

CLOUD²

BUSINESS AS UNUSUAL



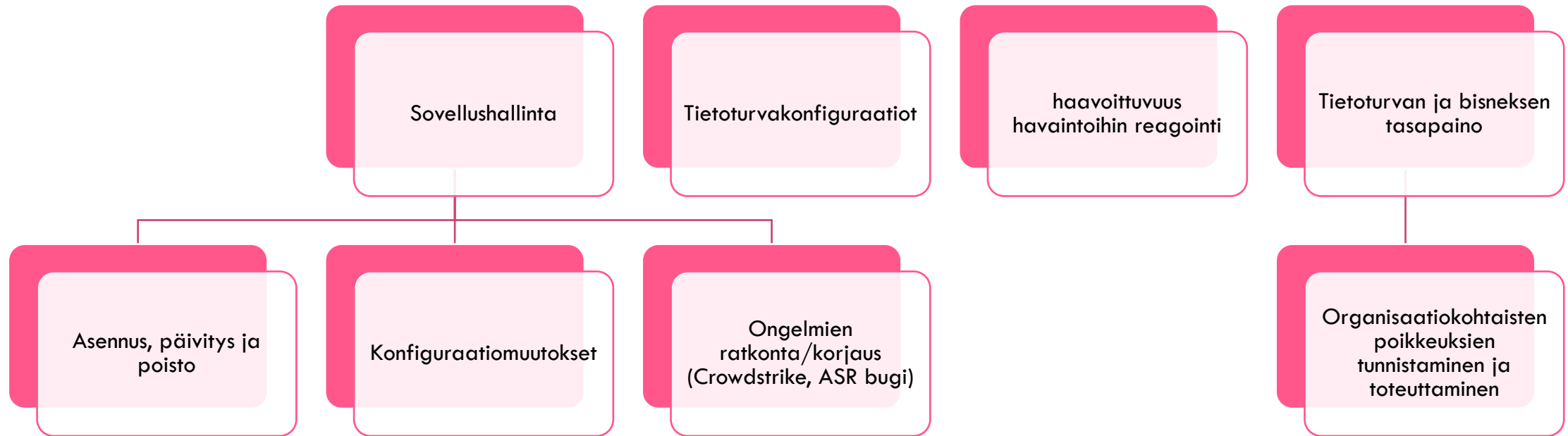
Defender for endpoint – Päätelaitehallinnan näkökulmasta

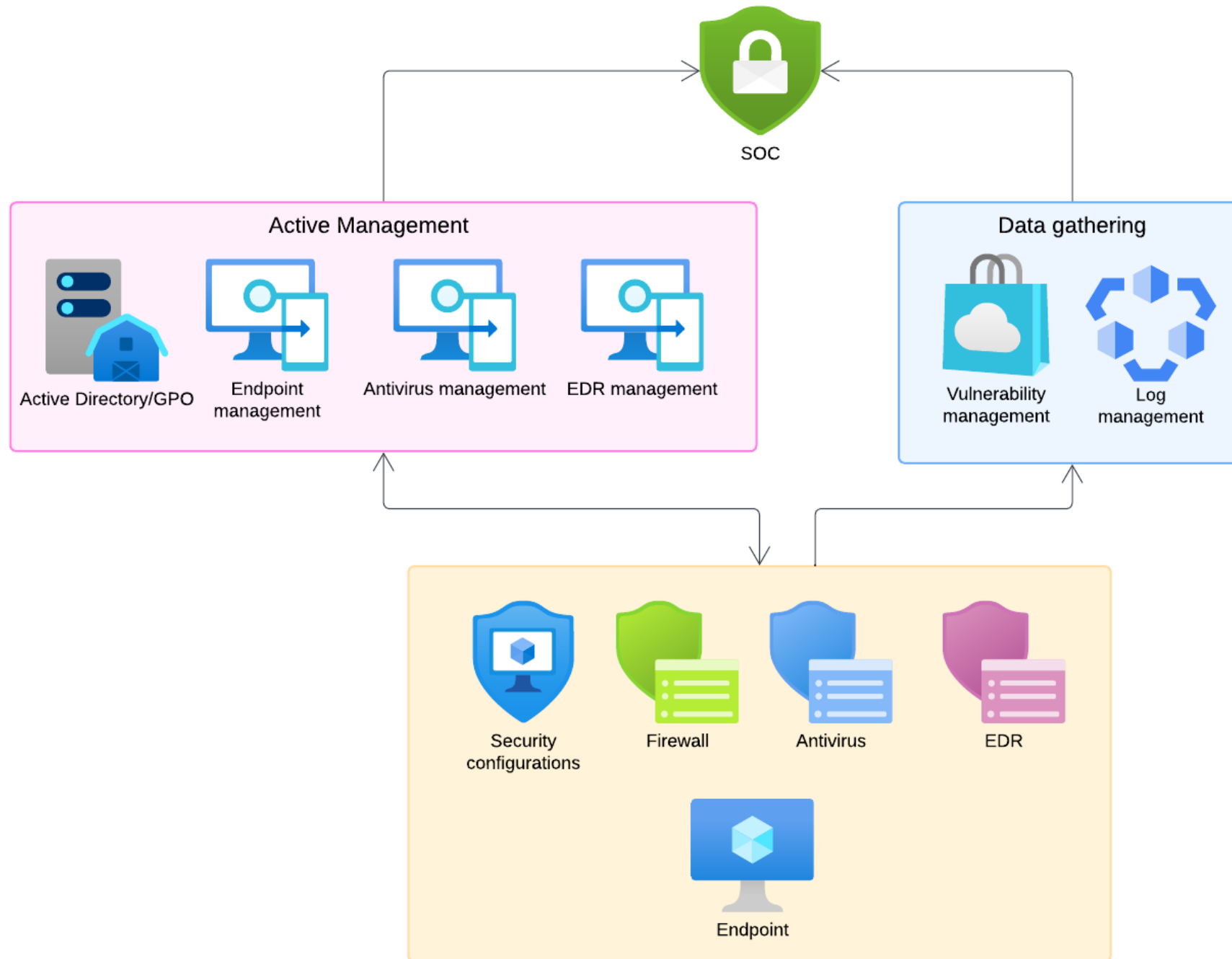
Esittely

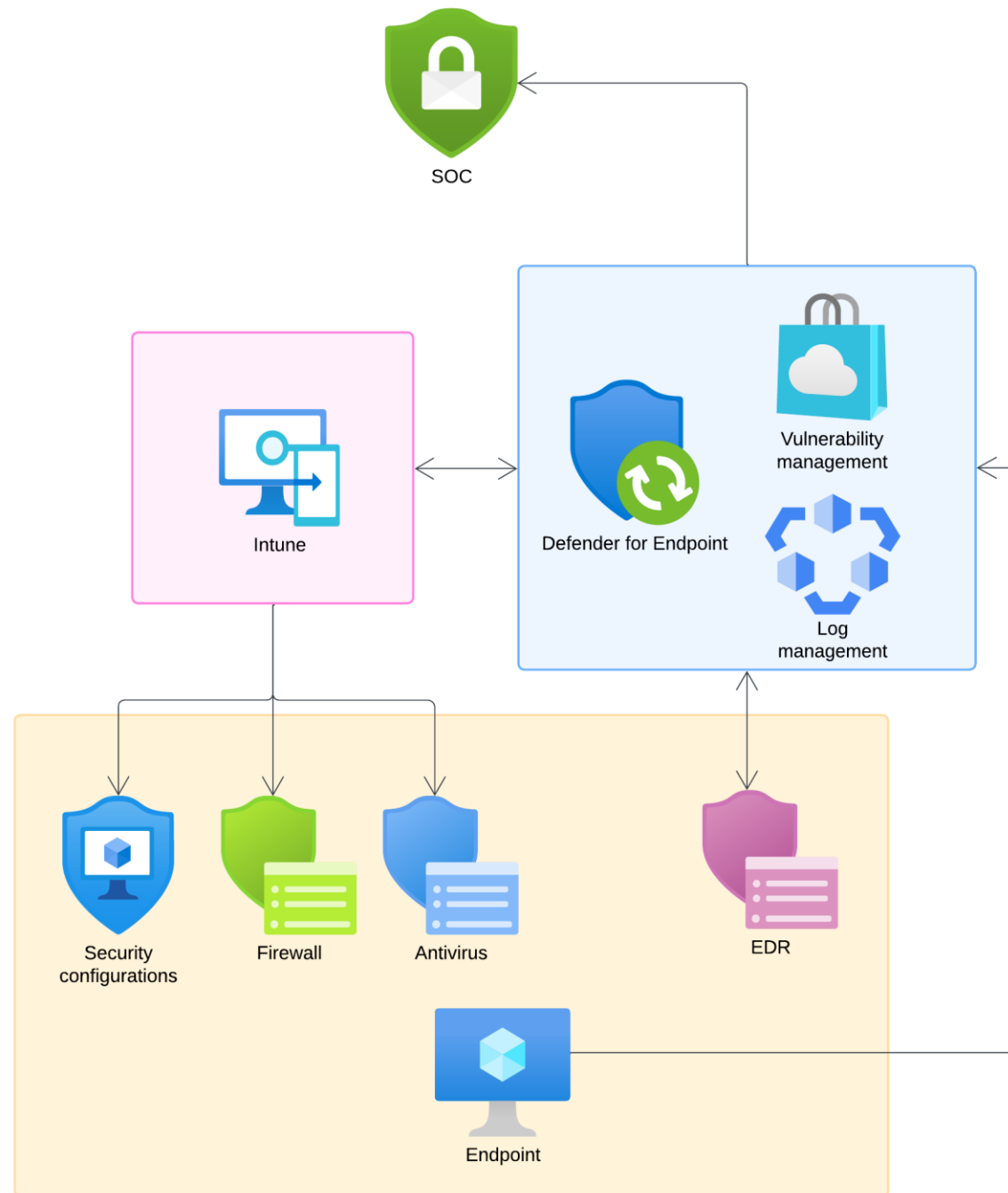
- Aku Suonpää
- Cloud2
- Alan hommissa 2004 lähtien
- Sovelluspaketointi, päätelaitehallinta
- Sipoo, kotoisin Urjalasta



Päätelaitehallinnan tehtävät tietoturvassa







Defenderin käyttöönnotossa huomioitavaa

Käytössä olevat tuotteet

- Konfiguraatioiden läpikäynti
- Tuotteiden poistaminen

Laiteryhmät (softa, rauta, käyttötarkoitus)

- OS, Desktop, Server, role, BYOD

Päätelaitteiden hallintaratkaisu

- Kuinka laitteet onboardataan
- Konfiguraatioiden jakelu

Käyttöönoton vaiheet

Defenderin konfigurointi

Laitteiden onboardaus

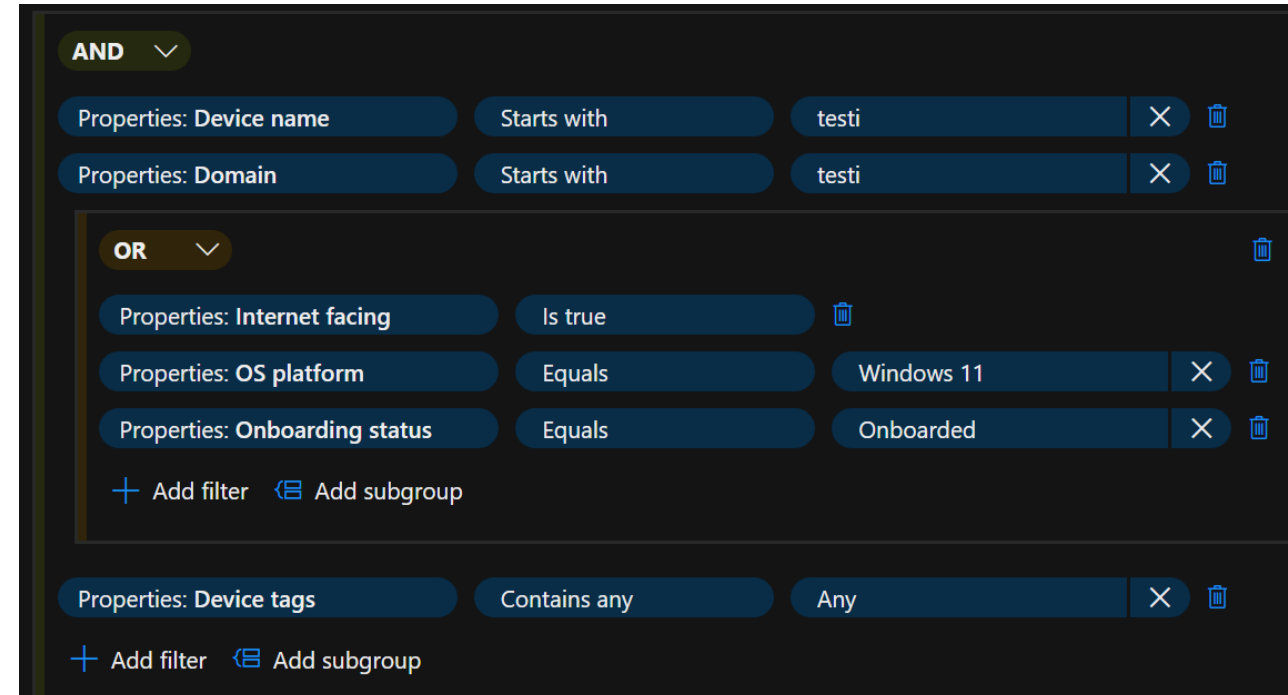
Vanhojen tuotteiden poisto

konfiguraatioiden jakelu

Vulnerability management prosessin aloittaminen

Device Tags

- Käytetään laitteiden tunnistamiseen ja toiminnallisuuksien kohdistamiseen
 - Filtteri tai laitteiden ryhmittely
 - Mixed license ja MDE onboardaus
- Tag määräytyy DFE:ssä määritetyn tai laitteeseen asetetun tiedon mukaan
 - Manual, Dynamic
 - Rekisteriavain, Intune configure ja app configure profile



The screenshot shows a configuration interface for Device Tags. It features a hierarchical structure with logical operators and filter rules.

- AND** (dropdown arrow)
 - Properties: Device name | Starts with | testi | [X] [trash]
 - Properties: Domain | Starts with | testi | [X] [trash]
- OR** (dropdown arrow) [trash]
 - Properties: Internet facing | Is true | [trash]
 - Properties: OS platform | Equals | Windows 11 | [X] [trash]
 - Properties: Onboarding status | Equals | Onboarded | [X] [trash]
 - + Add filter [Add subgroup]
- Properties: Device tags | Contains any | Any | [X] [trash]
- + Add filter [Add subgroup]

Device groups

Laiteryhmien tarkoitus

- Rajoittaa pääsyä hälytyksiin ja tietoihin
- Määrittää automaattiset korjaustoimet
- Suodattaa laiteluetteloita

Laite voi kuulua vain yhteen ryhmään

Jäsenyys määräytyy

- Ehtojen mukaan
- Käsittelyjärjestys

Remediation level *

Full - remediate threats automatically

No automated response

Semi - require approval for all folders

Semi - require approval for non-temp folders

Semi - require approval for core folders

Full - remediate threats automatically



And/Or	Condition	Operator	Value	
	Name	Starts with		+
And	Domain	Ends with		+
And	Tag	Equals		
Or	Tag	Contains		+ 🗑️
And	OS	In	Windows 11, Windows 10,...	▼



Raportit

Configuration settings [Edit](#)

✓ Firewall

^ Auditing

Object Access Audit Filtering Platform
Connection  

Object Access Audit Filtering Platform
Packet Drop  

✓ Endpoints (7)

★ Vulnerable devices

★ Attack surface reduction rules

★ Device control

★ Device health

★ Firewall

★ Monthly security summary

★ Web protection

Advanced hunting

- Kusto Query Language (KQL) –kieli
- Haettavia tietoja mm:
 - Tiedostotiedot, Prosessitiedot, Rekisteritiedot, Verkkoyhteystiedot, Laitetiedot, Käyttäjätiedot, Sovellustiedot, Turvallisuustapahtumat

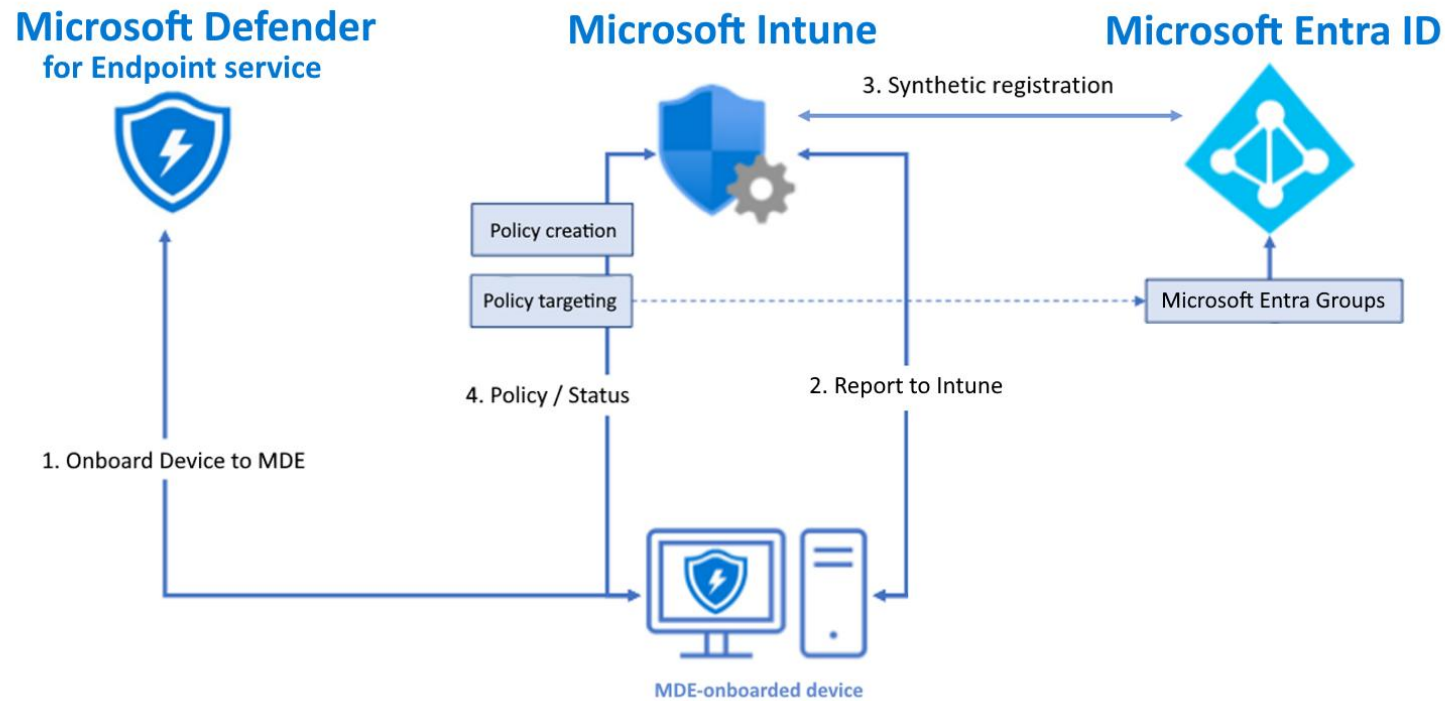
```
1 DeviceEvents
2 | where ActionType startswith 'AppControl'
3 | project Timestamp, DeviceName, ActionType, FileName, FolderPath, InitiatingProcessFileName, InitiatingProcessCommandLine
```

```
1 DeviceFileEvents
2 | where ActionType == "FileCreated"
3 | where FileName endswith ".crx"
4 | where InitiatingProcessFileName == "msedge.exe"
5 | summarize FileCount = count() by FileName
```

MDE onboard



How does it work?



Target

MDM, MicrosoftSense

MDM, MicrosoftSense

MDM, MicrosoftSense

MDM, MicrosoftSense

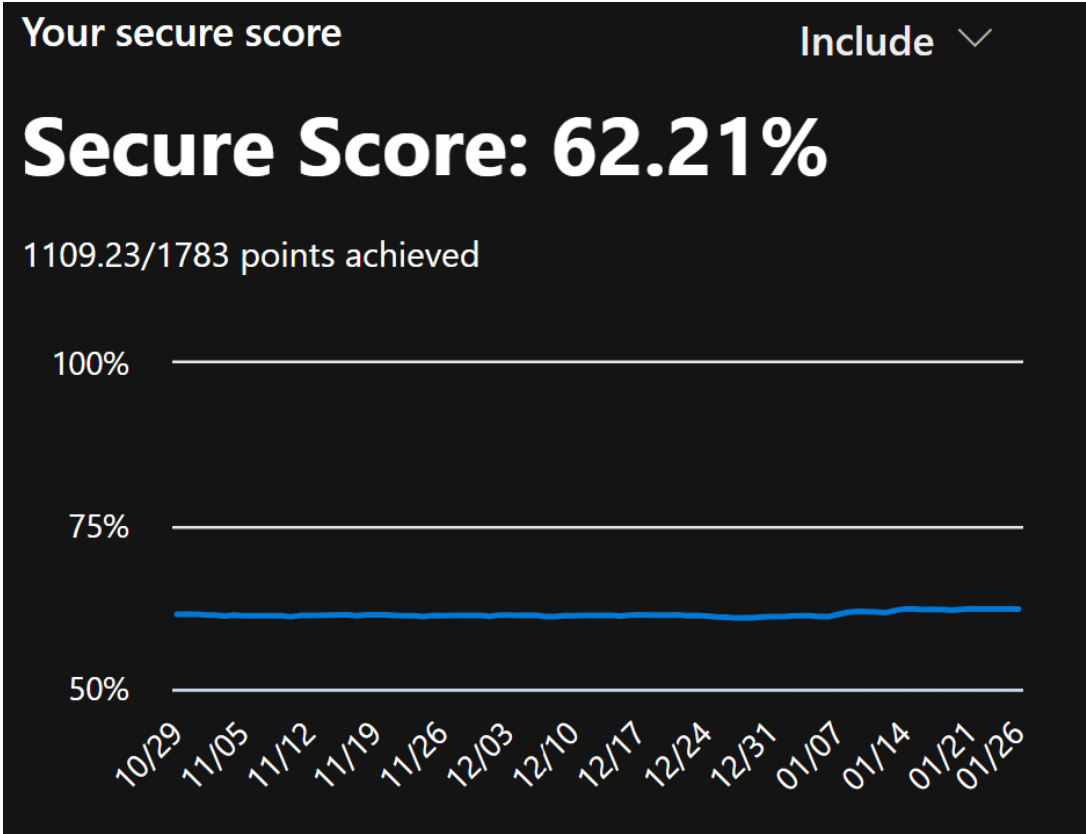
Managed by ↓

MDE

Co-managed

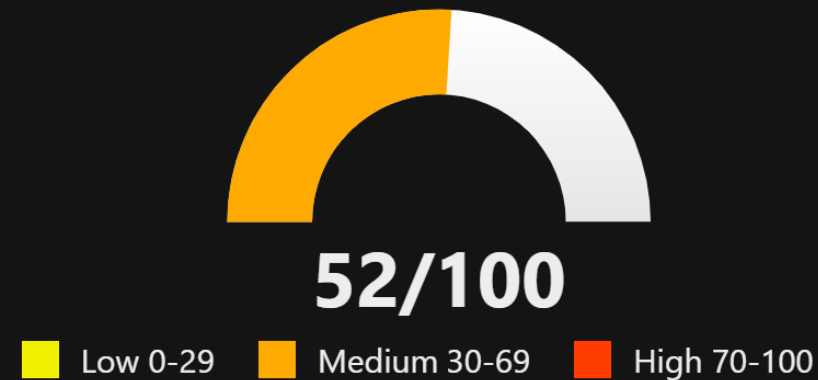
Co-managed

Scoret



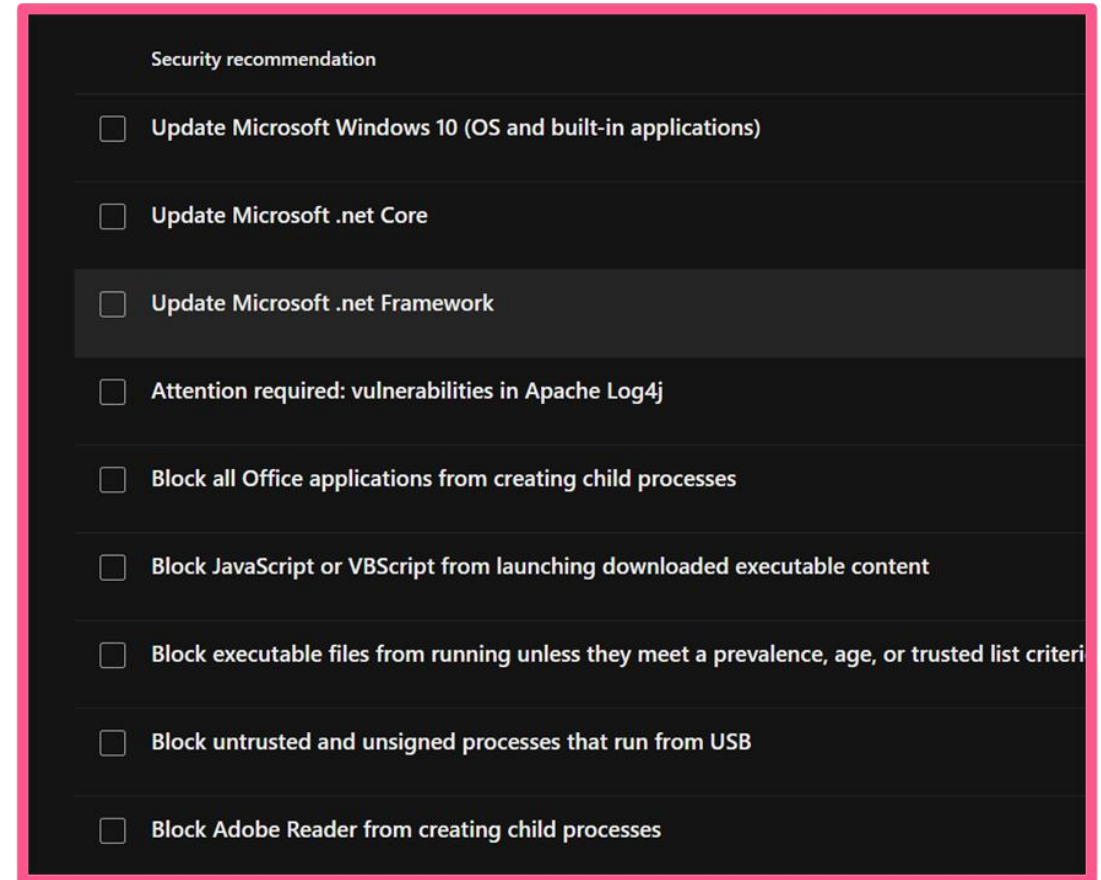
Exposure score

This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.



Vulnerability management

- Defender tuottaa haavoittuvuus dataa ympäristöstä
- Organisaatiosta riippuen datan käsittely vaatii eri toimijoiden yhteistyötä
 - Haavoittuvuushallinta: Käsittelee, viestii ja dokumentoi DFE:n datan
 - Palveluomistaja: Taho joka vastaa laiteryhmän tai sovellusten toiminnasta
 - Päätelehallinta: Toteuttaa ympäristön halutut muutokset



Vulnerability management käyttöönotto

1. Tunnistetaan sopivat laiteryhmät
2. Määritellään ja dokumentoidaan käsittelysäännöt
3. Käsitellään **lähtödata** käsittelysääntöjen mukaisesti
 1. Justification & Context
 2. Exception Duration
4. Palvelu on valmis ilmoittamaan automaattisesti käsittelyä vaativat havainnot
5. Sääntöjen jatkuva arviointi ja muuttaminen tarvittaessa osana jatkuvaa prosessia

Block all Office applications from

Remediation required

Human operated ransomware User impact assessment

Open software page Report inaccuracy

General Remediation options Expose

Description

Block Surface Reduction (ASR) rules are the most effective common attack techniques being used in cyberattacks. An ASR rule blocks Office apps from creating child processes, OneDrive, OneNote, and Access.

Note: Some legitimate line-of-business applications may require spawning a command prompt or using PowerShell.

This security control is only applicable for machines running Windows 10, Windows Server 2019, and Windows Server 2016.

Potential risk

Creating child processes is a typical malware behavior, especially for attacks that abuse Office as a vehicle to download and attempt to run additional malware.

Recommendation insights

- No devices in your organization are configured with this rule.
- This configuration is recommended by the Microsoft Security Baseline (STIG).

Get more insights into how well your organization is managing ransomware in exposure management.

User impact ⓘ

Request remediation

Exception options

Create exception

Block all Office applications from creating child processes

Create an exception if you currently cannot or do not want to remediate this recommendation. Creating an exception changes the recommendation status from "Active" to "Exception" (global) or "Partially active" (by device group). To remediate the recommendation after you have created an exception, you can either cancel or the exception expire.

Exception scope

Affects specific device groups chosen by you. If you choose "All," it will affect all machine groups in this list. Device groups that already have an exception will not be displayed.

Filter by device groups (1/72)

Justification and duration

Justification

Planned remediation (grace)

Provide justification context

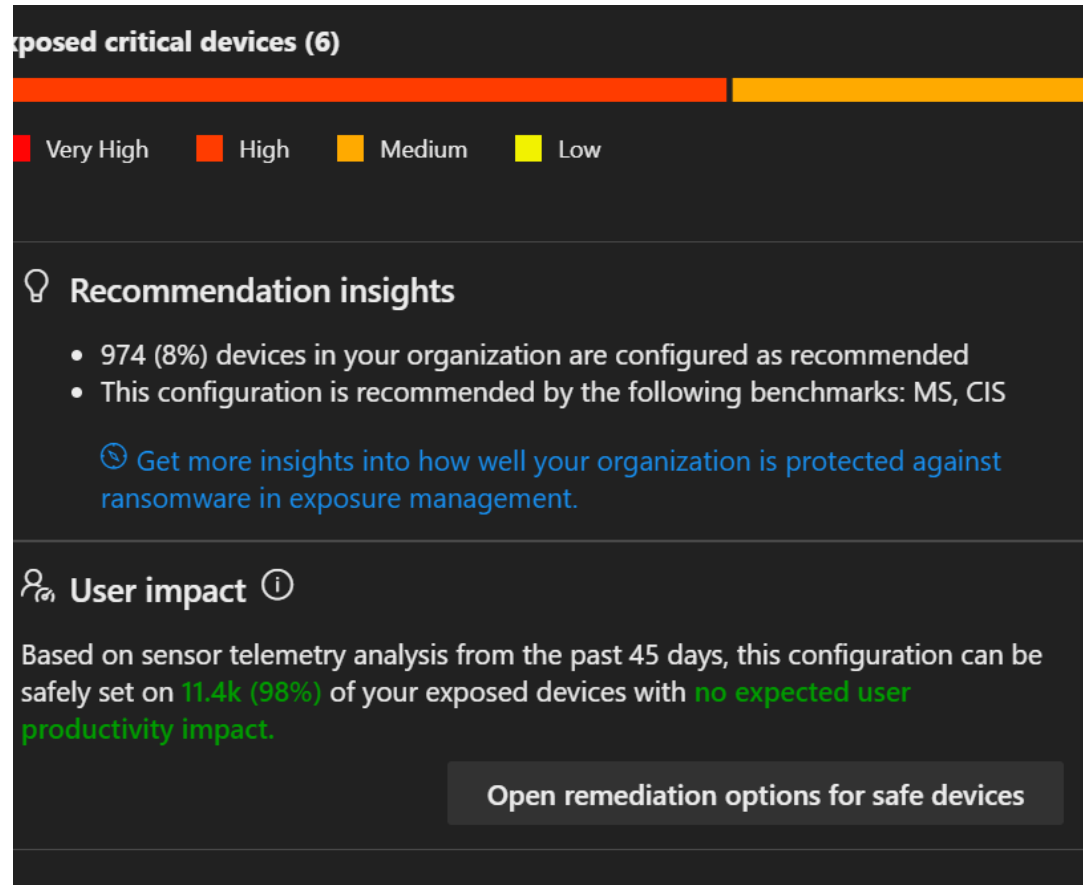
There is a remediation process in progress for this recommendation <provide additional information>. This process is expected to end by <provide date>

Exception duration

90 days

Submit

Vulnerability management prosessi



1. DFE raportoi haavoittuvuuden
2. Haavoittuvuuksienhallinta käsittelee havainnon ennalta määritettyjen sääntöjen mukaan
3. Palvelunomistaja käsittelee tiedon ja päättää mahdolliset muutokset
4. Haavoittuvuuksienhallinta dokumentoi suunnitelman DFE:lle
5. Päätelaitehallinta toteuttaa mahdollisen muutoksen
6. DFE hälyttää jos muutos ei toteudu suunnitellussa aikataulussa

Kysyttävää? Ajatuksia?





Google Cloud

**BUSINESS
AS UNUSUAL**