nic X edition

May 31 – June 2, Oslo Spektrum

10th anniversary

Sami Laiho

Zero Admins - Zero Problems

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, Windows Internals
  - 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

Zero Trust principles

Verify explicitly

Use least privileged access

Assume breach

Trust

Admin Epoch	Non-Admin Epoch	App Control Epoch
1985 - 2005	2005 - 2025	2025 - ?
Users run as local admin	**Users run as standard user**	Users run as standard user
Users install their own software	**Admins install software**	Admins install software
Apps trusted by default	Apps trusted by default	**Apps trusted when trust is earned**

Principle of Least Privilege

- Windows can’t quarantee security when a user logs on as an admin
- Security Subsystem for Windows was never built to withstand admin rights
- What do YOU GET when not logging in as an admin
  - Better Performance
  - Less tickets
  - Less reimaging
  - More productive users
  - Less malware
  - Lazier admins

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”

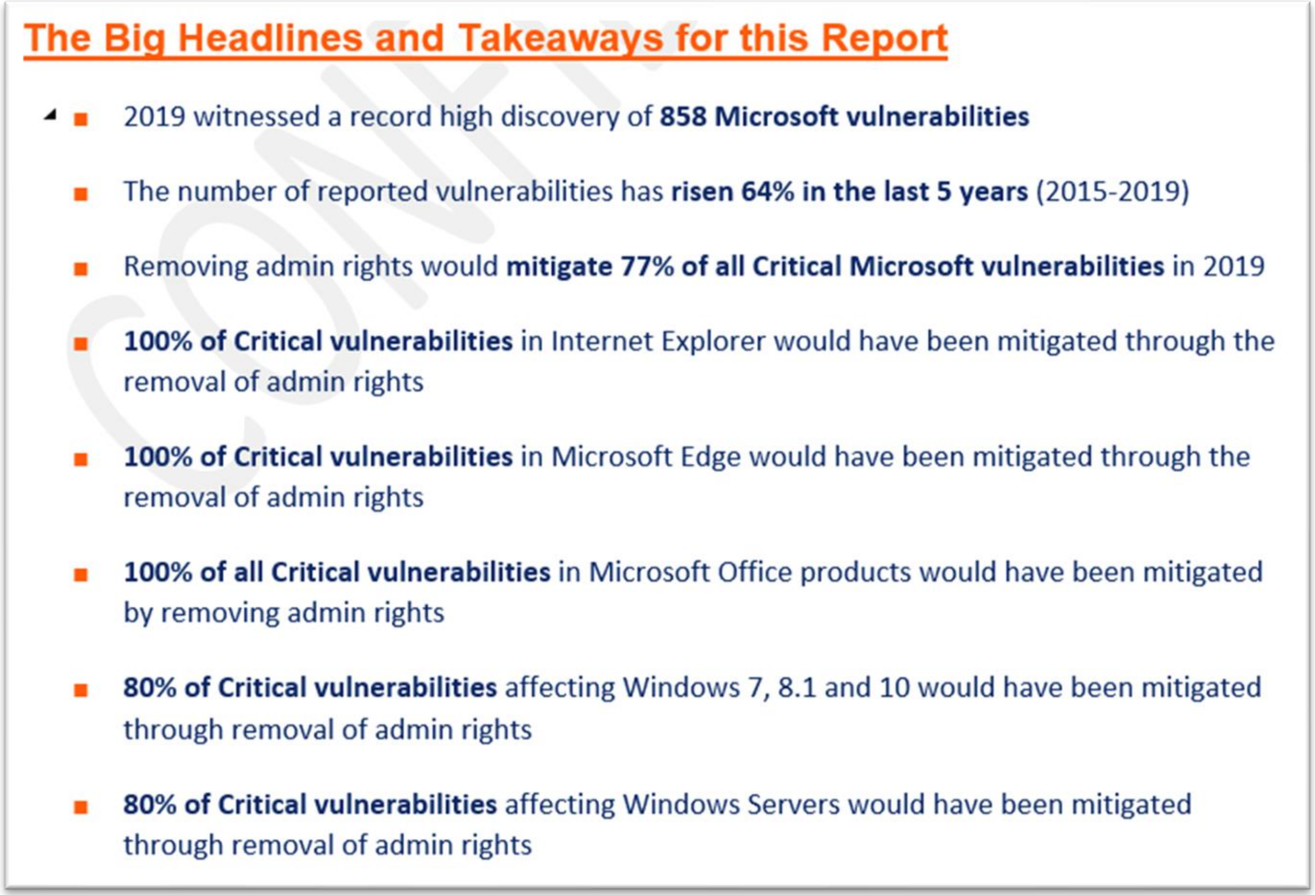
Executive Summary

Why Can’t Users Have Administrative Rights?

- Because it changes the risk from loss of one user’s assets to losing the whole company operations
- Because it allows the malicious tools to operate on Windows
- Because it prevents the company from controlling the computer settings and data
- Because it allows identity theft
- Because it allows Shadow IT
- Because Principle of Least Privilege is a Core Component of Zero Trust which Modern Workplace Client relies on

Why Shouldn’t Users Have Administrative Rights?

- Because it keeps computers’ performance better
- Because it decreases the need for reinstallations
- Because it increases productivity
- Because it helps the company in fighting against malware
- Because it decreases the amount of money needed in extra security solutions
- Because it patches more vulnerabilities than patching



The Big Headlines and Takeaways for this Report

- 2019 witnessed a record high discovery of **858 Microsoft vulnerabilities**
- The number of reported vulnerabilities has **risen 64% in the last 5 years** (2015-2019)
- Removing admin rights would **mitigate 77% of all Critical Microsoft vulnerabilities** in 2019
- **100% of Critical vulnerabilities** in Internet Explorer would have been mitigated through the removal of admin rights
- **100% of Critical vulnerabilities** in Microsoft Edge would have been mitigated through the removal of admin rights
- **100% of all Critical vulnerabilities** in Microsoft Office products would have been mitigated by removing admin rights
- **80% of Critical vulnerabilities** affecting Windows 7, 8.1 and 10 would have been mitigated through removal of admin rights
- **80% of Critical vulnerabilities** affecting Windows Servers would have been mitigated through removal of admin rights

	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%**

Vulnerabilities Soared in 2020

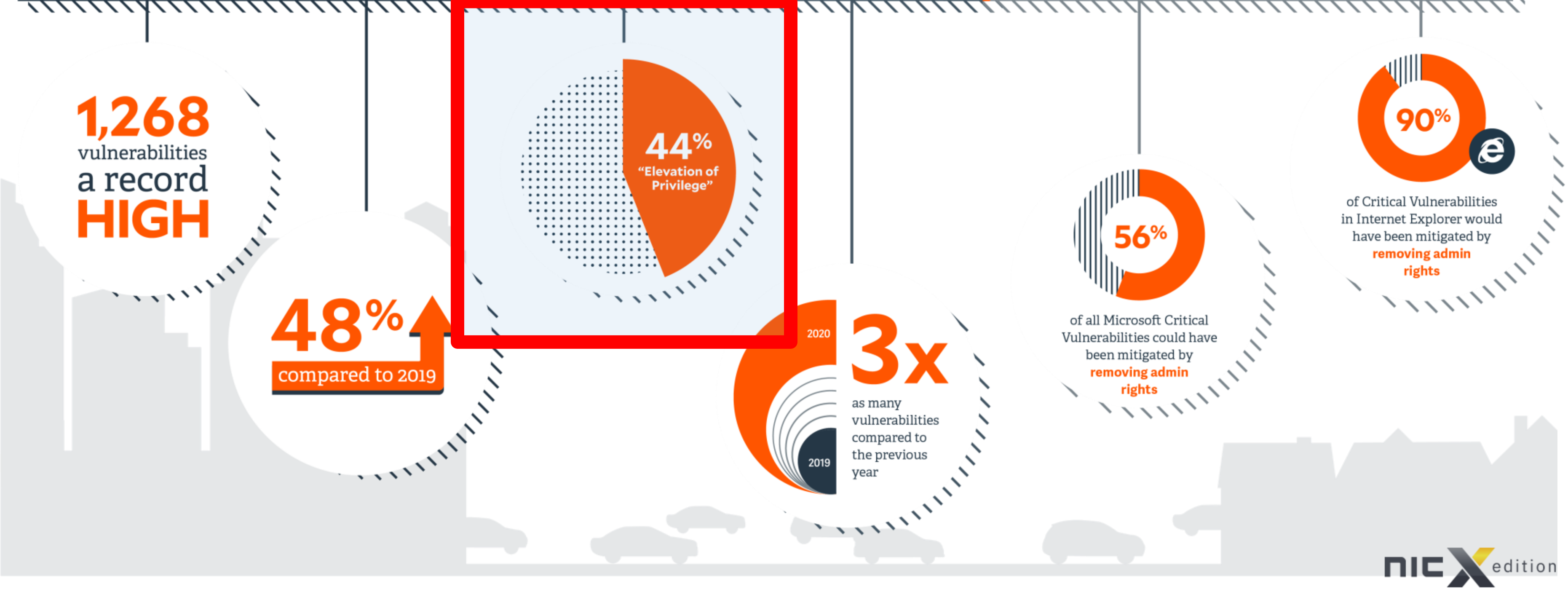
The threat landscape continues to **evolve and expand**, accelerated by the mass shift to **remote working**.

"Elevation of Privilege" was the #1 Category of Vulnerabilities

Attackers gain access to accounts and **increase the level of privileges** to compromise other IT assets.

Controlling Admin Rights Mitigates the Risk

Enforcing least privilege is the **fastest & most effective measure** to address this problem.



1,268 vulnerabilities a record HIGH

48% compared to 2019

44% "Elevation of Privilege"

3x as many vulnerabilities compared to the previous year

56% of all Microsoft Critical Vulnerabilities could have been mitigated by **removing admin rights**

90% of Critical Vulnerabilities in Internet Explorer would have been mitigated by **removing admin rights**

How does malware get into a computer?

95%+ of Attacks Happen Through Email or the Browser

- 90% of Critical vulnerabilities in internet explorer would have been mitigated through the removal of admin rights
- 85% of Critical Vulnerabilities in Microsoft edge would have been mitigated through he removal of admin rights.
- 100% of all critical vulnerabilities in Microsoft outlook would have been mitigated by removing admin rights.

Patching is like Anti-Malware – It’s reactive Security

How fast can you Patch?

Comparing to Patching, it’s way better…

Principle of Least Privilege is better – It’s Proactive Security

Let’s play “King of the CISOs” ☺

Which one is more secure?

Company 1

- World’s BEST in patching
- In 30days is FULLY PATCHED
- Users have admin rights

Company 2

- Doesn’t patch at all
- No admin rights

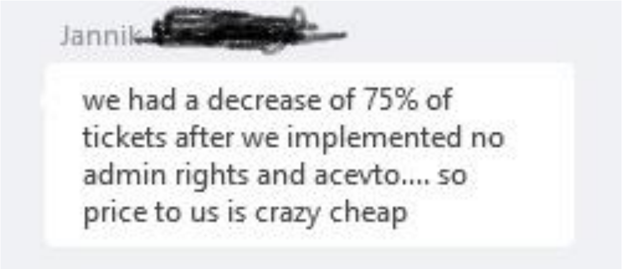
Servers are protected by protecting their endpoints and their ports!

- Servers are supposed to be headless…

Success!

This autumn!

Stop end-users from hurting their computers

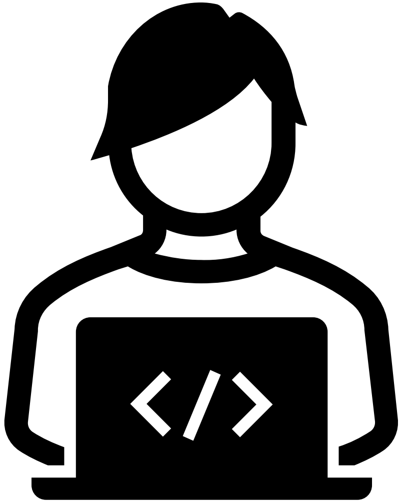


Jannik [redacted]

we had a decrease of 75% of tickets after we implemented no admin rights and acevto.... so price to us is crazy cheap

US Customer: 65% less reinstallations

GREEN MARINE
3



BUT SAMI… THERE ARE SOME THINGS IN WINDOWS YOU JUST CAN’T DO WITHOUT ADMIN RIGHTS…

I CALL BULLSHIT

- https://docs.microsoft.com/fi-fi/windows/desktop/win_cert/certification-requirements-for-windows-desktop-apps

DEMO

Shit’o’Meter
Permissions don’t protect…
Permissions can be bypassed
Group Policy / MDM can’t protect you…
Identities are not private
Sessions are not private…

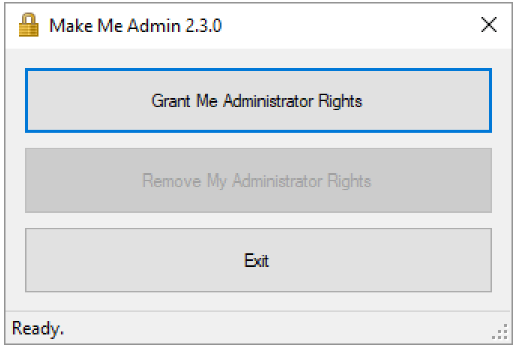
How do we fix this?

RunAs-solutions…

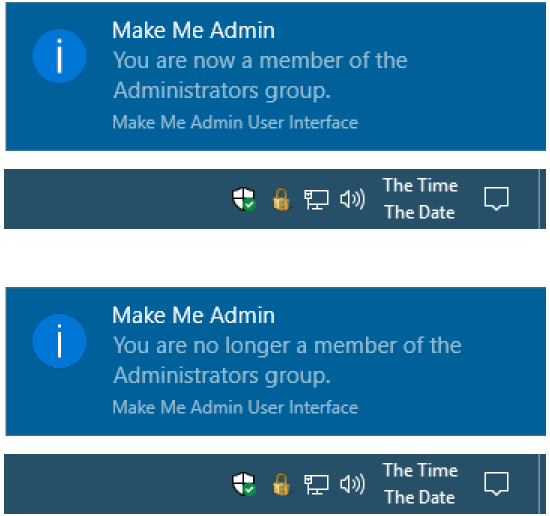
- Don’t really work
  - Erunas
  - Sudowin
  - Etc…
  - All use “CreateProcessWithLogonW”
- Except maybe for PowerShell JITJEA solutions for servers

MakeMeAdmin

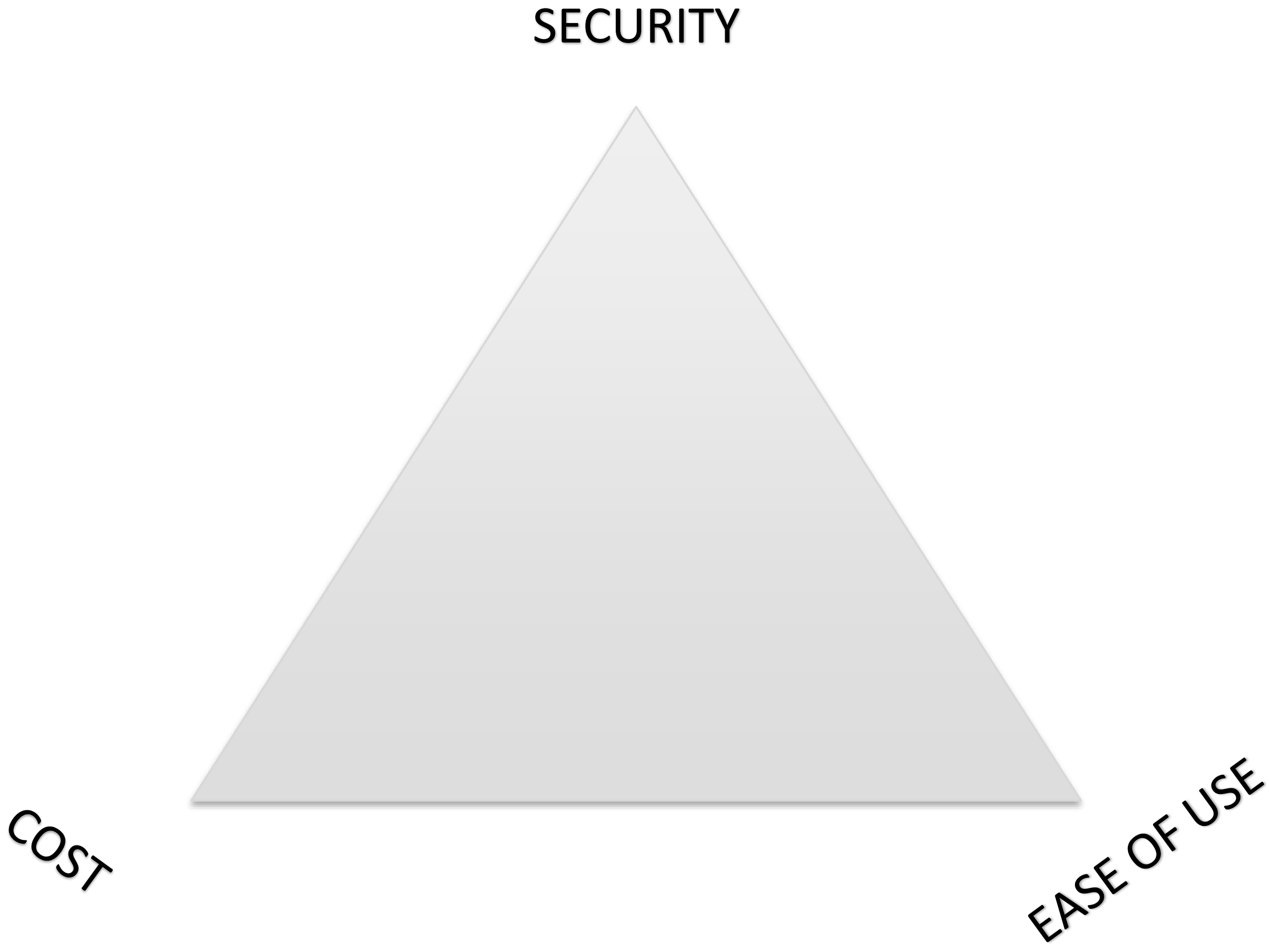
- https://github.com/pseymour/MakeMeAdmin/wiki/How-It-Works



Ready.


Make Me Admin
You are now a member of the Administrators group.
Make Me Admin User Interface

Make Me Admin
You are no longer a member of the Administrators group.
Make Me Admin User Interface



SECURITY

COST

EASE OF USE

Real solution

- If you ask me the real solution is to change from giving permissions to users or computers to giving permissions to processes
- Many solutions out there

BeyondTrust or equal to the rescue!

- The easiest way to just get rid of this problem!
- If you can’t afford BeyondTrust, try PolicyPak
- If you can’t afford any software you just have to try to do everything manually… ☹
- Check out: https://centero.fi/
  - Product: Carillon

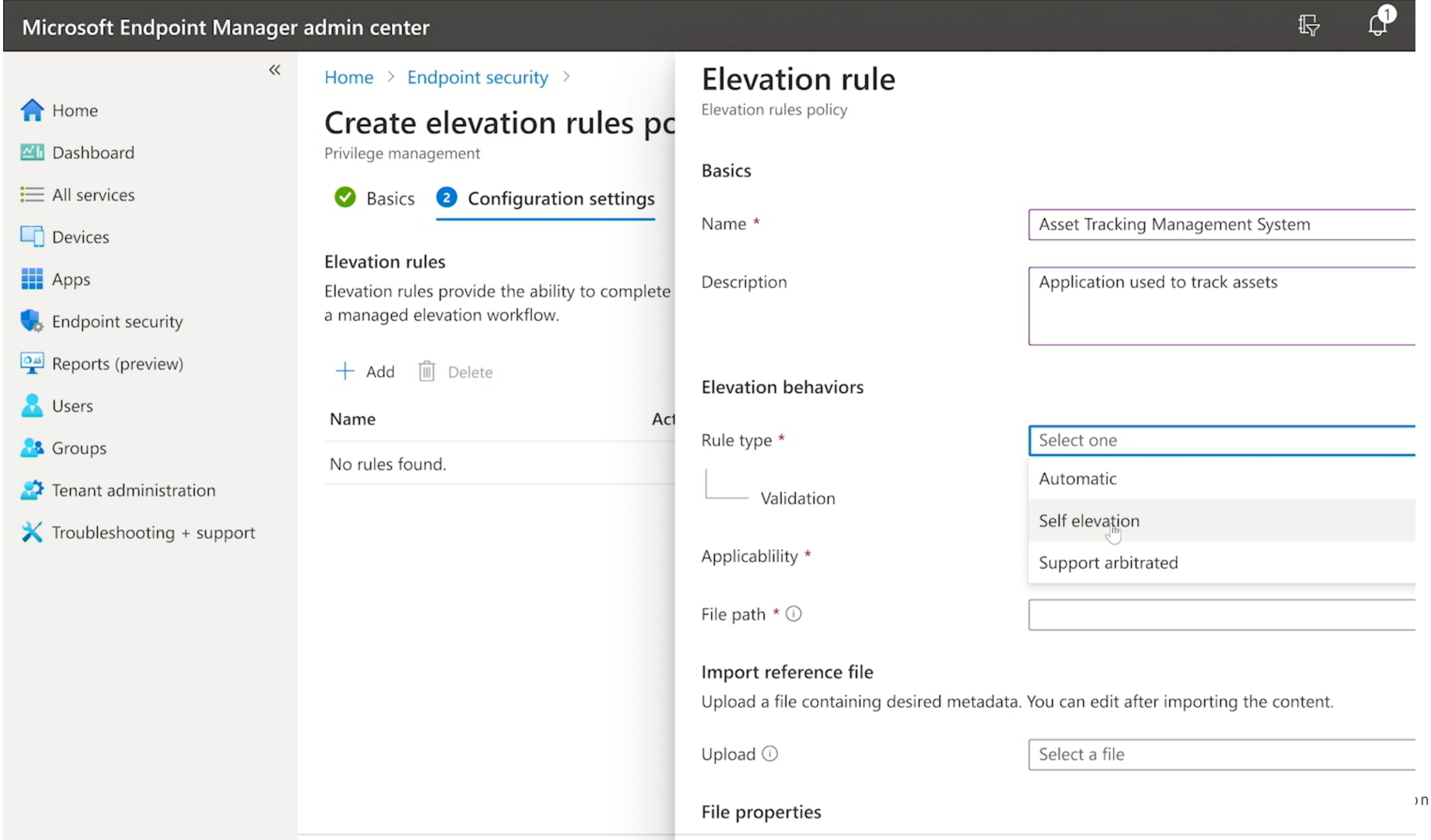
Price

- How to Buy & Licensing – PolicyPak
- BT: ~25-30€ per client + 25% for 1 year support
  - Varies greatly…
- Centero: 0,10€ / per client / month

Options

- On demand
    - Carillon
        - Can use the same account (with a network connection)
        - Self-elevation possible
- Rules based + On Demand
    - PolicyPak
        - Can use the same account (with a network connection)
        - Can elevate COM calls
        - Self-elevation possible
    - BeyondTrust
        - Can use the same account (with a network connection)
        - Self-elevation possible
        - Can elevate COM calls
        - More reporting

BUT WAIT!! WOOT??!



Create elevation rules pc

Privilege management

Elevation rules

Elevation rules provide the ability to complete a managed elevation workflow.

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

Applicablility *

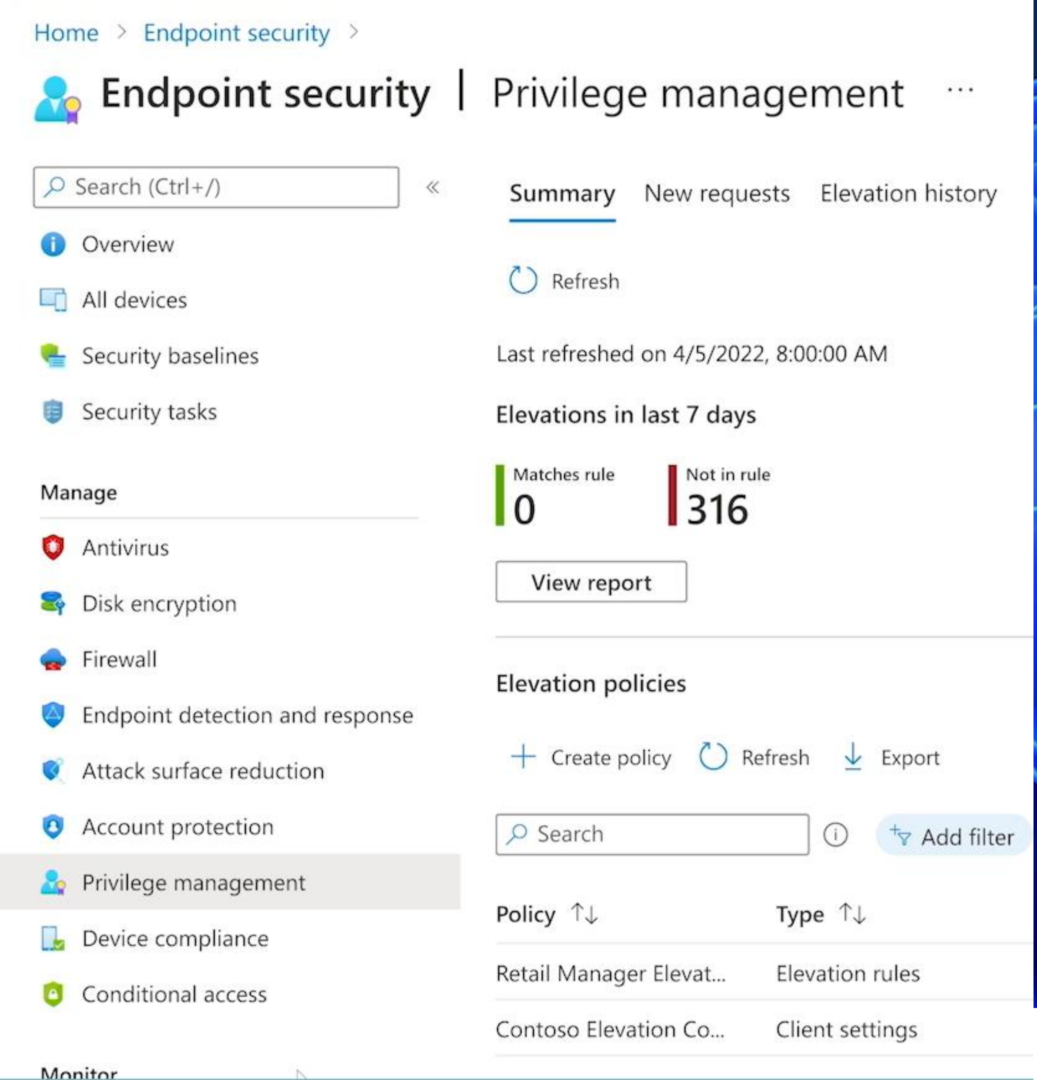
File path *

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

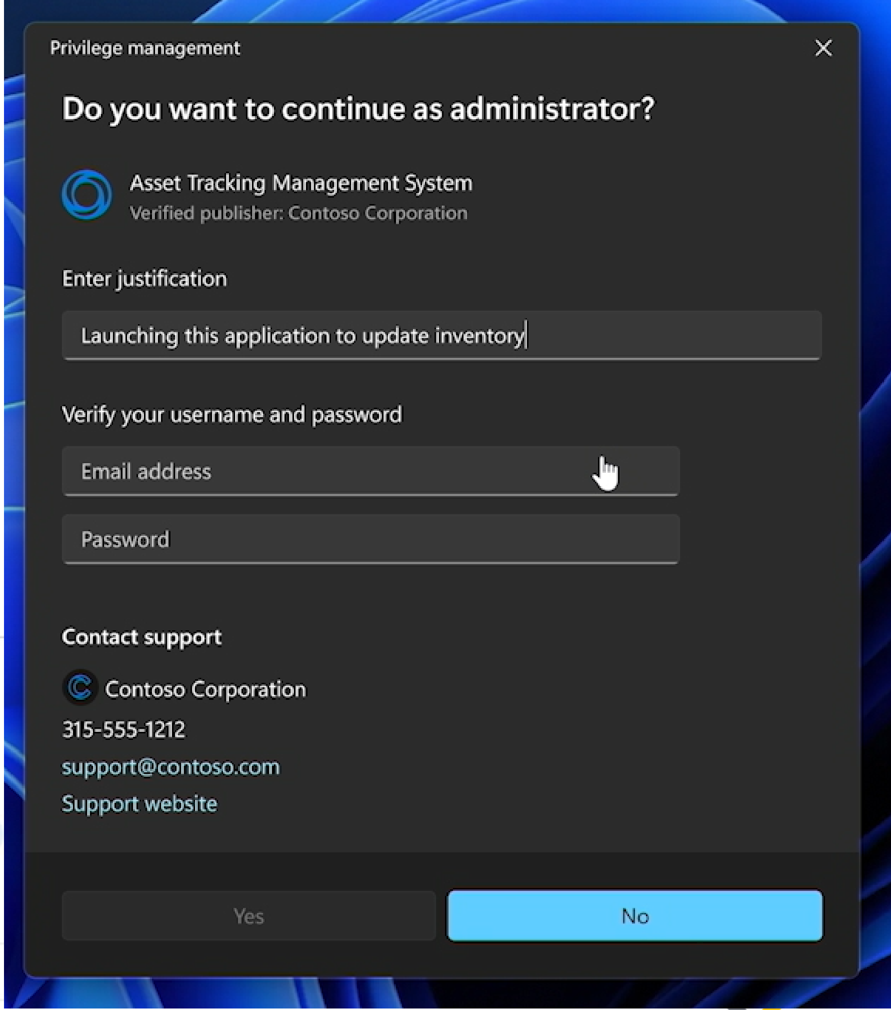
View report

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

Or…

- The **average cost** of a data breach in 2020 was **$3.86 million**
- The **average cost** of a breach caused by ransomware in 2020 was **$4.44 million** *(source: govtech.com)*
- According to an annual report on global cyber security, there were a total of **304 million ransomware attacks worldwide in 2020** *(source: statista.com)*

How to deal with Devs, Kids and Students?

Options

Self elevation	With or without explanation
Log only	Visibility is the key
Reduce rights	For enemy entry points

How I’ve lived without admin rights for 18 years?

DEMO

PAM

“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
- Slides and demos from the conference will be available at
  - https://github.com/nordicinfrastructureconference/2022