization to set their pronouns across Microsoft 365.
 Self-service password reset	Let users reset their own forgotten passwords rather than contacting your organiz
 Sharing	Control access for people outside your organization.

**Privacy profile** ✕

Set the URL to your organization's privacy policy, and the email address of your privacy contact.

**Organization privacy statement \***

**Organization privacy contact**

@

<https://admin.microsoft.com/Adminportal/Home#/Settings/SecurityPrivacy/Settings/L1/PrivacyProfile>



# Insufficient Phishing Protection and Awareness

## Key Point

- **Phishing is the most common initial attack vector:** *“Microsoft appeared as the most impersonated brand in phishing attacks during the third quarter of 2024, according to new research by CheckPoint. The tech firm topped the latest edition of Check Point Research's Brand Phishing Ranking, with 61% of brand phishing attempts leveraging Microsoft branding”*
- Overvalued MFA!

## Mitigation

- Active protection: anti-phishing, Defender for Office 365 or alternatives
- Conduct regular phishing simulations and user-awareness training.



Recycle Bin

Privacy error

Not secure | https://login.azure.lubomirosmiera.eu/xfzcqRwe

Restore pages

Microsoft Edge closed while you had some pages open.

Restore

!

Your connection isn't private

Attackers might be trying to steal your information from login.azure.lubomirosmiera.eu (for example, passwords, messages, or credit cards).

NET::ERR\_CERT\_AUTHORITY\_INVALID

Hide advanced

Go back

This server couldn't prove that it's login.azure.lubomirosmiera.eu; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Continue to login.azure.lubomirosmiera.eu \(unsafe\)](#)

LAB1Y7P20 - Virtual Machine Connection

Action Media Clipboard View Help

1 2 3 4

22:54

~/Desktop/evil

kali@kali: ~

File Actions Edit View Help

vilginx config

onfig domain azure.lubomirosmiera.eu

onfig ip 172.16.50.2

openssl genrsa -out ca.key 2048

openssl req -new -x509 -key ca.key -out ca.crt

phishlets hostname o365

phishlets enable o365

lures create o365

lures edit 0 redirect\_url https://portal.office.com

lures get-url 0

@white_fi	disabled	available
@An0nUD4Y	disabled	available
@mrgretzky	disabled	available
@jamescullum	enabled	available
@customsync	disabled	available
@meitar	disabled	available
@charlesbel	disabled	available
@mrgretzky	disabled	available
@jamescullum	disabled	available
@AN0NUD4Y	disabled	available
@perfectlylog...	disabled	available
@charlesbel	disabled	available
@audibleblink	disabled	available
@An0nUD4Y	disabled	available
@white_fi	disabled	available
@customsync	disabled	available
@Anonymous	disabled	available
@424f424f	disabled	available

```
: lures create o365
[22:51:48] [err] unknown command: lures
: phishlets enable o365
[22:52:10] [inf] enabled phishlet 'o365'
[22:52:10] [inf] setting up certificates for phishlet 'o365' ...
[22:52:10] [+++] successfully set up SSL/TLS certificates for domains: [login.azure.lubomirosmiera.eu login.azure.lubomirosmiera.eu]
: lures create o365
[22:52:20] [inf] created lure with ID: 1
: lures edit 0 redirect_url https://portal.office.com
[22:52:30] [inf] redirect_url = 'https://portal.office.com'
: lures get-url 0

https://login.azure.lubomirosmiera.eu/xfzcqRwe

: 2024/05/08 22:54:02 [002] WARN: Cannot handshake client login.microsoftonline.com remote
2024/05/08 22:54:02 [001] WARN: Cannot handshake client login.microsoftonline.com remote
2024/05/08 22:54:02 [003] WARN: Cannot handshake client login.microsoftonline.com remote
2024/05/08 22:54:02 [004] WARN: Cannot handshake client login.microsoftonline.com remote
```

Running

# Insufficient Phishing Protection and Awareness

- Awareness
  - Attacker in the middle
  - Device code flow
  - Browser in the browser
  - QR CODE attacks
- Technical restrictions
  - Mail tips
  - Safe links
  - Safe attachments
  - Conditional access

[https://www.youtube.com/watch?v=kg1F8afYrQ0&ab\\_channel=ALEFSecurity](https://www.youtube.com/watch?v=kg1F8afYrQ0&ab_channel=ALEFSecurity)  
<https://techcommunity.microsoft.com/blog/microsoftteamsblog/policy-changes-for-microsoft-teams-devices-using-device-code-flow-authentication/4399337>  
<https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/protect-your-organizations-against-qr-code-phishing-with-defender-for-office-365/4007041>

MICROSOFT TEAMS BLOG 2 MIN READ

## Policy changes for Microsoft Teams devices using device code flow authentication



Apr 01, 2025

First announced in February, Microsoft is rolling out a new Microsoft-managed policy to help further secure your tenants against potential threats to accounts using device code flow (DCF) authentication.

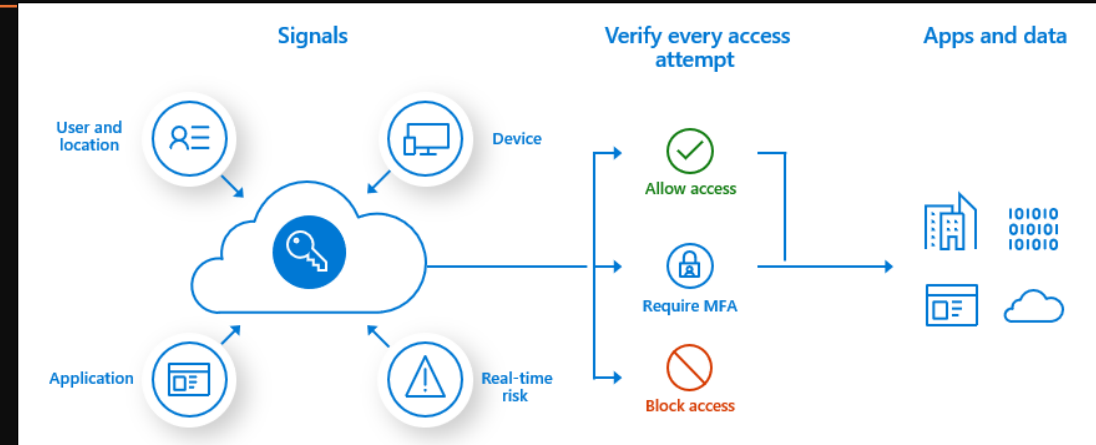
Rollout began in February and will continue until May. The policies will initially be created in report-only mode, allowing admins to review their impact before they're enforced. You'll have at least 45 days to evaluate and configure the policies before they're automatically moved to the "On" state. We recommend taking action as soon as possible to create exclusion lists if you are using Android devices in shared spaces.





# Conditional access policies

In general, there are a couple of Conditional Access policies that can prevent token theft by phishing:



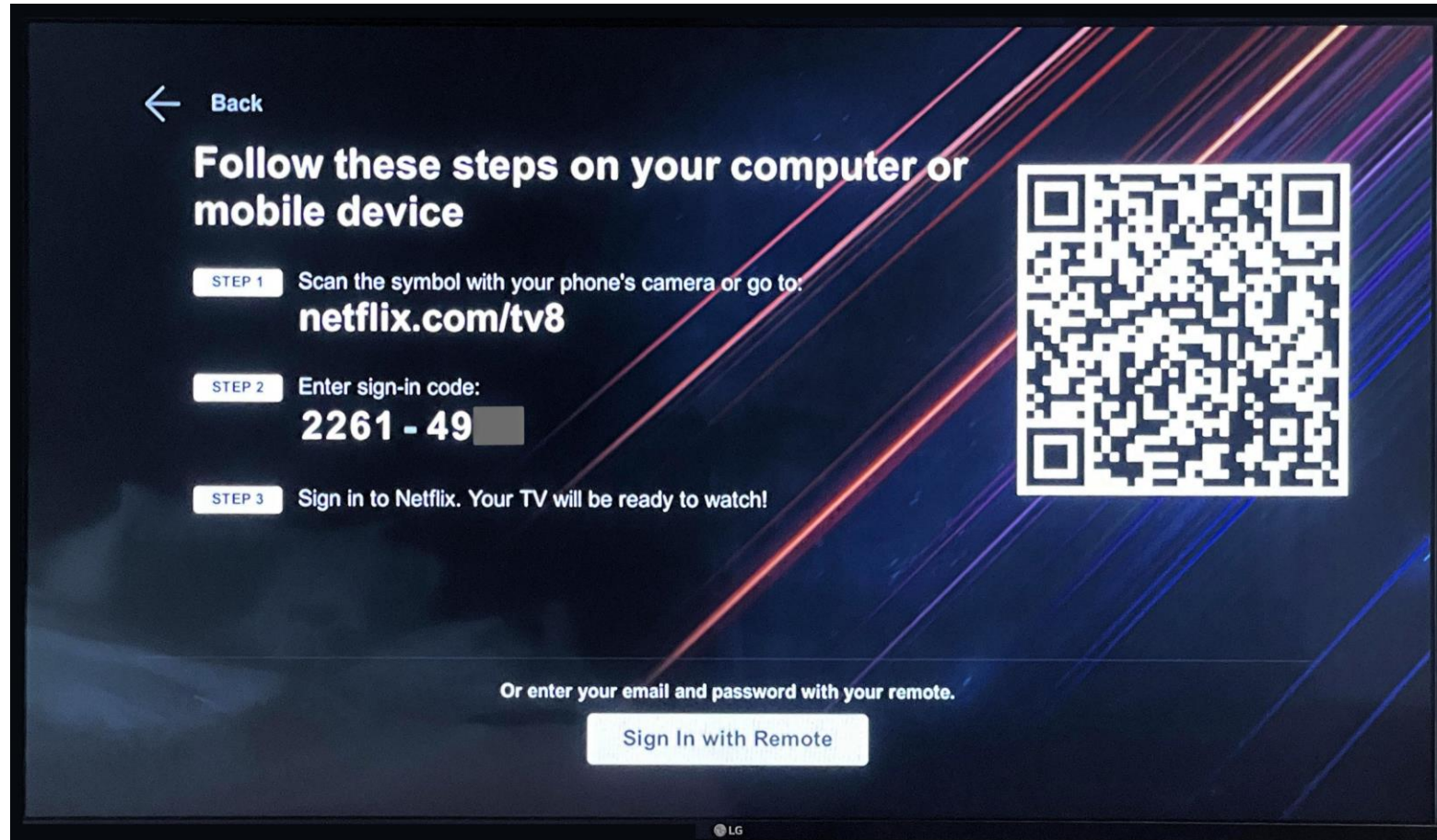
Enforce phishing-resistant MFA

Require Compliant or hybrid-joined device

Require Trusted Locations

Enforce compliant network with Microsoft Entra Internet Access

# Device code flow - explanation



# MFA competition

---

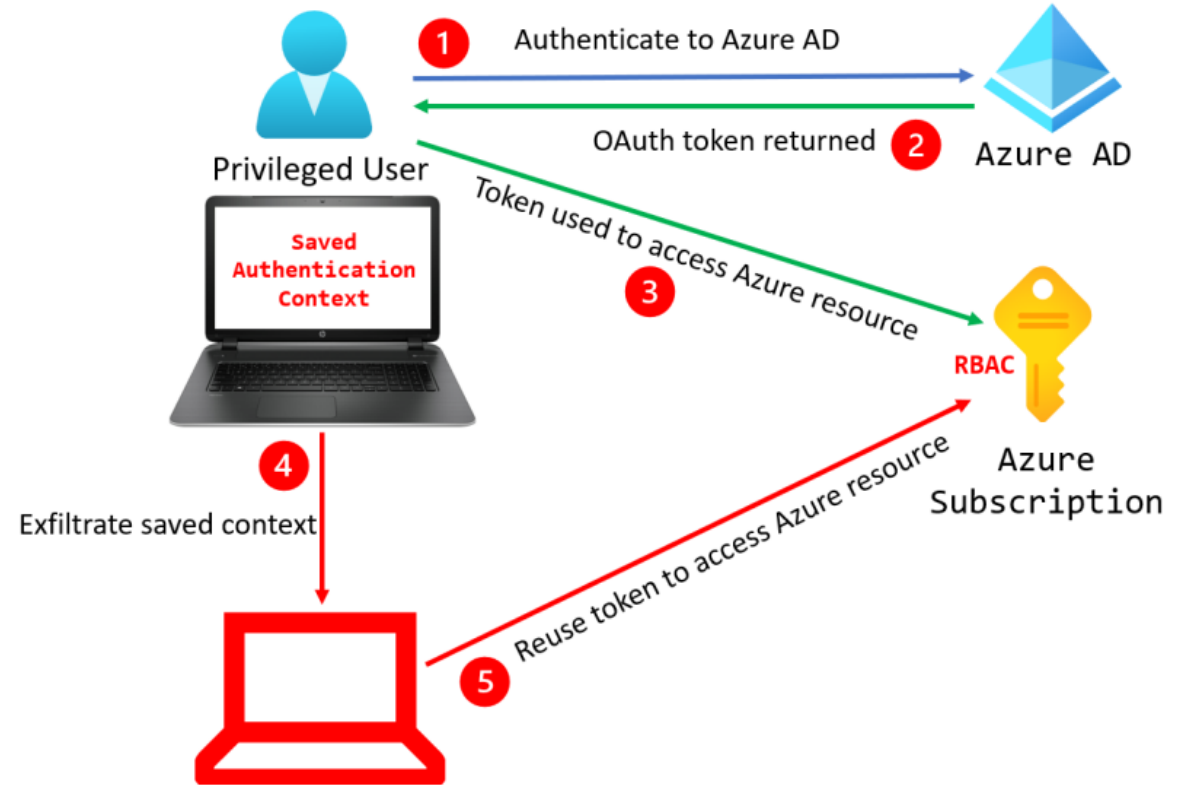
- Attacker can register MFA BEFORE user
- TAP attack also could be abuse.





# Dangerous Admin Access

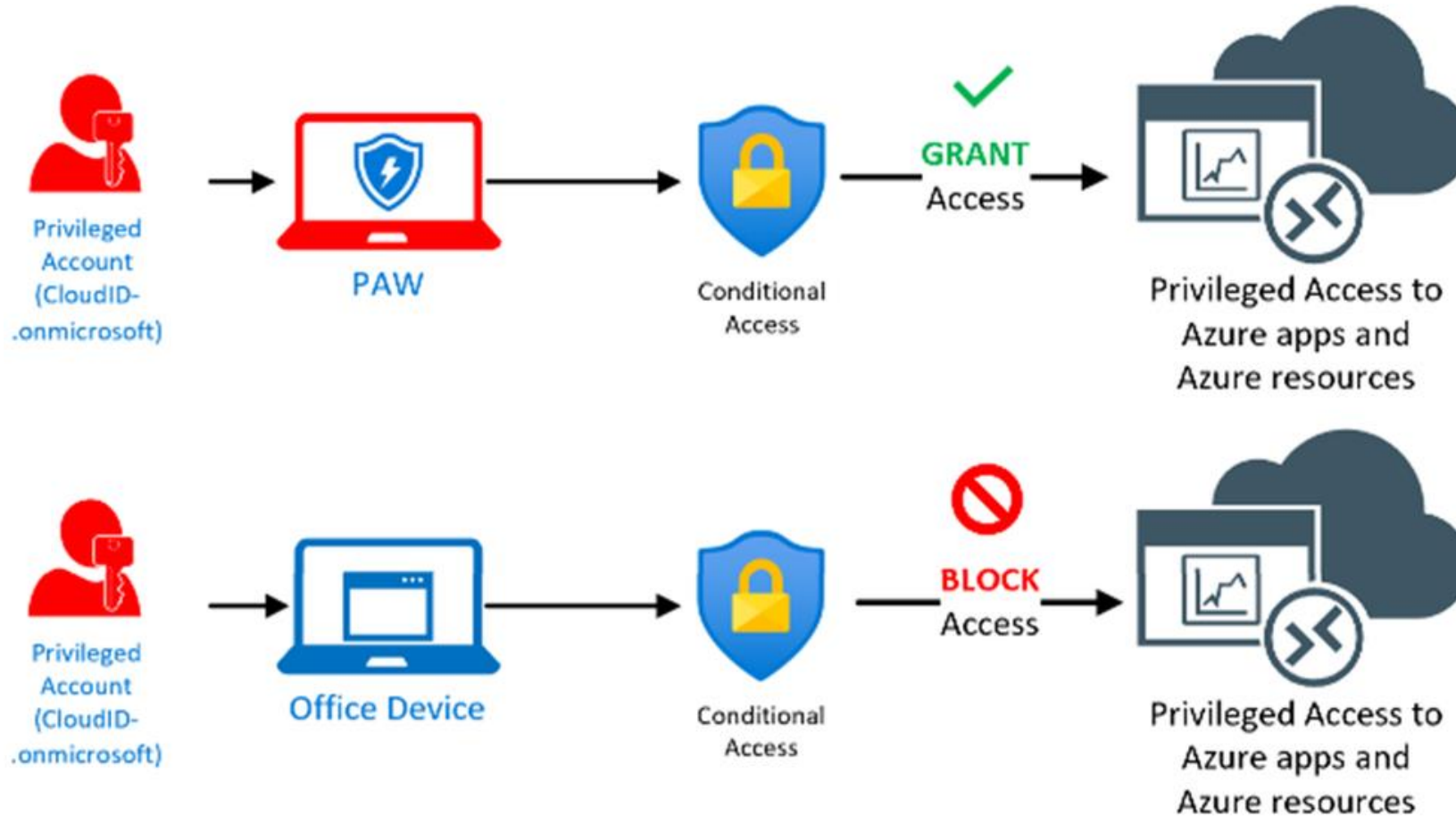
- **Weak least privilege model:** Too many Global Admin accounts broaden the attack surface. (Any compromised admin account can lead to full tenant takeover.)
- **Bad protection of admins** (only MFA is not sufficient countermeasure)
- **Access from any workstation**



```
PS C:\Users\lubos> Get-AzCoNTEXT
```

```
PS C:\Users\lubos>
```

# Conditional access: PAW



# Legacy Authentication Protocols Still Enabled

## Key Point

- Legacy protocols (POP3, IMAP, SMTP Basic, older Office clients) do not support modern auth or MFA.
- Attackers often password-spray or brute force through these endpoints to bypass MFA.

## Mitigation

- Disable legacy authentication in Azure AD (via Security Defaults or Conditional Access).
- Identify older apps still using basic auth and update them to modern auth.

# Legacy Authentication Protocols Still Enabled

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links for Diagnose & solve problems, Favorites, Identity (Overview, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities), Protection (Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities), and Learn & support.

The main content area is titled "Sign-in events" and includes a search bar and a Copilot button. Below the title, there are links for Download, Export Data Settings, Troubleshoot, Refresh, Columns, and Got feedback?. The filters section shows "Date : Last 1 month", "Show dates as : Local", "Client app : 13 selected", and "Add filters".

The table displays "User sign-ins (interactive)" and "User sign-ins (non-interactive)". The table headers are Date, Request ID, User, Application, Status, Sign-in error code, IP address, and Location. The table content shows "No sign-ins found".

# DLP is not in sufficient state

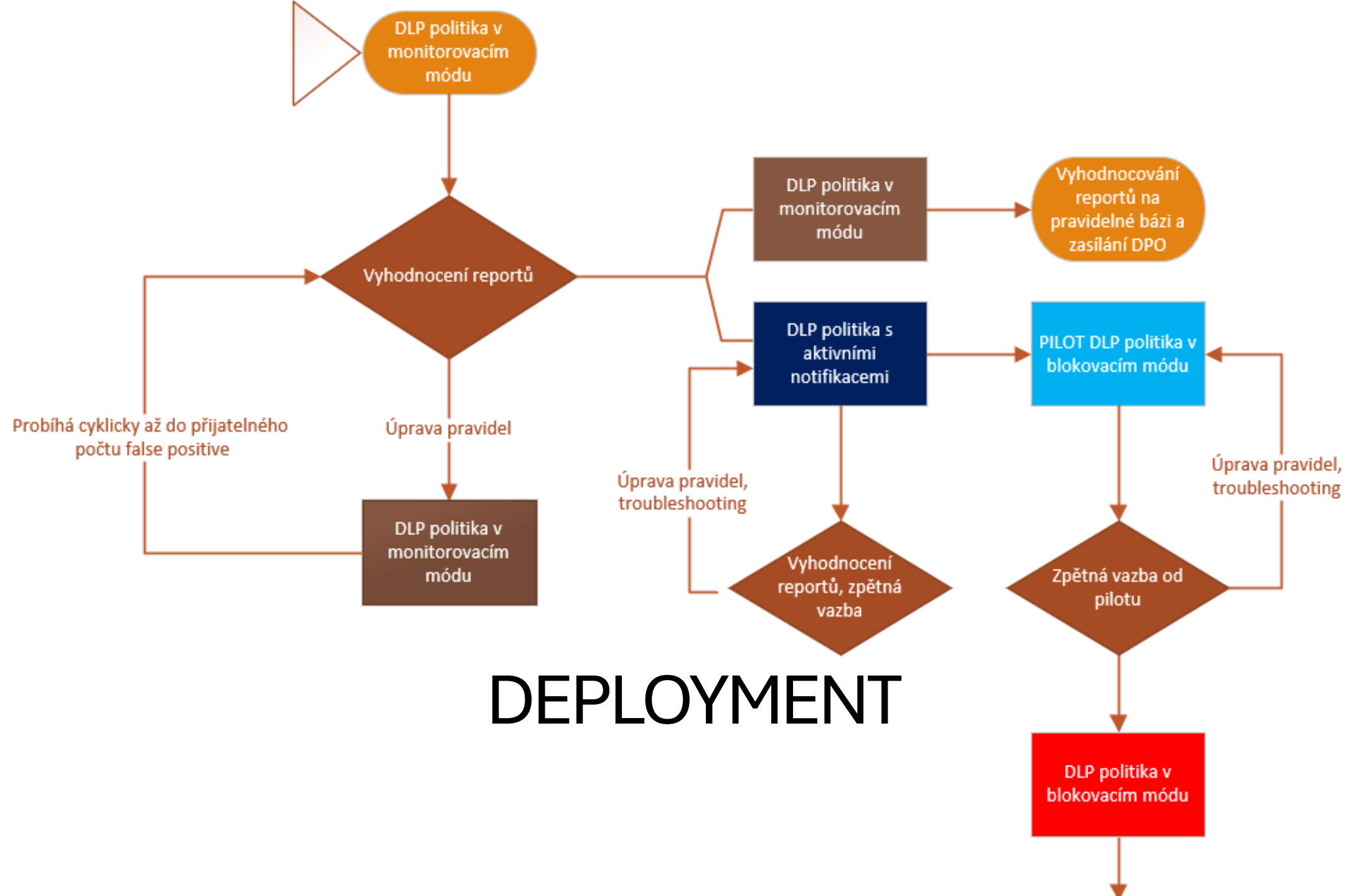
## Key Point

- Accidentally sharing details by email etc.
- User account compromise

## Mitigation

- OneDrive / SharePoint configuration
- DLP







# Email attachment filtering is not strongly strict

```
"7z", "a3x", "ace", "ade", "adp", "ani", "app", "appinstaller",  
"applescript", "application", "appref-ms", "appx", "appxbundle", "arj",  
"asd", "asx", "bas", "bat", "bgi", "bz2", "cab", "chm", "cmd", "com",  
"cpl", "crt", "cs", "csh", "daa", "dbf", "dcr", "deb",  
"desktopthemepackfile", "dex", "diagcab", "dif", "dir", "dll", "dmg",  
"doc", "docm", "dot", "dotm", "elf", "eml", "exe", "fxp", "gadget", "gz",  
"hlp", "hta", "htc", "htm", "htm", "html", "html", "hwp", "ics", "img",  
"inf", "ins", "iqy", "iso", "isp", "jar", "jnlp", "js", "jse", "kext",  
"ksh", "lha", "lib", "library-ms", "lnk", "lzh", "macho", "mam", "mda",  
"mdb", "mde", "mdt", "mdw", "mdz", "mht", "mhtml", "mof", "msc", "msi",  
"msix", "msp", "msrcincident", "mst", "ocx", "odt", "ops", "oxps", "pcd",  
"pif", "plg", "pot", "potm", "ppa", "ppam", "ppkg", "pps", "ppsm", "ppt",  
"pptm", "prf", "prg", "ps1", "ps11", "ps11xml", "ps1xml", "ps2",  
"ps2xml", "psc1", "psc2", "pub", "py", "pyc", "pyo", "pyw", "pyz",  
"pyzw", "rar", "reg", "rev", "rtf", "scf", "scpt", "scr", "sct",  
"searchConnector-ms", "service", "settingcontent-ms", "sh", "shb", "shs",  
"shtm", "shtml", "sldm", "slk", "so", "spl", "stm", "svg", "swf", "sys",  
"tar", "theme", "themepack", "timer", "uif", "url", "uue", "vb", "vbe",  
"vbs", "vhd", "vhdx", "vxd", "wbk", "website", "wim", "wiz", "ws", "wsc",  
"wsf", "wsh", "xla", "xlam", "xlc", "xll", "xlm", "xls", "xlsb", "xlsm",  
"xlt", "xltm", "xlw", "xnk", "xps", "xsl", "xz", "z"
```

[Emotet adopts Microsoft OneNote attachments](#)  
([malwarebytes.com](#))

# Antispam outbound is poorly configured

- Outbound messages limits miss.
- Autoforwarding to external domains is not blocked

# Not controlled Teams applications

## 8.4.1 (L1) Ensure app permission policies are configured (Manual)

### Profile Applicability:

- E3 Level 1

### Description:

This policy setting controls which class of apps are available for users to install.

### Rationale:

Allowing users to install third-party or unverified apps poses a potential risk of introducing malicious software to the environment.

### Impact:

Users will only be able to install approved classes of apps.

### Audit:

#### To audit using the UI:

1. Navigate to Microsoft Teams admin center <https://admin.teams.microsoft.com>.
2. Click to expand Teams apps select Manage apps.
3. In the upper right click Actions > Org-wide app settings.
4. For Microsoft apps verify that Let users install and use available apps by default is On or less permissive.
5. For Third-party apps verify Let users install and use available apps by default is Off.
6. For Custom apps verify Let users install and use available apps by default is Off.
7. For Custom apps verify Upload custom apps for personal use is Off.

**Note:** The Global Reader role is not able to view the Teams apps blade, Teams Administrator or higher is required.

### Remediation:

#### To remediate using the UI:

1. Navigate to Microsoft Teams admin center <https://admin.teams.microsoft.com>.
2. Click to expand Teams apps select Manage apps.
3. In the upper right click Actions > Org-wide app settings.
4. For Microsoft apps set Let users install and use available apps by default to On or less permissive.
5. For Third-party apps set Let users install and use available apps by default to Off.
6. For Custom apps set Let users install and use available apps by default to Off.
7. For Custom apps set Upload custom apps for personal use to Off.

### Default Value:

Microsoft apps: On

Third-party apps: On

Custom apps: On

### References:

1. <https://learn.microsoft.com/en-us/microsoftteams/app-centric-management>
2. <https://learn.microsoft.com/en-us/defender-office-365/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#disabling-third-party-custom-apps>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.5 Allowlist Authorized Software</b> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	<b>2.7 Utilize Application Whitelisting</b> Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

# Not Monitoring Suspicious Sign-In Activity and Audit Logs

- Entra ID Sign in logs
- Entra ID Audit logs
- Defender logs
- Office 365 unified logs
- Azure activity logs
- Diagnostic logs

# Kontakt, další spolupráce

Healtchecky, konzultace, pentesty, red teaming, security tuning:

Emailem na: [lubomir@osmera.tech](mailto:lubomir@osmera.tech)

<https://www.lubomirosmerna.cz/securitytuning/>

Kurzy:

Zabezpečení cloudového prostředí Microsoft – 2 dny intenzivní praktický workshop dotovaný z 82 % přes MPSV. **Nutnost přihlášení nejpozději do 3. 7. 2025**  
<https://www.uradprace.cz/vyhledani-rekvalifikacniho-kurzu#/rekvalifikacni-kurz-detail/15843>

Hacking and pentesting Azure – 5 denní kurz obsahující ukázky útoků na MS cloud a obranu proti nim  
[https://www.gopas.cz/microsoft-azure-hacking-a-penetracni-testovani\\_goc238](https://www.gopas.cz/microsoft-azure-hacking-a-penetracni-testovani_goc238)

Bezpečnost hybridního prostředí Microsoft – 5 denní komplexní kurz zaměřený na zabezpečení MS hybridního prostředí  
[https://www.gopas.cz/microsoft-365-bezpecnost-hybridniho-prostredi\\_goc215](https://www.gopas.cz/microsoft-365-bezpecnost-hybridniho-prostredi_goc215)

# Zdroje

- Learn.microsoft.com
- Altered security courses
- Janbakker.com
- Blog.admindroid.com
- Medium.com
- [hub.trimarcsecurity.com](https://hub.trimarcsecurity.com)
- Penetration Testing Azure for Ethical Hackers, author David Okeyode, Karl Fosaaen
- Microsoft Azure Security Technologies Certification and Beyond, author David Okeyode
- Cybersecurity - Attack and Defense Strategies - Second Edition, author Diogenes Yuri