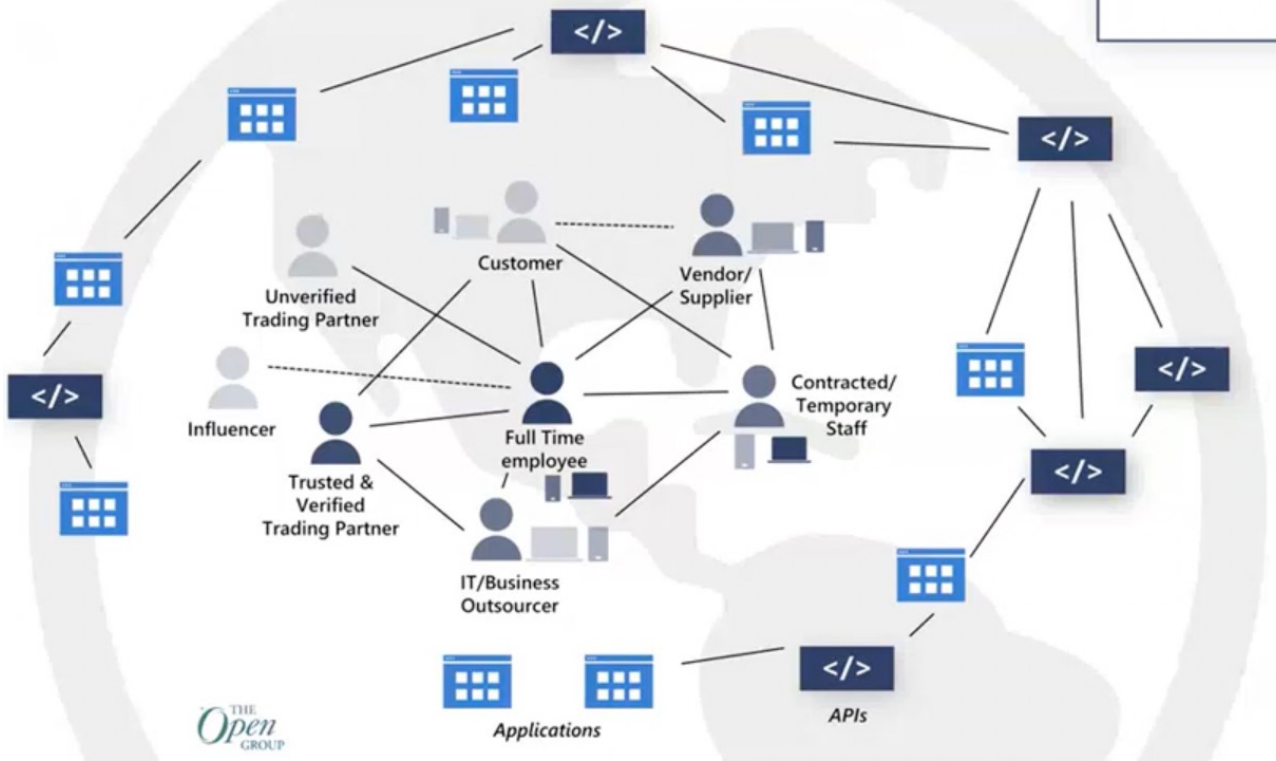
Tietoturva pilvimaailmassa: Zero Trust

mikko.koivunen@iki.fi

08/2021

Mistä on kyse?



Muuttuvat työtavat

- Etätyön ja liikkuvan työn normalisoituminen.
- Jatkuvasti kasvava ja hajautuva IT-palveluluettelo.
- Jatkuvasti muuttuva kumppani- ja toimittajakenttä.

Muuttuvat tietoturvatarpeet

- **Automaattinen pääsynhallinta** – kyky julkaista kaikki palvelut yhtenäisellä tavalla, ketterästi ja matalin kustannuksin.
- **Mukautuva identiteetinhallinta** – kyky tukea jatkuvia roolien, vastuiden ja suhteiden muutostarpeita.
- **Data- ja omaisuuskeskeinen tietoturva**
  - Resurssien kiinnitys oikeisiin kohteisiin, suojataan se mikä on tärkeää.
  - Parempi havainnointikyky palveluiden ja käyttäjien sijainnista riippumatta.

Miksi tarvitaan muutos?

1. IT-palveluiden turvaaminen on vaikeaa
   - Laitteiden määrä
   - Käyttäjien määrä
   - Yhteyksien määrä

2. “Turvallinen sisäverkko” strategia ei toimi
   - Matalampi turvallisuustaso verkon sisäpuolella ei enää perusteltua
   - Palomuurisääntö ei ole riittävä kontrolli palvelun käyttöön

3. Laitteet ja palvelut liikkuvat
   - BYOD
   - Etätyö
   - Mobiilikäyttö
   - SaaS-palvelut

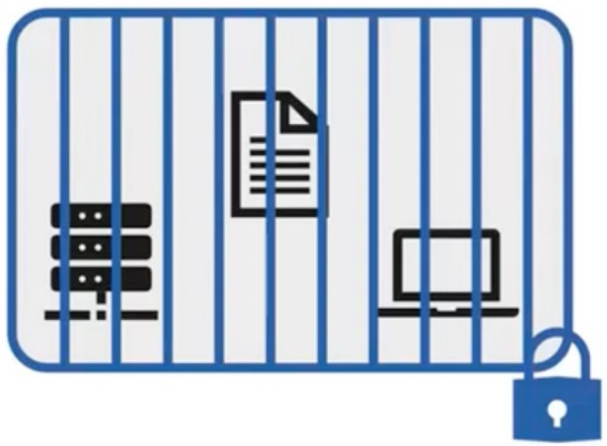
3. Hyökkääjät vaihtavat strategiaa
   - Phishing ja tunnusten murto
   - Etsitään ensisijaisesti heikkoja sovelluksia ja tietokantoja
   - Tietoturvatiimit ylikuormittuneita, työkalut puutteellisia kattavaan havainnointiin

Ratkaisuna kehitetty “Zero Trust” on pitkän kehitystyön tulosta:

Kaikkien iteraatioiden perusperiaate on yksinkertainen:
Keep Assets away from Attackers.

Mitä Zero Trust on?

Omaisuuden ja palveluiden suojaaminen sijainnista riippumatta.



Perinteinen malli – Suojaa assetit sijoittamalla ne suojattuihin verkkoihin.

Zero Trust – Suojaa assetit paikkariippumattomasti keskitetyllä policyllä.

Yksi keskitetty “policy engine”

Jatkuva päätelaitteen ja identiteetin tietoturvan arviointi

Automaattinen reagointi ja mukautuminen

Yleiset periaatteet julkisissa lähteissä

1. *The network is always assumed to be hostile.*
2. *External and internal threats exist on the network at all times.*
3. *Network locality is not sufficient for deciding trust in a network.*
4. *Every device, user and network flow is authenticated and authorized.*
5. *Policies must be dynamic and calculated from as many sources of data as possible.*

Zero Trust Networks: Building Secure Systems in Untrusted Networks, Evan Gilman & Doug Barth

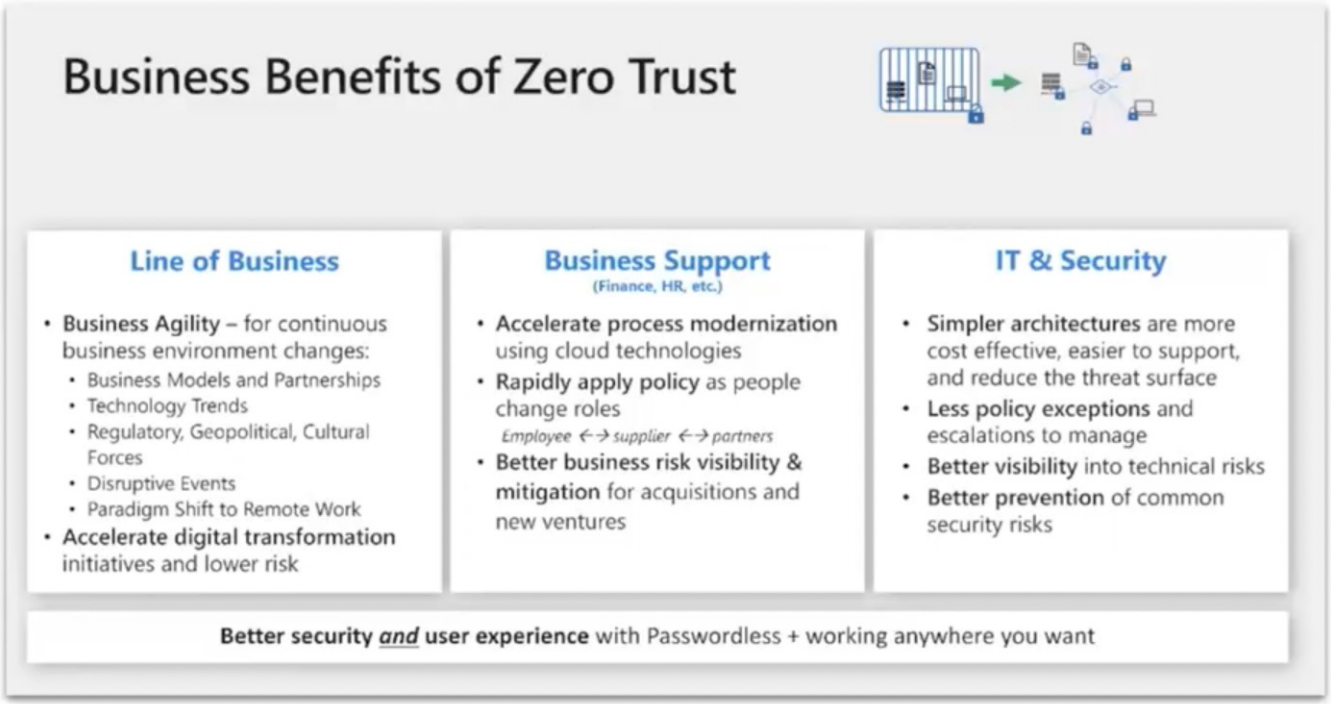
Microsoft Zero Trust Principles

In short, no person/device/application in the enterprise network should be trusted by default, no matter it is in the internal or external network. The fundamental basis of the trust should be based on the refactored access control using right authentication and authorization. Zero Trust Architecture has paradigmically changed traditional access control mechanism, and its essence is adaptive trusted access control based on identity.

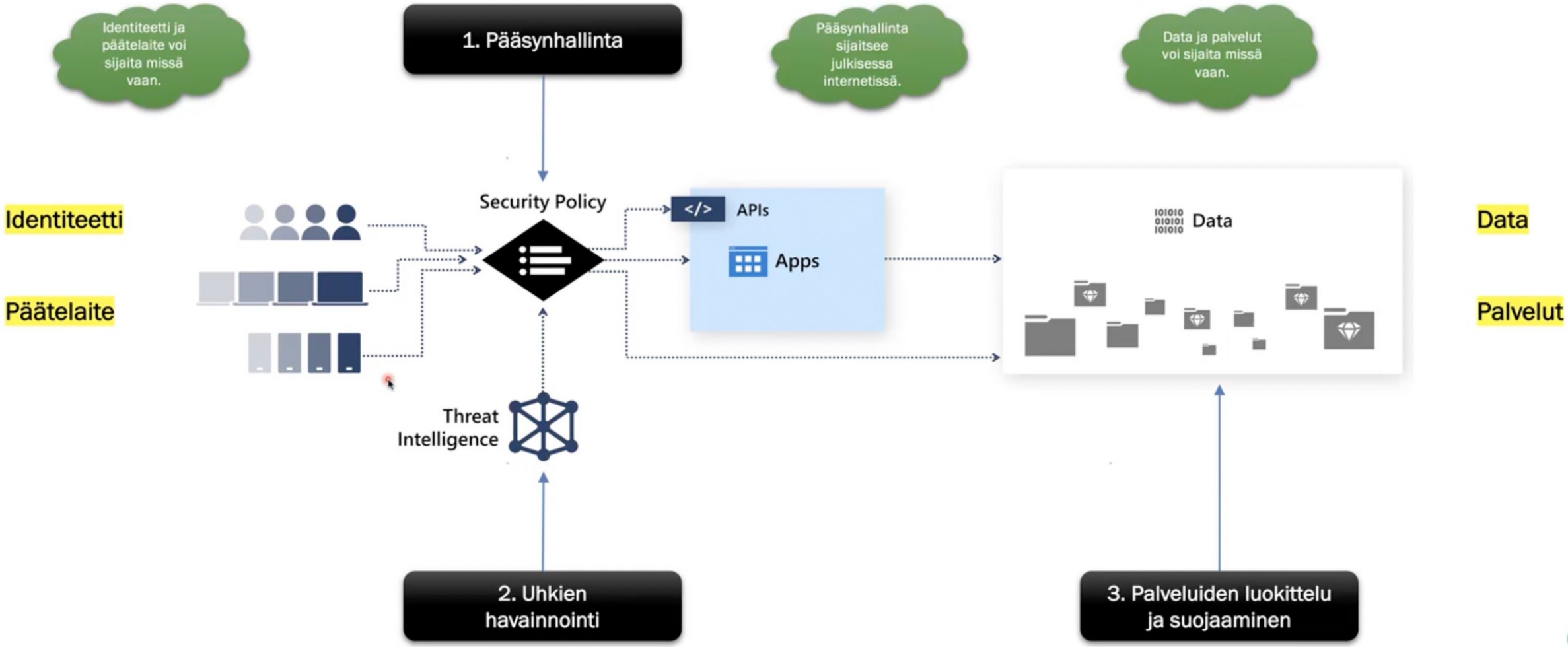
Gartner

Hyödyt yritykselle, käyttäjälle ja IT:lle

- Ketteryys – yksi malli minkä tahansa uuden palvelun käyttöönottoon.
- Yksinkertainen arkkitehtuuri.
- Parempi näkyvyys palveluihin.
- Kohonnut tietoturvataso.
- Selkeä ja positiivinen käyttäjäkokemus.



Tekniset komponentit



Miten aloitetaan?

User Access (Productivity Environment)

Increase and explicitly validate trust for
- **User Accounts** - Require Passwordless or MFA to access applications + apply threat intelligence and UEBA
- **Devices** - Require Device Integrity for Access (critically important step)

Increase security for accessing
- **Apps** - Modern apps + Legacy on-premises/IaaS apps by *modernizing VPN security* or going *beyond VPN* with App Proxy
- **Data** - Increased discovery and protection for sensitive data (CASB, CA Access Control, Azure Info Protection)

Governance to continuously monitor and reduce risk (including legacy protocols and applications)

Roll out to IT Admins first
- Targeted by Attackers
- High potential impact
- Provide technical feedback

Modernize Security Operations

- **Streamline response** to common attacks (Endpoint/Email/Identity)
- **Reduce manual effort** - using automated investigation/remediation, enforcing alert quality, and proactive threat hunting

OT and IoT Environments

- **Visibility** – Discover and classify assets with business critical, life safety, and operational/physical impact
- **Protection** – isolate assets from unneeded internet/production access with static and dynamic controls
- **Monitor** – unify threat detection and response processes for OT, IT, and IoT assets

ZT is similar to Classic Security
Align to cloud migration schedule *or* start after other ZT projects

Datacenter Security

- **Retire Legacy** - Retire or isolate legacy computing platforms (Unsupported OS/Applications)
- **Network Microsegmentation** - Additional network restrictions (dynamic trust-based and/or static rules)

Verkon suojaus ja segmentointi edelleen tärkää, jotta dataan ei pääse keskitetyn pääsynhallintapisteen ohi.

Microsoft

Priorisoidaan suurimman positiivisen vaikutuksen tehtävät
(liikkuvan työn mahdollistaminen ja turvaaminen)

Miten toteutetaan?

1. Jokainen kirjautuminen ja sessio arvioidaan keskitetyssä policyssä – luetaan roolit ja pääsyoikeudet, tarkistetaan sijainti, tarkistetaan MFA-vaatimukset, tunnistetaan poikkeamat normaalista.

2. Laitteen hallittavuus ja konfiguraatio verifioidaan – varmistetaan ohjelmistoversiot, tiedon salaus, PIN/salasana-asetukset.

3. Pääsy rajataan - käyttäjän ja laitteen arvioinnin jälkeen tehdään pääsynhallintapäätös: sallitaan, evätään tai sallitaan osittain.

Miltä ZT näyttää Microsoft ekosysteemissä?