THANKS FOR THE SPONSORS!

PATCH MY PC

Microsoft

PLENTICS

Metropolia

twoday

NETOX

DELL

Workplace Ninja User Group Finland

intel

Workplace Ninja

User Group Finland

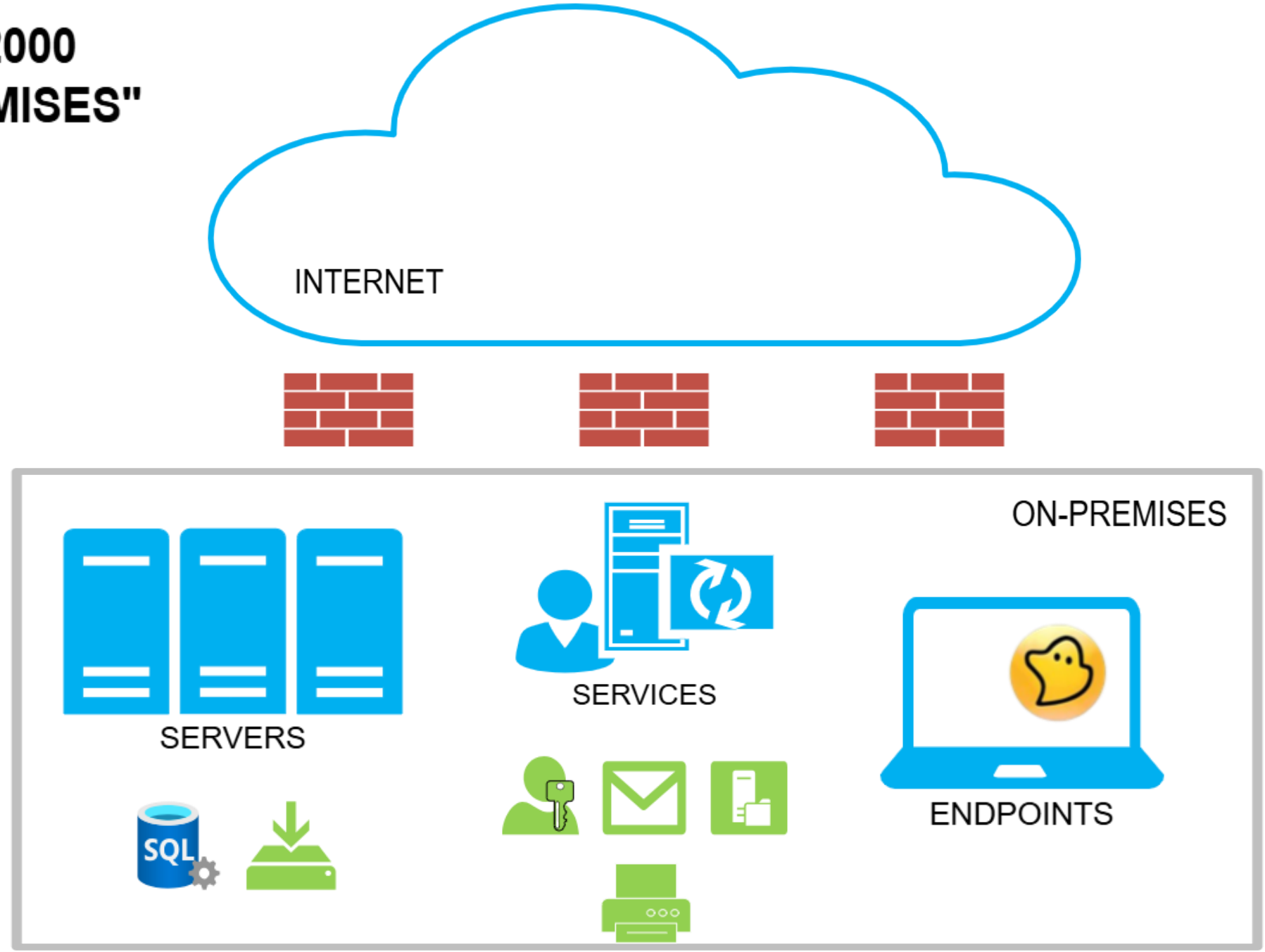
Pilvihallintaan siirtymien:
Yksi tavoite, monta reittiä

Aku Suonpää
Angry Advisor Oy
Endpoint management, Software packaging
Alan hommissa vuodesta 2004

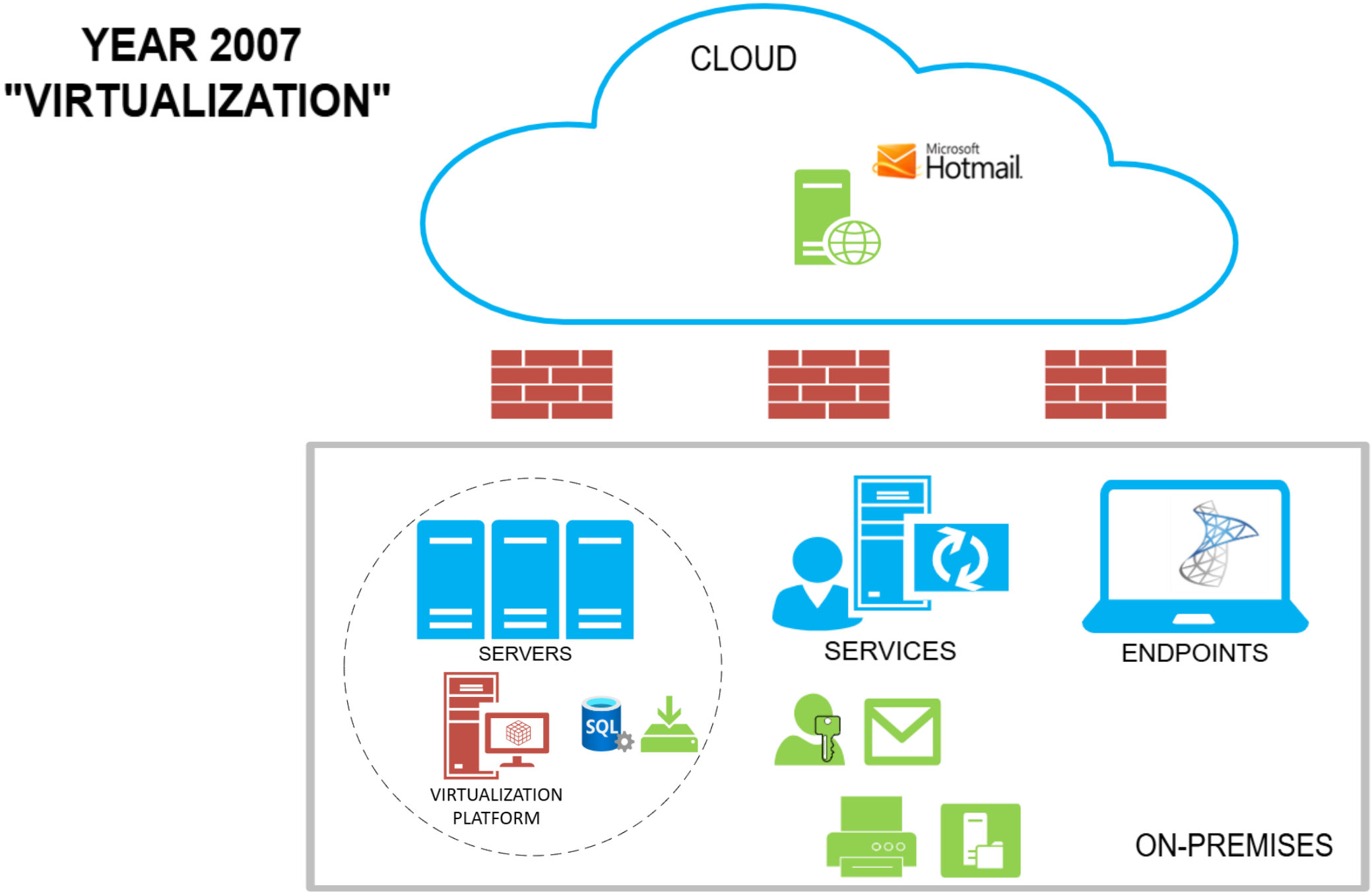
Esityksen tavoite ja scope

- Tavoite:
  - Tarjota kokemuksia ja näkemyksiä Windows päätelaitehallinnan siirtämisestä pilveen
- Scope:
  - Organisaatiot joilla on historiallisesti on-premises ratkaisuja
  - Tarkastelu näkökulma: Microsoft-ekosysteemi (periaatteet sovellettavissa muihinkin tuotteisiin)
- Ei suositella: organisaatio tai laiteryhmä joka vaatii tiukkaa vakiointia ja hallintaa
  - Pilvihallintajärjestelmät ovat SAAS palveluita -> Et voi hallita kaikkia muutoksia!
  - Vertaa kryptovaluuttojen sanontaan ”Not your keys, not your coins”

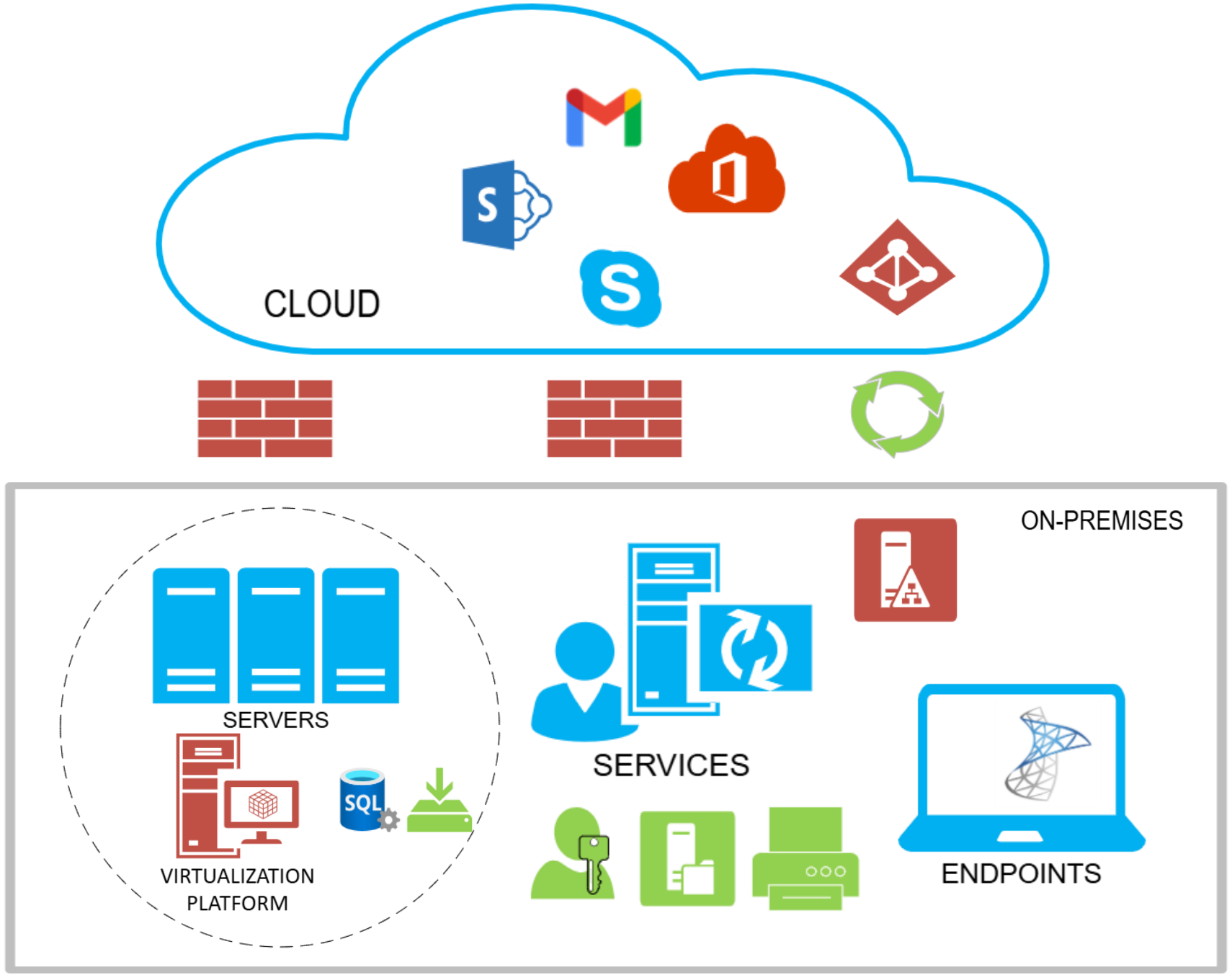
YEAR 2000
"ON-PREMISES"



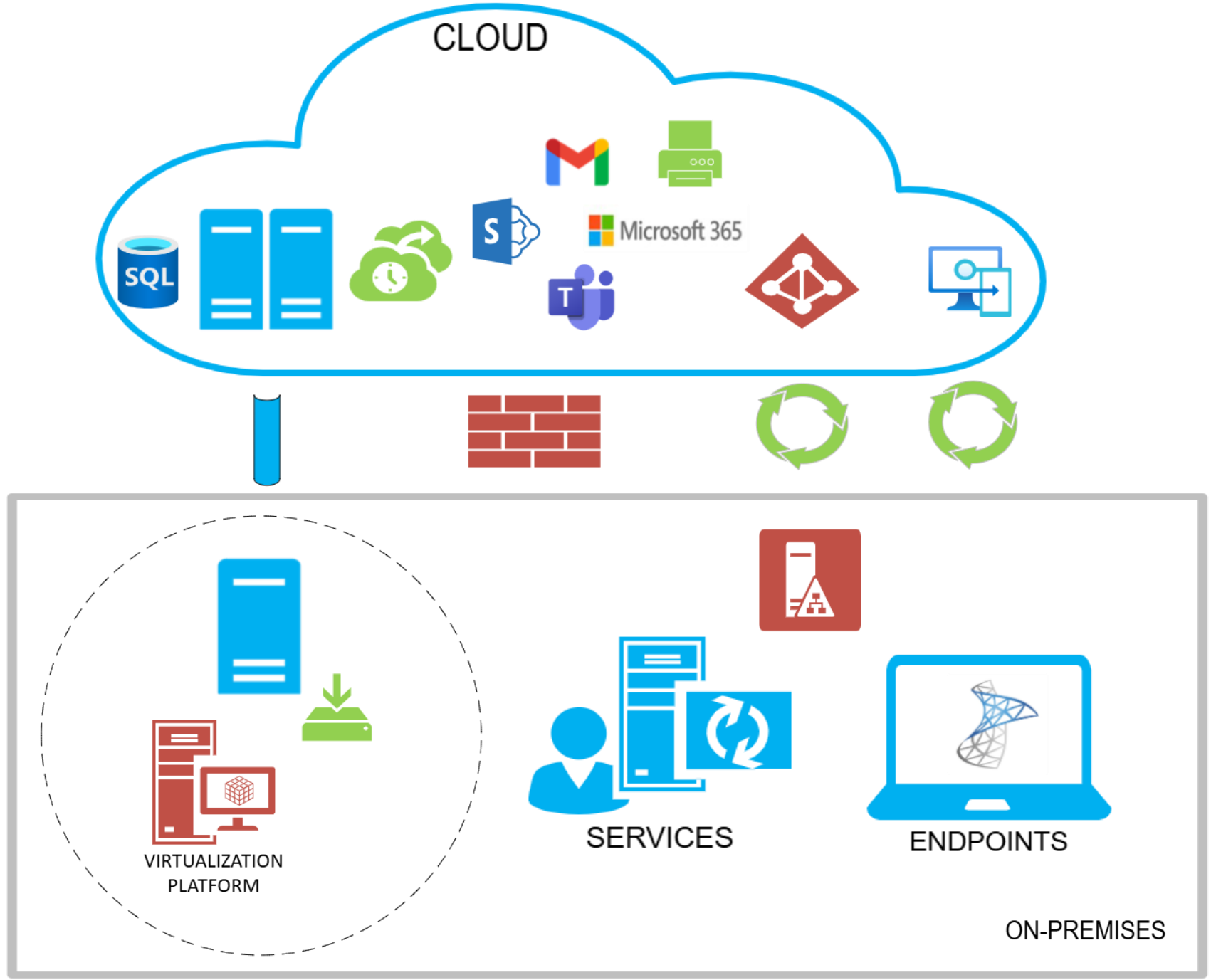
YEAR 2007
"VIRTUALIZATION"



YEAR 2014
"HYBRID"



YEAR 2021
"CLOUD"



Pilvihallinnan hyödyt eri näkökulmista

Liikkeenjohto

- Strateginen ketteryys – nopea reagointi muutoksiin
- Ennustettavat kustannukset – Investoinneista kuukausimaksuihin
- Riskienhallinta – parempi tietoturva ja compliance
- Työntekijäkokemus – tehokkaampi työskentely

IT-osasto

- Etähallinta ilman monimutkaisia VPN-ratkaisuja
- Nopeampi sääntöjen ja päivitysten jakelu
- Reaaliaikainen näkyvyys ja raportointi
- Laitteiden mallintaminen yksinkertaisempaa
- Vähemmän infrastruktuuria ylläpidettäväksi

Loppukäyttäjä

- Nopea käyttöönotto ja vähemmän häiriöitä
- Parempi tietoturva automaattisesti
- Joustava työskentely missä tahansa
- Helpompi ja nopeampi tuki

Ajattelutavan ja toimintamallien suurimmat muutokset

Hallintainfrastruktuuri	• Ei enää omia palvelimia – hallinta tapahtuu pilvestä, internet-yhteys kriittinen
Identiteetin hallinta	• Siirtyminen moderniin todennukseen ja pilvipohjaiseen identiteettiin
Laitteiden provisiointi	• Imaging-mallit väistyvät – automaattinen provisiointi ja standardointi
Tietoturvamalli	• Zero Trust -ajattelu korvaa perinteisen verkon luottamuksen
Sovellusten jakelu	• Paketoinnista pilvipohjaiseen jakeluun, jatkuva päivitysmalli
Raportointi ja seuranta	• Reaaliaikainen näkyvyys ja analytiikka ohjaavat päätöksiä

Ennen siirtymää pohdittavat asiat

Nykytilan kartoitus	• laitekanta, hallintaratkaisut, tietoturvapolitiikat
Tavoitetilan määrittely	• täysi pilvihallinta vai hybridimalli
Tietoturva ja compliance	• auditointivaatimukset, Zero Trust -periaatteet
Käyttäjäkokemus	• häiriöiden minimointi, viestintä ja koulutus
Tekniset riippuvuudet	• identiteetti- ja sovellushallinnan integraatiot
Vaiheistus ja aikataulu	• pilotti → laajennus → täysi käyttöönotto
Resurssit ja osaaminen	• projektin roolit, koulutustarpeet
Riskienhallinta	• fallback-suunnitelma ja varautuminen

Hybrid vs Entra ID Join

	HYBRID ENTRA ID JOIN	ENTRA ID JOIN
Käyttötarkoitus	On-prem AD + pilvi	Täysin pilvipohjainen
Vaatii on-prem AD	Kyllä	Ei, mutta käytettävissä
Vaatii Entra ID Connect	Kyllä	Ei, mutta voidaan hyödyntää
Laitehallinta	SCCM + Intune	Intune
Kirjautuminen	AD-tunnus + SSO Entra	Entra ID + SSO AD
Offline-käyttö	Mahdollinen	Mahdollinen
Group Policy	Kyllä	Ei (Intune-politiikat)
Conditional Access	Kyllä	Kyllä
Käyttöönotto	Monimutkaisempi	Yksinkertaisempi
Tyypillinen siirtymäpolku	AD → Hybrid → Entra	AD → Entra

Co-management vs Intune

	CO-MANAGEMENT (SCCM + INTUNE)	INTUNE-ONLY
Käyttötarkoitus	Siirtymävaihe organisaatioille, joilla on SCCM käytössä	Täysin pilvipohjainen hallinta ilman SCCM:ää
Vaatii SCCM	Kyllä	Ei
Vaatii Intune	Kyllä	Kyllä
Hallintamalli	Jaettu hallinta: osa asetuksista SCCM:ssä, osa Intunessa	Kaikki hallinta Intunessa
Tyypillinen käyttöönotto	AD Join + Hybrid Join + SCCM + Intune	Entra ID Join + Intune
Koneen asennus	Task Sequence, Autopilot	Autopilot
Windows Updates	SCCM tai Intune (valittavissa)	Intune (Windows Update for Business)
Sovellusten jakelu	SCCM + Intune (valittavissa)	Intune (Win32, Store, LOB)
Raportointi	SCCM:n laajat raportit + Intune	Intune-raportointi
Hallinta ilman internet-yhteyttä	Kyllä	Ei

Erilaiset kombinaatiot

Hybrid + Co-management

- Laite on AD-domainissa ja Entra ID:ssa, hallinta jaettu SCCM:n ja Intunen välillä

Hybrid + Intune-only

- Laite on AD-domainissa ja Azure AD:ssa, mutta hallinta siirretty kokonaan Intuneen

Entra ID Join + Intune-only

- Täysin pilvipohjainen malli, laite liittyy suoraan Entra ID:hen ja hallitaan Intunella

Entra ID Join + Co-management

- Harvinainen, mutta mahdollinen jos SCCM säilytetään pilvimallissa

To do Entra ID Join + Intune-only

GPO -> Intune configure profile

- Kannattaa olla kriittinen

Sovelluspaketit -> Intunewin (win32)

Koneiden esiasennus ja elinkaari

- Image, rekisteröinti, oikeudet

Varmista vanhojen palveluiden toimivuus

“Rusinat pullasta”

- Windows updatet puhtaasti pilvestä
  - Autopatch!
- Defender for Endpoint
  - Tietoturvakonfiguraatiot pilvestä
- Bitlocker ja LAPS tiedot pilveen
- Compliance ja conditional access
- Endpoint analytics
- Remote actions
- Rusina, joka kannattaa unohtaa: Autopilot

> **Important**
>
> Microsoft recommends deploying new devices as cloud-native using Microsoft Entra join. Deploying new devices as Microsoft Entra hybrid join devices isn't recommended, including through Windows Autopilot. For more information, see Microsoft Entra joined vs. Microsoft Entra hybrid joined in cloud-native endpoints: Which option is right for your organization.

Entra ID join maailman “yllätykset”

Etähallintatyökalut

- C$, remote registry, RDP, Winrm jne

Kone on Workgroup liitetty AD:n näkökulmasta

- Konetiliä ei löydy AD domainista
- Luvittaminen onnistuu vain käyttäjän mukaan (jos AD:sta synkattu tili)
- DNS ei automaattisesti selvitä domainin nimiä

Kirjautuminen tapahtuu Entra ID:tä vasten

“Intune only” ongelmat/bugit

Autopilot ei validoi laitenimen ainutkertaisuutta → riskinä duplikaatit.	• Ei riko mitään, mutta hallinnollisesti haastava
Intune menee rikki tai laitteen yhteys Intuneen hajoaa!	• Varajärjestelmä hallinnointiin?
Intunen raportointi on vajaata	• Toinen järjestelmä täydentämään raportointia?
Hallinta ilman internet-yhteyttä	
Intune suite on todella kallis	• 3rd party ratkaisuja löytyy ja ovat edullisempia
Intune konfiguraatioiden varmuuskopiointi ja palautus	

Pilvilaitehallinnan tulevaisuus

Autopatch ja sen kaltaiset ratkaisut lisääntyvät

Integraatio eri järjestelmien välillä syvenee

Intune + Defender

Autonomous endpoint management

Laitehallinta siirtyy kohti itseohjautuvia malleja.

Thank you!

Workplace Ninja
User Group Finland

THANK YOU ALL AND
A SPECIAL THANKS TO OUR SPONSORS!