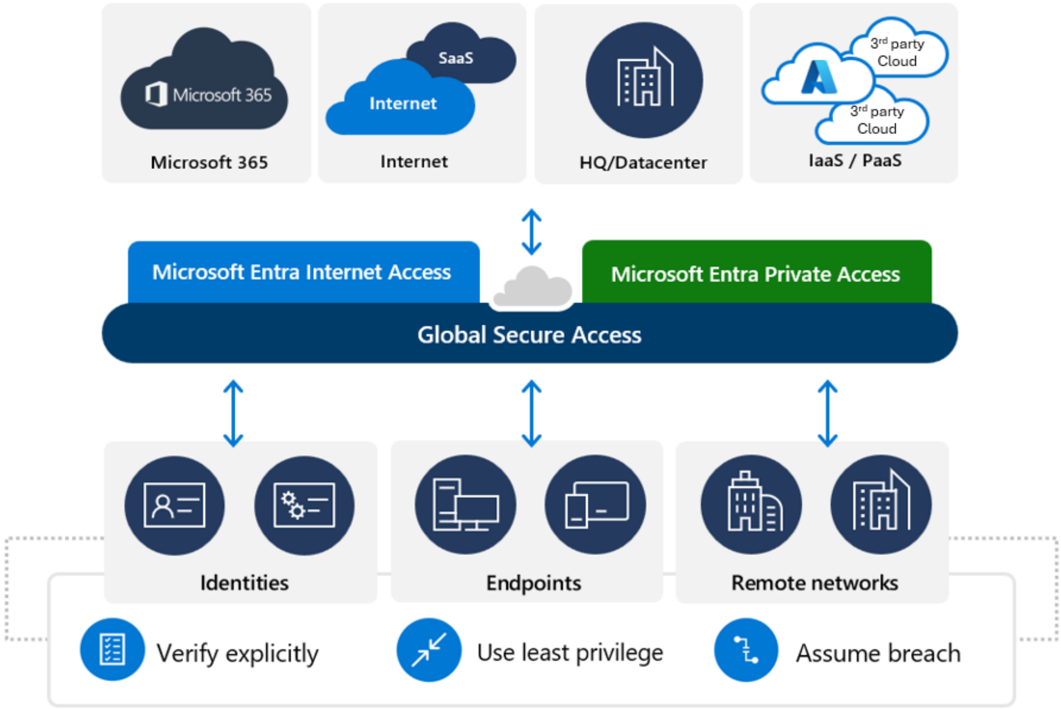
IAM Cheat Sheet | SC-900 Notes

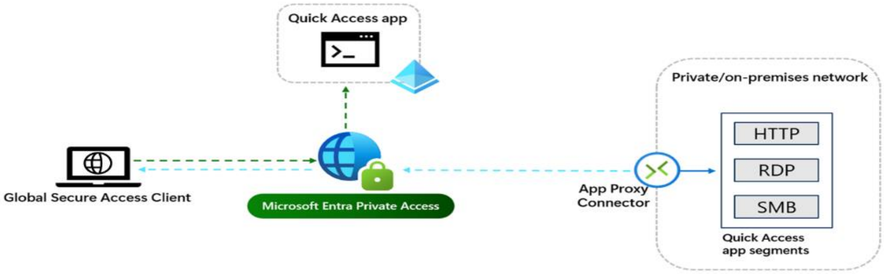
Conditional Access policy (MSFT Entra) – Resources:

- Conditional Access
- Grant controls in Conditional Access policy
- Session controls in Conditional Access policy

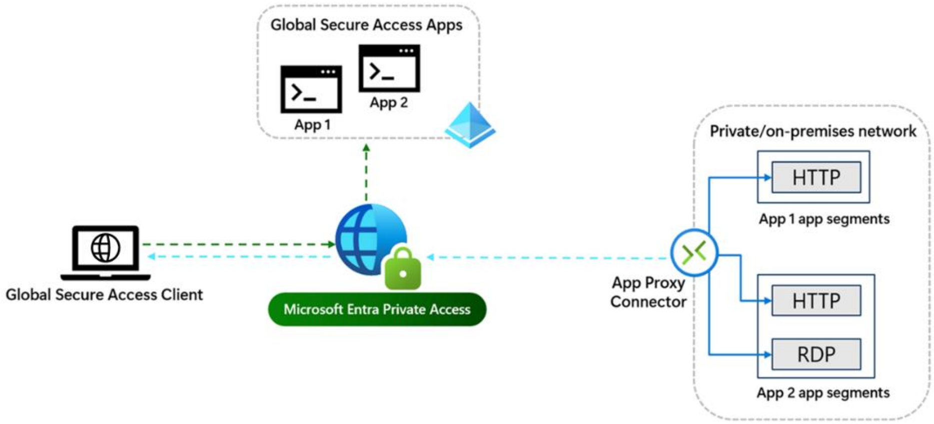
MSFT Global Secure Access – combines Internet & Private access, which creates a new network security category called Security Service Edge (SSE)



Quick App:


Quick Access app
Global Secure Access Client
Microsoft Entra Private Access
App Proxy Connector
Private/on-premises network
HTTP
RDP
SMB
Quick Access app segments

Access app (Per-app):

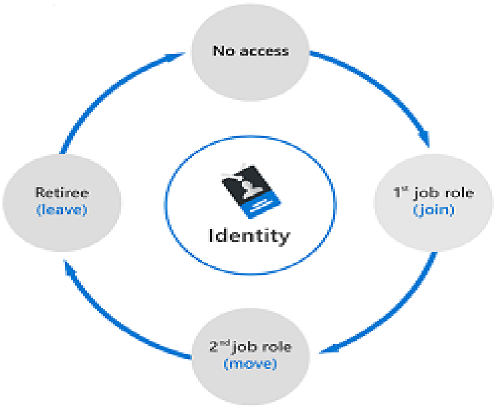

Global Secure Access Apps
App 1
App 2
Private/on-premises network
HTTP
App 1 app segments
Global Secure Access Client
Microsoft Entra Private Access
App Proxy Connector
HTTP
RDP
App 2 app segments

Entra ID Governance: ability to do these tasks

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.
- [What is Microsoft Entra ID Governance?]

It's intended to help organizations address these **four key questions**:

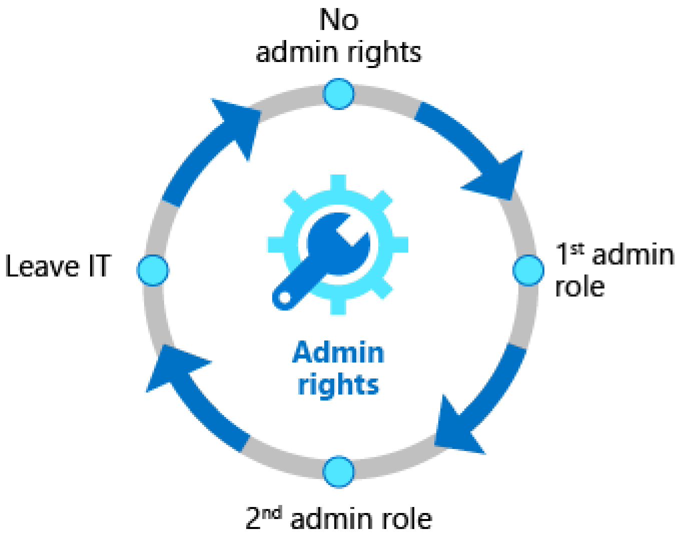
- Which users should have access to which resources?
- What are those users doing with that access?
- Are there effective organizational controls for managing access?
- Can auditors verify that the controls are working?



Privileged Identity Mgmt:

- PIM helps minimize the # of ppl who have access to resources across Entra ID, Azure & other MSFT online services

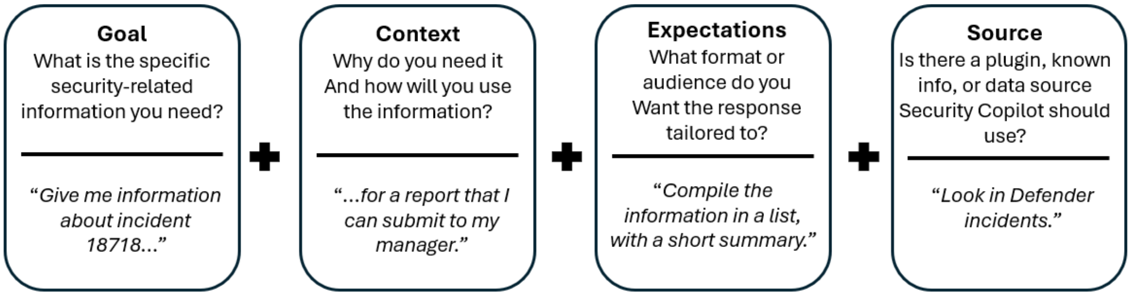
- Microsoft Entra Privileged Identity Management



Microsoft Security Copilot:

Effectiveness of prompts

- Goal - specific, security-related information that you need
- Context - why you need this information or how you'll use it
- Expectations - format or target audience you want the response tailored to
- Source - known information, data sources, or plugins Copilot should use



Goal
What is the specific security-related information you need?

"Give me information about incident 18718..."

➕

Context
Why do you need it And how will you use the information?

"...for a report that I can submit to my manager."

➕

Expectations
What format or audience do you Want the response tailored to?

"Compile the information in a list, with a short summary."

➕

Source
Is there a plugin, known info, or data source Security Copilot should use?

"Look in Defender incidents."

"Give me a list of entities involved" "including a list of known indicators of compromise and tools, tactics, and procedures (TTPs)" ← Good to prompt after your initial request.

SCUs Security Compute Units

Azure Virtual Network (VNet) - enables network segmentation allowing creation of multiple vns per region and multiple subnets within each of those vns

Network Security Group (NSG) - used to filter inbound/outbound traffic to Azure resources in a VNet

Web App Firewall (WAF) - provides centralized protection of your web apps form exploits and vulnerabilities. Patches known weaknesses w/o having to secure each app.

Azure Bastion - a deployable service allowing connection to a VM through your browser and the azure portal. Protecting against exposing RDP/SSH to the outside world. (Remote Desktop Protocol/Secure Shell)

Azure Key Vault - cloud service for securely storing and accessing secrets (ie. API keys, passwords, certificates, cryptographic keys)

Microsoft Defender for Cloud - a Cloud Native App Protection platform (CNAPP) designed with set security measures and best practices to protect cloud-based apps from various cyber threats and vulnerabilities. Unifies devSecOps mgmt, improves security posture, and protects cloud workloads.

Microsoft Defender XDR - enterprise defense suite that provides integrated protection against sophisticated attacks - that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications.

Policy definitions - Azure policy is a rule about specific security conditions that you want controlled

Security Initiatives - a collection of Azure Policy definitions, or rules, grouped together towards a specific goal or purpose.

Microsoft Sentinel - a cloud-native SIEM/SOAR solution (Security orchestration automated response) and threat intelligence across enterprise

Azure Logic Apps - used to automate workflows for example, when using ServiceNow it can automate a ticket each time a certain alert or incident occurs

MITRE ATT&CK® framework, a global database of adversary tactics and techniques

Workbooks - interactive visual reports for monitoring security data collected by Microsoft Sentinel

Microsoft Intune - device identity can be achieved by ensuring standards for security and compliance are met for (MDM) Mobile Device Mgmt

DATA SECURITY (MSFT PURVIEW)

Microsoft Purview (Info protection) – data protection through sensitivity labels and policies

- **Trainable classifiers** AI/ML for data classification pre-trained “ready to use” & custom
- **Sensitivity labels** act as watermarks or stickers (labeling & protection of content)

- **Label policies** enforce rules and where to/how to/when to directions
- **DLP policy –** the monitoring of activities users take on data at rest/in transit/in use
- **Insider Risk Mgmt –** policy/ insider alerts/ triage
- **Adaptive Protection –** ML to identify critical risks and proactively & dynamically apply protection controls from
    - DLP
    - MSFT Purview Data Lifecycle Mgmt
    - MSFT Entra Conditional Access

Data Loss Prevention (DLP) – detects risky behavior and prevent info from being shared inappropriately. **DLP policy** – identify, monitor, & auto protect sensitive items across M365 services, office apps, OS, cloud apps, on-prem file shares, and power BI

DATA COMPLIANCE (MSFT PURVIEW)

https://learn.microsoft.com/en-us/training/modules/describe-purview-risk-compliance-governance/1-introduction

- eDiscovery and Audit – process of identifying & delivering electronic info that can be used as evidence in legal cases
- Compliance Manager – helps assess and manage compliance across your multicloud environment
- Communication Compliance – insider risk solution that helps you detect, capture and act on inappropriate messages that can lead to data security/compliance incidents
- Data Lifecycle Management – tools and capabilities to retain need content and delete unneeded content
- Records Management -mgmt solution for reg., legal, & business-critical records across their corporate data.

DATA GOVERNANCE (MSFT PURVIEW)

https://learn.microsoft.com/en-us/training/modules/describe-purview-data-governance/1-introduction

Terraform with azure - https://click.linksynergy.com/link?id...
Powershell - https://click.linksynergy.com/link?id... -
Free cloud security training: https://www.varonis.com/free-security...

Access controls worksheet

	Note(s)	Issue(s)	Recomm
Authorization /authentication	**Objective:** Make 1-2 notes of information that can help identify the threat: - *Robert Taylor Jr. Legal attorney* - *10/03/2023 at 8:29 AM* - *Computer (Up2-NoGud) with an IP 152.207.255.255*	**Objective:** Based on your notes, list 1-2 authorization issues: - *The user has access to the admin profile which ultimately gives him access to finance.* - *His account shouldn't be active as an admin as his contract ended in 2019*	**Objective** recomme prevent th - *Us exp* - *The rou da use ens sep* - *En*