Implementing Privileged Access Workstations

- Sami Laiho
- Senior Technical Fellow @ Adminize
- Twitter @samilaiho
- MVP

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC — VIRTUAL SUMMIT —

Sami Laiho

Senior Technical Fellow
adminize.com / Sulava

- 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

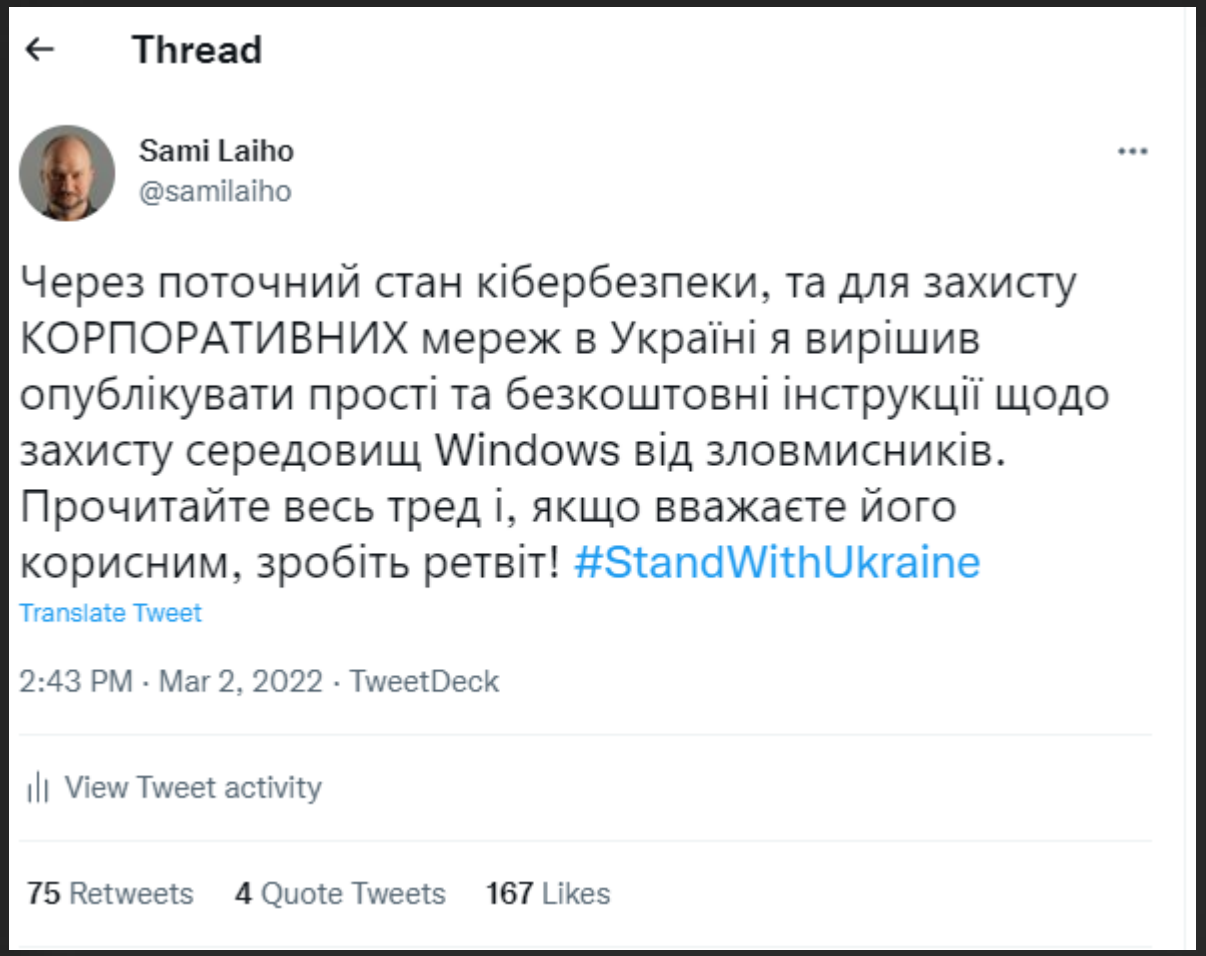
A big thanks to our sponsors

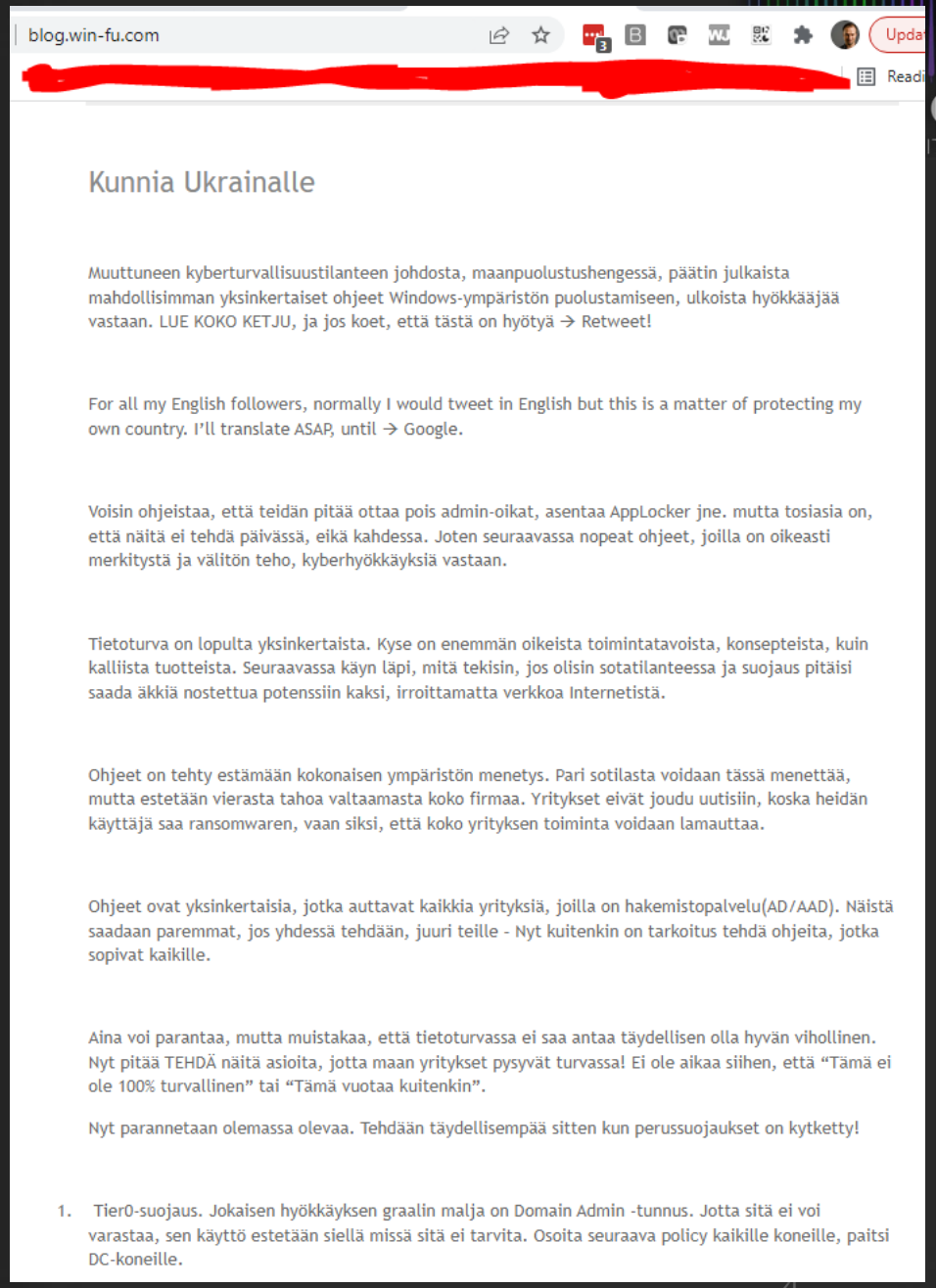
NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

RECAST SOFTWARE

Wartime…


Thread
Sami Laiho
@samilaiho
Через поточний стан кібербезпеки, та для захисту КОРПОРАТИВНИХ мереж в Україні я вирішив опублікувати прості та безкоштовні інструкції щодо захисту середовищ Windows від зловмисників. Прочитайте весь тред і, якщо вважаєте його корисним, зробіть ретвіт! #StandWithUkraine
Translate Tweet
2:43 PM · Mar 2, 2022 · TweetDeck
View Tweet activity
75 Retweets
4 Quote Tweets
167 Likes


blog.win-fu.com
Kunnia Ukrainalle
Muuttuneen kyberturvallisuustilanteen johdosta, maanpuolustushengessä, päätin julkaista mahdollisimman yksinkertaiset ohjeet Windows-ympäristön puolustamiseen, ulkoista hyökkääjää vastaan. LUE KOKO KETJU, ja jos koet, että tästä on hyötyä → Retweet!
For all my English followers, normally I would tweet in English but this is a matter of protecting my own country. I'll translate ASAP, until → Google.
Voisin ohjeistaa, että teidän pitää ottaa pois admin-oikat, asentaa AppLocker jne. mutta tosiasia on, että näitä ei tehdä päivässä, eikä kahdessa. Joten seuraavassa nopeat ohjeet, joilla on oikeasti merkitystä ja välitön teho, kyberhyökkäyksiä vastaan.
Tietoturva on lopulta yksinkertaista. Kyse on enemmän oikeista toimintatavoista, konsepteista, kuin kalliista tuotteista. Seuraavassa käyn läpi, mitä tekisin, jos olisin sotatilanteessa ja suojaus pitäisi saada äkkiä nostettua potenssiin kaksi, irroittamatta verkkoa Internetistä.
Ohjeet on tehty estämään kokonaisen ympäristön menetys. Pari sotilasta voidaan tässä menettää, mutta estetään vierasta tahoa valtaamasta koko firmaa. Yritykset eivät joudu uutisiin, koska heidän käyttäjä saa ransomwaren, vaan siksi, että koko yrityksen toiminta voidaan lamauttaa.
Ohjeet ovat yksinkertaisia, jotka auttavat kaikkia yrityksiä, joilla on hakemistopalvelu(AD/AAD). Näistä saadaan paremmat, jos yhdessä tehdään, juuri teille - Nyt kuitenkin on tarkoitus tehdä ohjeita, jotka sopivat kaikille.
Aina voi parantaa, mutta muistakaa, että tietoturvassa ei saa antaa täydellisen olla hyvän vihollinen. Nyt pitää TEHDÄ näitä asioita, jotta maan yritykset pysyvät turvassa! Ei ole aikaa siihen, että "Tämä ei ole 100% turvallinen" tai "Tämä vuotaa kuitenkin".
Nyt parannetaan olemassa olevaa. Tehdään täydellisempää sitten kun perussuojaukset on kytketty!
1. Tier0-suojaus. Jokaisen hyökkäyksen graalin malja on Domain Admin -tunnus. Jotta sitä ei voi varastaa, sen käyttö estetään siellä missä sitä ei tarvita. Osoita seuraava policy kaikille koneille, paitsi DC-koneille.

Security is simple at the end…

Don’t let accounts that can take down your environment logon to devices with access to malware…

Don’t let computers that can take down your environment talk to Facebook…

NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

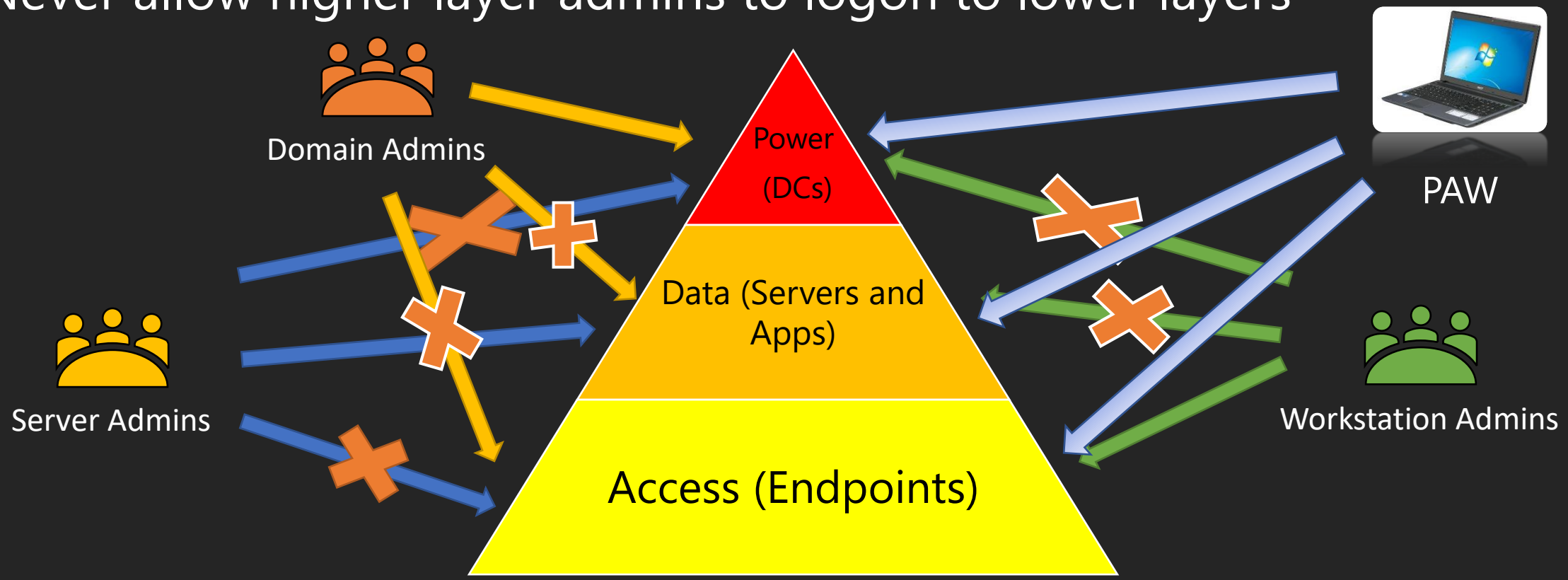
RECAST SOFTWARE

Tier Model & PAW's

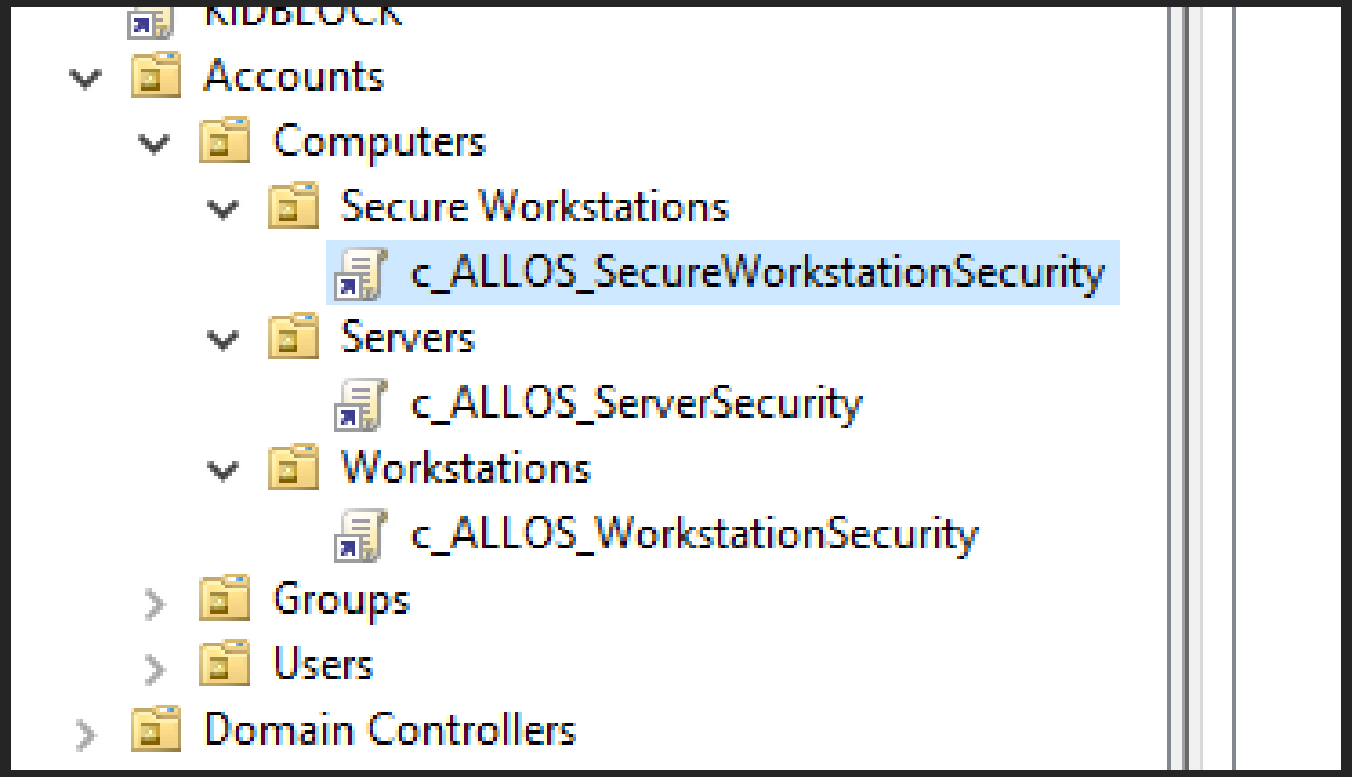
Mitigating PtH

Split your environment into three layers (Azure minimum 2 layers)

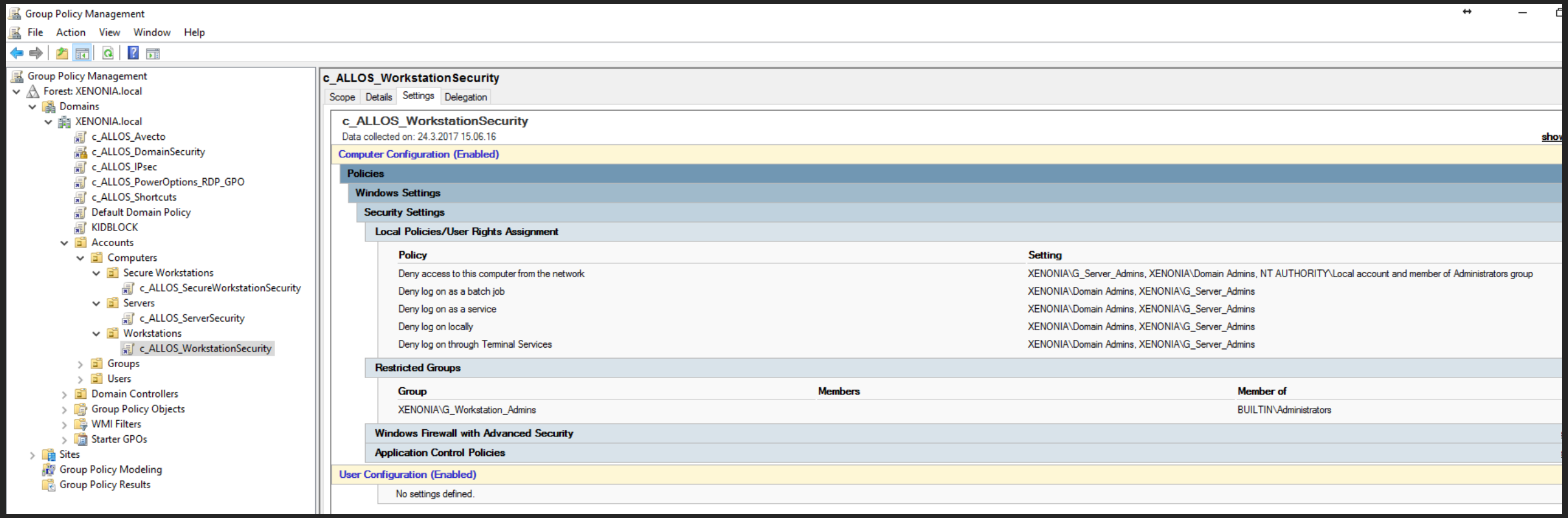
Never allow higher layer admins to logon to lower layers



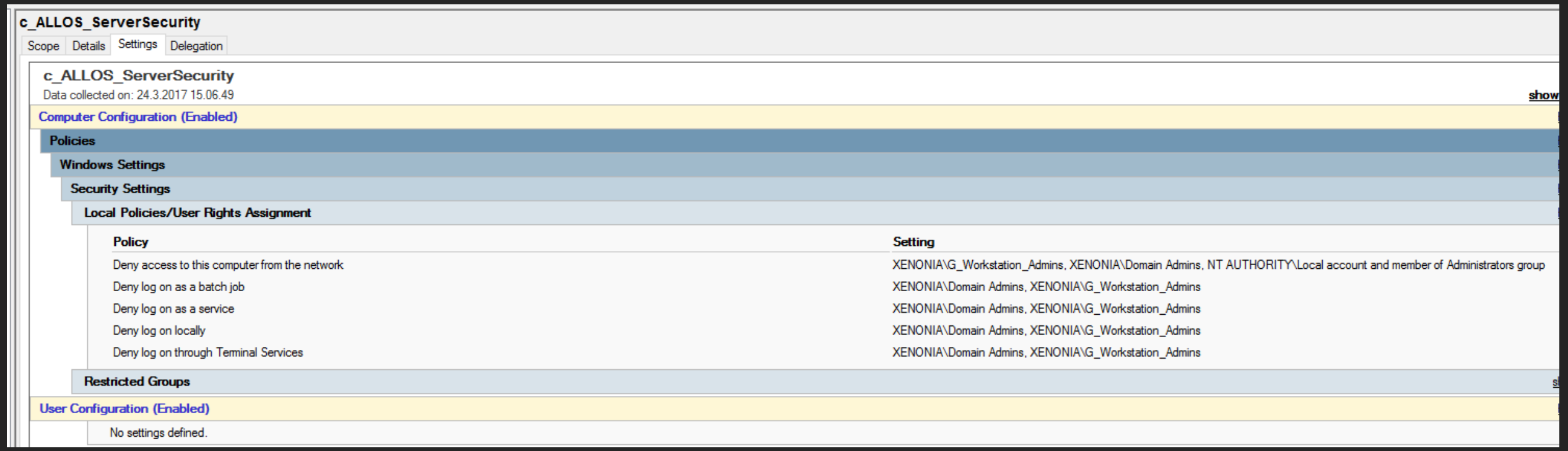
My AD


KIDBLOCK
Accounts
Computers
Secure Workstations
c_ALLOS_SecureWorkstationSecurity
Servers
c_ALLOS_ServerSecurity
Workstations
c_ALLOS_WorkstationSecurity
Groups
Users
Domain Controllers

Normal Workstation



Servers



c_ALLOS_ServerSecurity

Scope | Details | Settings | Delegation

c_ALLOS_ServerSecurity

Data collected on: 24.3.2017 15.06.49

show

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	XENONIA\G_Workstation_Admins, XENONIA\Domain Admins, NT AUTHORITY\Local account and member of Administrators group
Deny log on as a batch job	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins
Deny log on as a service	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins
Deny log on locally	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins
Deny log on through Terminal Services	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins

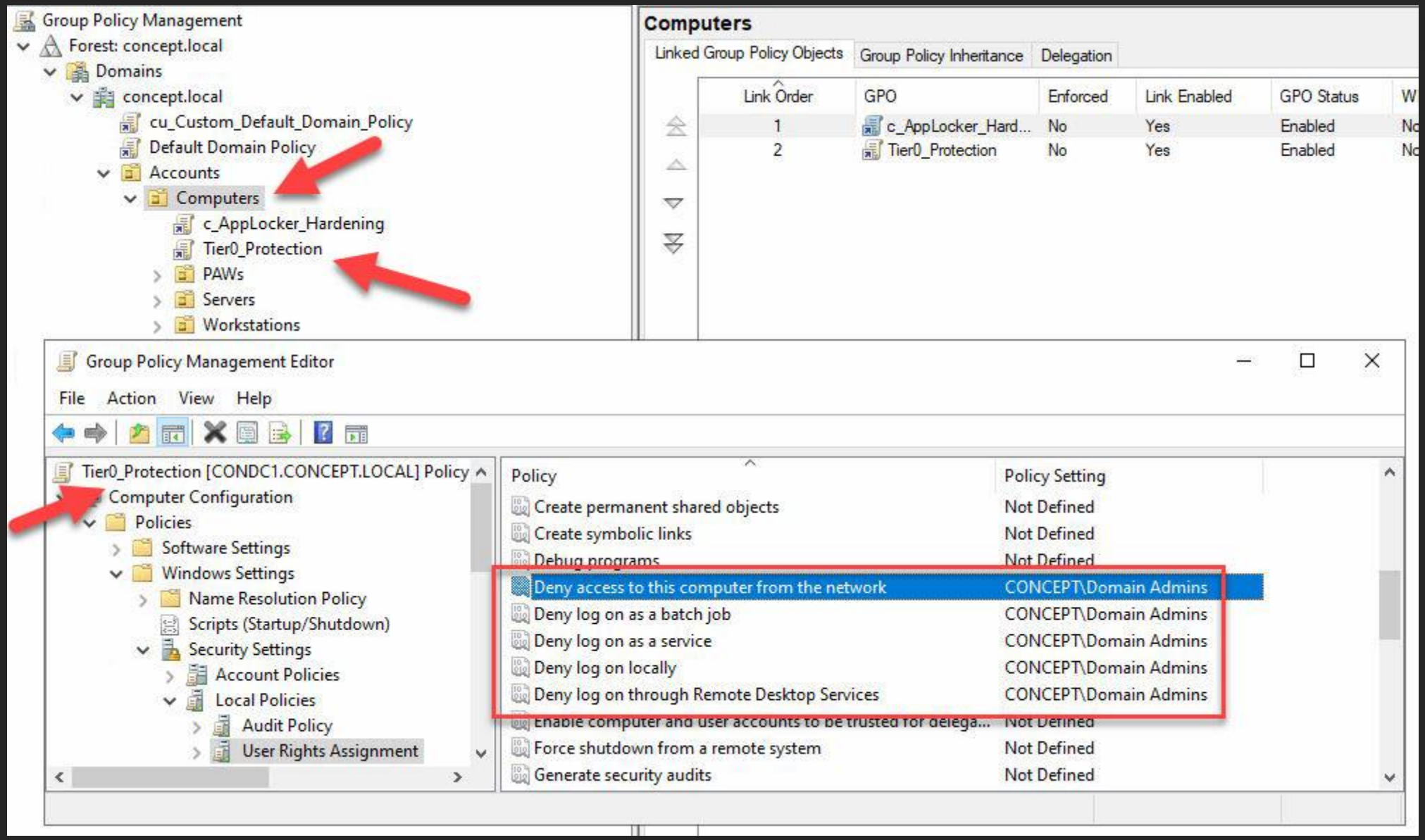
Restricted Groups

User Configuration (Enabled)

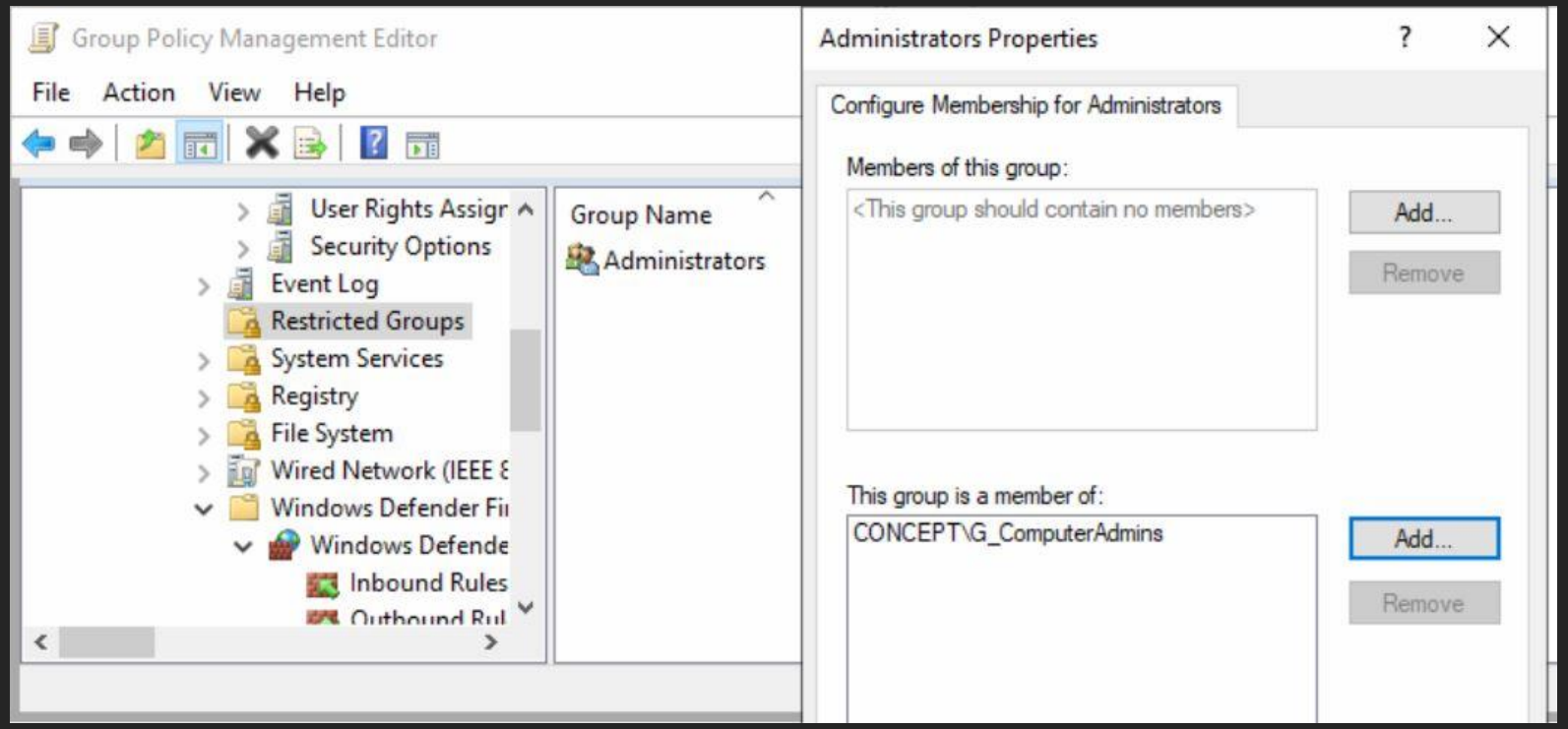
No settings defined.

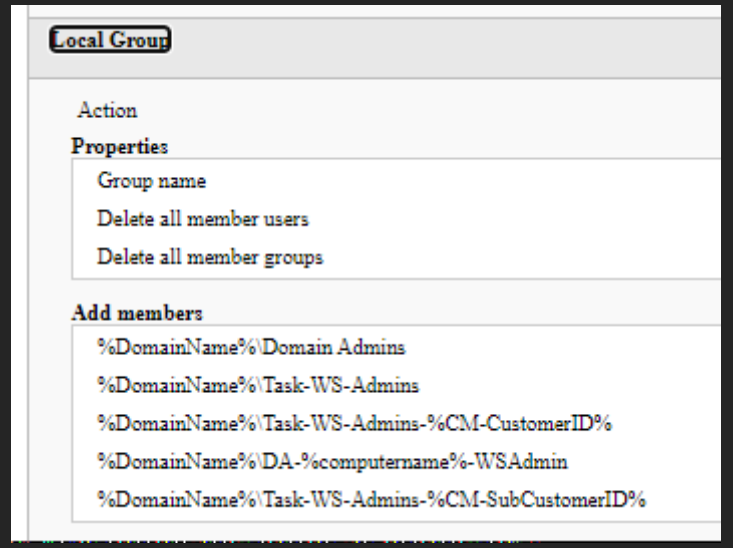
Good start

- https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/initially-isolate-tier-0-assets-with-group-policy-to-start/ba-p/1184934


Group Policy Management
Forest: concept.local
Domains
concept.local
cu_Custom_Default_Domain_Policy
Default Domain Policy
Accounts
Computers
c_AppLocker_Hardening
Tier0_Protection
PAWs
Servers
Workstations
Computers
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
1
c_AppLocker_Hard...
No
Yes
Enabled
2
Tier0_Protection
No
Yes
Enabled
Group Policy Management Editor
File
Action
View
Help
Tier0_Protection [CONDC1.CONCEPT.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Policy
Policy Setting
Create permanent shared objects
Not Defined
Create symbolic links
Not Defined
Debug programs
Not Defined
Deny access to this computer from the network
CONCEPT\Domain Admins
Deny log on as a batch job
CONCEPT\Domain Admins
Deny log on as a service
CONCEPT\Domain Admins
Deny log on locally
CONCEPT\Domain Admins
Deny log on through Remote Desktop Services
CONCEPT\Domain Admins
Force shutdown from a remote system
Not Defined
Generate security audits
Not Defined

Managing Groups (GP or GPP)

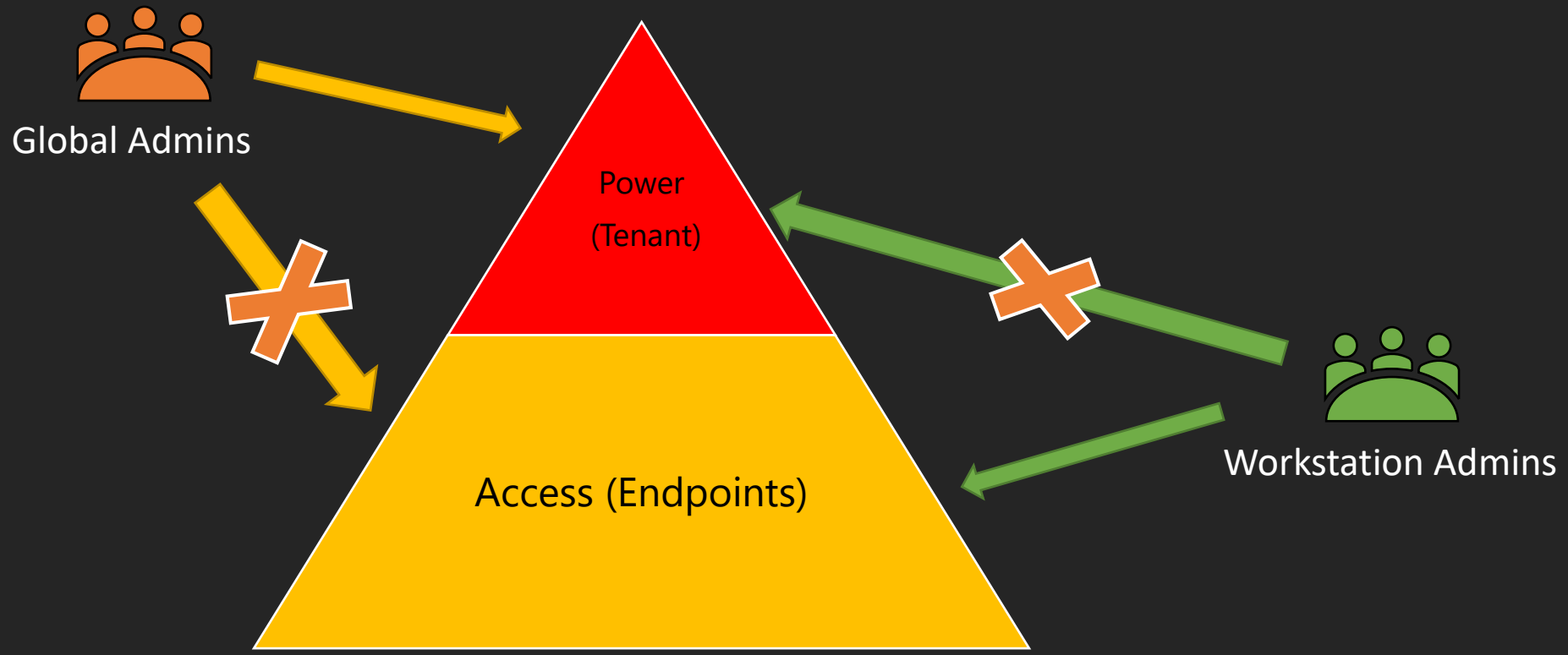


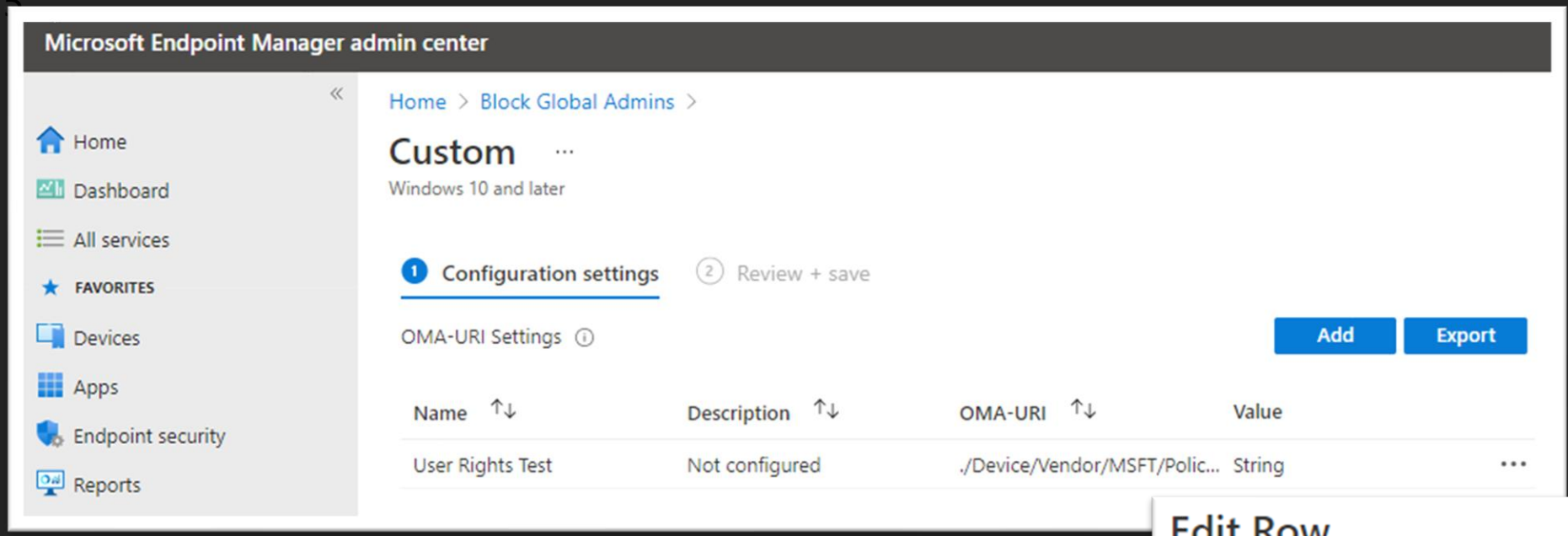


Mitigating PtH (Native Cloud)

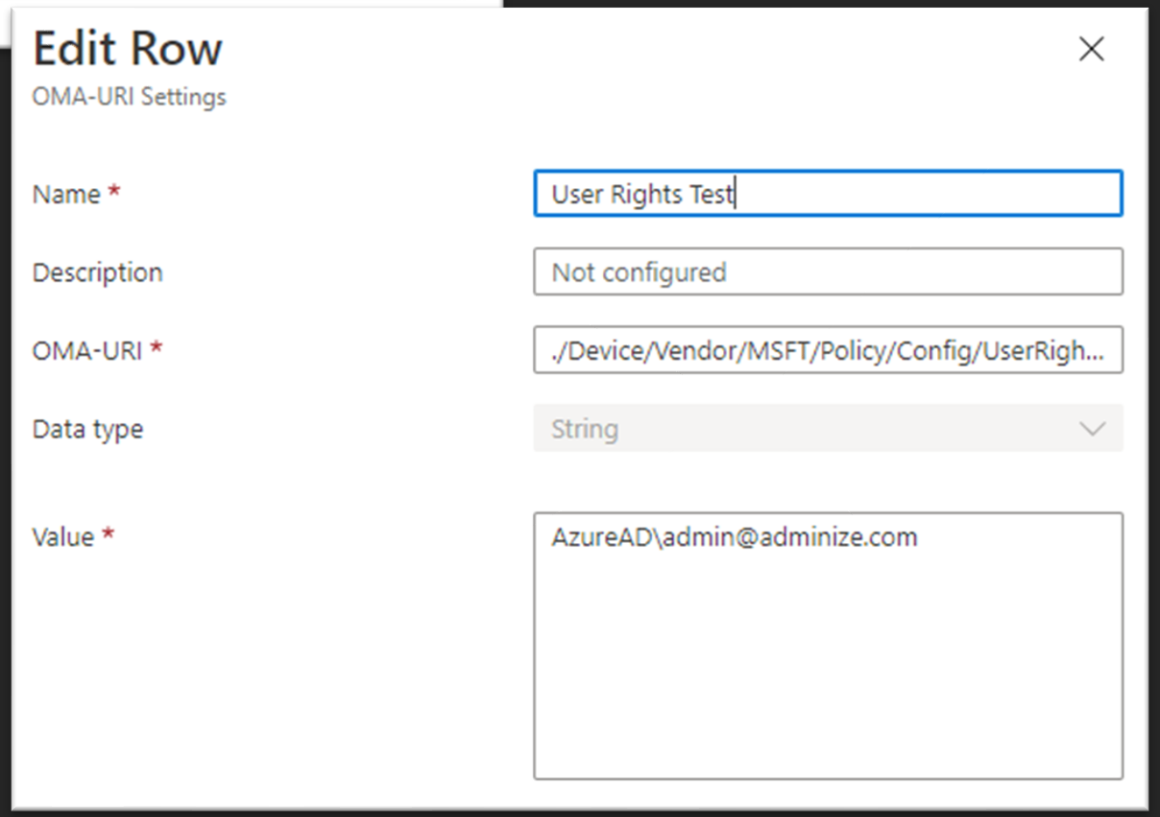
Split your environment into two layers

Never allow higher layer admins to logon to lower layers

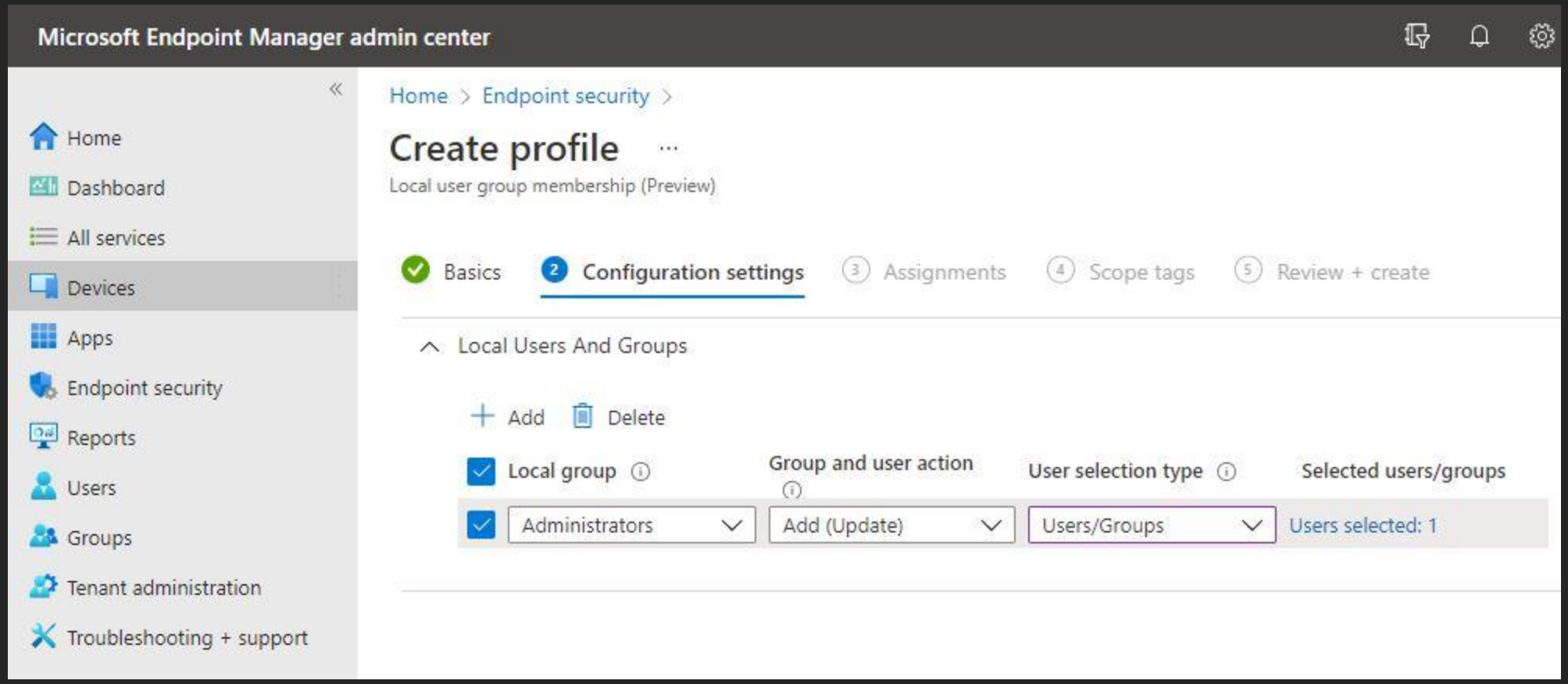



Microsoft Endpoint Manager admin center
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Home > Block Global Admins >
Custom
Windows 10 and later
1 Configuration settings
2 Review + save
OMA-URI Settings
Add
Export
Name
Description
OMA-URI
Value
User Rights Test
Not configured
./Device/Vendor/MSFT/Polic...
String


./Device/Vendor/MSFT/Policy/Config/UserRights/DenyLocalLogOn

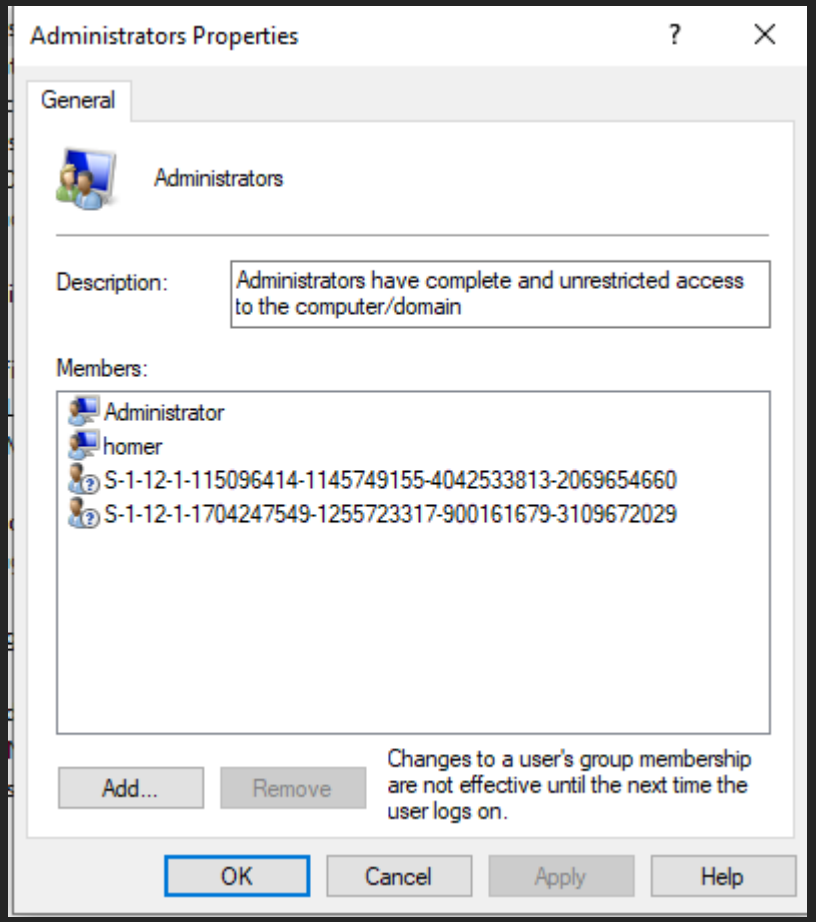

Edit Row
OMA-URI Settings
Name *
User Rights Test
Description
Not configured
OMA-URI *
./Device/Vendor/MSFT/Policy/Config/UserRigh...
Data type
String
Value *
AzureAD\admin@adminize.com

Managing Groups with Intune



Don’t remove these

- Applies to all “Azure admins” including “Device Administrators”

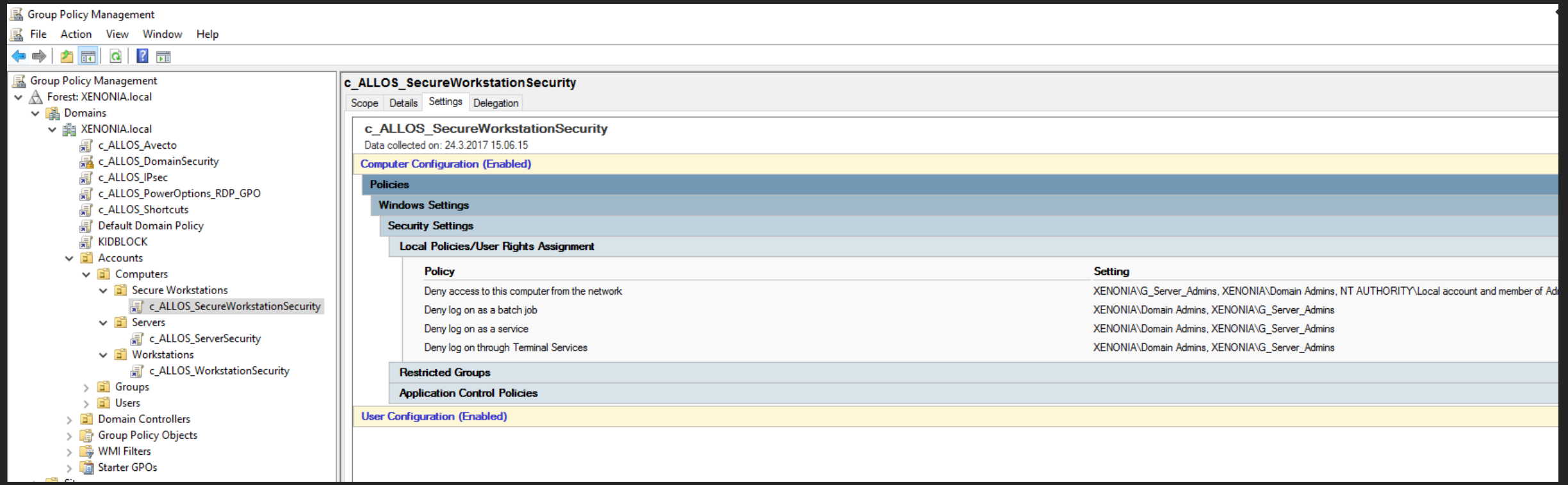


Privileged Access Workstation (PAW)

PAW-workstations

- Management WS
  - RSAT installed
  - Allowed to use Windows Admin Center
  - Allowed to logon with administrative users (and usually only by them)
    - Hopefully not interactively though
- https://blogs.technet.microsoft.com/datacentersecurity/2017/10/13/privileged-access-workstationpaw/

PAW


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: XENONIA.local
Domains
XENONIA.local
c_ALLOS_Avecto
c_ALLOS_DomainSecurity
c_ALLOS_IPsec
c_ALLOS_PowerOptions_RDP_GPO
c_ALLOS_Shortcuts
Default Domain Policy
KIDBLOCK
Accounts
Computers
Secure Workstations
c_ALLOS_SecureWorkstationSecurity
Servers
c_ALLOS_ServerSecurity
Workstations
c_ALLOS_WorkstationSecurity
Groups
Users
Domain Controllers
Group Policy Objects
WMI Filters
Starter GPOs
c_ALLOS_SecureWorkstationSecurity
Scope Details Settings Delegation
c_ALLOS_SecureWorkstationSecurity
Data collected on: 24.3.2017 15.06.15
Computer Configuration (Enabled)
Policies
Windows Settings
Security Settings
Local Policies/User Rights Assignment
Policy
Setting
Deny access to this computer from the network
XENONIA\G_Server_Admins, XENONIA\Domain Admins, NT AUTHORITY\Local account and member of Ad
Deny log on as a batch job
XENONIA\Domain Admins, XENONIA\G_Server_Admins
Deny log on as a service
XENONIA\Domain Admins, XENONIA\G_Server_Admins
Deny log on through Terminal Services
XENONIA\Domain Admins, XENONIA\G_Server_Admins
Restricted Groups
Application Control Policies
User Configuration (Enabled)

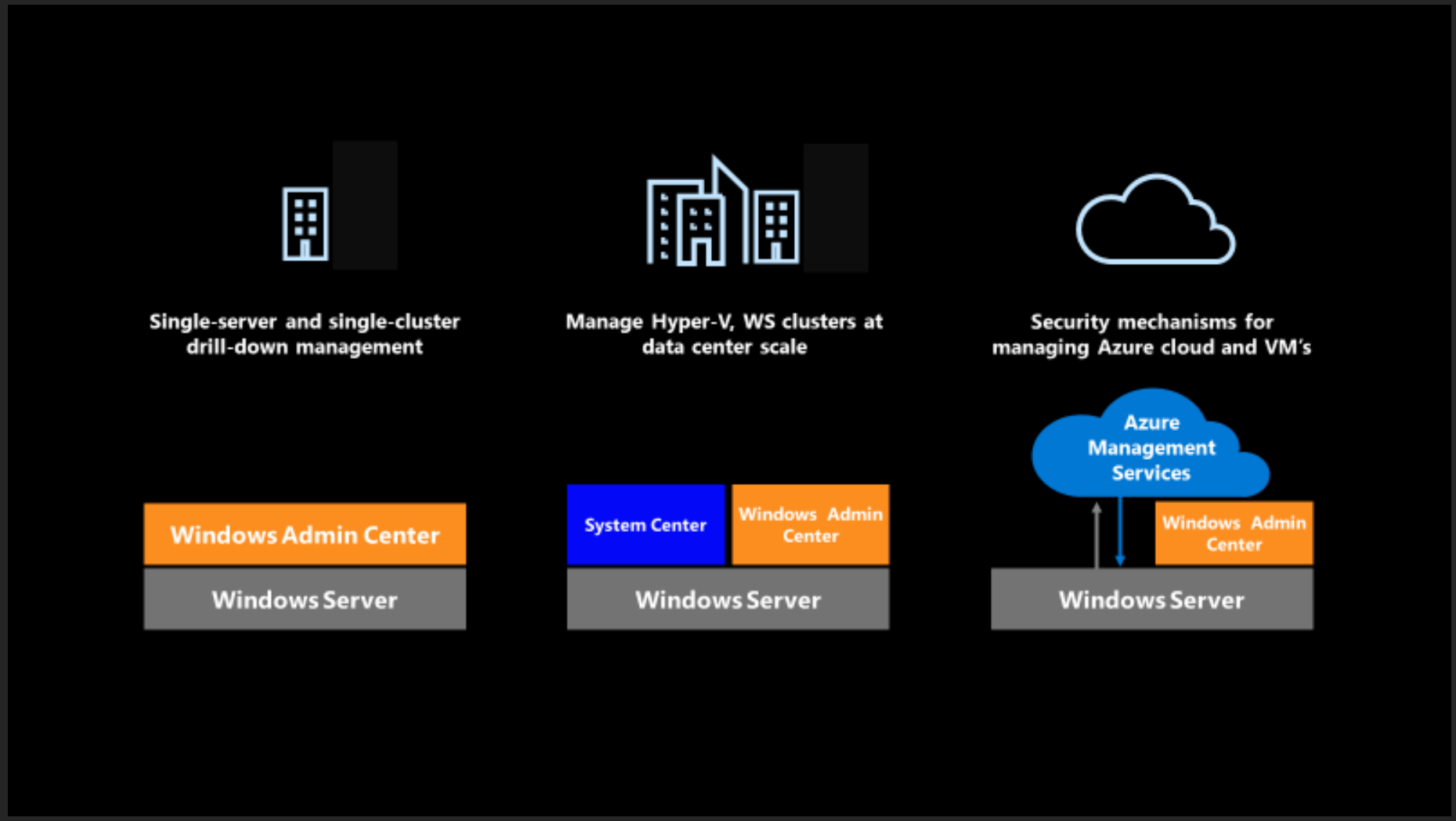
NORDIC
– VIRTUAL SUMMIT –
PATCH MY PC
RECAST SOFTWARE

Why?

Why?

NORDIC
– VIRTUAL SUMMIT –

- Management tools just were not meant to work on servers
- RDP is an emergency console with two licenses
- No GUI
- High privileged user accounts can’t be used “where ever”



https://cloudblogs.microsoft.com/windowsserver/2019/04/29/its-time-to-update-your-windows-management-strategy/

How?

Platforms?

NORDIC
– VIRTUAL SUMMIT –

- Platform Level 1
  - A workstation is either a normal or a privileged one
- Platform Level 2
  - Admins have a VM
    - Running the admin stuff on the VM
    - Running the admin stuff on the Host
- Platform Level 3
  - Admins have separate computers for normal and privileged use

NORDIC
– VIRTUAL SUMMIT –
PATCH MY PC
RECAST SOFTWARE

What about Jump Servers?

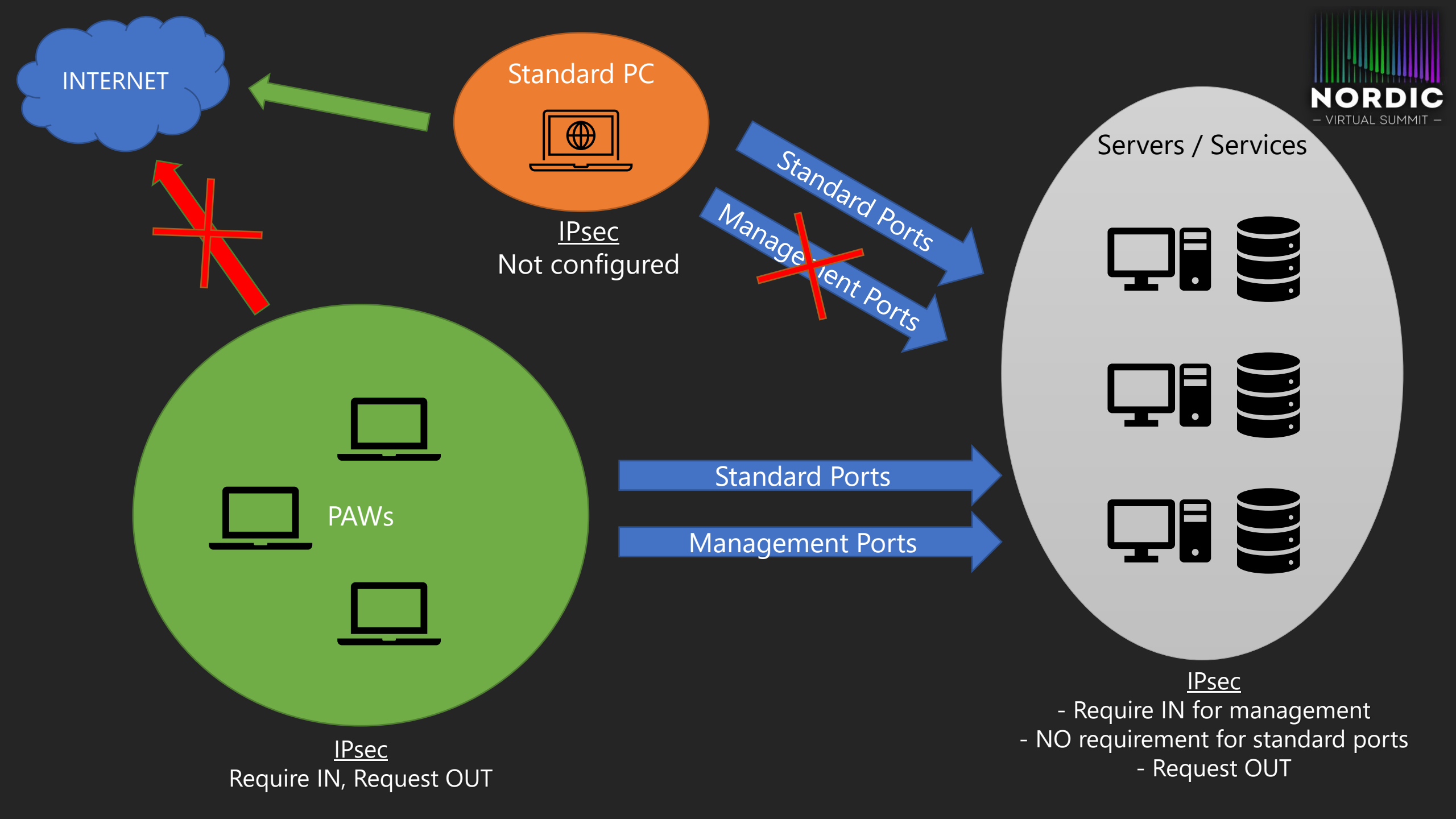
Jump Servers

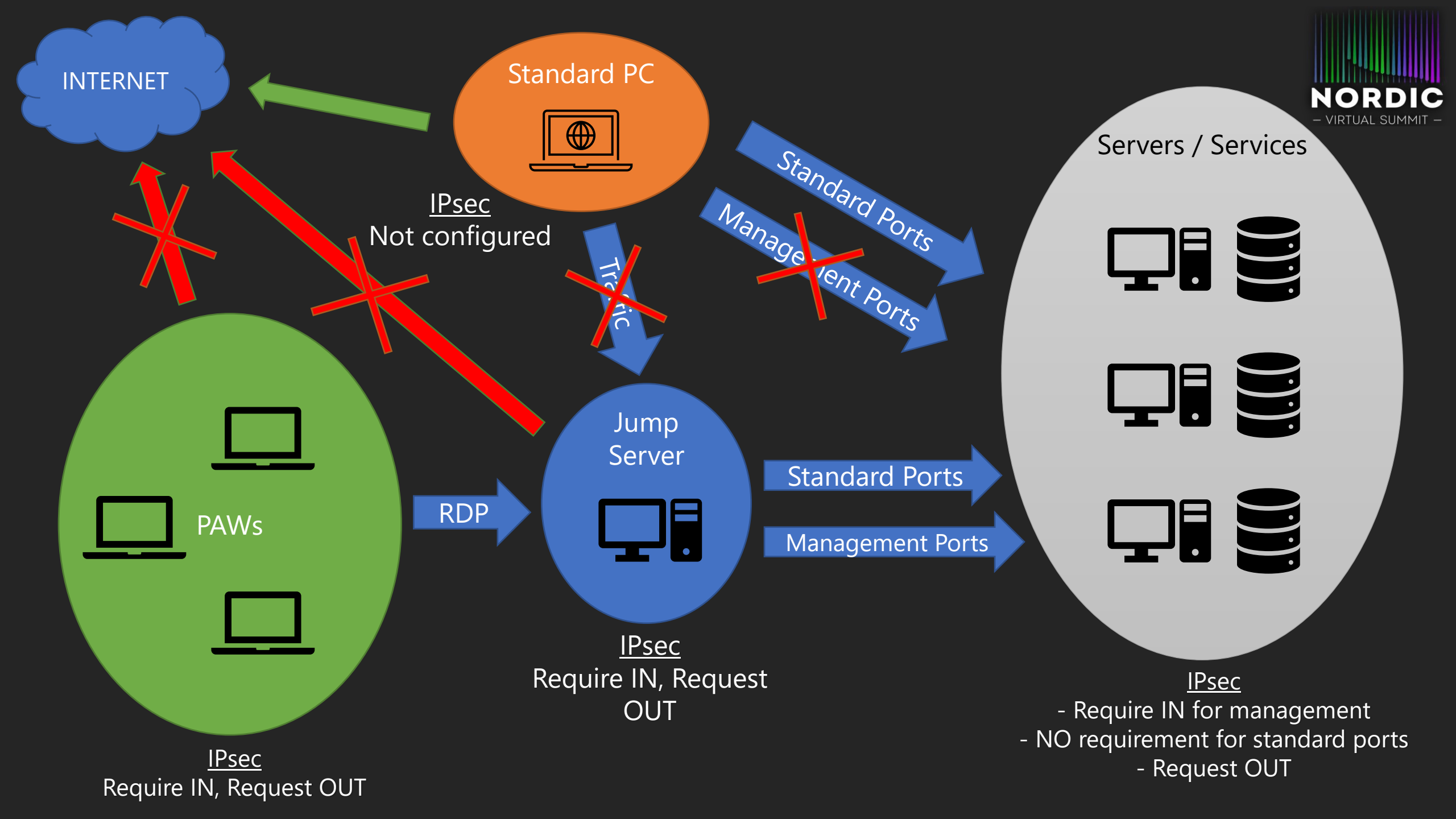
NORDIC
– VIRTUAL SUMMIT –

- This approach is frequently proposed to mitigate risk to administration and does provide some security assurances, but the jump server approach by itself is vulnerable to certain attacks because it violates the "clean source" principle. The clean source principle requires all security dependencies to be as trustworthy as the object being secured.

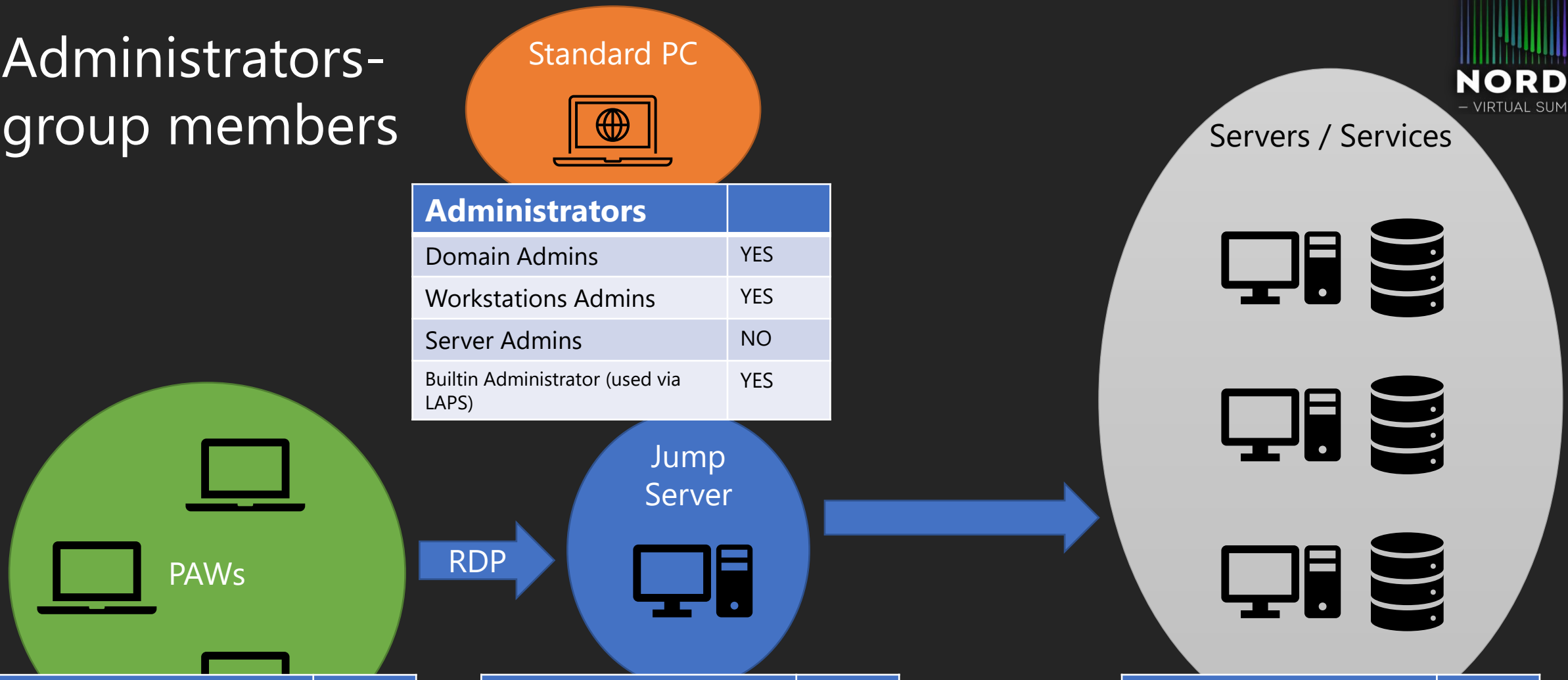
Jump Servers

- The administrative session on the jump server relies on the integrity of the local computer accessing it. If this computer is a user workstation subject to phishing attacks and other internet-based attack vectors, then the administrative session is also subject to those risks.


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

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

NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

RECAST SOFTWARE

IPsec

Recommended Reading

Good run-through for AD-environment's IPsec

- https://improsec.com/tech-blog/setup-rdp-dc-jumphost-paw-ipsec

NORDIC
– VIRTUAL SUMMIT –

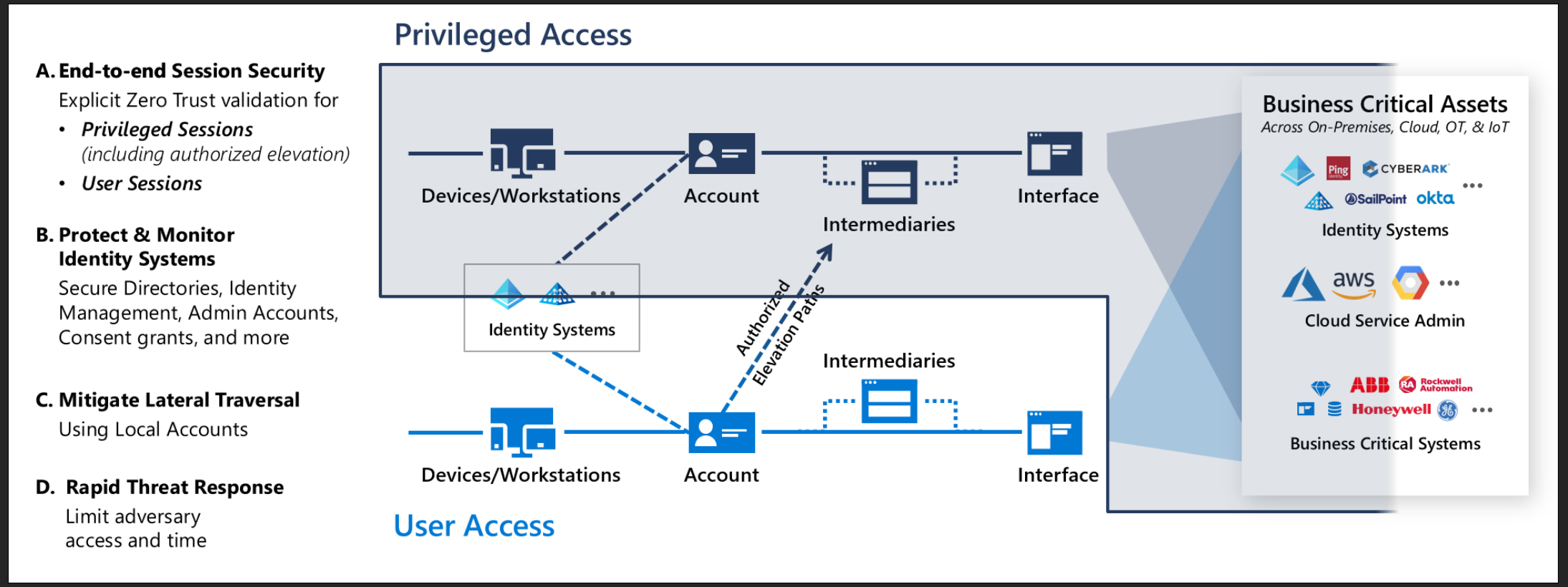
PATCH MY PC

RECAST SOFTWARE

Azure PAW

Microsoft RAMP

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



Recommended Reading

Good run-through for AAD-environments

- https://call4cloud.nl/2021/11/paw-love-and-thunder/

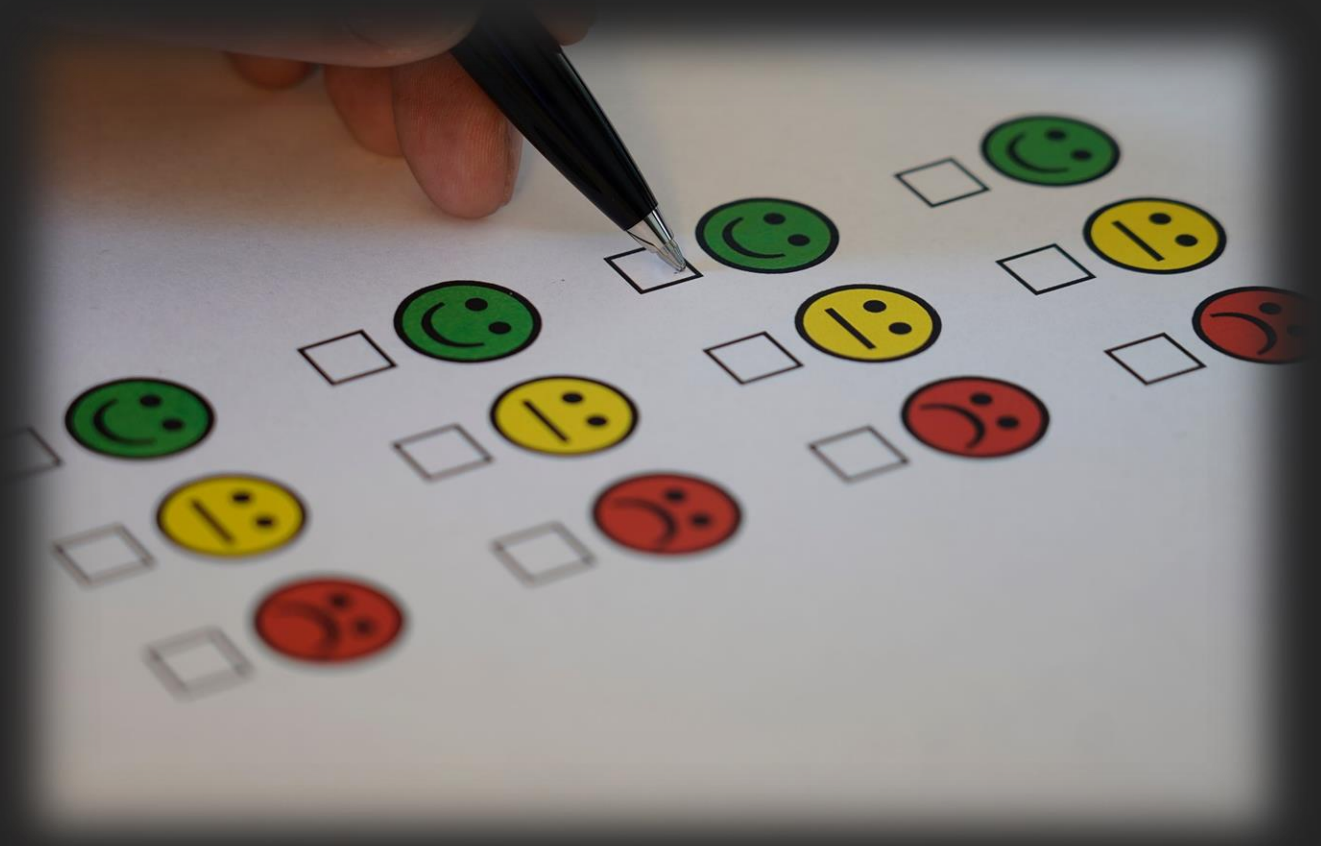
Conditional Access for Devices

- https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices

Thank you!

Please remember to fill out the evals!

https://stream.nordicvirtualsummit.com/feedback



NORDIC
– VIRTUAL SUMMIT –