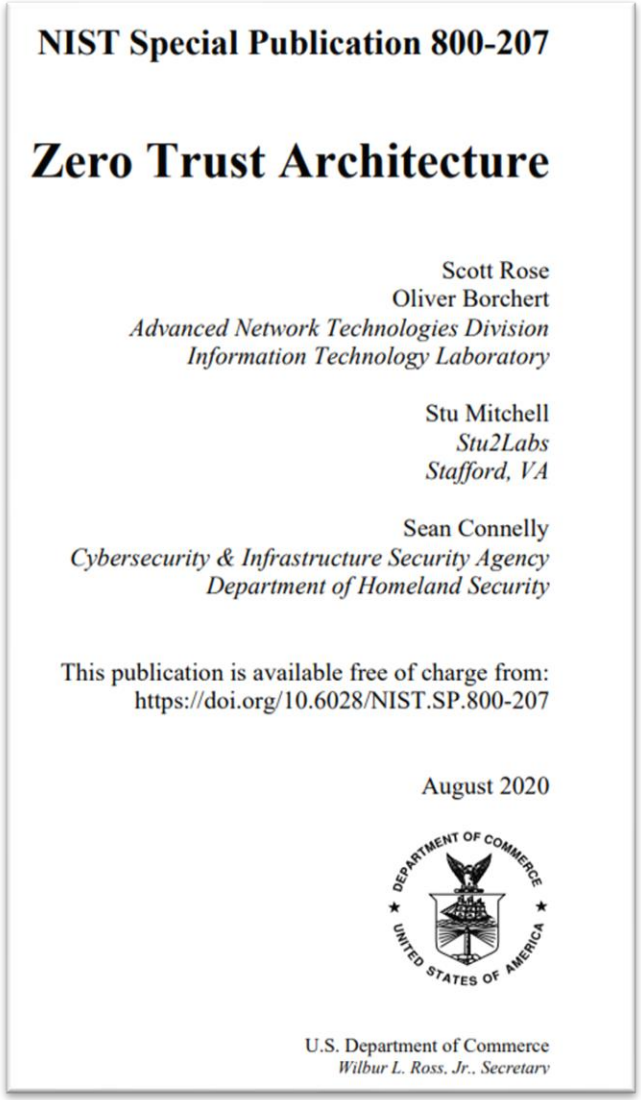
Zero Trust

Ilkka Hyvönen & Roope Seppälä
Microsoft Oy

Periaate - ei tuote.

Useampi tulkinta: NIST, Microsoft, Forrester, Gartner ...



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Advanced Network Technologies Division
Information Technology Laboratory

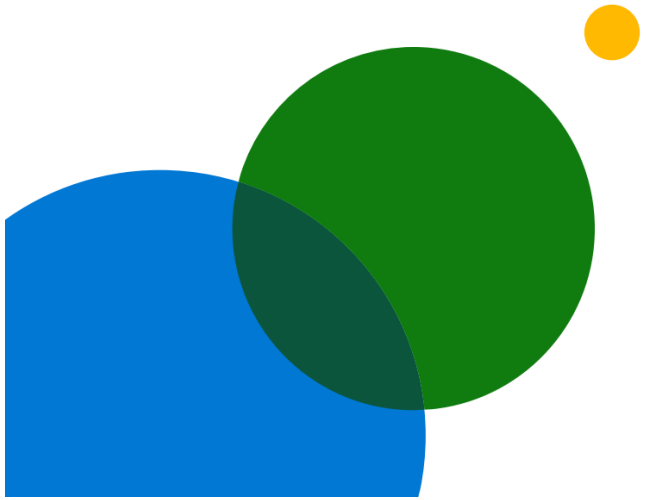
Stu Mitchell
Stu2Labs
Stafford, VA

Sean Connelly
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

August 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary



Evolving Zero Trust

How real-world deployments and attacks are shaping the future of Zero Trust strategies

Microsoft

A Look Back At Zero Trust: Never Trust, Always Verify

Chase Cunningham, VP, Principal Analyst AUG 24 2020

What exactly is Zero Trust? For those of you who've been hiding away in a cave for the past decade, Zero Trust (ZT) is a concept founded by Forrester alum John Kindervag in 2009 that centers on the belief that trust is a vulnerability, and security

Gartner Research

Zero Trust Is an Initial Step on the Roadmap to CARTA

Summary

Customer interest in and vendor marketing of a "zero trust" approach to networking are growing. It starts with an initial security posture of default deny. But, for business to occur, security and risk management leaders must establish and continuously assess trust using Gartner's CARTA approach.

Published: 10 December 2018

Luottamus 0.

Zero Trust on proaktiivinen ja integroitu lähestyminen tietoturvaan kaikilla sen tasoilla läpi koko digitaalisen toimintaympäristön, joka yksiselitteisesti ja jatkuvasti vahvistaa jokaisen toiminnon, edellyttää mahdollisimman vähäisiä oikeuksia, luottaa keinoälyyn, edistyneeseen havainnointikykyyn, sekä reaaliaikaiseen uhkien torjumiseen.

Älä oleta, vaan kysy.

“Zero Trust is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats.”

- Microsoft Zero Trust whitepaper

Prinsiipit

Varmenna – Verify explicitly

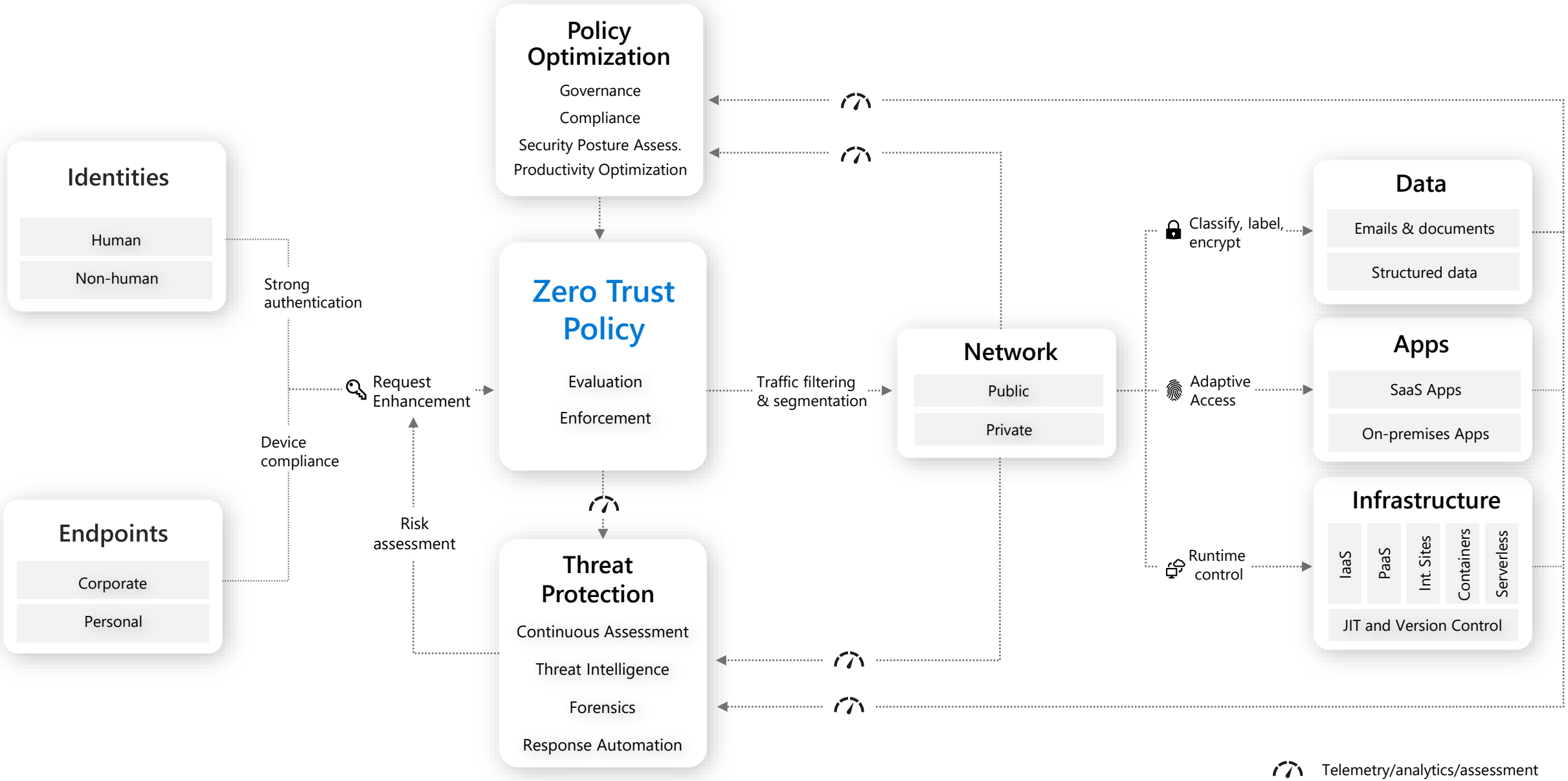
Rajoita – Use least privilege access (JIT = just in time access)

Epäile – Assume breach

<u>Mahdollista tuottava ja turvallinen työskentely.</u>

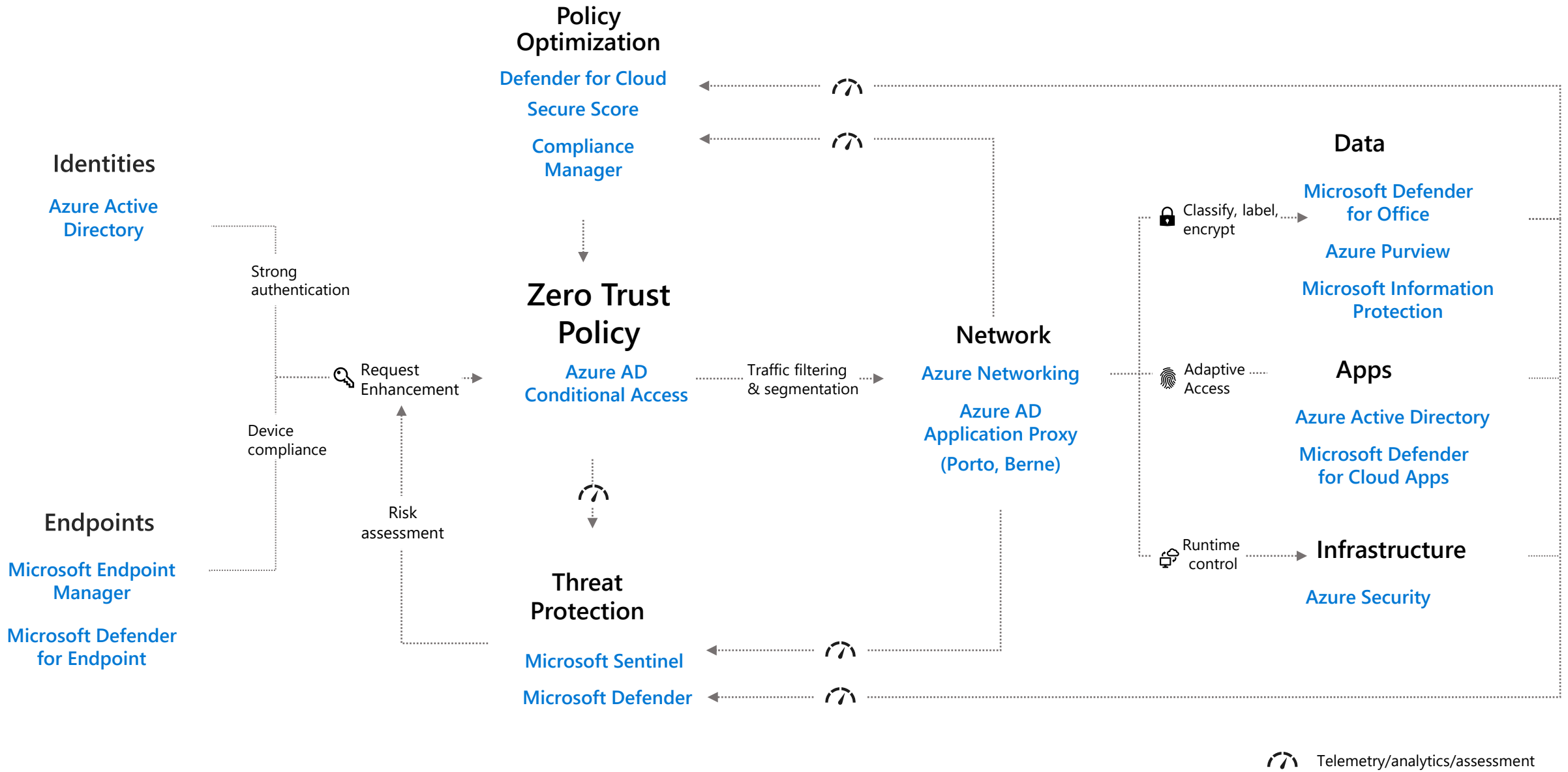
Zero Trust architecture

Microsoft Security



Microsoft Zero Trust architecture

Microsoft Security



Microsoftin oman IT:n matka

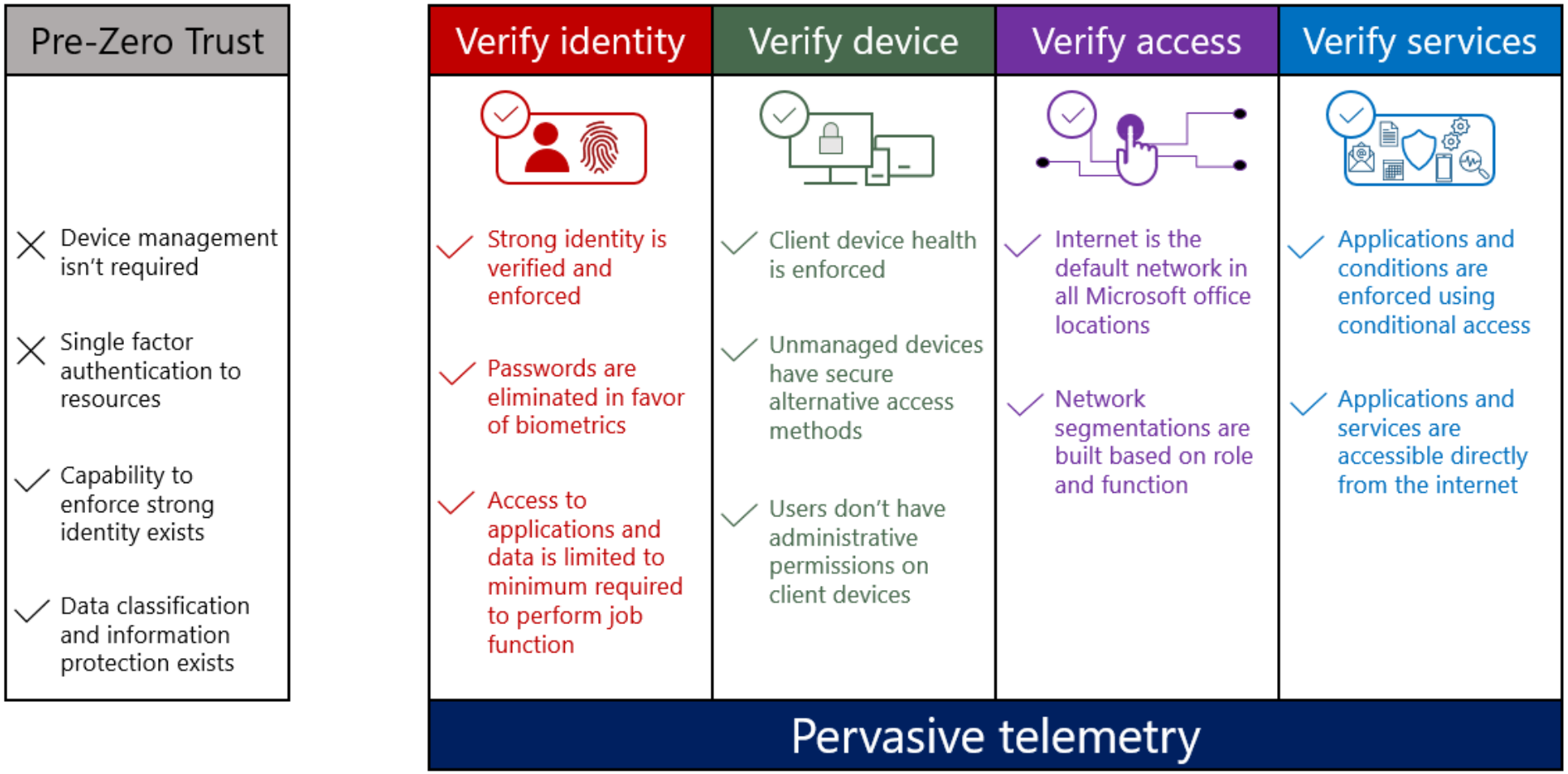


Figure 1. The major goals for each Zero Trust pillar

[>> Implementing a Zero Trust security model at Microsoft]

Konkreettiset stepit Microsoft IT:n ympäristössä

- Toimistoverkko ei ole sisäverkko
- Sovellusten siirto pilveen ja modernisointi samalla
  - Niiden sovellusten joita ei ole järkeä tai pystytä siirtämään tehdään julkaisu internetiin Azure AD Application Proxy:llä
  - Muutama sovellus, jotka on tietoisesti jätetty vain sisäverkkoon vaativat VPN yhteyden myös toimistoverkosta
- Kaikki laitteet valvottuja Endpoint managerilla (SCCM&Intune), joiden kautta myös määritellään compliance policy
- Ympäristön valvonta (ja reagointi) arkkitehtuurikuvan tuotteilla jne.
  - Automaatio ja riskien valvonta hoitaa “perushuolet” -> filtteröi ja vapauttaa aikaa keskittyä isompiin hyökkäyksiin
- Pääsynhallinta ehdollista sovelluskohtaisesti
- Salasanojen eliminointi ja siirtyminen Windows Hello for business käyttöön (biometriikka pääosin autentikointitapa)