Sami Laiho
Senior Technical Fellow, MVP

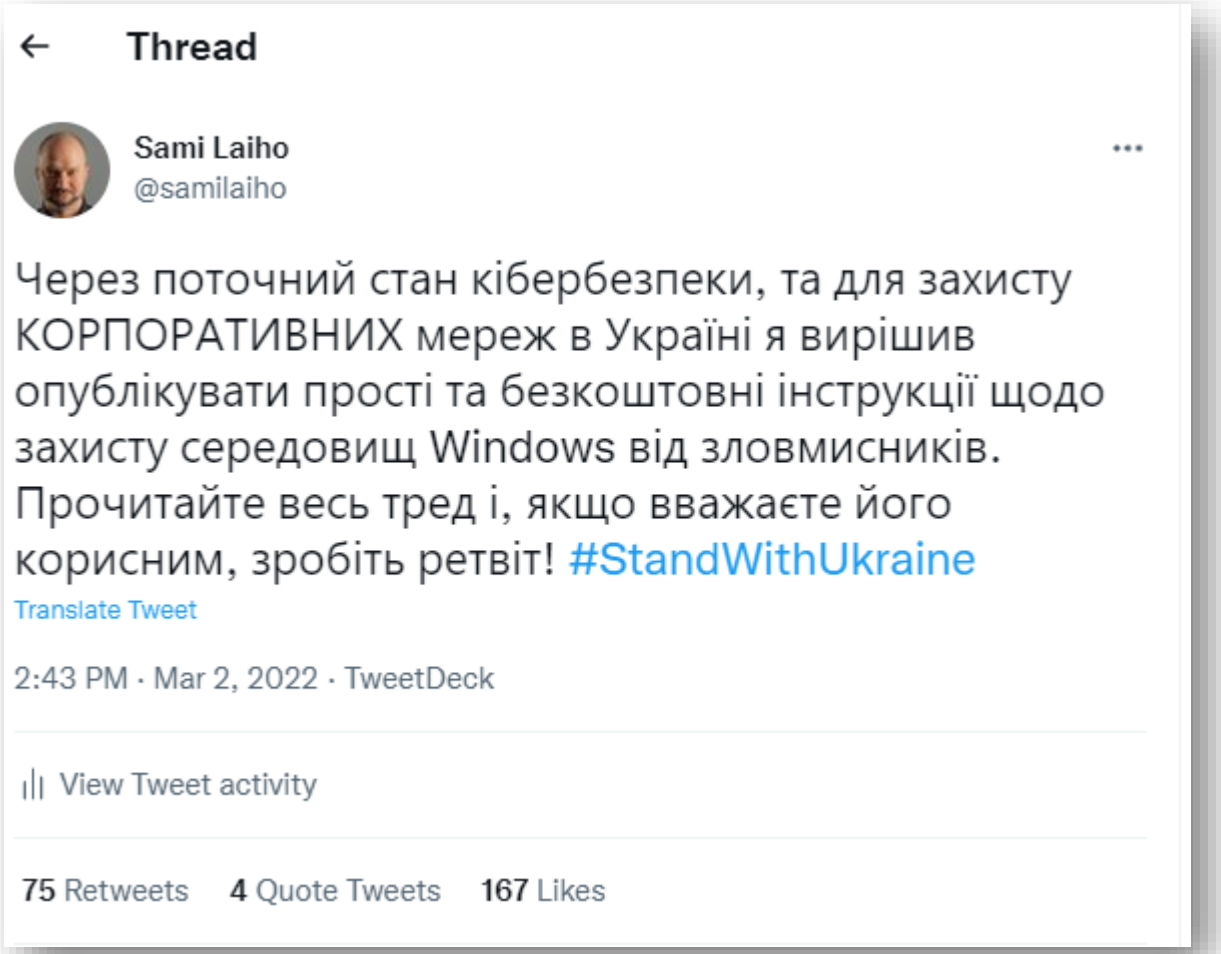
Tietoturva Nyt ja Tulevaisuudessa!

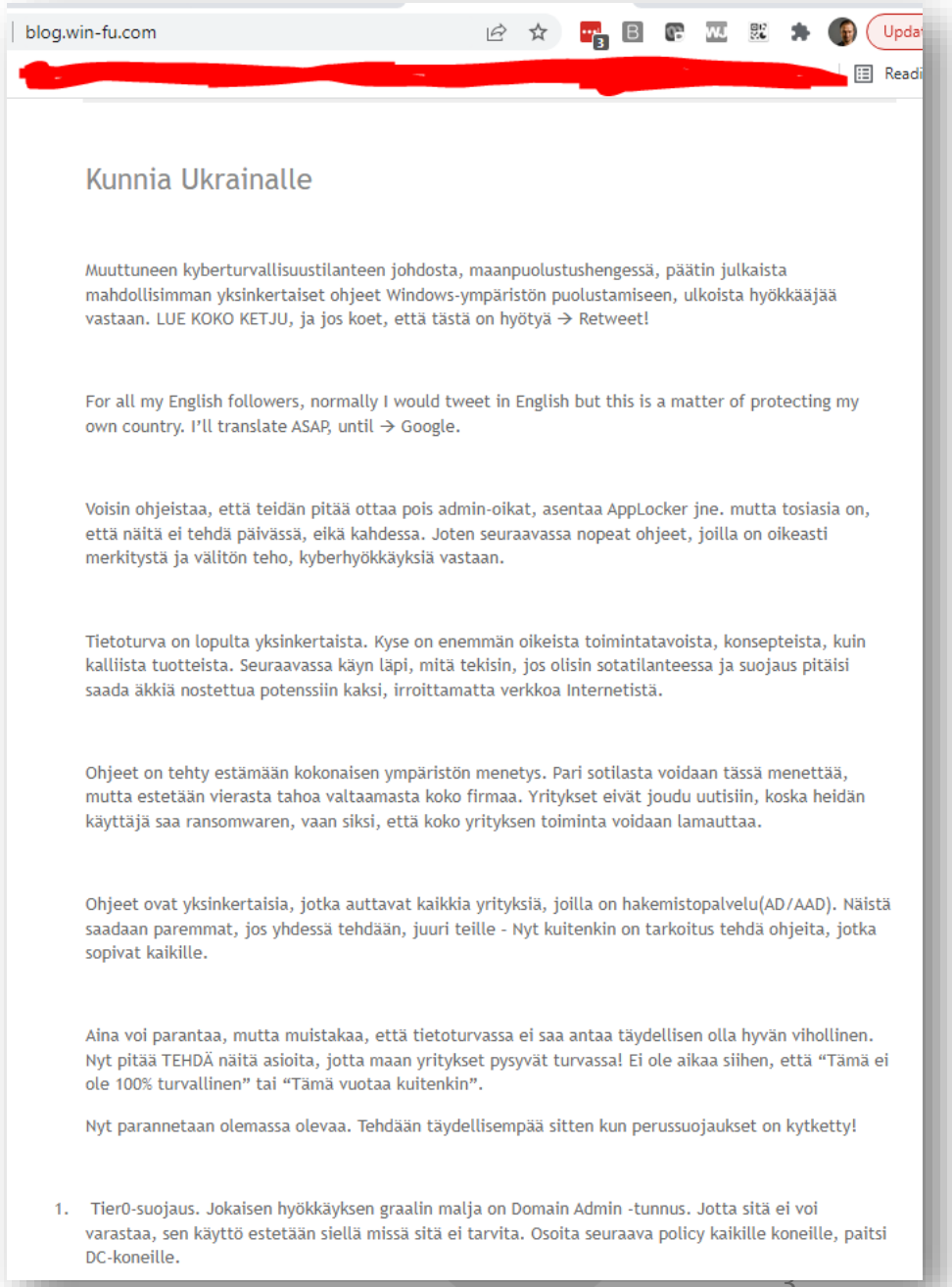
Sami Laiho

Senior Technical Fellow
adminize.com

- IT Admin since 1996
- MVP in Windows OS since 2011
- **”100 Most Influencal people in IT in Finland” – TiVi’2019→**
- Specializes in and trains:
  - Troubleshooting
  - Security, Social Engineering, Auditing
- Trophies:
  - **Ignite 2018 – Best Session and #2 (out of 1708) !**
  - Best speaker at Advanced Threat Summit 2020, Poland
  - Best Speaker at NIC, Oslo 2016, 2017, 2019 and 2020
  - Best Session at AppManagEvent 2017, 2018, Utrecht
  - TechEd Europe and North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker

Ukrainan tilanne…



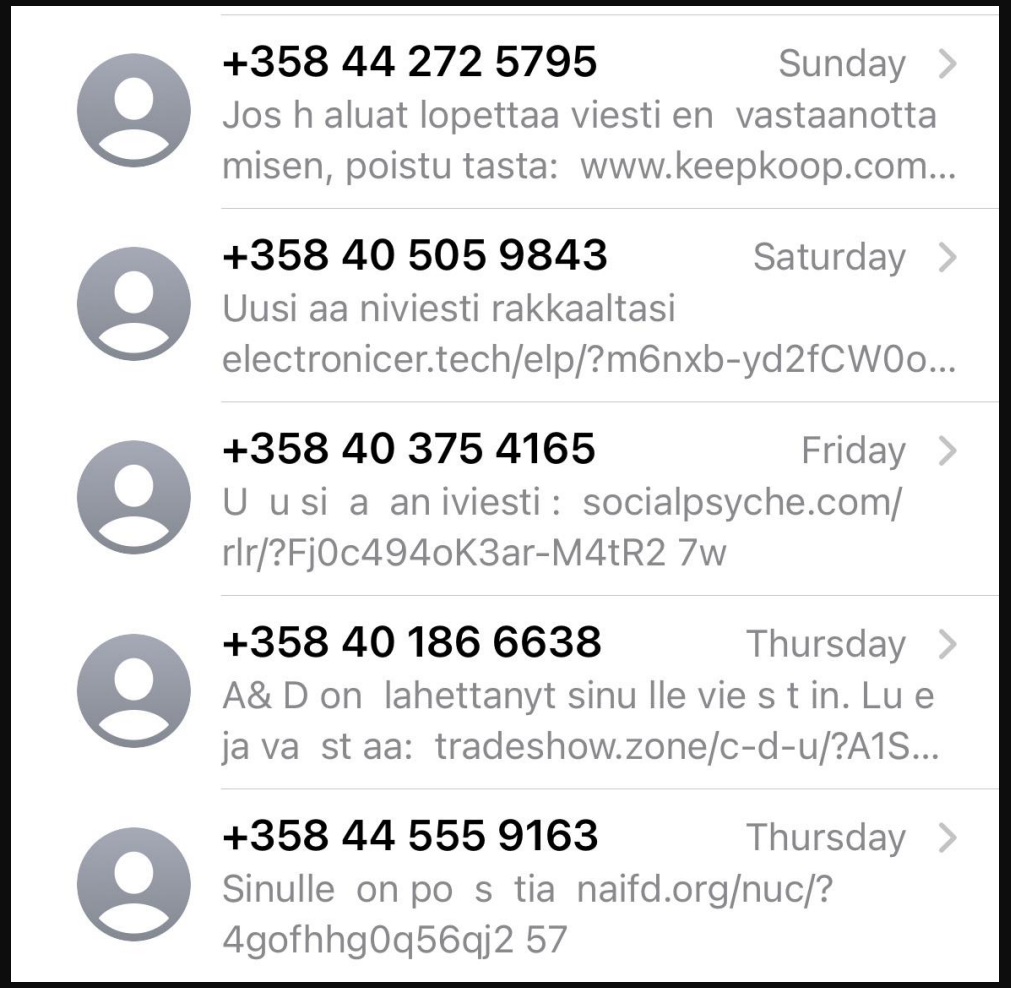


Tietoturva on lopulta aika yksinkertaista


“You don’t have to make your security perfect, just better than your neihbour’s”
Mikko Hyppönen

Windows vs Android
PC vs Mobile

FluBot


+358 44 272 5795
Sunday
Jos h aluat lopettaa viesti en vastaanotta misen, poistu tasta: www.keepkoop.com...
+358 40 505 9843
Saturday
Uusi aa niviesti rakkaaltasi electronicer.tech/elp/?m6nxb-yd2fCW0o...
+358 40 375 4165
Friday
U u si a an iviesti : socialpsyche.com/ rlr/?Fj0c494oK3ar-M4tR2 7w
+358 40 186 6638
Thursday
A& D on lahettanyt sinu lle vie s t in. Lu e ja va st aa: tradeshow.zone/c-d-u/?A1S...
+358 44 555 9163
Thursday
Sinulle on po s tia naifd.org/nuc/? 4gofhhg0q56qj2 57

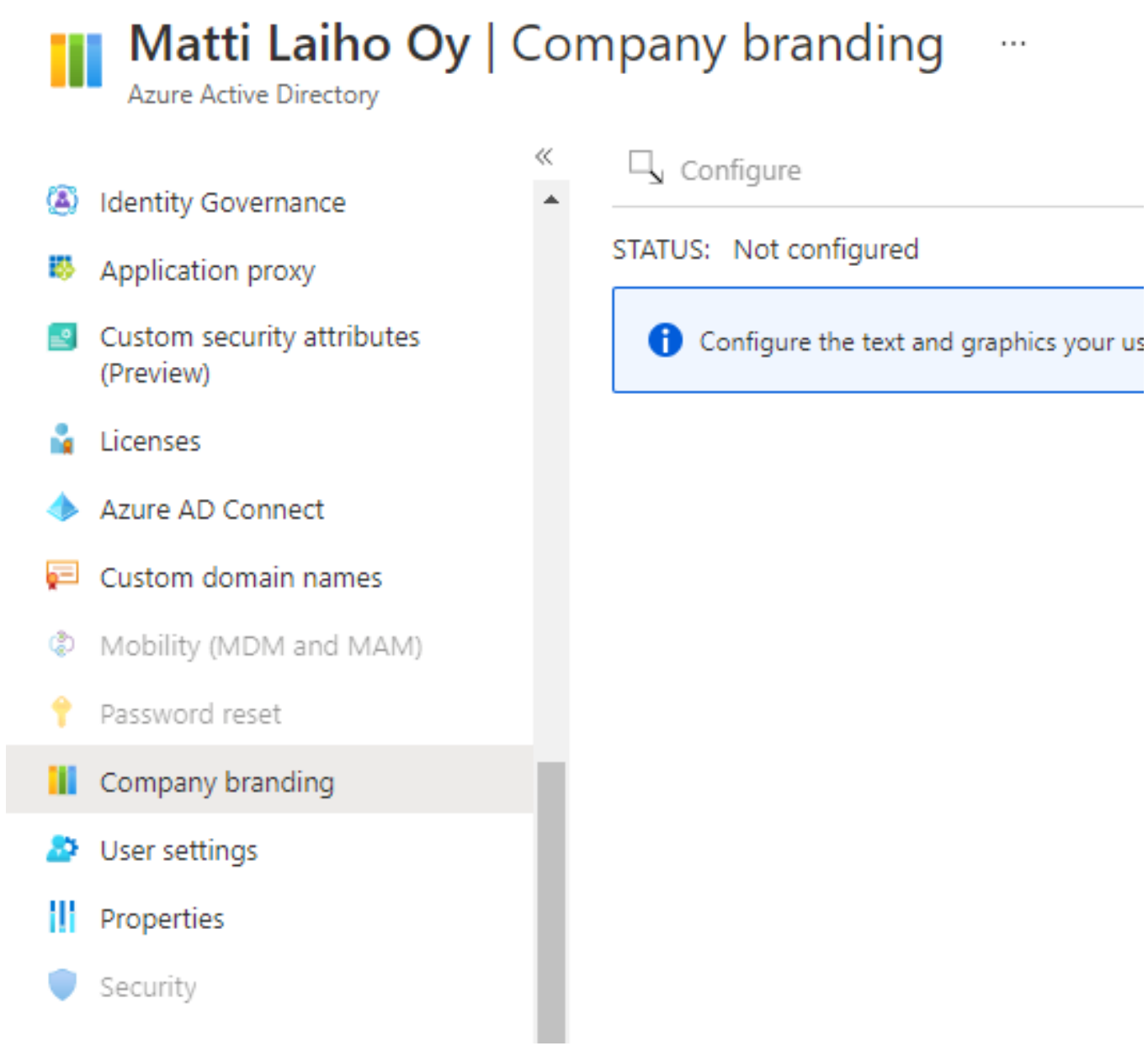
Sisältö

- Älä näytä “osaamattomalta”
- Rajoita kovimpien tunnusten käyttöä radikaalisti
- Estä tunnusten, joilla ympäristöä voi vahingoittaa eniten, käyttö muualta, kuin missä niille on tarve
- Estä hallintaohjelmien yms. ajaminen niiltä koneilta joilta pääsee Facebookiin
- Estä koneita puhumasta järjestelmille, jos ei ole tarvetta
- Estä pelkkien salasanojen käyttö
- Salaa kaikkien koneiden levyt
- Älä anna käyttäjille admin-oikeuksia
- Tärkeimmät tietoturvakontrollit ovat: Ajantasalla olevat rauta- ja softainventaario
- Perusta/ulkoista SoC

Ulkoinen evaluointi

Älä näytä amatööriltä

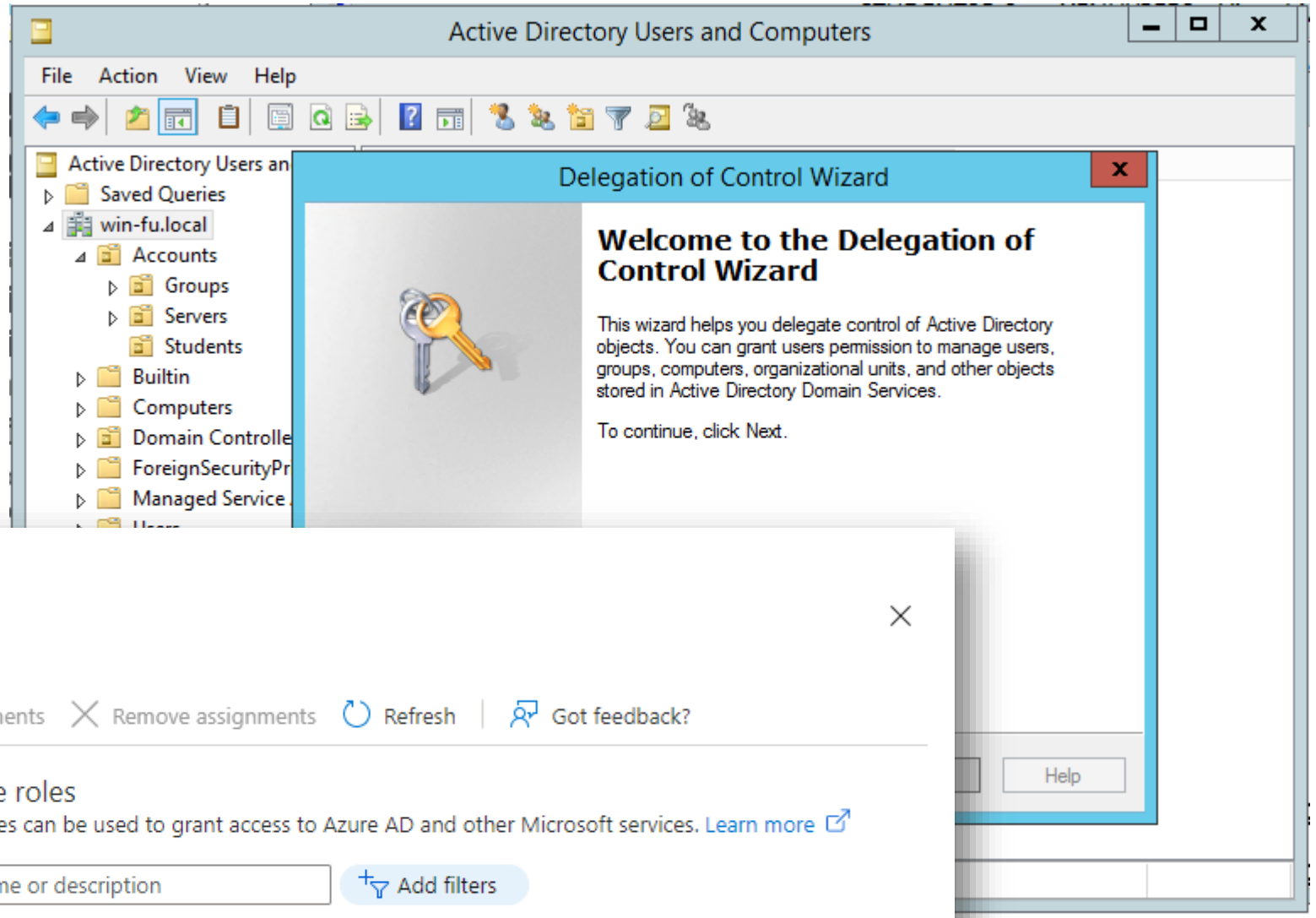
Company Branding

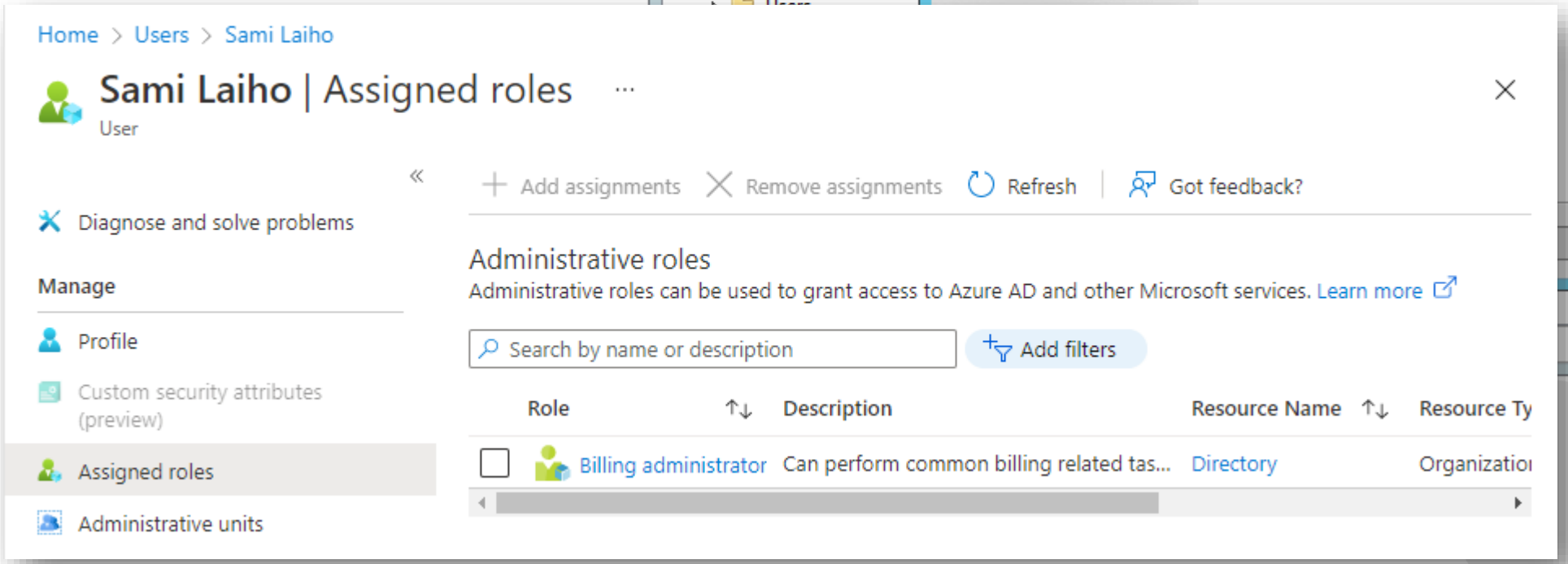


Global Adminien minimointi

3 on monelle liikaa, 1 aina liian vähän

Delegoi


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users an
Saved Queries
win-fu.local
Accounts
Groups
Servers
Students
Builtin
Computers
Domain Controlle
ForeignSecurityPr
Managed Service
Delegation of Control Wizard
Welcome to the Delegation of Control Wizard
This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.
To continue, click Next.
Help

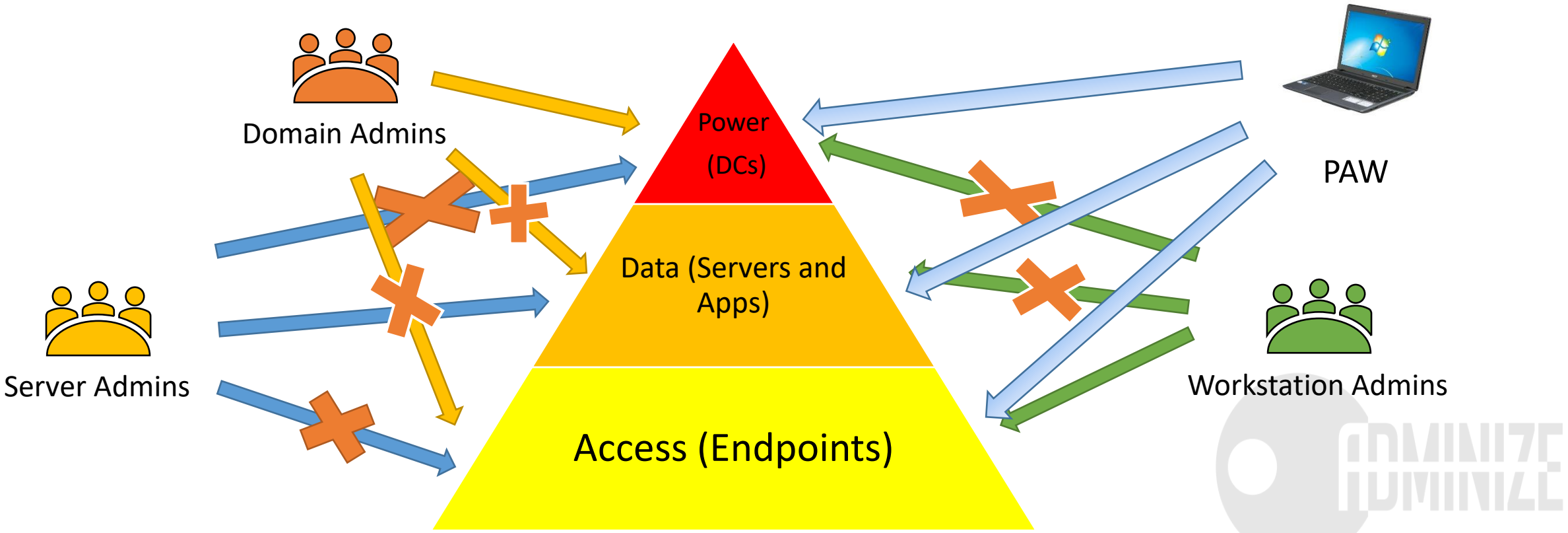

Home > Users > Sami Laiho
Sami Laiho | Assigned roles
User
Diagnose and solve problems
Manage
Profile
Custom security attributes (preview)
Assigned roles
Administrative units
Add assignments
Remove assignments
Refresh
Got feedback?
Administrative roles
Administrative roles can be used to grant access to Azure AD and other Microsoft services. Learn more
Search by name or description
Add filters
Role
Description
Resource Name
Resource Ty
Billing administrator
Can perform common billing related tas...
Directory
Organizatio

Tier-malli & PAW

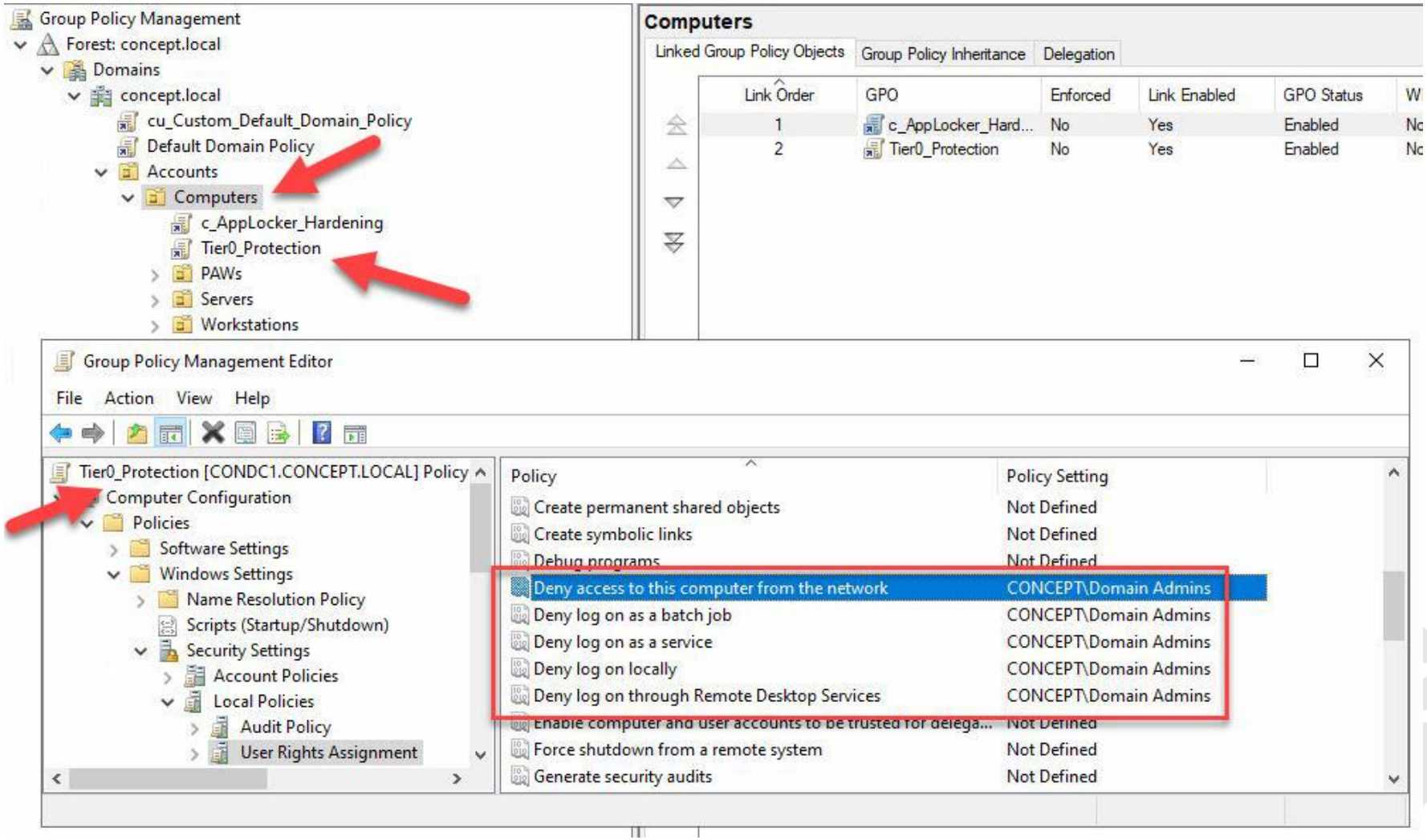
Estä vaarallisten käyttäjien käyttö, tarpeettomissa paikoissa

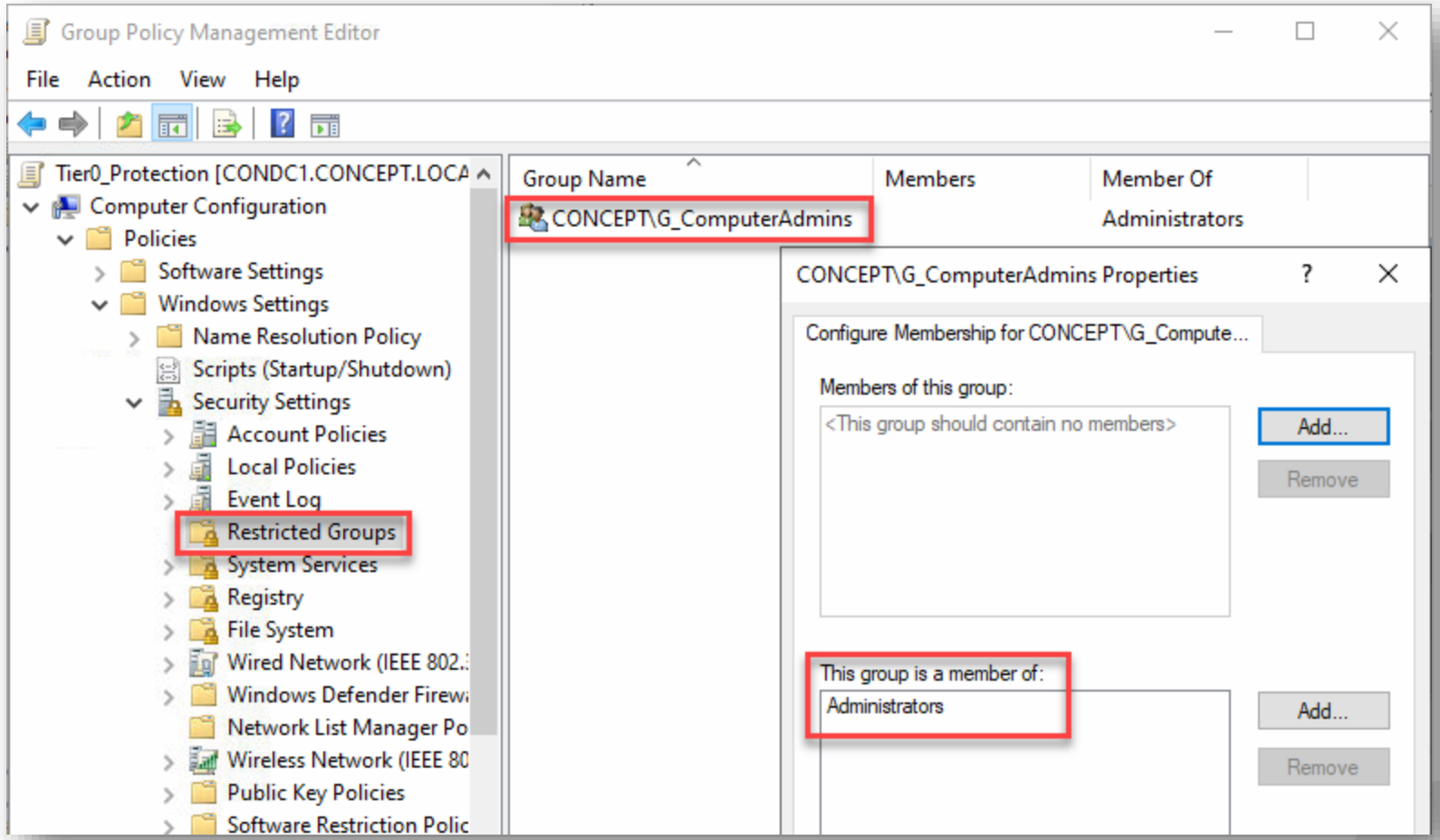
AD:n kerrostaminen (AD Tiering)

- Ympäristö jaetaan osiin, jotta kaikkea ei menetetä, jos tuulettimeen osuu
- Ylemmän tason ylläpitäjät eivät voi kirjautua alemmille tasoille



Jos ei muuta, niin ainakin tämä!

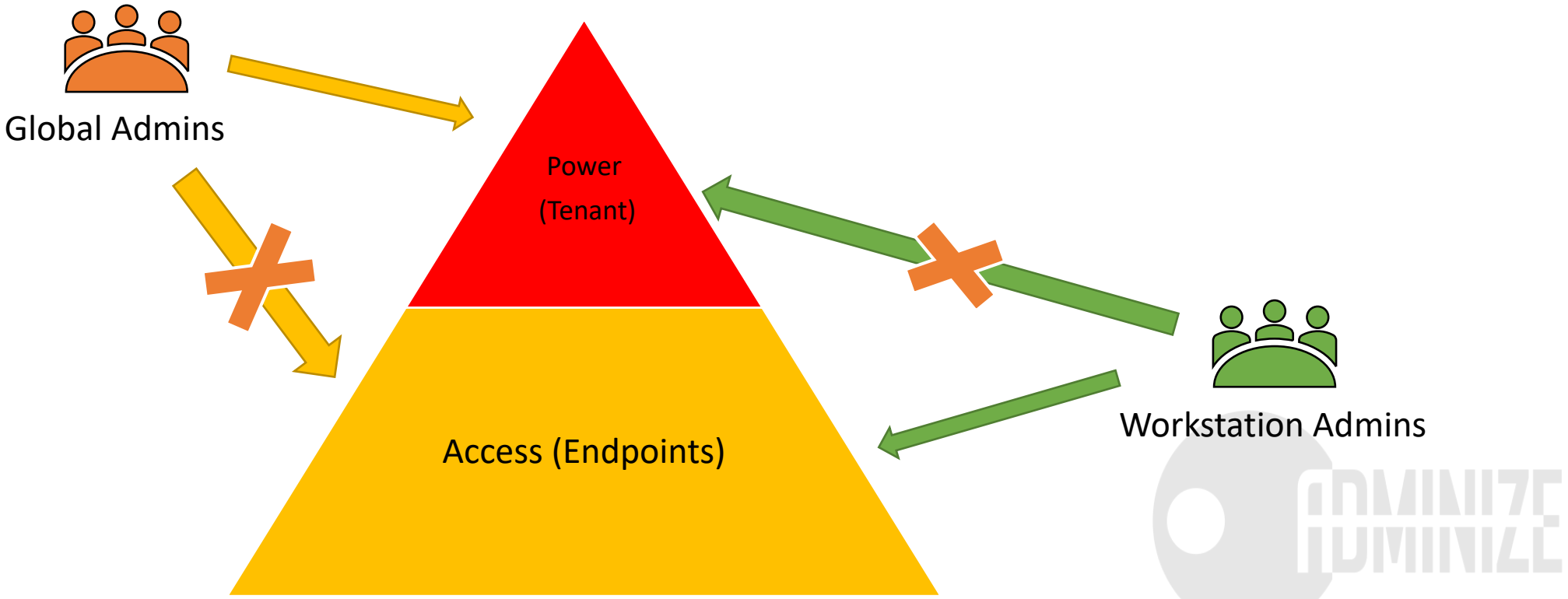



Group Policy Management Editor
File
Action
View
Help
Tier0_Protection [CONDC1.CONCEPT.LOCA
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.
Windows Defender Firew
Network List Manager Po
Wireless Network (IEEE 80
Public Key Policies
Software Restriction Polic
Group Name
Members
Member Of
CONCEPT\G_ComputerAdmins
Administrators
CONCEPT\G_ComputerAdmins Properties
Configure Membership for CONCEPT\G_Compute...
Members of this group:
<This group should contain no members>
Add...
Remove
This group is a member of:
Administrators
Add...
Remove

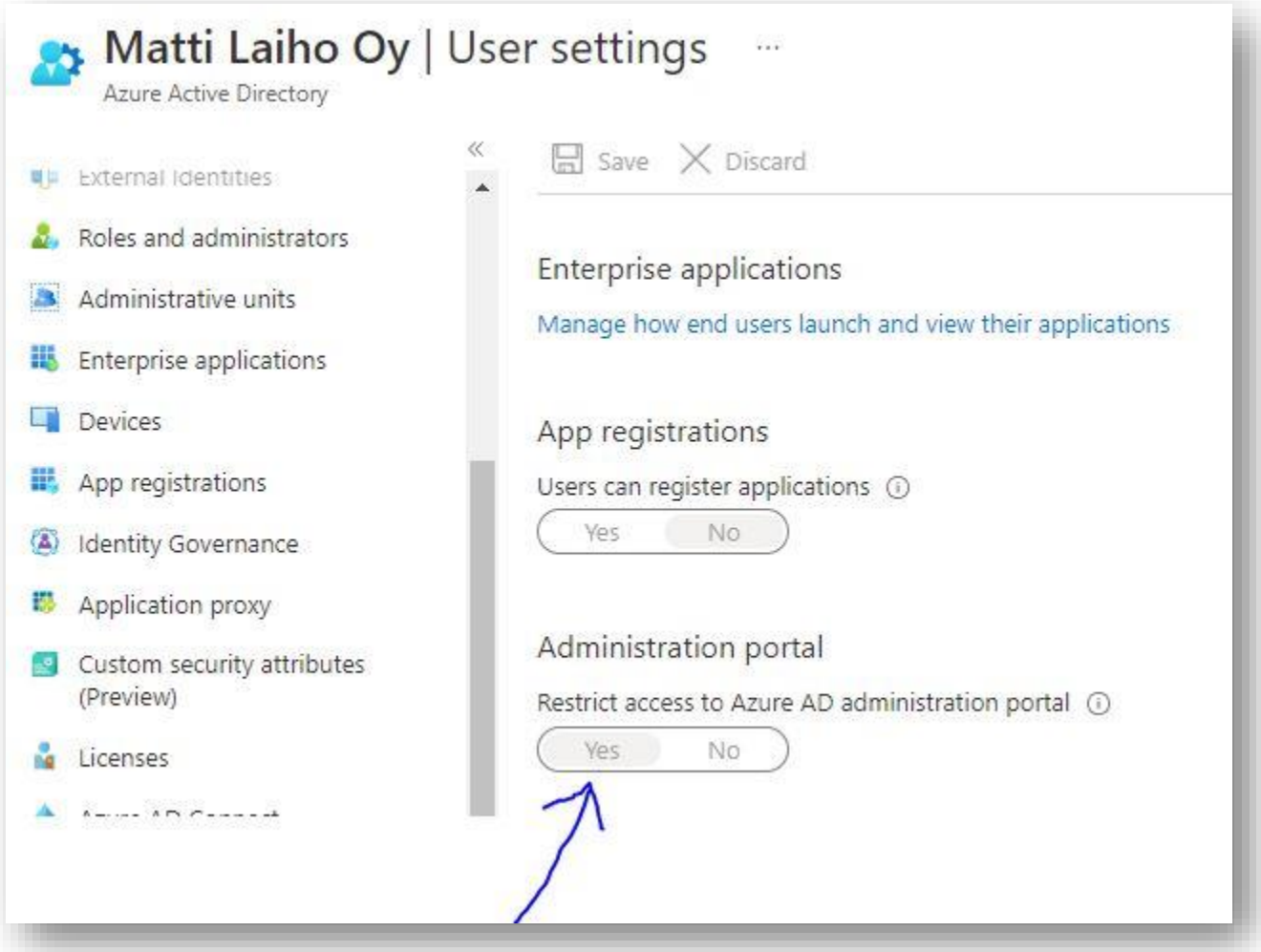

Pilvessä?
cloud

ADD Tiering (Native Cloud)

- Ympäristö jaetaan osiin, jotta kaikkea ei menetetä, jos tuulettimeen osuu
- Ylemmän tason ylläpitäjät eivät voi kirjautua alemmille tasoille



Käyttäjien esto pääsemästä AAD-portaaliin

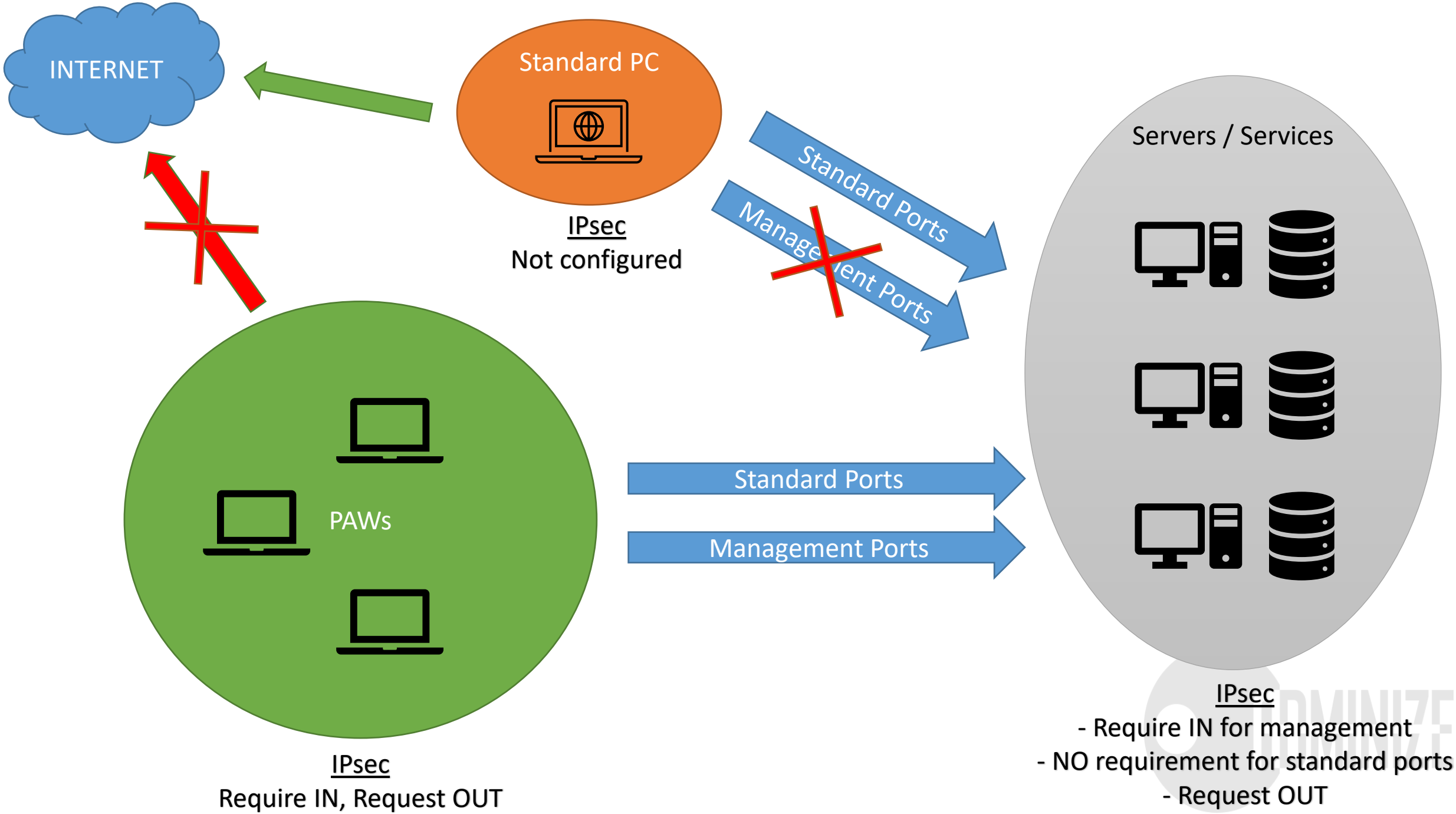


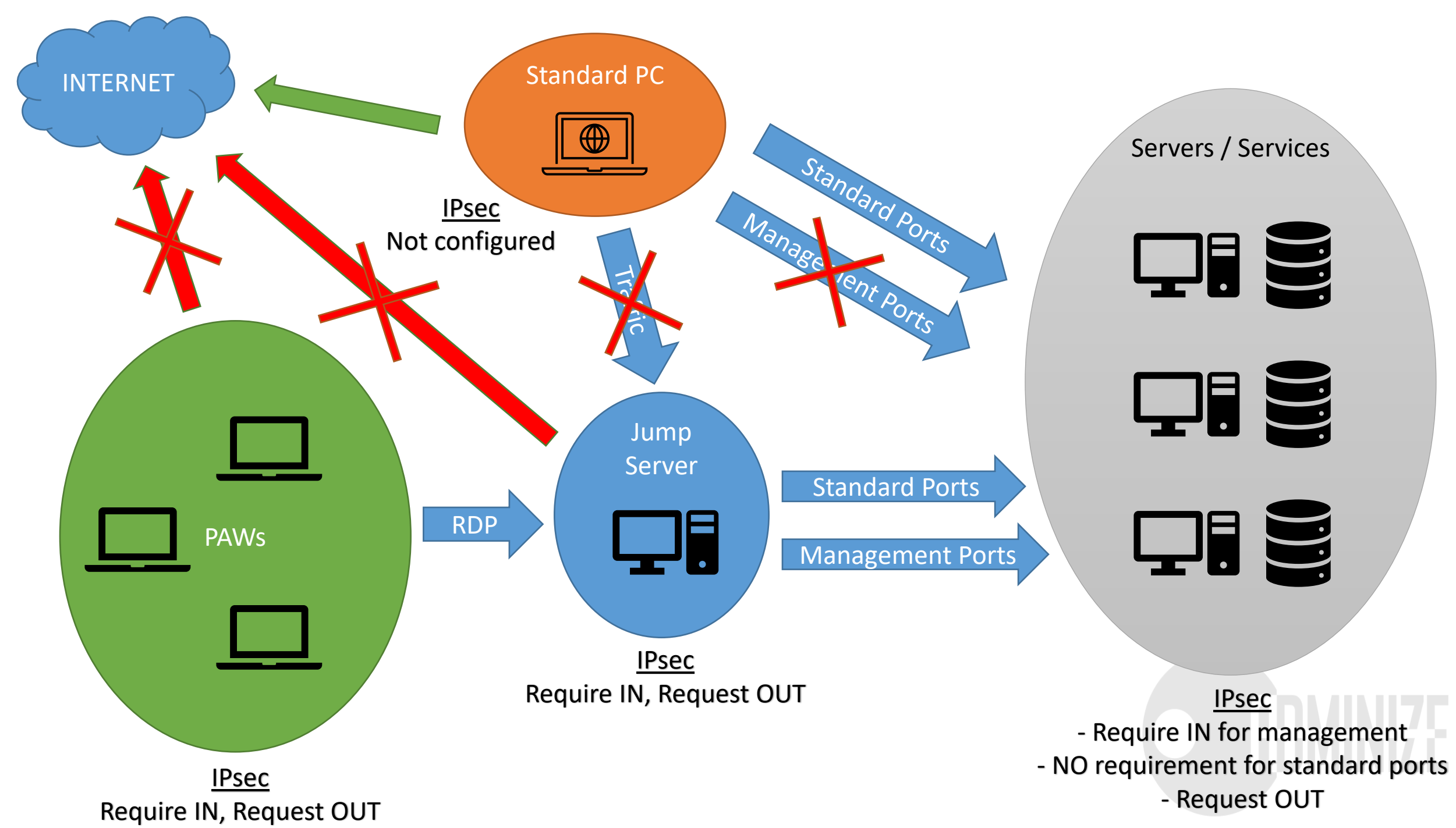
Jos koneelta voi hallita, sieltä ei pitäisi voida käyttää Facebookia...

Privileged Access Workstation (PAW)

PAW-työasema

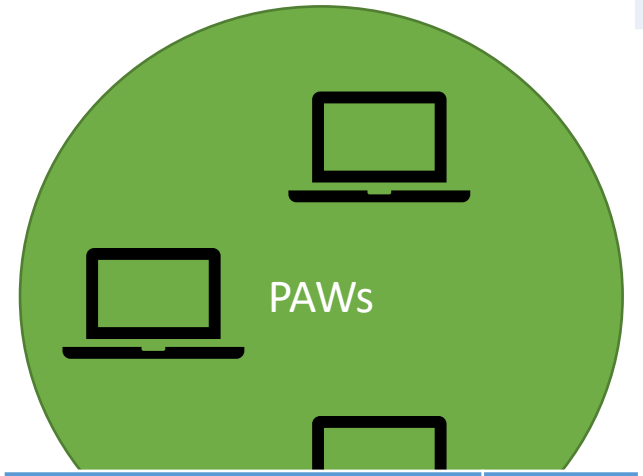
- Vain hallintaan omistettu työasema (virtuaalinen tai fyysinen)
- Hallintatyökalut asennettuna
- Vain IT-osasto pystyy käyttämään
- Kovempi tietoturvataso kuin normaalilla työasemalla
- Ei (vapaata) pääsyä Internetiin
- Ei Office-sovelluksia ym.


INTERNET
Standard PC
IPsec
Not configured
Standard Ports
Management Ports
Servers / Services
PAWs
Standard Ports
Management Ports
IPsec
Require IN, Request OUT
IPsec
- Require IN for management
- NO requirement for standard ports
- Request OUT

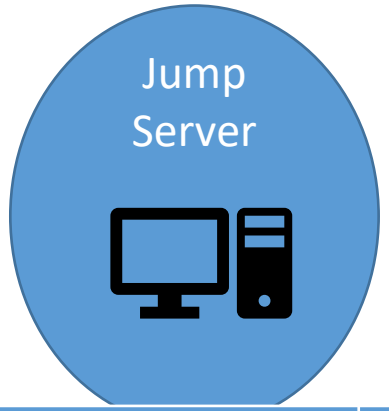

INTERNET
Standard PC
IPsec
Not configured
Standard Ports
Management Ports
Servers / Services
PAWs
RDP
Jump
Server
Standard Ports
Management Ports
IPsec
Require IN, Request OUT
IPsec
Require IN, Request OUT
IPsec
- Require IN for management
- NO requirement for standard ports
- Request OUT

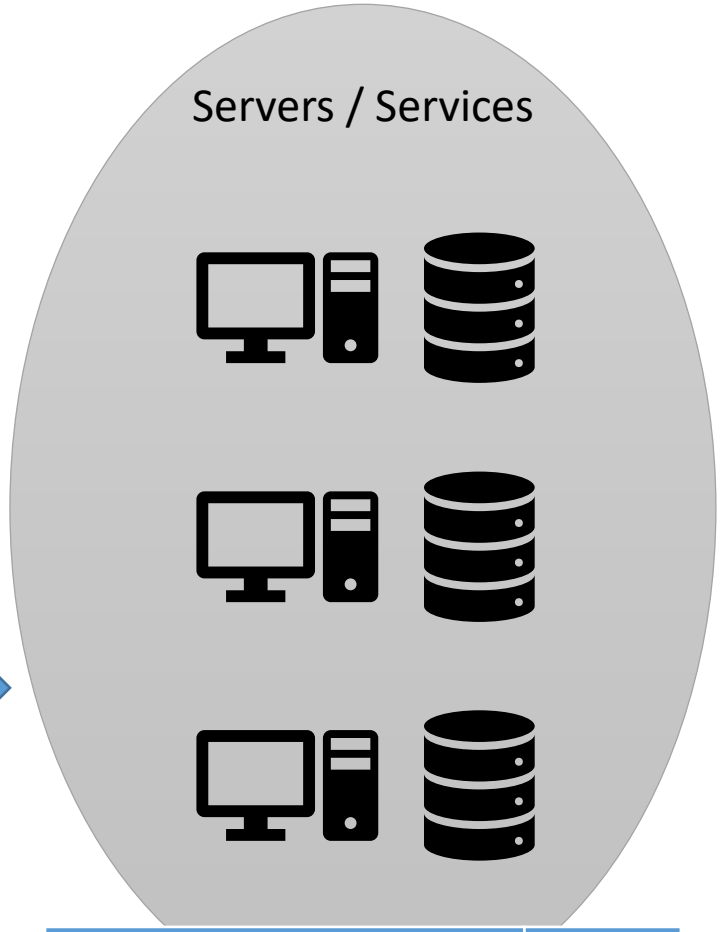
Administrators-group members

Administrators	
Domain Admins	YES
Workstations Admins	YES
Server Admins	NO
Builtin Administrator (used via LAPS)	YES



RDP





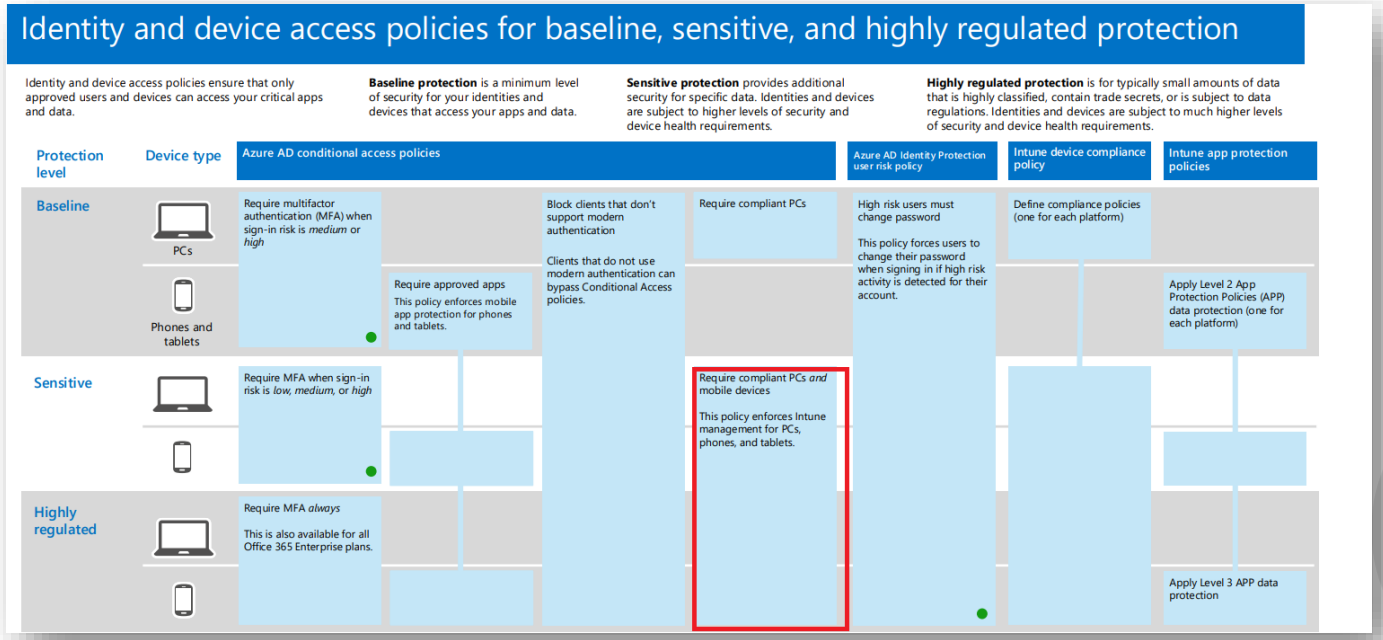
Administrators	
Domain Admins	NO
Workstations Admins	NO
Server Admins	NO
Builtin Administrator (used via LAPS)	YES

Administrators	
Domain Admins	NO
Workstations Admins	NO
Server Admins	NO
Builtin Administrator (used via LAPS)	YES

Administrators	
Domain Admins	YES
Workstations Admins	NO
Server Admins	YES
Builtin Administrator (used via LAPS)	YES

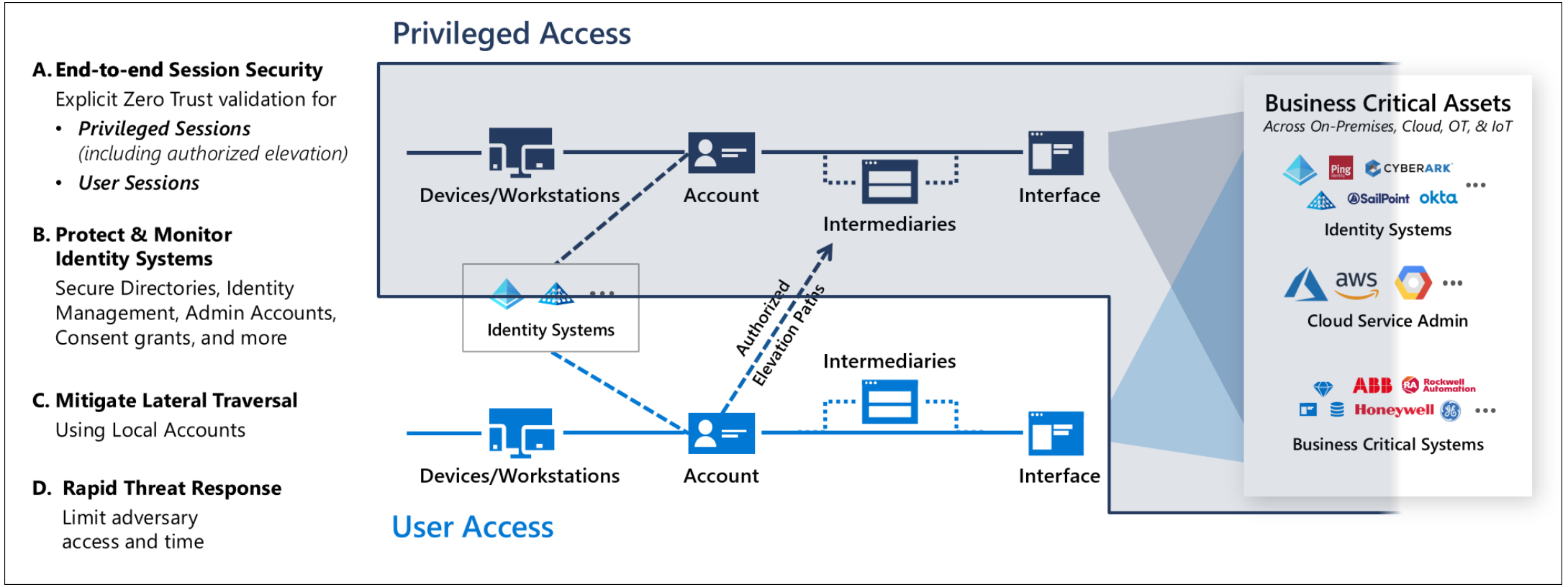
Native Azure PAW

- Loistava ohje, miten tehdään CA:n avulla!
  - https://call4cloud.nl/2021/11/paw-love-and-thunder/
- Microsoftin oma: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices



Microsoft RAMP

- https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan



Älä käytä pelkkiä salasanoja

“MFA Everything!”
“If you RDP, you MFA!”

Biometrics

- Really a game changer
- Great second factor!
  - There are still issues to think about

Smart Cards are difficult, Virtual Smart Cards will be deprecated… So let me introduce the Future of 2FA……..

Name: Token

Token Type: Live, Hedgehog

Token lifetime: 5-8 years

Tamper Protection: Yes

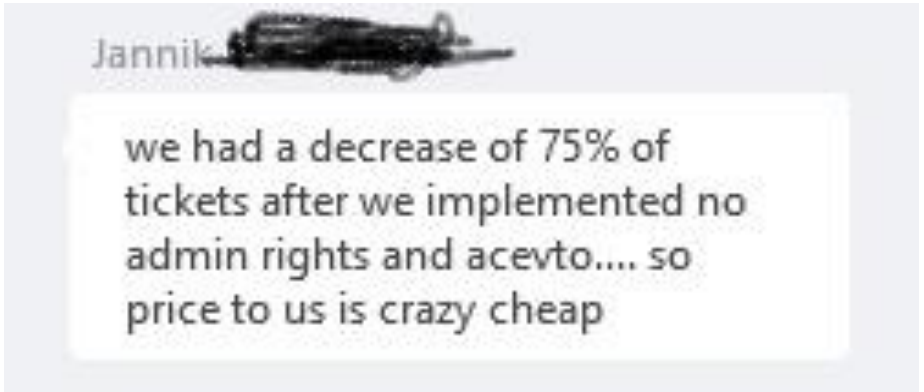

MFA

Ei admin oikkia!

Users: “If I don’t have admin rights, I can’t fix my computer”

Reality: “If you don’t have admin rights, you can’t break your computer”

Estä loppukäyttäjiä vahingoittamasta koneita!



US Customer: 65% less reinstallations

	2020	2019	2018	2017	2016
Number of vulnerabilities	1,268	858	701	685	451
Number of Critical vulnerabilities	196	192	189	235	153
% as Critical	15%	22%	27%	34%	34%
Number of Critical vulnerabilities mitigated	109	147	154	185	142
Number of Critical vulnerabilities mitigated %	**56%**	**77%**	**81%**	**79%**	**93%**

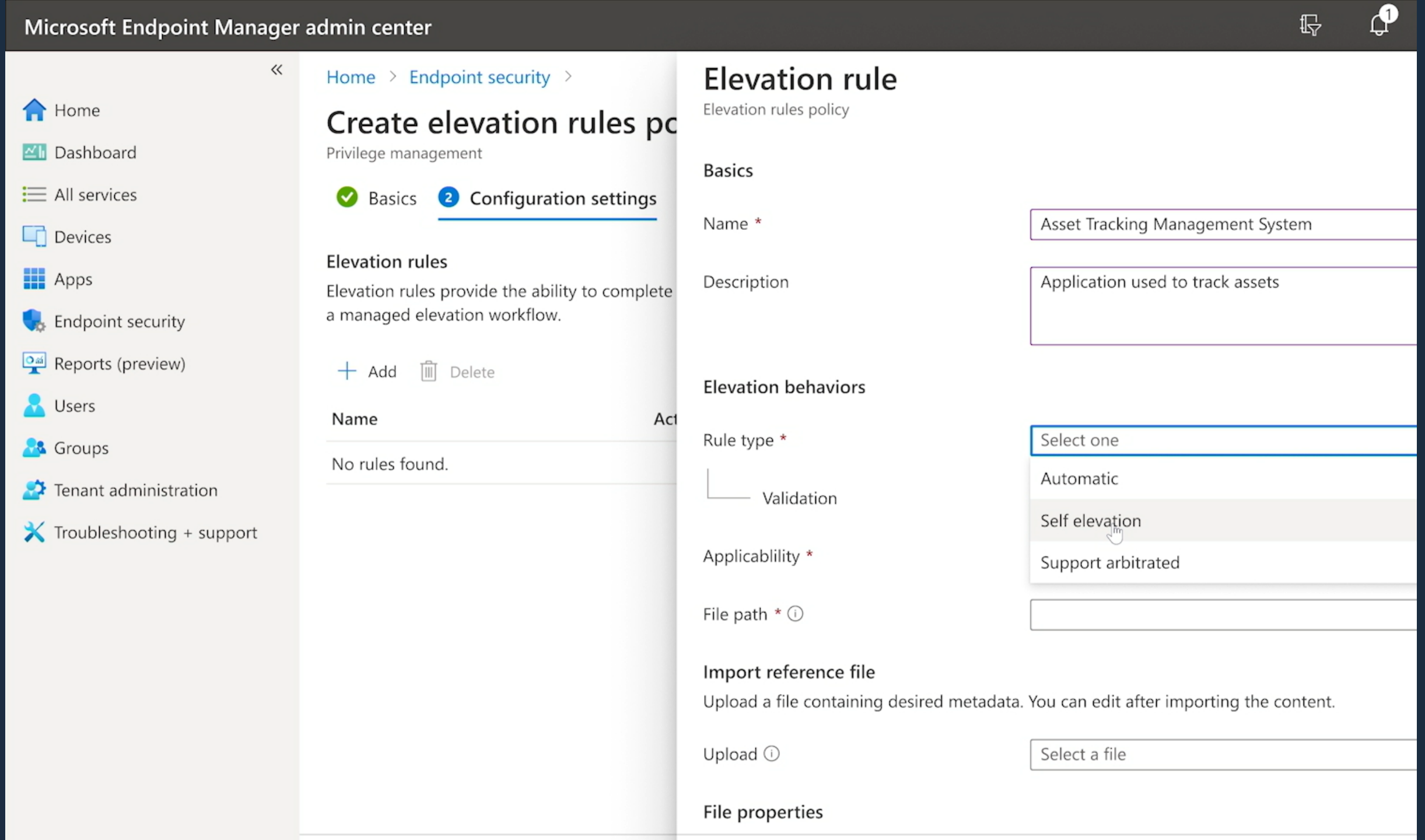
Vaihtoehtoja millä ratkaista

Tarpeen mukaan

- Carillon
  - Hyvä perus Office-käyttäjille

Sääntöpohjainen + On Demand

- PolicyPak
  - Hyvä perus Office-käyttäjille
  - Soveltuu myös sovelluskehittäjille
- BeyondTrust
  - Hyvä perus Office-käyttäjille
  - Soveltuu myös sovelluskehittäjille
  - Paras/kallein


Microsoft Endpoint Manager admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports (preview)
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security >
Create elevation rules pc
Privilege management
Basics
2 Configuration settings
Elevation rules
Elevation rules provide the ability to complete a managed elevation workflow.
Add
Delete
Name
Act
No rules found.
Elevation rule
Elevation rules policy
Basics
Name *
Asset Tracking Management System
Description
Application used to track assets
Elevation behaviors
Rule type *
Select one
Automatic
Validation
Self elevation
Applicablility *
Support arbitrated
File path *
Import reference file
Upload a file containing desired metadata. You can edit after importing the content.
Upload
Select a file
File properties

Home > Endpoint security >

Endpoint security | Privilege management

Search (Ctrl+/)

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Privilege management
- Device compliance
- Conditional access

Monitor

Summary | New requests | Elevation history

Refresh

Last refreshed on 4/5/2022, 8:00:00 AM

Elevations in last 7 days

Matches rule	Not in rule
0	316

View report

Elevation policies

Create policy | Refresh | Export

Search | Add filter

Policy	Type
Retail Manager Elevat...	Elevation rules
Contoso Elevation Co...	Client settings

Privilege management

Do you want to continue as administrator?

Asset Tracking Management System
Verified publisher: Contoso Corporation

Enter justification

Launching this application to update inventory

Verify your username and password

Email address

Password

Contact support

Contoso Corporation
315-555-1212
support@contoso.com
Support website

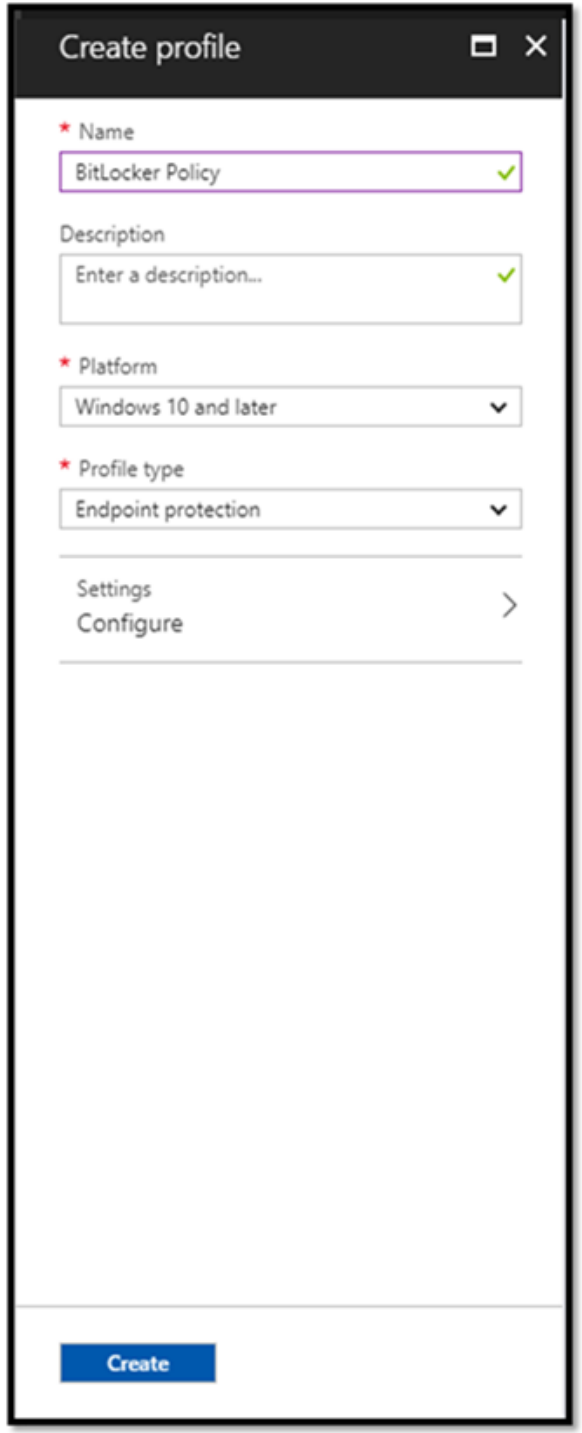
Yes | No

Kaikki koneet salataan!

BitLocker

Miksi BitLocker tarvitaan kaikilla koneilla?

- Se varmistaa laitteen eheyden
- Koska yli 800000 laitetta varastetaan/katoaa vuosittain lentokentillä
- Mahdollistaa turvallisen kierrätyksen


Create profile
* Name
BitLocker Policy
Description
Enter a description...
* Platform
Windows 10 and later
* Profile type
Endpoint protection
Settings
Configure
Create


Windows encryption
Windows Settings
BitLocker base settings
BitLocker OS drive settings
BitLocker fixed data-drive settings
BitLocker removable data-drive settings
OK


Are you ready to start encryption?
Disk encryption software other than BitLocker or Windows device encryption will prevent Windows from starting after you encrypt your device. If this happens, you'll need to reinstall Windows, and all data on your device will be lost.
I don't have any other disk encryption software installed.
Don't ask me again.
Learn more
Yes
No

Laitteiden hallinta

Local Group Policy Editor

File Action View Help

Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Privilege Management Settings
  - Administrative Templates
    - Control Panel
    - Microsoft Edge
    - Microsoft Edge - Default Settings (users
    - Microsoft Edge Update
    - Microsoft Edge WebView2
    - Network
    - Printers
    - Server
    - Start Menu and Taskbar
    - System
      - Access-Denied Assistance
      - App-V
      - Audit Process Creation
      - Credentials Delegation
      - Device Guard
      - Device Health Attestation Service
      - Device Installation
        - Device Installation Restrictions

13 setting(s)

Device Installation Restrictions

Prevent installation of devices using drivers that match these device setup classes

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for driver packages that Windows is prevented from installing. By default, this policy setting takes precedence over any other policy setting that allows Windows to install a device.

NOTE: To enable the "Al
installation of devices th
any of these device IDs"
and "Allow installation c
that match any of these
instance IDs" policy sett

Extended Standard

Setting	State
Allow administrators to override Device Installation Restriction policies	Enabled
Apply layered order of evaluation for Allow and Prevent device installation policies across ...	Not configured
Allow installation of devices using drivers that match these device setup classes	Not configured
Prevent installation of devices using drivers that match these device setup classes	Enabled
Display a custom message when installation is prevented by a policy setting	Enabled
Display a custom message title when device installation is prevented by a policy setting	Enabled
Allow installation of devices that match any of these device IDs	Not configured
Prevent installation of devices that match any of these device IDs	Not configured
Allow installation of devices that match any of these device instance IDs	Not configured
Prevent installation of devices that match any of these device instance IDs	Not configured
Time (in seconds) to force reboot when required for policy changes to take effect	Not configured
Prevent installation of removable devices	Not configured
Prevent installation of devices not described by other policy settings	Not configured

Prevent installation of devices using drivers that match these device setup classes

Prevent installation of devices using drivers that match these device setup classes

Previous Setting | Next Setting

Not Configured
Enabled
Disabled

Comment:

Supported on: At lea

Options:

Prevent installation of devices using drivers fo
these device setup classes:

Show...

To create a list of device classes, click Show. In
Show Contents dialog box, in the Value colum

type a GUID that represents a device setup cla

(for example, {25DBCE51-6C8F-4A72-8A6D-
B54C2B4FC835}).

Also apply to matching devices that are already installed.

If you enable this policy setting, Windows is prevented from installing or updating driver packages whose device setup class

Show Contents

Prevent installation of devices using drivers for these device setup classes:

Value
{4d36e967-e325-11ce-bfc1-08002be10318}

OK

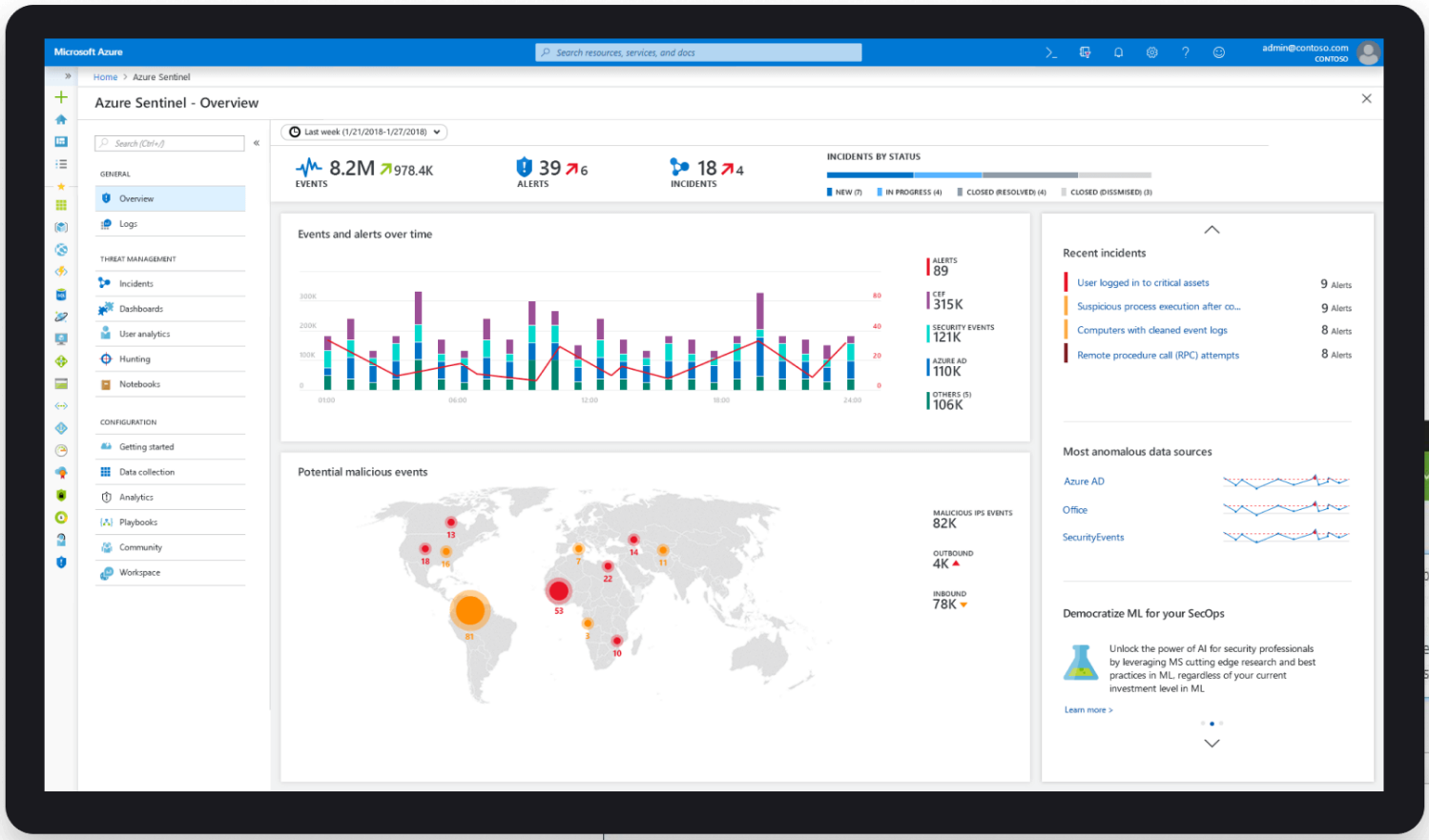
Settings

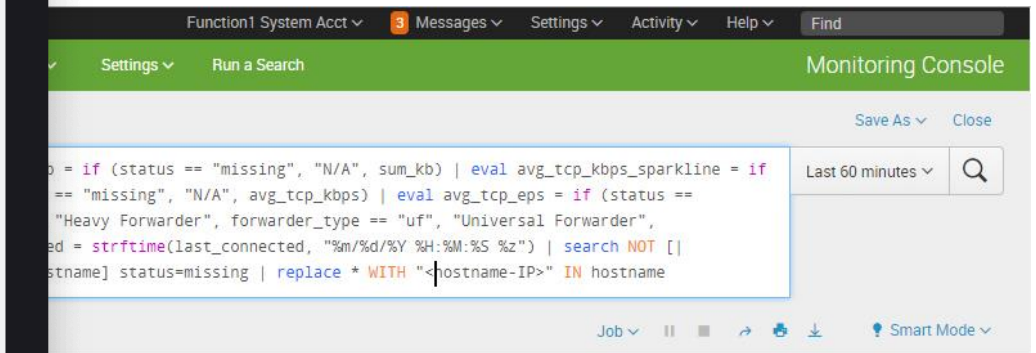
BLOCKED DEVICE!
If you need access to USB driver, contact SD!

2°C Pilvistä ENG 11.55 8.3.2022

Valvonta

SIEM & SOC





arch	avg_tcp_eps	avg_tcp_kbps	avg_tcp_kbps_sparkline	forwarder_type	guid	hostname	last_connected	os	status	sum_kb	version
x86_64	N/A	N/A	N/A	Universal Forwarder	0B985568-4102-4FAF-982B-C6309499D7C6	<hostname-IP>	09/25/2017 16:03:02 -0400	Linux	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	156AA180-1AF3-4772-BD04-1DD71312C462	<hostname-IP>	09/25/2017 16:00:12 -0400	Linux	missing	N/A	6.5.2
x64	N/A	N/A	N/A	Universal Forwarder	36041654-7EC1-45AA-A5D1-5CEC67339FE0	<hostname-IP>	10/05/2017 05:16:56 -0400	Windows	missing	N/A	6.4.8
x86_64	N/A	N/A	N/A	Universal Forwarder	3E47DAE9-9220-4260-A730-A15C8797668E	<hostname-IP>	09/25/2017 15:59:41 -0400	Linux	missing	N/A	6.5.2
x64	N/A	N/A	N/A	Universal Forwarder	529042BB-1D51-481C-9300-B35C67F55DF8	<hostname-IP>	10/09/2017 05:16:39 -0400	Windows	missing	N/A	6.5.0
x64	N/A	N/A	N/A	Universal Forwarder	58F0F461-0D4D-4BC9-8C8C-47957CE8DED1	<hostname-IP>	09/26/2017 03:07:44 -0400	Windows	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	69A60123-7714-4BA9-B193-C20598EF8BFD	<hostname-IP>	09/25/2017 16:03:16 -0400	Linux	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	6CA0E7FE-BE4F-4479-AF48-1ADD1F94F036	<hostname-IP>	09/25/2017 16:00:58 -0400	Linux	missing	N/A	6.5.2

“In Security don’t let perfect be the enemy of good”

Contact

- sami@adminize.com
- Twitter: @samilaiho
- Blog: http://blog.win-fu.com/
- Free newsletter: http://eepurl.com/F-GOj
- My trainings:
  - https://win-fu.com/events
  - https://win-fu.com/dojo/
    - **Free for one month!! Code:”Trial2018”**
  - PluralSight: If you need a code email me!