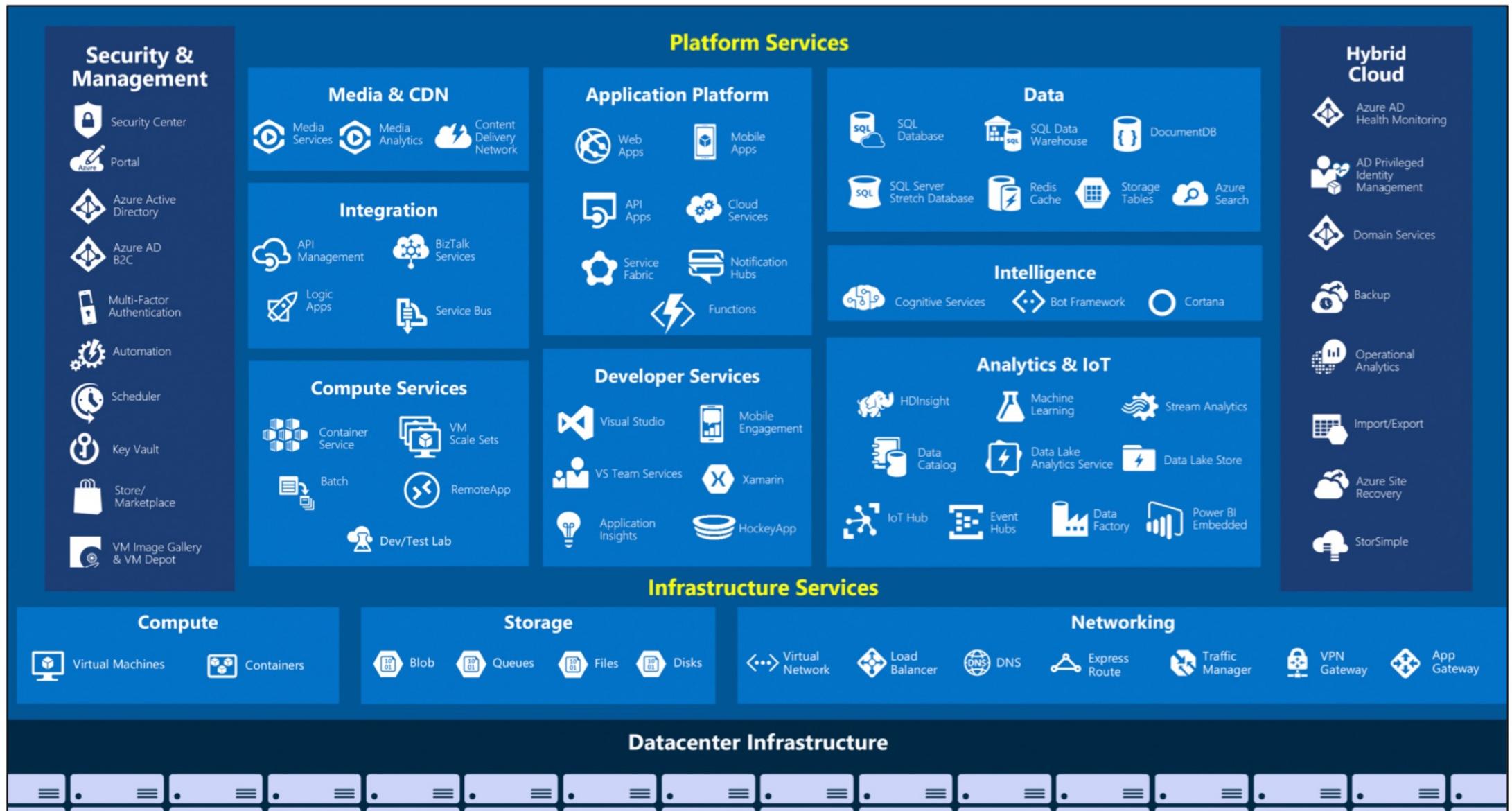


Tietoturva pilvipalveluissa: Azure

08/2021

Mitä Azure on?



Palvelumallit ja jaettu vastuu

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Microsoft	Microsoft	Customer	Customer
Application	Microsoft	Microsoft	Customer	Customer
Network controls	Microsoft	Microsoft	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

Microsoft Customer

Jaetun vastuun malli kuvailee miten vastuu jakautuu palveluntarjoajan ja käyttäjän välillä julkisilven palvelumalleissa.

Azuren tarjoamat palvelumallit ovat IaaS ja PaaS.

Riippumatta palvelumallista, käyttäjä vastaa aina vähintään seuraavista:

- Palveluun tallennettu tieto
- Identiteetit ja pääsynhallinta

“One of the only things that doesn’t appear to have changed significantly is the bad habits from cloud customers due to the poor understanding of the cloud security shared responsibility model”

- Cloud Security Alliance



Service Trust portal

Miten Microsoft toteuttaa oman osuutensa jaetun vastuun mallin periaatteista?

<https://servicetrust.microsoft.com>

- Auditointiraportit ja sertifikaatit
- Murtotestaukset ja haavoittuvuuskartoitukset
- White Paperit, FAQt, Compliance Guidet



SOC



FedRAMP



ISO 27001



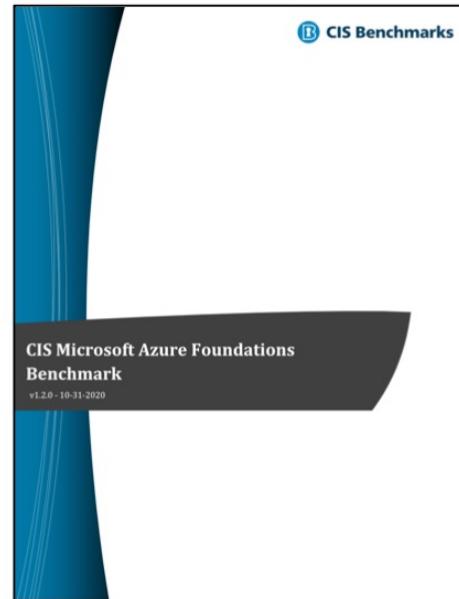
PCI/DSS

IaaS ja PaaS tietoturvan standardit ja referenssit



Azure Security Benchmark (V2)

- Security Controls (v2)
 - Overview of Azure security controls
 - Network security
 - Identity management
 - Privileged access
 - Data protection
 - Asset management
 - Logging and threat detection
 - Incident response
 - Posture and vulnerability management
 - Endpoint security
 - Backup and recovery
 - Governance and Strategy



SECURITY GUIDANCE

For Critical Areas of Focus
In Cloud Computing v4.0



Yleiset uhat ja haasteet



cloudsecurityalliance.org

Table of Contents

Acknowledgments	5
Executive Summary	6
1. Security Issue: Data Breaches	7
2. Security Issue: Misconfiguration and Inadequate Change Control	10
3. Security Issue: Lack of Cloud Security Architecture and Strategy	13
4. Security Issue: Insufficient Identity, Credential, Access and Key Management	16
5. Security Issue: Account Hijacking	20
6. Security Issue: Insider Threat	22
7. Security Issue: Insecure Interfaces and APIs	25
8. Security Issue: Weak Control Plane	28
9. Security Issue: Metastructure and Applistructure Failures	31
10. Security Issue: Limited Cloud Usage Visibility	35
11. Security Issue: Abuse and Nefarious Use of Cloud Services	38
Conclusion	41
Appendix: Methodology	42
About Our Sponsor	43

82% of companies unknowingly give 3rd parties access to all their cloud data

Shir Tamari, Head of Research | January 14, 2021 | Research



TL;DR

Cloud identity permissions are complex. So complex, that innocent looking permissions provided to 3rd party vendors can lead to unintended exposure of all of your data. The Wiz Research team conducted extensive research of permissions provided to 3rd party vendors in cloud environments and the results should be a wake-up call:

wiz.io

Resurssien organisointi tietoturvallisen hallinnan ytimessä

Azure tarjoaa neljään erilaiseen tasoon perustuvan hierarkian, jonka avulla pilven resurssit ja palvelut organisoidaan:

Management group

- Luo ryhmää pääsynhallinnan, tietoturvan ja policyjen periytymisen hallintaa varten.

Subscription

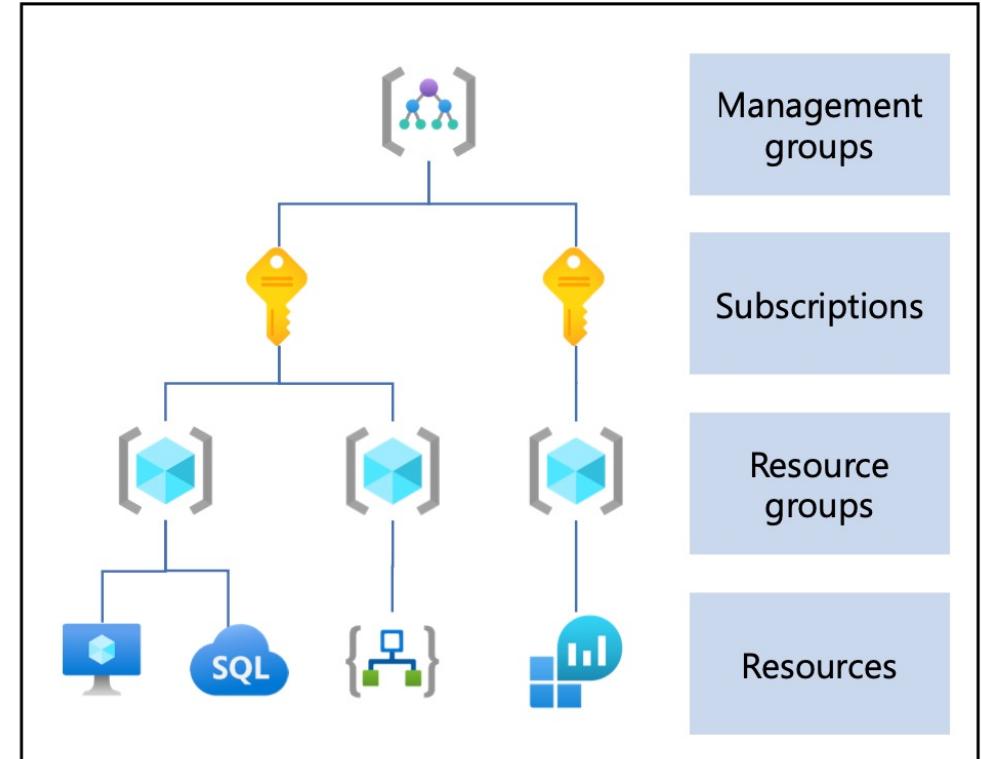
- Luo rajoitetun alueen tietyyn tyyppisille resursseille, joita yhdistää esimerkiksi sama omistajuus ja samat hallintaperiaatteet.

Resource group

- Luo loogisen säiliön tietyin rajatun kokonaisuuden resursseille, joilla on yleensä sama elinkaari. Esimerkiksi yksittäisen sovelluksen tarvitsemat resurssit.

Resource

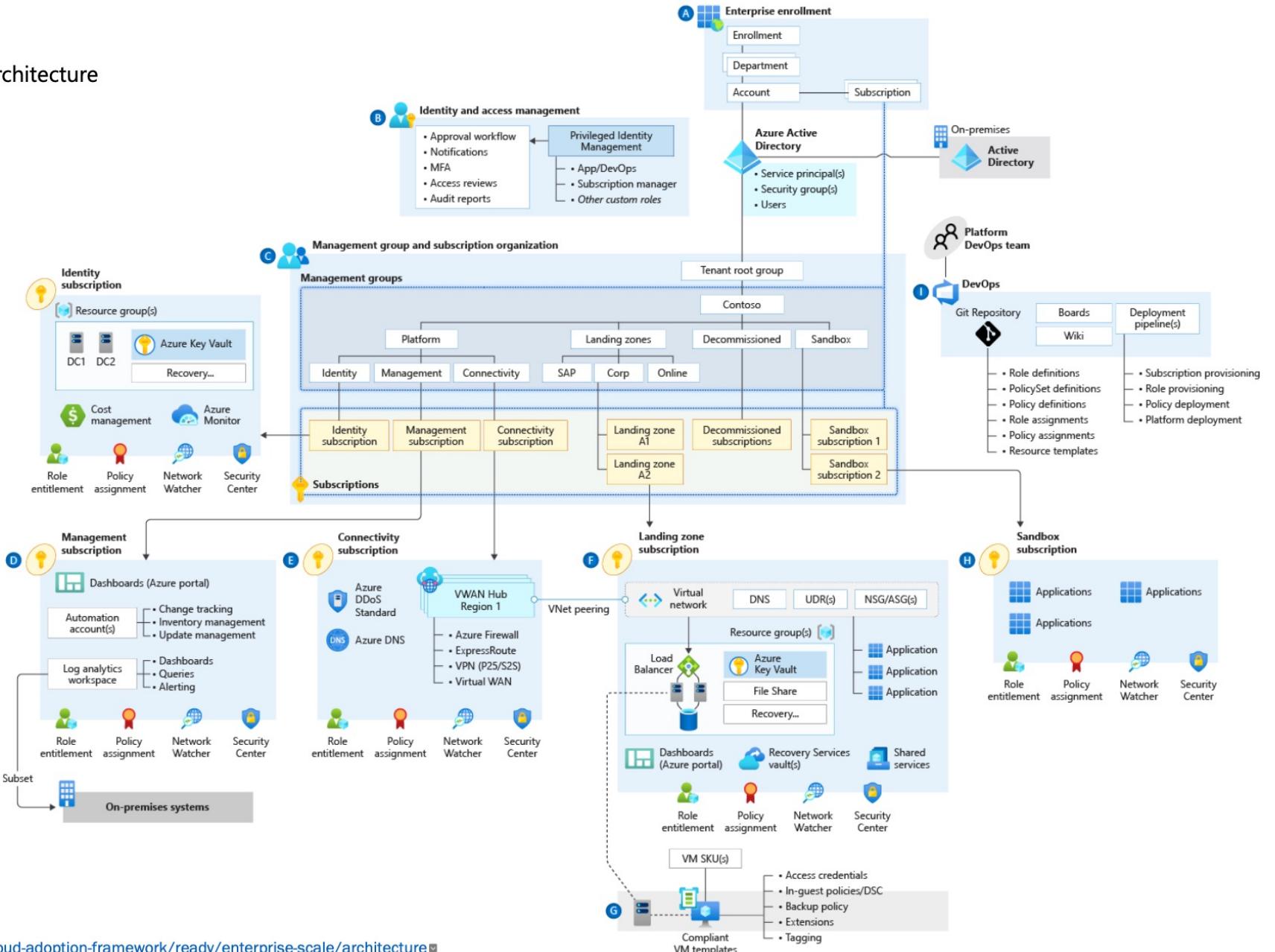
- Yksittäiset pilvipalvelut kuten virtuaalikone, tietokanta, web-palvelu, ...



Asetukset periytyvät ylhäältä alas.

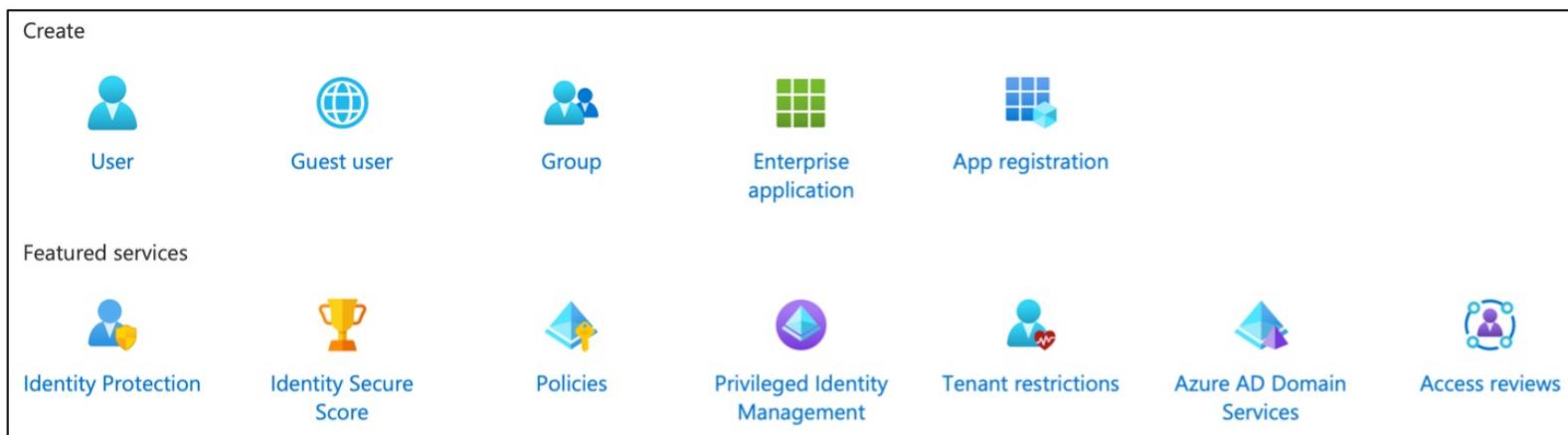
Cloud Adoption Framework

Enterprise-scale landing zone architecture



Azure vs Azure AD

- Azure AD on Microsoftin globaali pilvi-identiteettien ja pääsynhallinnan palvelu.
- Azure AD muodostaa **Tenantin**, joka määrittelee organisaation hallinnolliset rajat kaikissa Microsoftin pilvipalveluissa: Office365, Azure, Dynamics 365, Intune...
- Identiteetti voi olla henkilö, sovellus tai Azure-resurssi.
- Sisältö voidaan synkronoida perinteisestä Windows Active Directorystä (AD Connect).
- Käytössä olevat ominaisuudet riippuu lisenssitasosta (Free, Premium 1, Premium 2).



Azure AD

Azure AD B2B

Azure AD B2C

Azure IAM

Identiteettityypit:

- User (Cloud, Directory Synced, Guest)
- Service Principal
- Managed Identity

Vakioidut roolit Azure-palveluissa:

- Owner voi hallita kaikkea, sisältäen pääsynhallinnan asetuksia.
- Contributor voi hallita kaikkea, paitsi pääsynhallinnan asetuksia.
- Reader voi lukea ja nähdä kaiken, muttei tehdä muutoksia.
- Custom role voi yhdistellä eri oikeuksia, käytettävä harkiten.

Parhaat käytännöt roolien määrittelyyn:

- Roolit annetaan Azure AD ryhmille, ei käyttäjille.
- Subscription-tason yleiset roolit Management Groupien avulla (ylläpito, tietoturva, kustannusten hallinta).
- Yksittäisten sovellusten ja palveluiden roolit Resource Group tasolla sopiville tukiryhmille.
- Resurssitasolla vain automaatioihin tarvittavat oikeudet.
- Oikeudet aina minimitasolla (least-privilege access).

Azure IAM & RBAC

	Reader	Resource-specific or custom role	Contributor	Owner
Subscription	Observers	Users managing resources		Admins
Resource group				
Resource		Automated processes		

Keskeiset hallinta- ja tietoturvapalvelut

Seuraavia Azure AD tenantin laajuisia palveluita käytetään koko pilviympäristön hallinnointiin:

Azure Active Directory

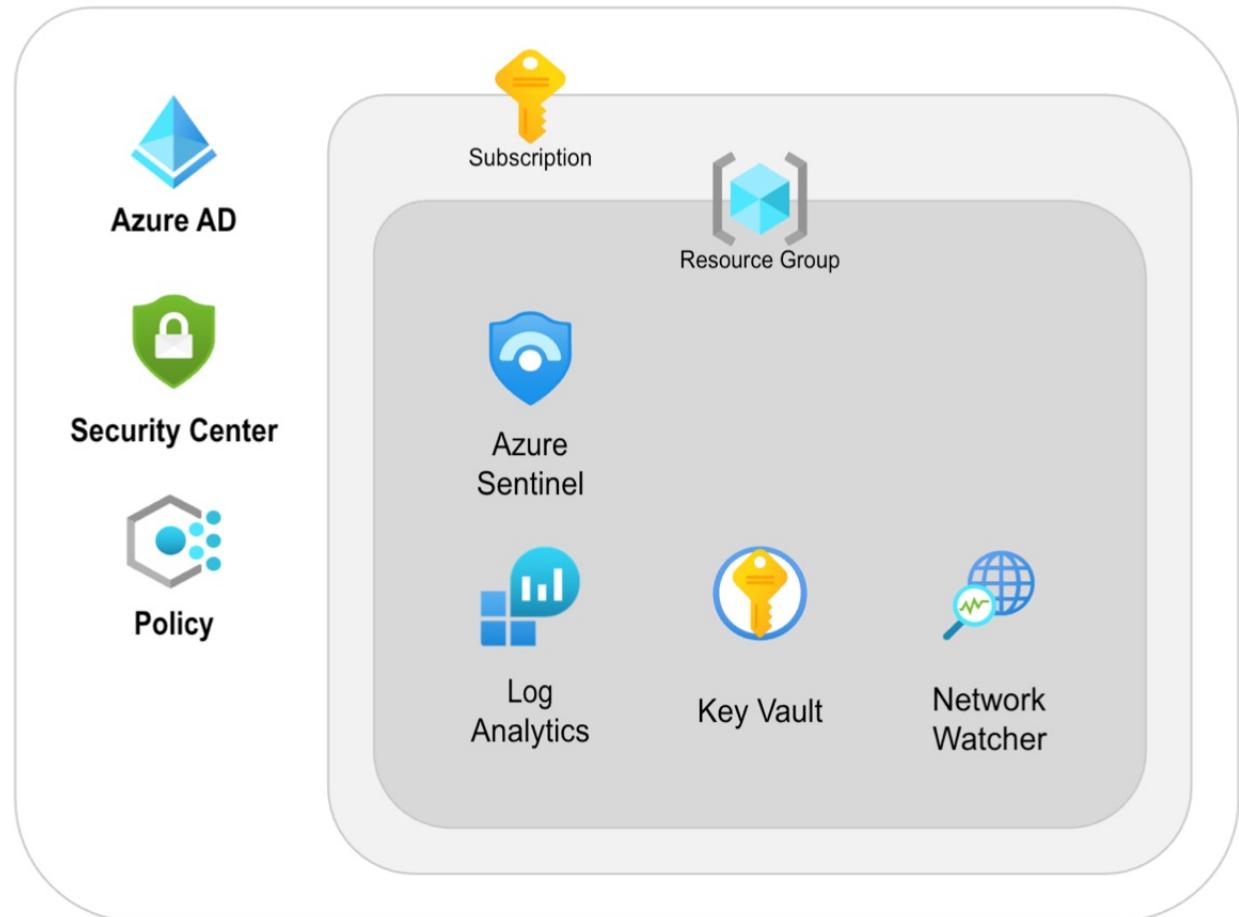
- Identiteettien- ja pääsynhallinta.
- Identiteettitapahtumien ja riskien valvonta.

Azure Security Center

- Raportoi resurssien ja konfiguraation tietoturvan sekä vaatimuksenmukaisuuden (Free Tier).
- Aktiivinen uhkien ja hyökkäysten torjunta (Standard Tier).

Azure Policy

- Sääntöjen ja vaatimusten luonti Azure-resursseille.
- Mitä saa luoda? Mihin? Millä ominaisuuksilla?
- Pakotus vs auditointi.



Keskeiset hallinta- ja tietoturvapalvelut

Seuraavia Azure-subscriptioniin perustettavia palveluita käytetään koko pilviympäröön tai valikoitujen osien hallintaan Azure-hierarkiassa:

Azure Sentinel

- Keskitetty tietoturvatapahtumien hallinta-, valvonta ja orkestrointipalvelu.

Log Analytics

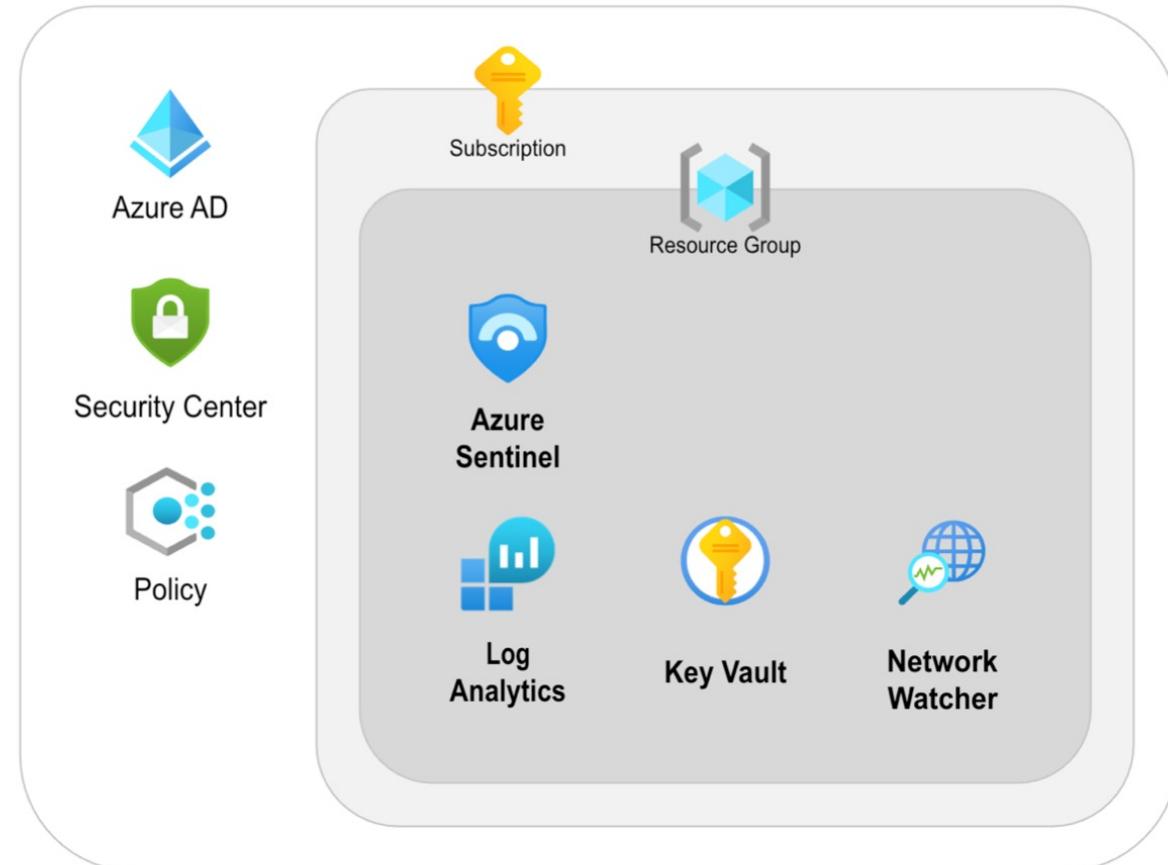
- Lokienhallintopalvelu johon voidaan kytkeä auditointi- ja käyttölokit lähes kaikista Azure-palveluista ja resursseista

Key Vault

- Palvelu salausavainten ja muiden salaisuuksien hallintaan ja automatisointiin.

Network Watcher

- Palveluiden tietoliikenteen suorituskyvyn, saatavuuden ja poikkeamien valvonta.



Azure Security Center & Azure Defender

The screenshot shows the Azure Security Center Overview page. It displays the following key metrics:

- Azure subscriptions: 1
- Active recommendations: 26
- Security alerts: 1
- Secure score: 44% (24.76 points)
- Regulatory compliance: Azure Security Benchmark (76% - 28/37 passed controls), SOC TSP, PCI DSS 3.2.1, ISO 27001.
- Azure Defender status: Off
- Advanced protection features: VM vulnerability assessment (3 unprotected), Just-in-time VM access (3 unprotected), Adaptive application control (None unprotected), SQL vulnerability assessment (None unprotected), File integrity monitoring, Network map, IoT security.

The screenshot shows the Azure Security Center | Azure Defender page. It displays the following information:

- Azure Defender coverage: 8 total resources (Servers: 3/3, Storage: 1/1, Key Vault: 1/1, Resource Manager subscriptions: 1/1, Azure SQL database servers: 1/1, DNS subscriptions: 1/1).
- Azure Defender status: On
- Advanced protection features: VM vulnerability assessment (3 unprotected), Just-in-time VM access (3 unprotected), Adaptive application control (None unprotected), SQL vulnerability assessment (None unprotected), File integrity monitoring, Network map, IoT security.

Azure Security Center (Free)

- Tietoturvatason pistetys, Secure score.
- Palveluiden ja resurssien konfiguraation valvonta.

Azure Defender (€€€)

- Aktiivinen tietoturvatapahtumien, uhkien ja haavoittuvuuksien valvonta resursseille (mm. virtuaalikoneet, tietokannat, kontit).
- Tuki hybridipilvelle, on-premise palvelimet kytettäväissä.

Cloud Security Posture Management CSPM

Cloud Workload Protection Platform CWPP

Tietoliikenteen suojauspalvelut

					
DDoS Protection	Web Application Firewall	Azure Firewall	Network Security Groups	Service Endpoints	Security Appliances
Sovellusten suojaaminen			Segmentointi		

DDoS suojaus aina kaikissa palveluissa (Basic, ilmainen). Mukautetut säännöt ja raportointi (Standard, €€€)

Web-palveluiden suojaus yleisiä hyökkäyksiä ja haavoittuvuuksia vastaan.

Keskitetty outbound ja inbound tietoliikenteen ja sovellusten muuraus (L3-L7)

Hajautettu inbound ja outbound (L3-L4) muuraus virtuaalikoneille, konteille ja aliverkoille.

Pääsyn rajaus PaaS-resursseihin Azuren sisäisiin virtuaaliverkkoihin.

Kolmannen osapuolen tuotteet, BYOD lisenssit, Azure Marketplace.

Kehityksen ja operoinnin automaatio tietoturvan takaajana

- Suurista pilviympäristöistä vastaavat organisaatiot päätyvät usein seuraavaan periaatteeseen pilvipalveluiden kehityksessä ja operoinnissa:
 - Konfiguraatiota ei tehdä manuaalisesti hallintaportaalissa.
 - Palveluiden julkaisu ja muutokset toteutetaan automaatiotyökaluilla.
 - Palveluiden konfiguraation master = git-repository.
- Organisaation on valittava sopiva automaation taso ja sitouduttava siihen kaikessa toiminnassa.
- Automaatio helpottaa tietoturvan toteutumista, mutta samalla luo kokonaan uuden suojaavan kerroksen.
- Azurella on monta vaihtoehtoa automaatiotyökalun valintaan: ARM templatet, Azure Blueprintit, PowerShell, Terraform.
- Azurella on oma pilvinäivi DevOps-palvelu, joka on yksi tapa rakentaa perusta automaatiolle.



Azure
Boards

Plan, track, and discuss work across teams, deliver value to your users faster.



Azure
Repos

Unlimited cloud-hosted private Git repos. Collaborative pull requests, advanced file management, and more.



Azure
Pipelines

CI/CD that works with any language, platform, and cloud. Connect to GitHub or any Git provider and deploy continuously to any cloud.



Azure
Test Plans

The test management and exploratory testing toolkit that lets you ship with confidence.



Azure
Artifacts

Create, host, and share packages. Easily add artifacts to CI/CD pipelines.



Azure DevOps

Palvelun tuottaminen useille organisaatioille

Miten palveluntarjoaja-organisaatiot hallitsevat Azure-ympäristöjä?

- Organisaation oma tenant on aina oikea paikka organisaation palveluille!
- Palveluntarjoaja tarvitsee hallintamallin asiakkaidensa tenanteissa tehtävään työhön.
- Pääsynhallinnan vaihtoehdot asiakkaiden tenantien hallintaan:
 - Natiivi tunnus asiakkaan tenantissa.
 - Guest-tunnus asiakkaan tenantissa (Azure AD B2B).
 - Palveluntarjoajan tenantin integrointi asiakkaan tenantiin (Azure Lighthouse).
- Muistettava myös kolmannet osapuolet ja alihankintaketju; asiakkaan sopimuskumppanit, palveluntarjoajan konsultit...
- Mitkä konfiguraatiot ja periaatteet ovat kaikille asiakkaille yhteisiä, mistä saa poiketa?

Turvallisen pilvioperoinnin perusteita

- **Hallintamalli**
 - Toimintamallit ja periaatteet on dokumentoitu ja jalkautettu.
 - Ytimessä pääsynhallinta ja resurssien konfiguraation laatu.
- **Tarkoituksenmukainen hybridি-arkkitehtuuri**
 - Yhteydet toimipisteiden ja pilven privaattiverkkojen välillä.
 - Hallinta- ja valvontapalvelut.
 - Varmistus- ja palautuskyvykkyyks.
 - Mikä on pilvinatiivia, mikä jaetaan on-premisen kanssa?
- **Tietoturvapalvelut käyttöön**
 - Jatkuvan parantamisen käytännöt.
 - Kaikki palvelut huomioitava (prod ja non-prod).
 - Kustannukset huomioitava heti alkuvaiheessa.
- **Resurssit, osaaminen ja yhteistyö koko organisaatiossa**
 - Tukipalvelut, kehitys, operointi, tietoturva.