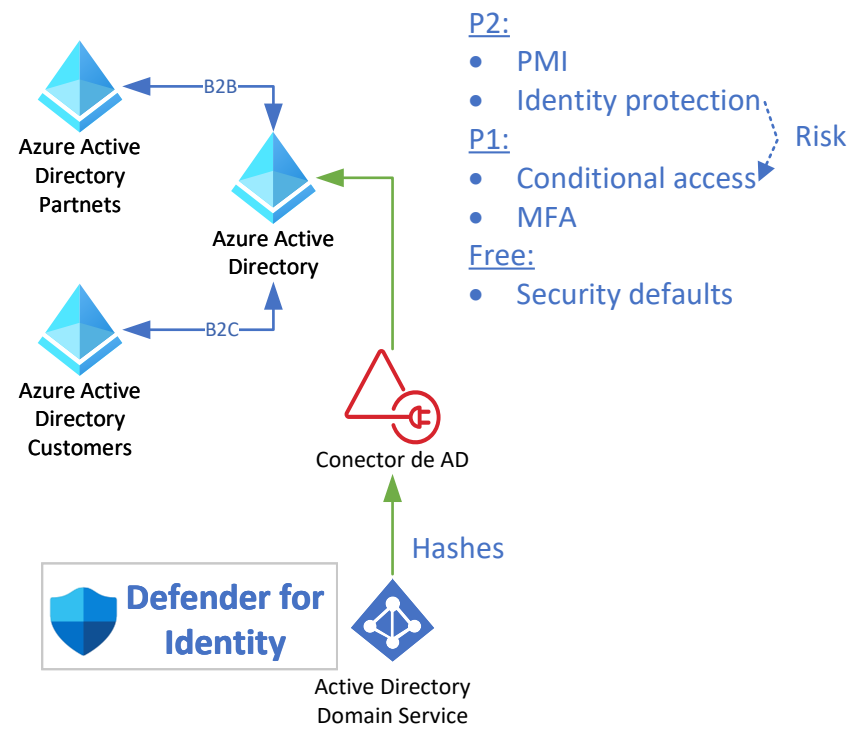


SC-100 STUDY CRAM

<https://onboardtoazure.com>



Identity



Zero Trust

- 1 – Verify explicitly
- 2 – Use least privilege
- 3 – Assume breach

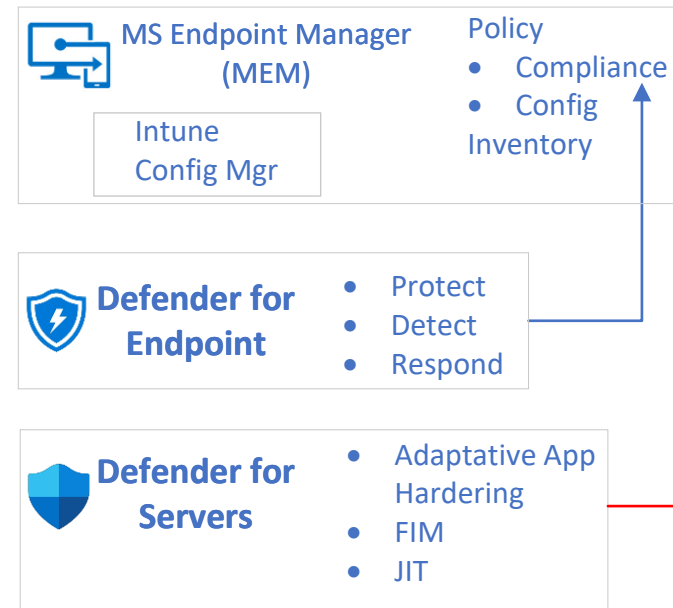
Least Privileges

- RBAC
- JIT
- AAD PIM (P2)
 - AAD Rules
 - ARM Rules
- PAM

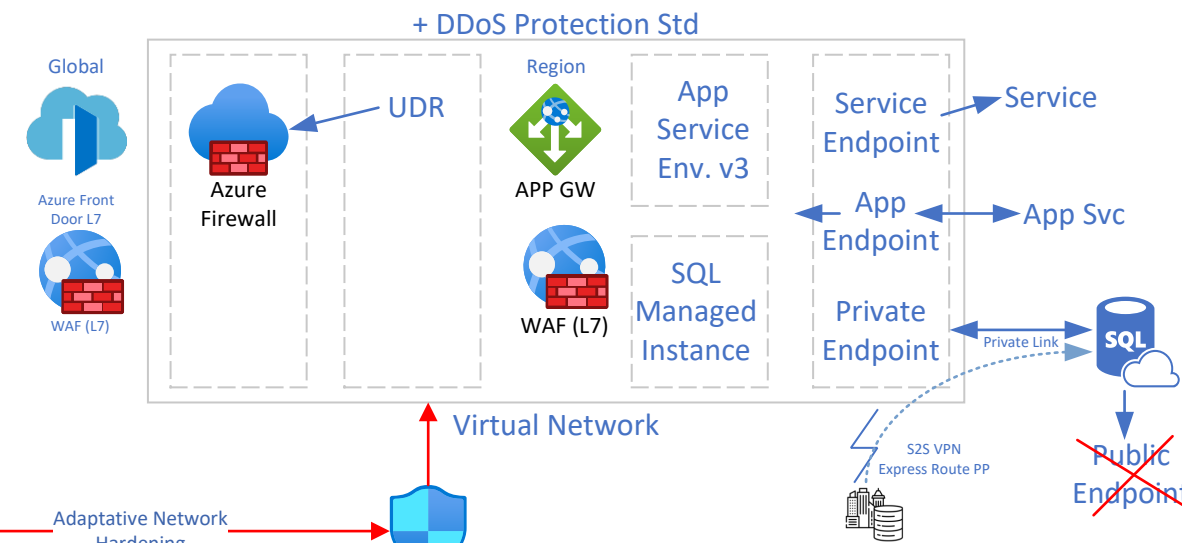
Azure Active Directory

Active Directory Domain Service Onpremise

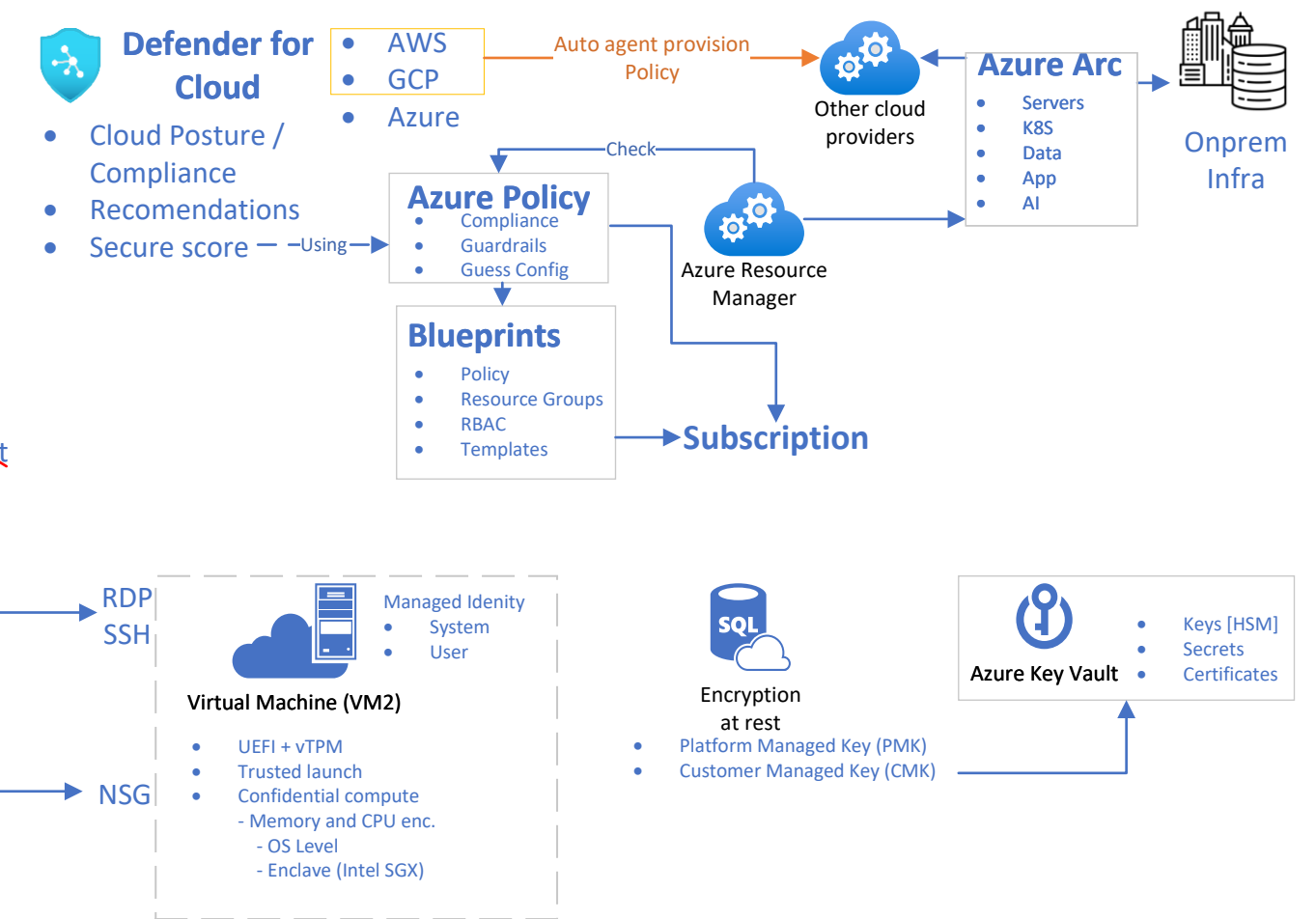
Endpoint



Network



Infrastructure



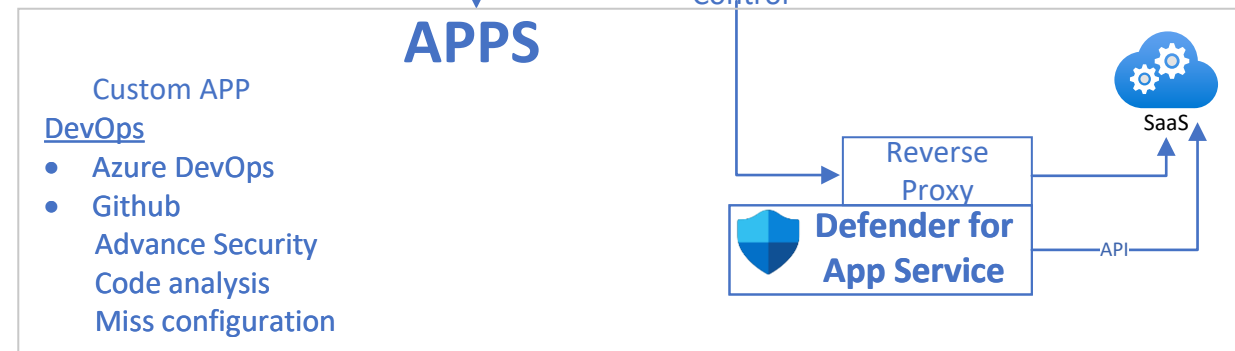
Signals

Context

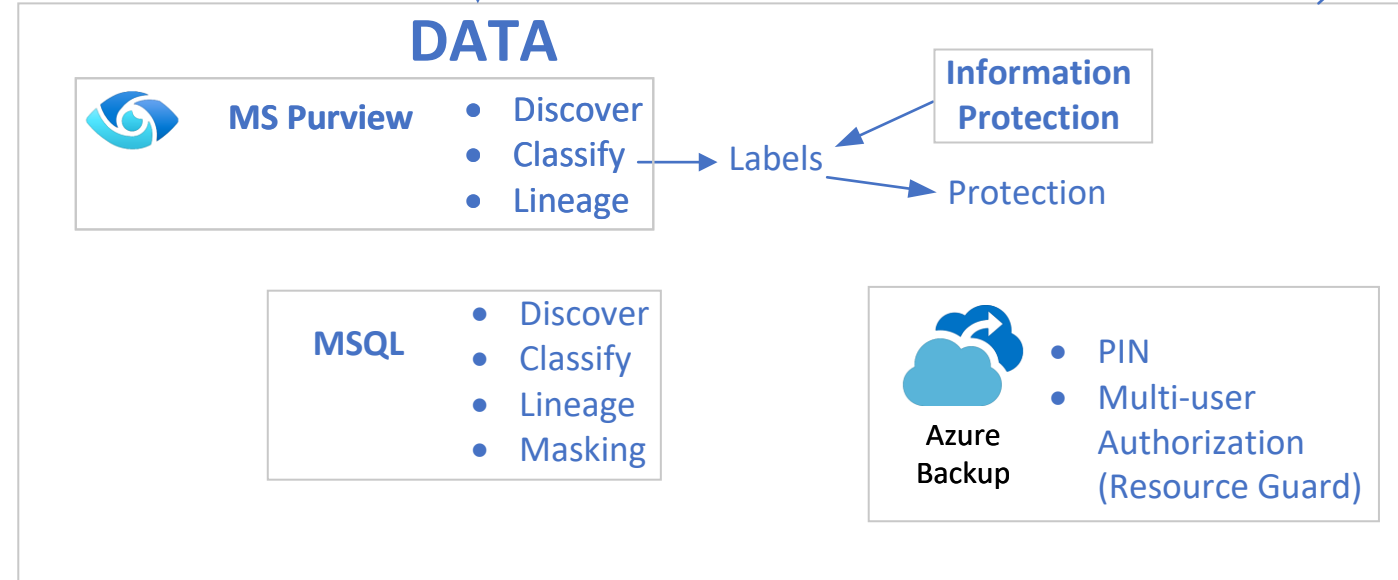
Azure Active Directory P1/P2

Conditional Access Control

APPS



DATA



1 - Collect

Connectors

- AAD
- O365
- Syslog
- FW
- ...

SIEM / SOAR

Azure Sentinel

Log Analytics Workspace

KQL

2 - Detect

Analytics

- Analytics
- Hunting
- Intelligence

Incidents

3 - Investigate

4 – Respond

- Automation Rules
- Playbook

Logic Apps