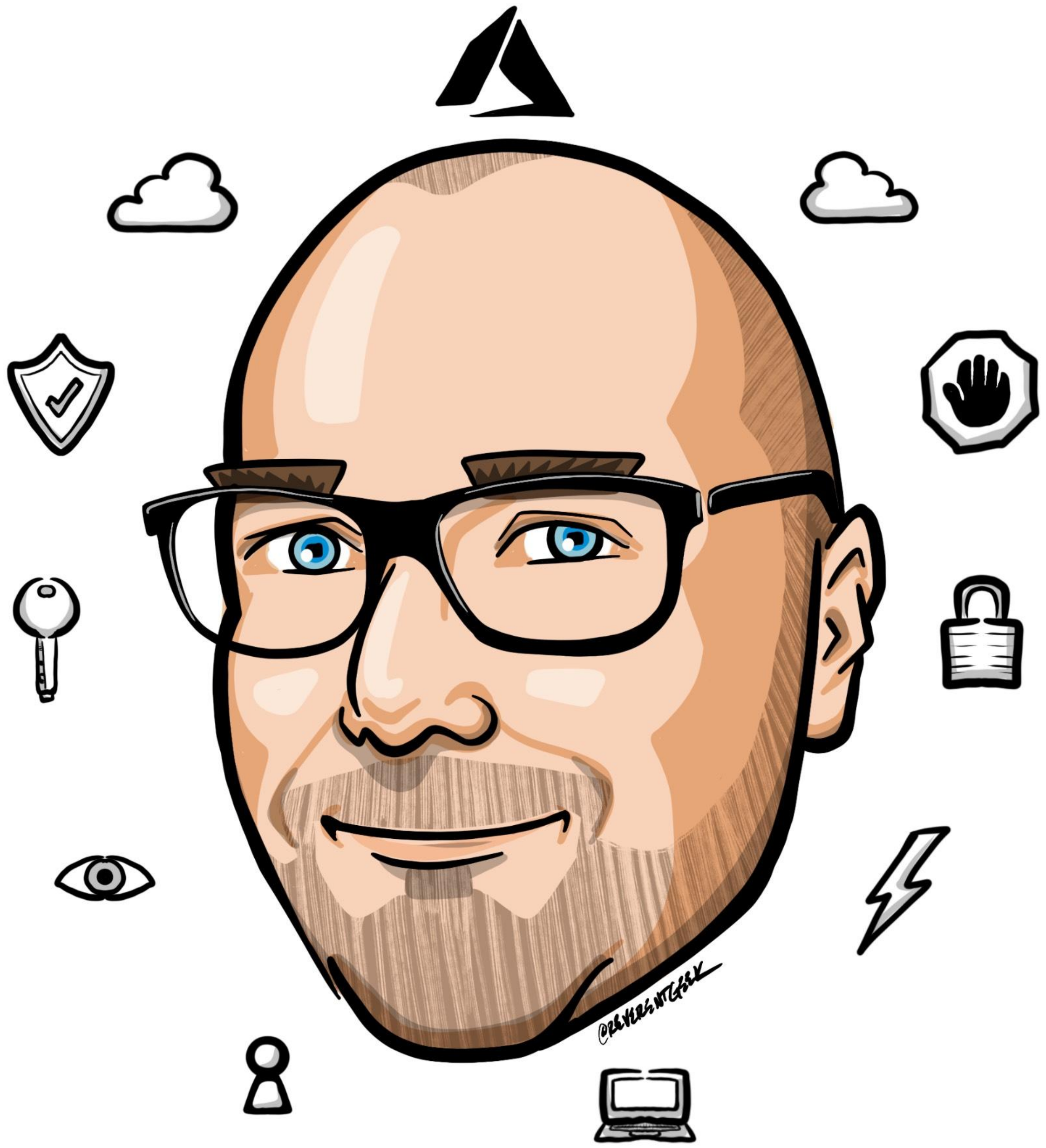
Microsoft

Secure Azure OpenAI at scale with custom policies

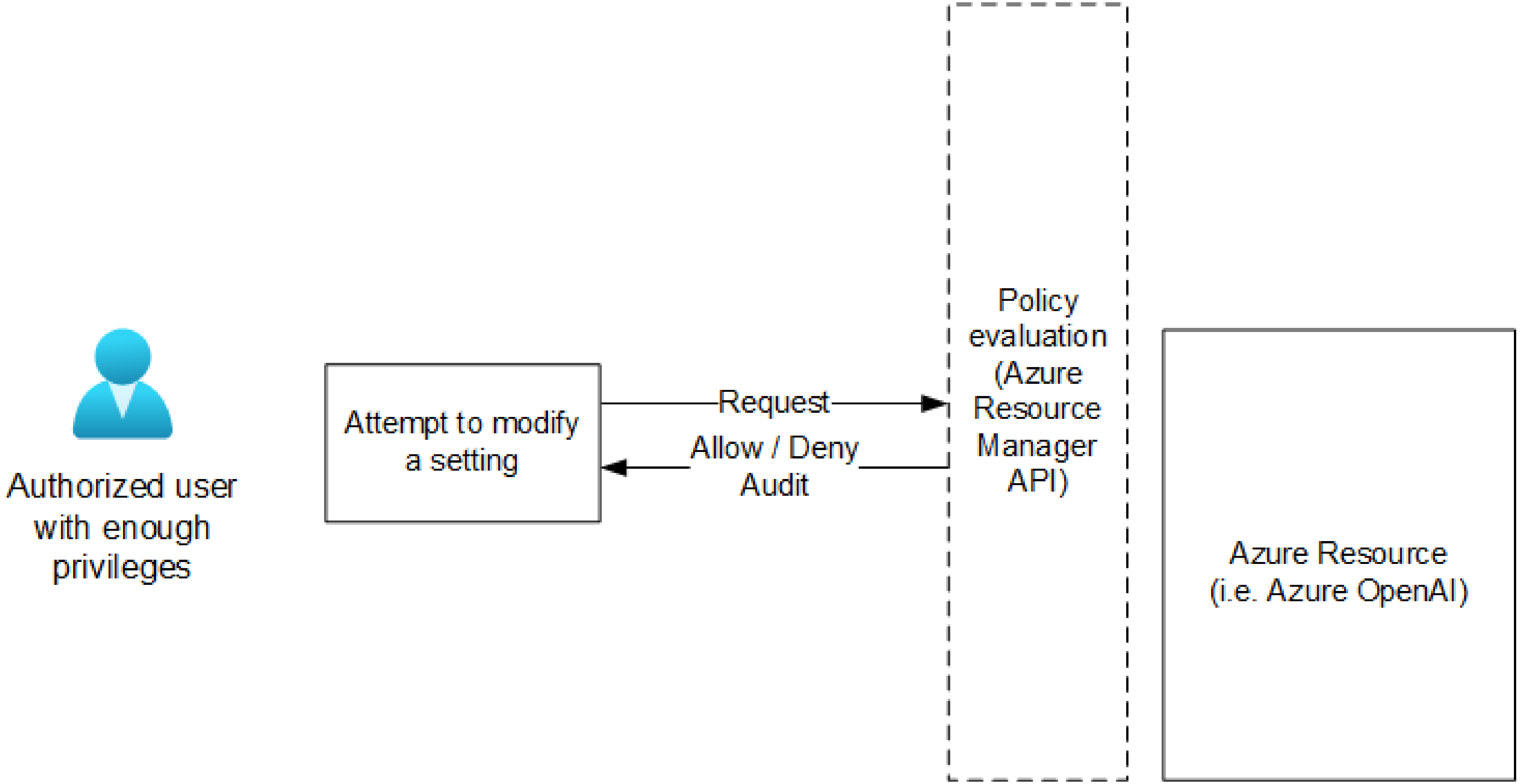
Karl Ots, EPAM Systems

Karl Ots

Head of Cloud Security @ EPAM
Microsoft RD & Security MVP



Azure Policies – native security guardrails

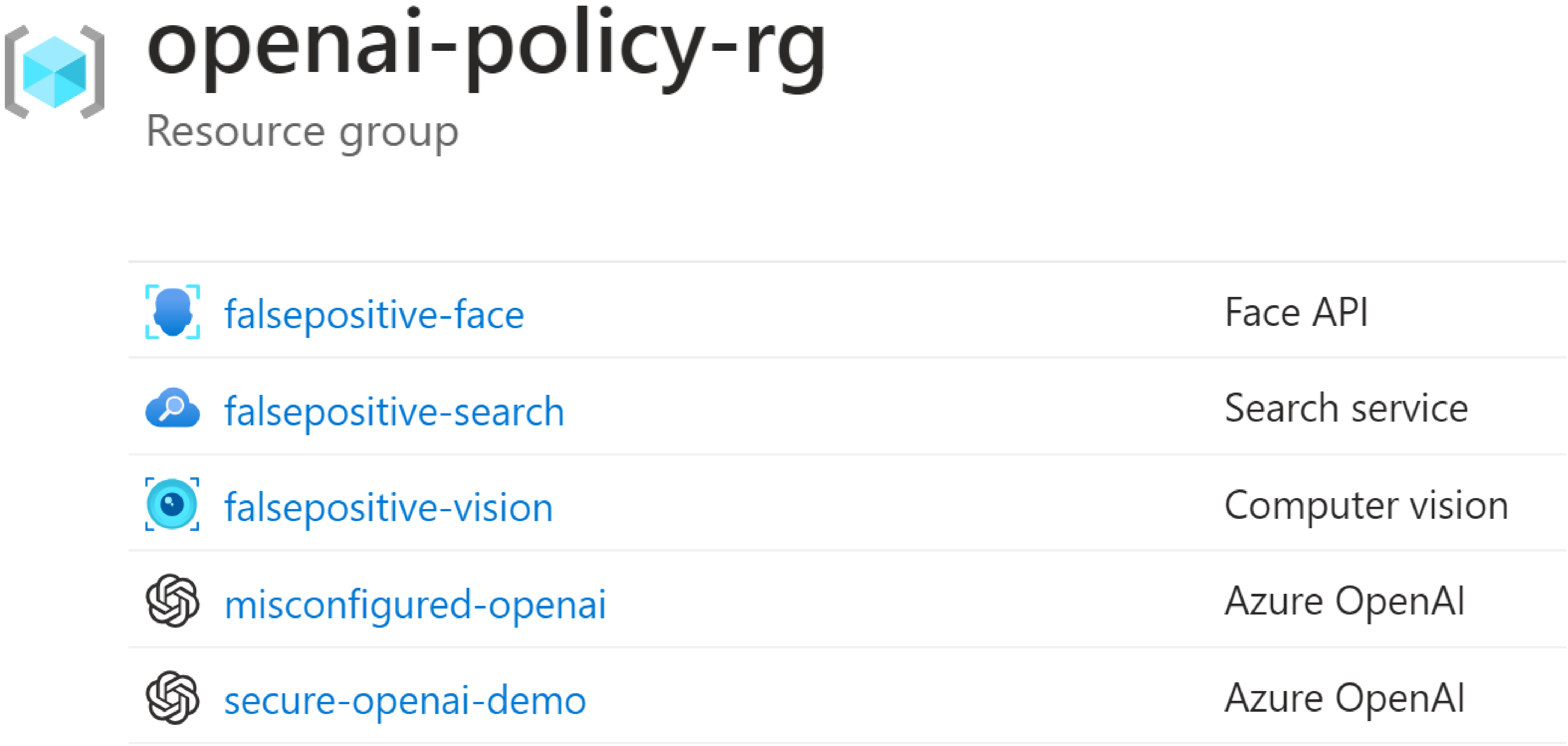

Authorized user with enough privileges
Attempt to modify a setting
Request
Allow / Deny Audit
Policy evaluation (Azure Resource Manager API)
Azure Resource (i.e. Azure OpenAI)

Azure Policies for Azure OpenAI

- There are no exclusive built-in policies for Azure OpenAI
- Many Microsoft.CognitiveServices policies are applicable – but beware of false positives
- Policy aliases are under Microsoft.CognitiveServices

Applicable built-in policies

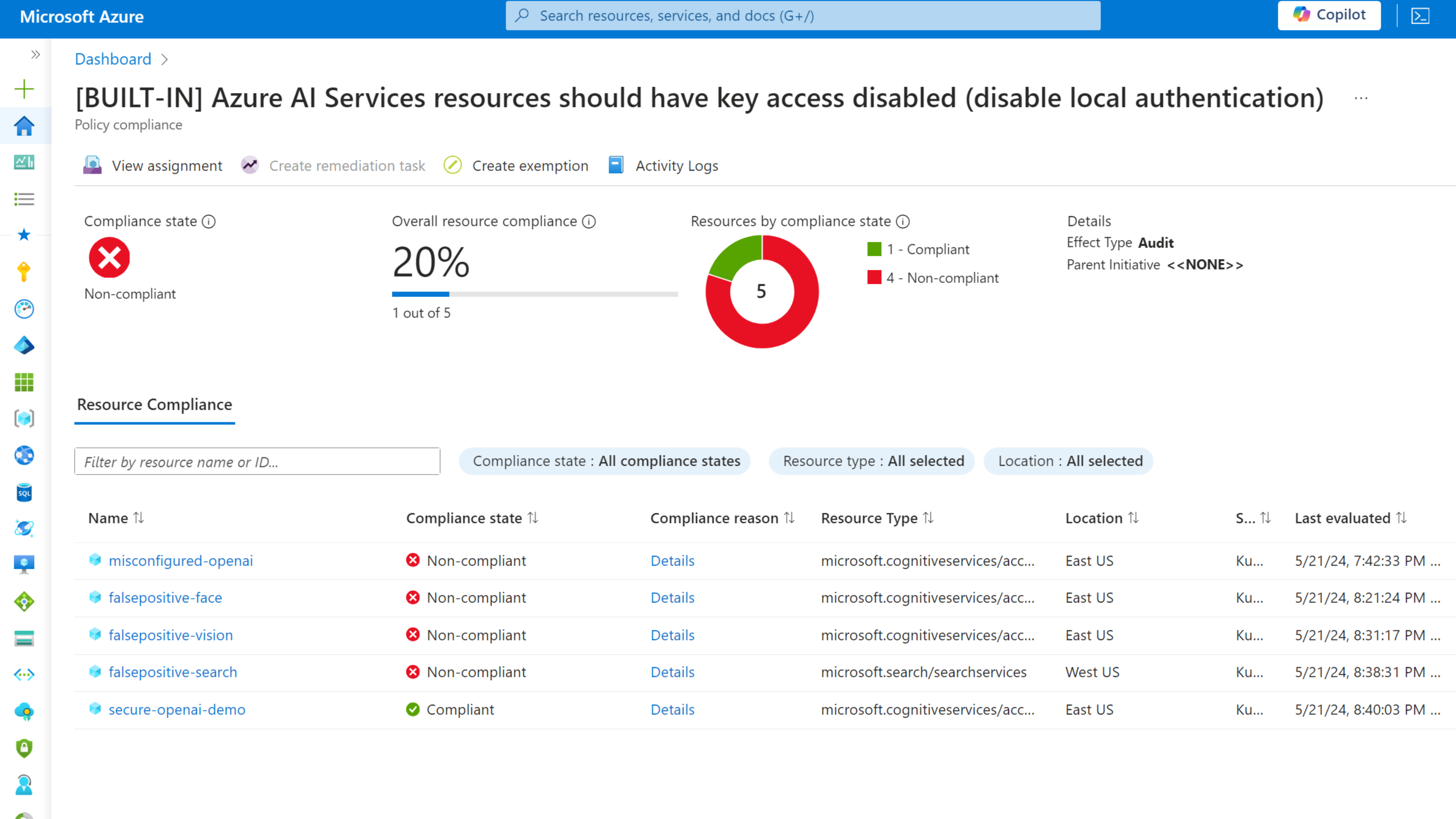
- Cognitive Services accounts should restrict network access
- Cognitive Services accounts should have local authentication methods disabled
- Cognitive Services accounts should enable data encryption with a customer-managed key
- Cognitive Services accounts should use a managed identity



openai-policy-rg

Resource group

falsepositive-face	Face API
falsepositive-search	Search service
falsepositive-vision	Computer vision
misconfigured-openai	Azure OpenAI
secure-openai-demo	Azure OpenAI



[BUILT-IN] Azure AI Services resources should have key access disabled (disable local authentication)

Policy compliance

Compliance state ⓘ

Non-compliant

Overall resource compliance ⓘ

20%

1 out of 5

Resources by compliance state ⓘ

🟩 1 - Compliant

🟥 4 - Non-compliant

Details

Effect Type **Audit**

Parent Initiative **<<NONE>>**

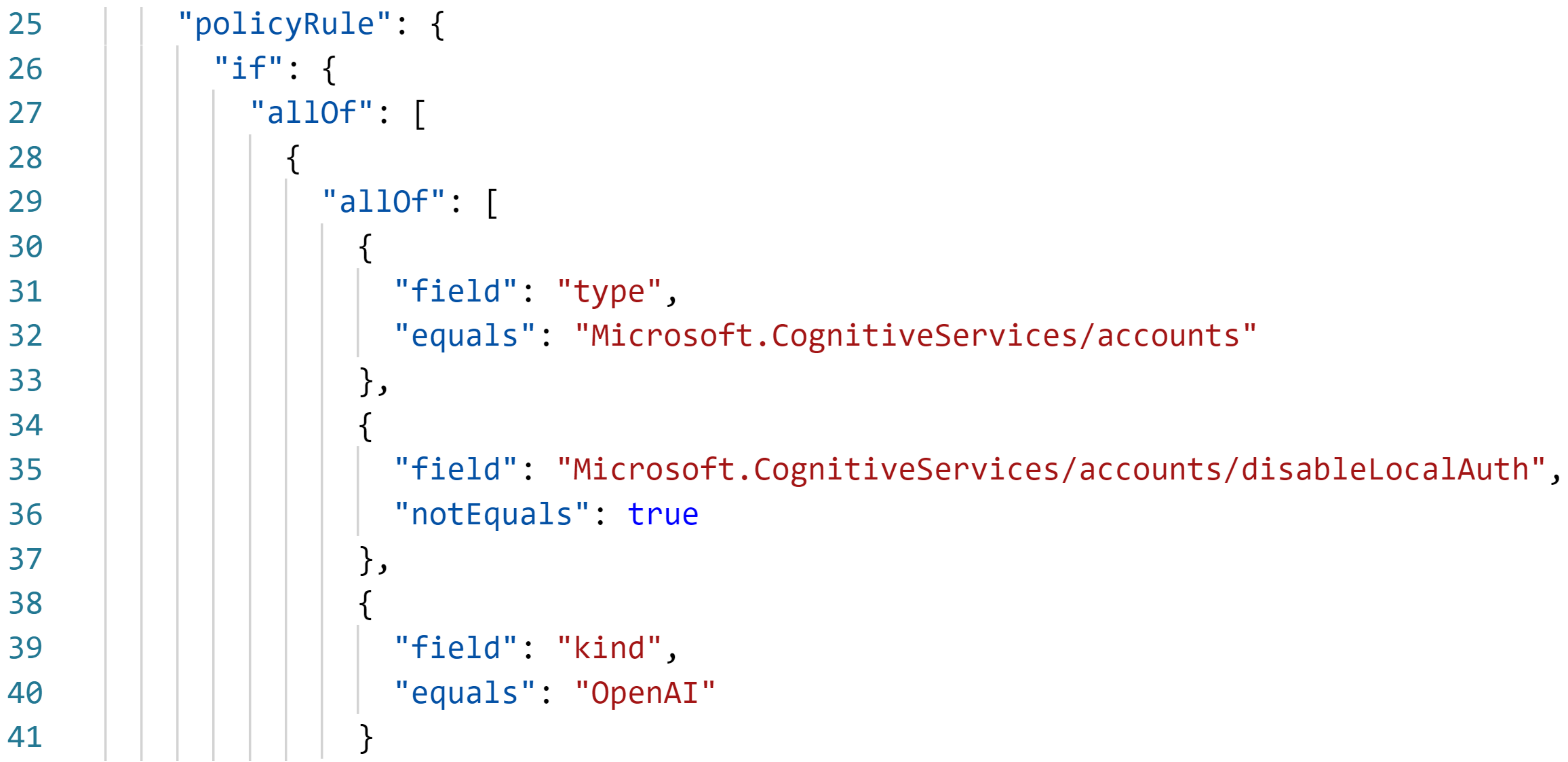
Resource Compliance

Compliance state : **All compliance states**

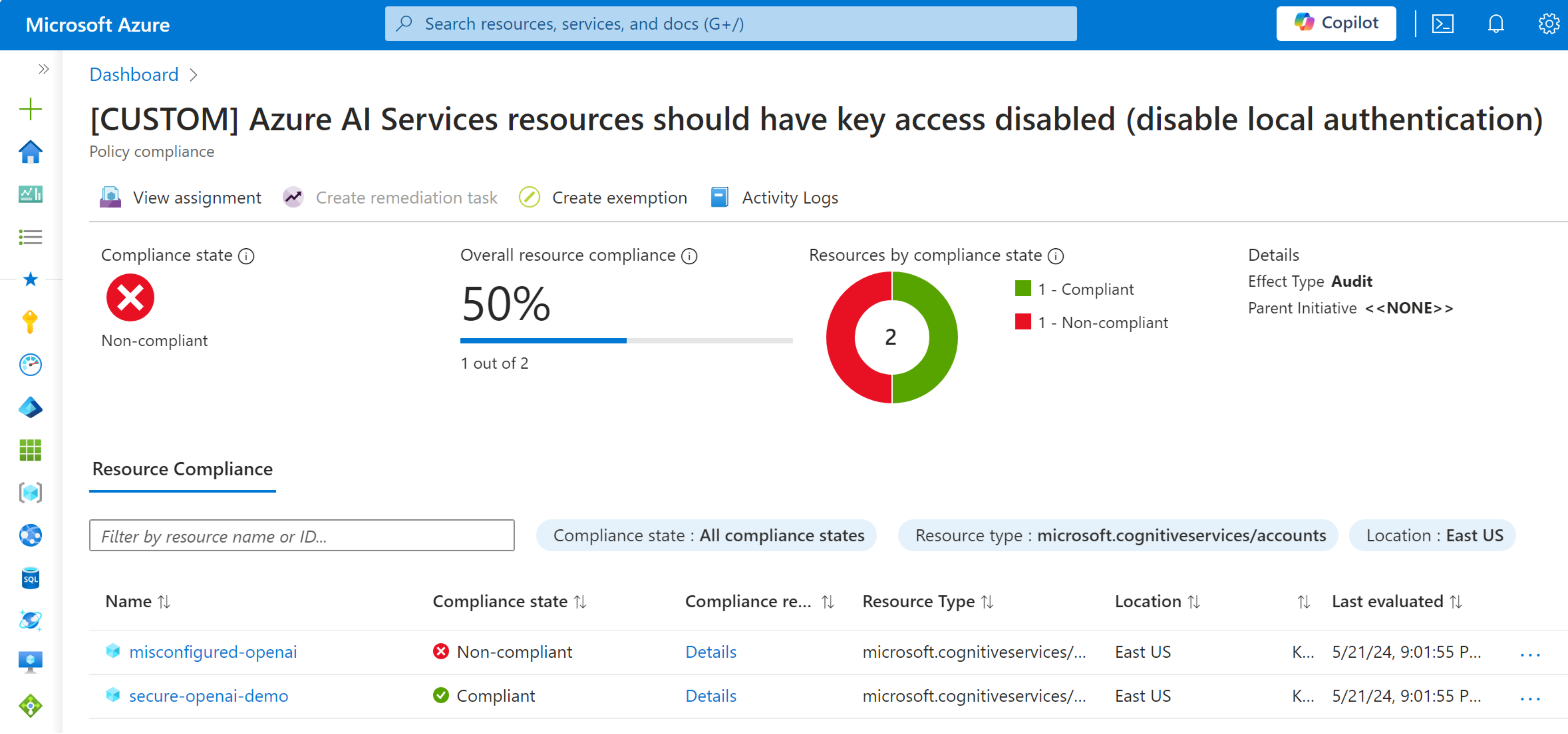
Resource type : **All selected**

Location : **All selected**

Name	Compliance state	Compliance reason	Resource Type	Location	S...	Last evaluated
misconfigured-openai	Non-compliant	Details	microsoft.cognitiveservices/acc...	East US	Ku...	5/21/24, 7:42:33 PM ...
falsepositive-face	Non-compliant	Details	microsoft.cognitiveservices/acc...	East US	Ku...	5/21/24, 8:21:24 PM ...
falsepositive-vision	Non-compliant	Details	microsoft.cognitiveservices/acc...	East US	Ku...	5/21/24, 8:31:17 PM ...
falsepositive-search	Non-compliant	Details	microsoft.search/searchservices	West US	Ku...	5/21/24, 8:38:31 PM ...
secure-openai-demo	Compliant	Details	microsoft.cognitiveservices/acc...	East US	Ku...	5/21/24, 8:40:03 PM ...



```
      "policyRule": {
        "if": {
          "allOf": [
            {
              "allOf": [
                {
                  "field": "type",
                  "equals": "Microsoft.CognitiveServices/accounts"
                },
                {
                  "field": "Microsoft.CognitiveServices/accounts/disableLocalAuth",
                  "notEquals": true
                },
                {
                  "field": "kind",
                  "equals": "OpenAI"
                }
```



[CUSTOM] Azure AI Services resources should have key access disabled (disable local authentication)

Policy compliance

Compliance state ⓘ

☒ Non-compliant

Overall resource compliance ⓘ

50%

1 out of 2

Resources by compliance state ⓘ

2

🟩 1 - Compliant

🟥 1 - Non-compliant

Details

Effect Type **Audit**

Parent Initiative **<<NONE>>**

Resource Compliance

Filter by resource name or ID...

Compliance state : **All compliance states**

Resource type : **microsoft.cognitiveservices/accounts**

Location : **East US**

Name ⇅	Compliance state ⇅	Compliance re... ⇅	Resource Type ⇅	Location ⇅	⇅	Last evaluated ⇅	
misconfigured-openai	☒ Non-compliant	Details	microsoft.cognitiveservices/...	East US	K...	5/21/24, 9:01:55 P...	...
secure-openai-demo	✓ Compliant	Details	microsoft.cognitiveservices/...	East US	K...	5/21/24, 9:01:55 P...	...

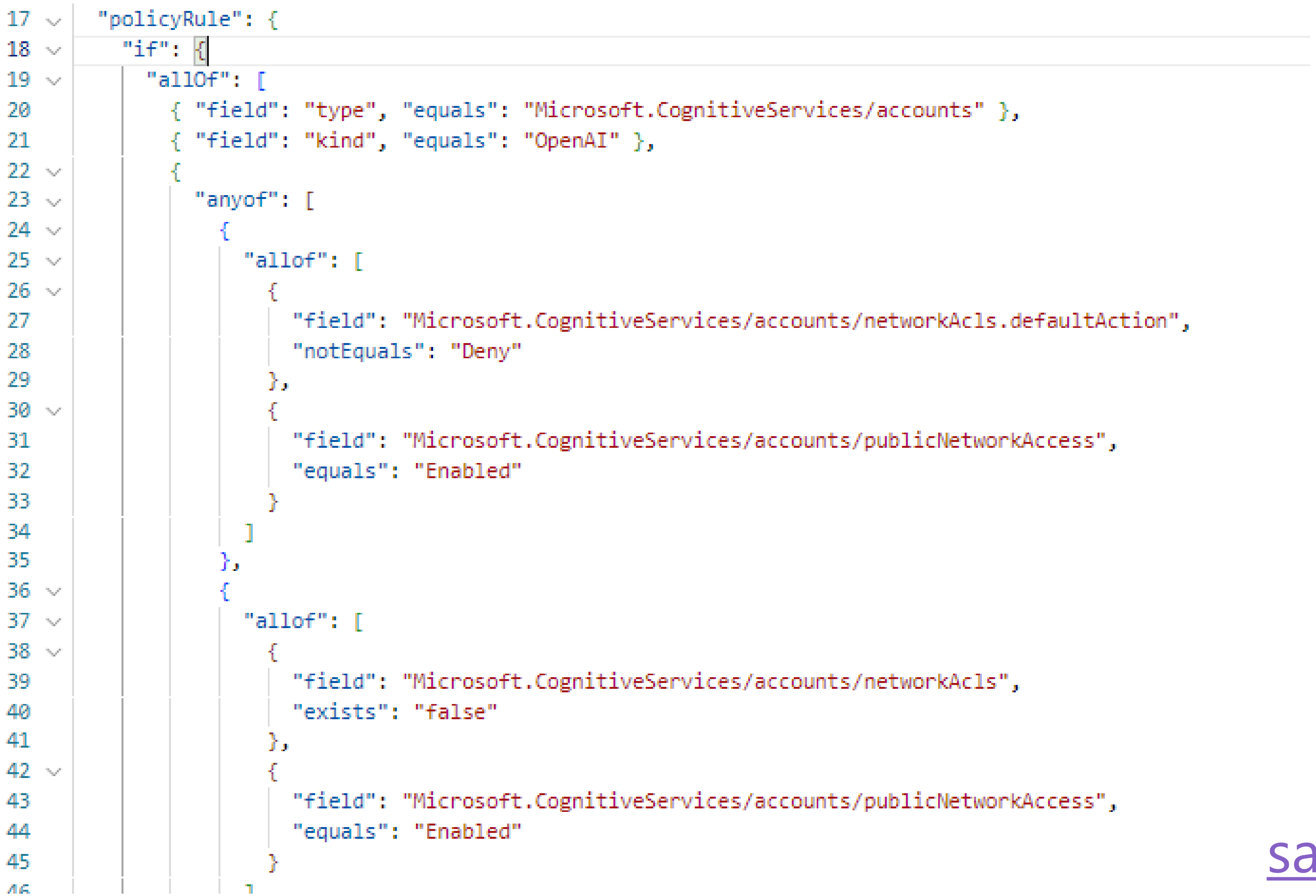
Community policies

- Good community effort starting, shared in Azure Community Policy GitHub!
- These extend Microsoft.CognitiveServices policies to close the feature gap to other Microsoft AI products.

Warning! These are NOT Built-in policies hence are not tested or validated in any form by the Azure Policy Release Team. Please be wary of this and always TEST your policies before enforcing

github.com/Azure/Community-Policy

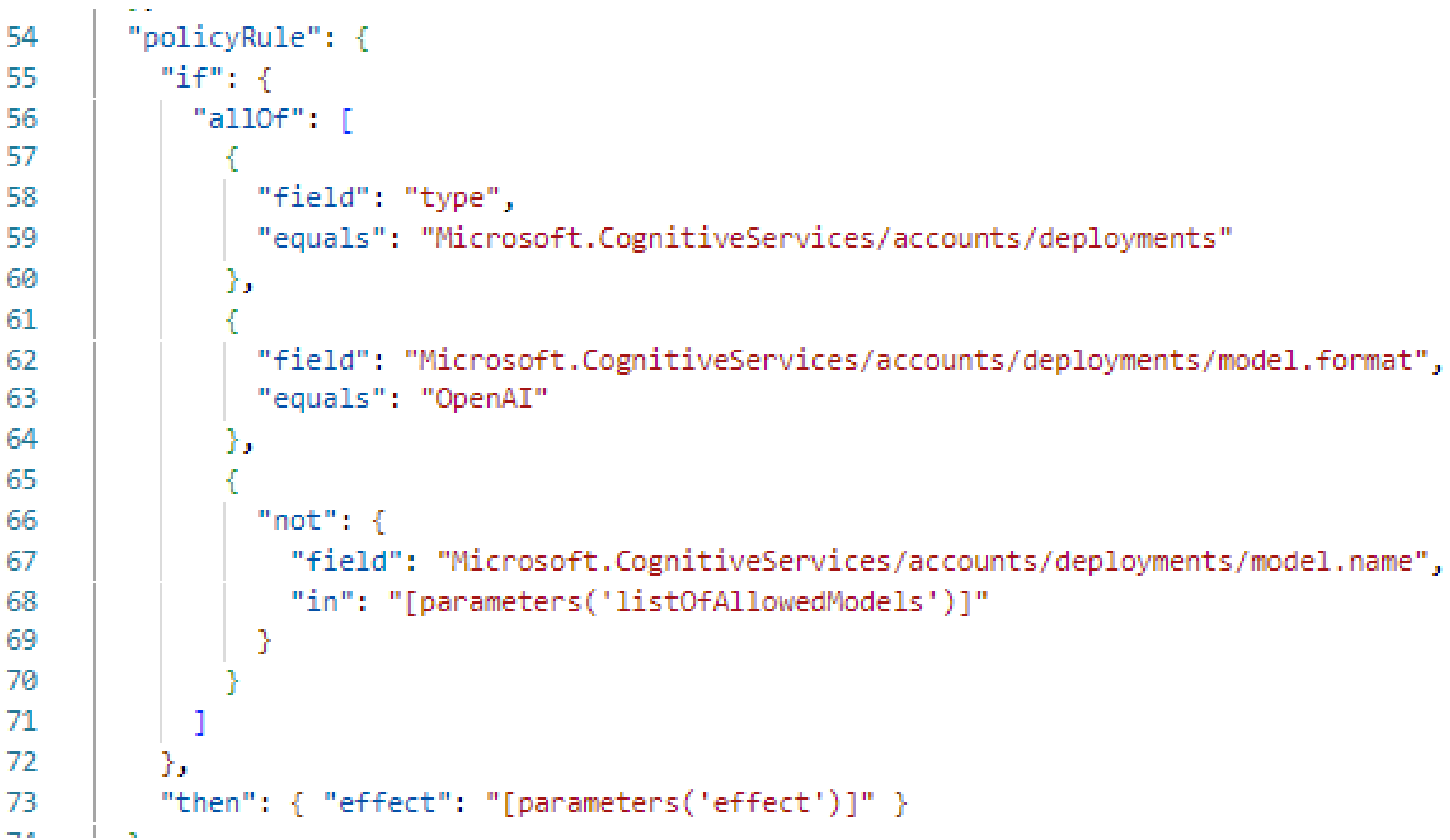
Audit OpenAI instances public access enabled



```
"policyRule": {
  "if": {
    "allOf": [
      { "field": "type", "equals": "Microsoft.CognitiveServices/accounts" },
      { "field": "kind", "equals": "OpenAI" },
      {
        "anyof": [
          {
            "allof": [
              {
                "field": "Microsoft.CognitiveServices/accounts/networkAcls.defaultAction",
                "notEquals": "Deny"
              },
              {
                "field": "Microsoft.CognitiveServices/accounts/publicNetworkAccess",
                "equals": "Enabled"
              }
            ]
          },
          {
            "allof": [
              {
                "field": "Microsoft.CognitiveServices/accounts/networkAcls",
                "exists": "false"
              },
              {
                "field": "Microsoft.CognitiveServices/accounts/publicNetworkAccess",
                "equals": "Enabled"
              }
            ]
```

sarajoshi@Github

Permit only approved OpenAI models



```
  "policyRule": {
    "if": {
      "allOf": [
        {
          "field": "type",
          "equals": "Microsoft.CognitiveServices/accounts/deployments"
        },
        {
          "field": "Microsoft.CognitiveServices/accounts/deployments/model.format",
          "equals": "OpenAI"
        },
        {
          "not": {
            "field": "Microsoft.CognitiveServices/accounts/deployments/model.name",
            "in": "[parameters('listOfAllowedModels')]"
          }
        }
      ]
    },
    "then": { "effect": "[parameters('effect')]" }
```

techlake@Github

Cloud Security Benchmark for Azure OpenAI (7/35)

Data Protection	DP-2	Monitor anomalies and threats targeting sensitive data	Data Leakage/Loss Prevention
Data Protection	DP-5	Use customer-managed key option in data at rest encryption when required	Data at Rest Encryption Using CMK
Data Protection	DP-6	Use a secure key management process	Key Management in Azure Key Vault
Identity Management	IM-8	Restrict the exposure of credential and secrets	Secrets Support Integration and Storage in Azure Key Vault
Logging and threat detection	LT-4	Enable network logging for security investigation	Azure Resource Logs
Network Security	NS-2	Secure cloud services with network controls	Disable Public Network Access
Network Security	NS-2	Secure cloud services with network controls	Azure Private Link

Related sessions

	Session code	Title
Breakout	BRK225	Secure your AI application transformation with Microsoft Security
	BRK134	Take an Azure OpenAI chat application from PoC to enterprise-ready
Demo Session	DEM763	Securing AI Workloads with Microsoft Purview Sensitivity Labels

Thank you!

- Sample code at github.com/karlgots/openai
- Stop by the Expert Meet-up to get your questions answered
- Your feedback is important! Visit https://aka.ms/MicrosoftBuildEvals to complete your session evaluations

Microsoft