May 31 – June 2, Oslo Spektrum

10th anniversary

Sami Laiho

Protecting Endpoints in a ZeroTrust world!

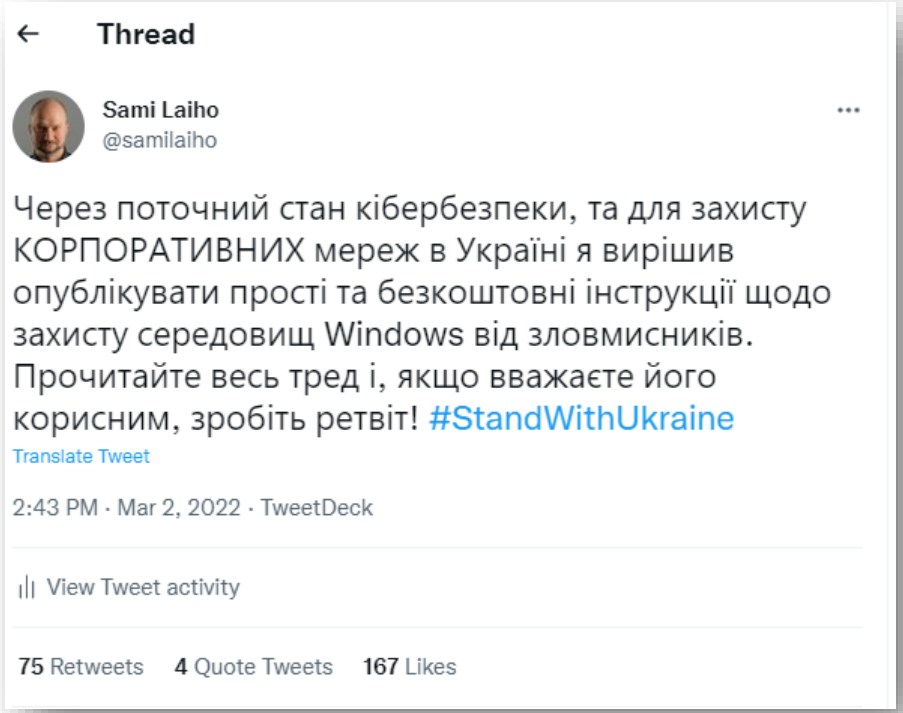
Sami Laiho

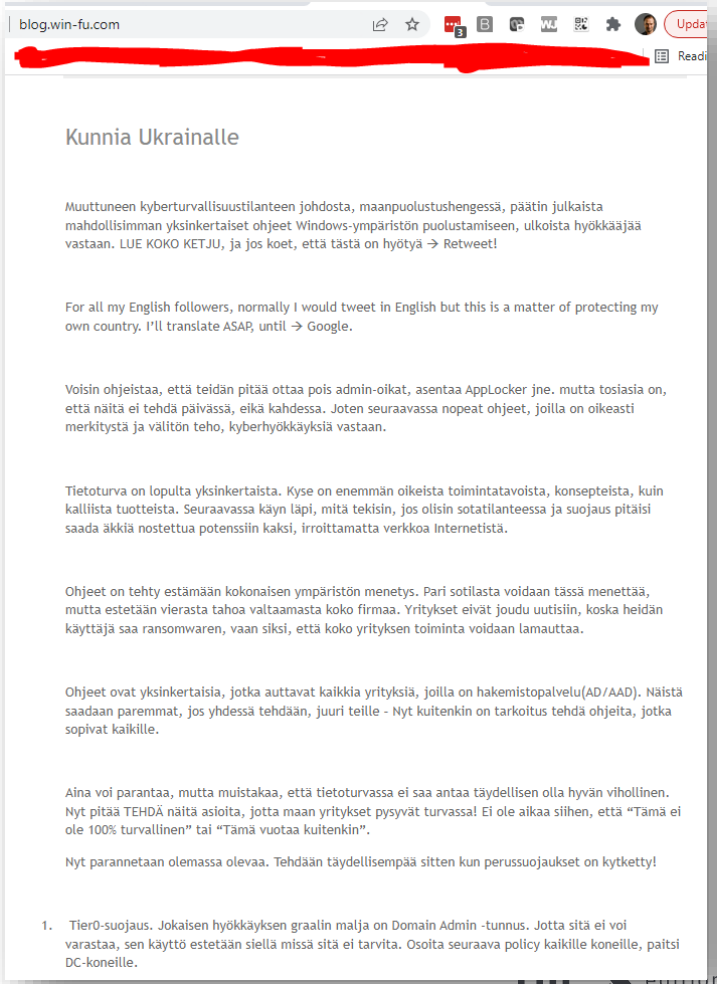
Senior Technical Fellow
adminize.com

- 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

Meanwhile in Finland...

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.

BYOD

New Zero-Trust Era

Why Zero Trust?

- Empower your users to work more securely anywhere and anytime, on any device
- Enable digital transformation with intelligent security for today’s complex environment
- Close security gaps and minimize risk of lateral movement

Zero Trust principles

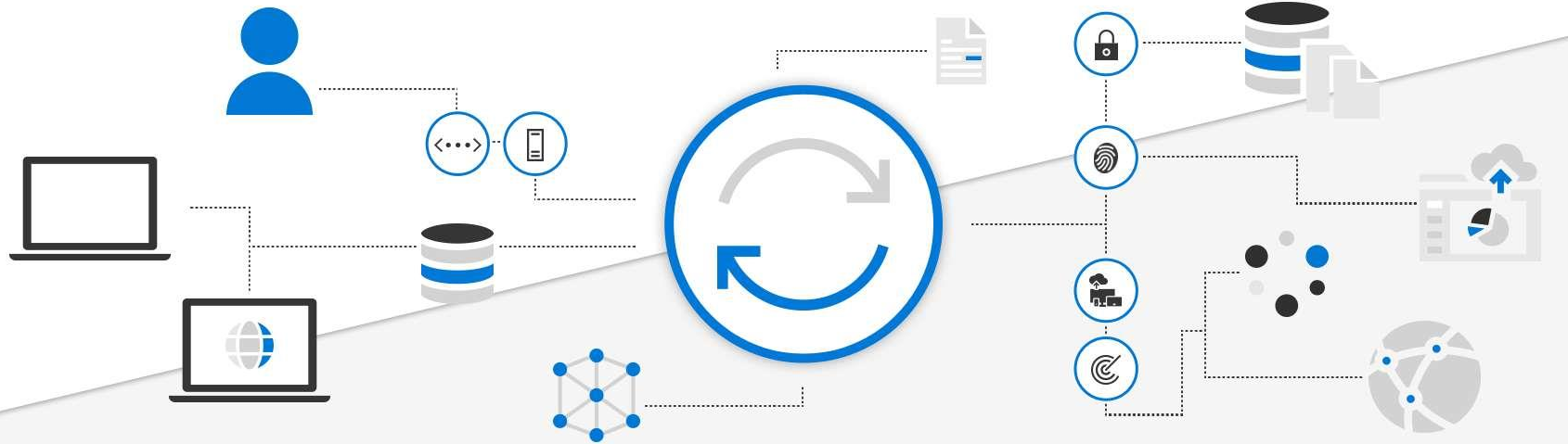
Verify explicitly

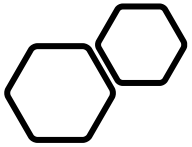
Use least privileged access

Assume breach

Zero Trust defined

- Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network





“Never trust, always verify”

Zero Trust Components

- Identities
  - Verify and secure each identity with strong authentication across your entire digital estate.
- Devices
  - Gain visibility into devices accessing the network. Ensure compliance and health status before granting access.
- Applications
  - Discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, and monitor and control user actions.

Zero Trust Components

- Data
  - Move from perimeter-based data protection to data-driven protection. Use intelligence to classify and label data. Encrypt and restrict access based on organizational policies.
- Infrastructure
  - Use telemetry to detect attacks and anomalies, automatically block and flag risky behavior, and employ least privilege access principles.
- Network
  - Encrypt all internal communications, limit access by policy, and employ microsegmentation and real-time threat detection.

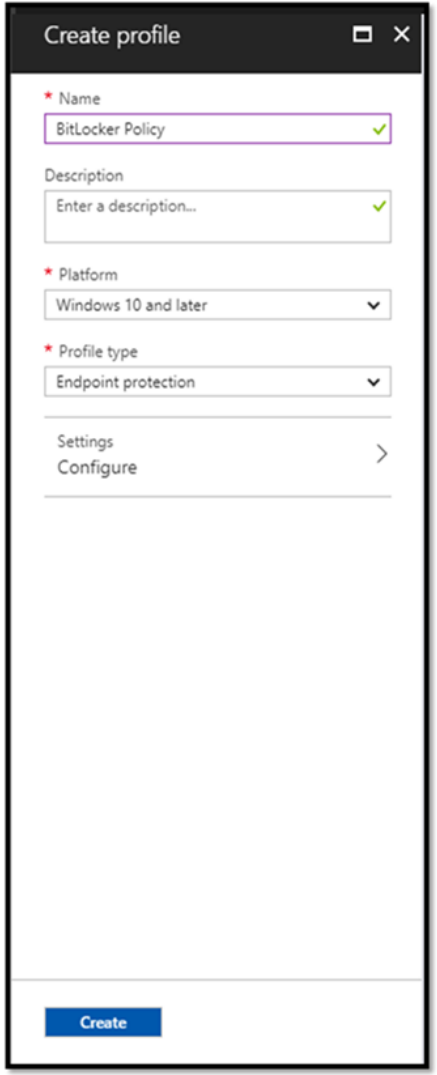
Security is simple

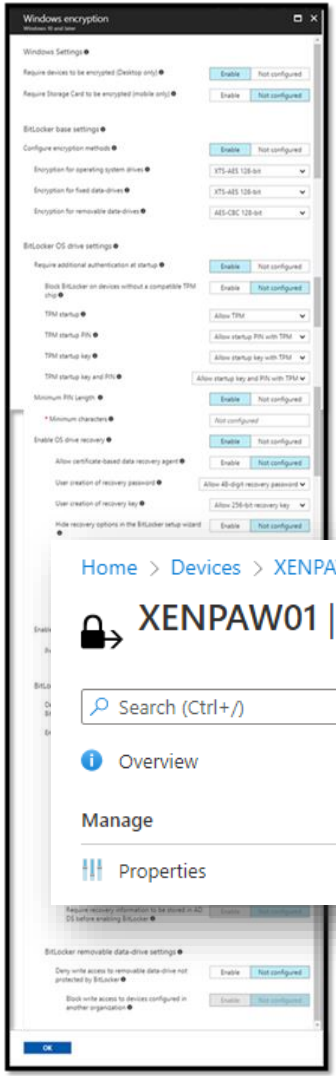
- Don’t look like a rookie – You don’t need to be perfect, just better than your neighbor
- Limit the amount of Domain Admins / Global Admins
- Prevent usage of privileged accounts, that can take down the environment, from being used on computers that can get malware
- Prevent management of your systems from endpoints that can “go to Facebook”
- Prevent computers from talking to each other if they don’t have to
- Enforce Multi-Factor Authentication
- Encrypt all disks
- Don’t give end-users and devs admin rights
- Keep your Hardware and Software Inventory up to date
- Establish or outsource a SoC

Encrypt all Devices!

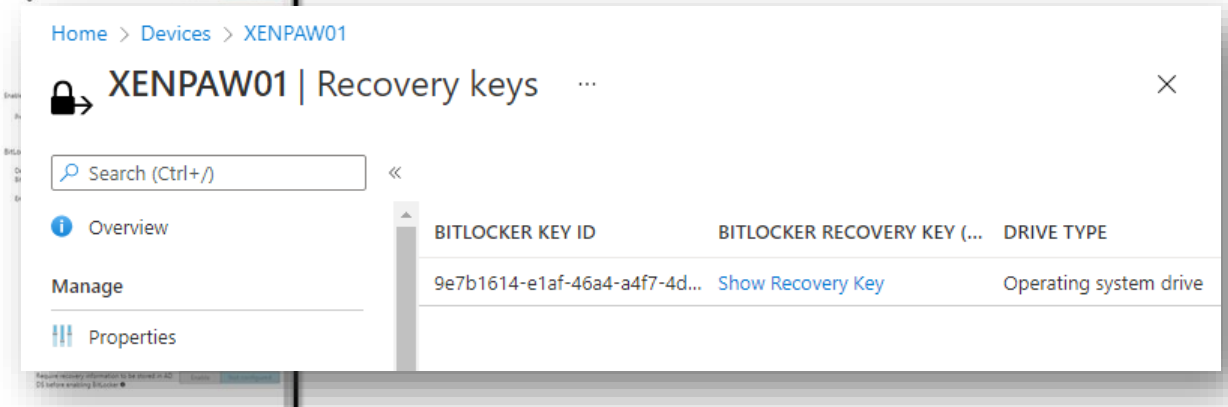
Why we need encryption?

- Data wise because over 800000 devices get lost or stolen on the biggest airports in US and Europe yearly
- Security wise because all Windows versions can be cracked with a single command
- Secure decommissioning
  - The format utility (since Windows Vista) deletes the volume metadata and overwrites those sectors to securely delete any BitLocker keys and by doing so makes the volume instantly unreadable


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


Windows encryption


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


Home > Devices > XENPAW01
XENPAW01 | Recovery keys
Search (Ctrl+/)
Overview
Manage
Properties
BITLOCKER KEY ID
BITLOCKER RECOVERY KEY (...
DRIVE TYPE
9e7b1614-e1af-46a4-a4f7-4d...
Show Recovery Key
Operating system drive

Forget INTERNAL networks!

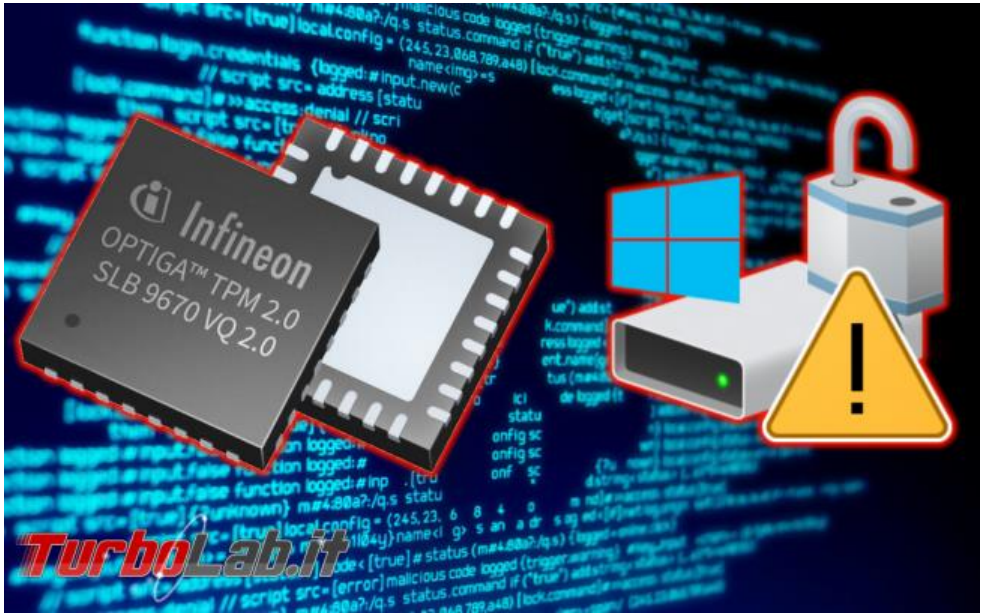
Welcome VPNs and IPsec!

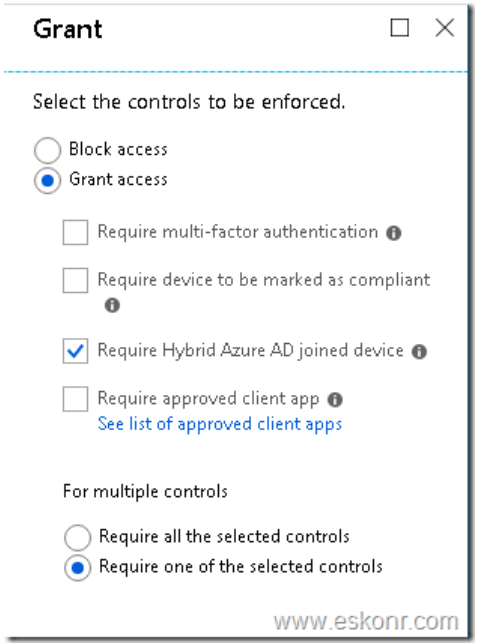
DEMO - IPsec

Known and Healthy Devices

MFA & Biometrics

- PIN is a lot safer than a password! Just keep that in mind!
- I love biometrics!





“MFA Everything!”

“If you RDP, you MFA!”

DEMO - MFA

Principle of Least Privilege

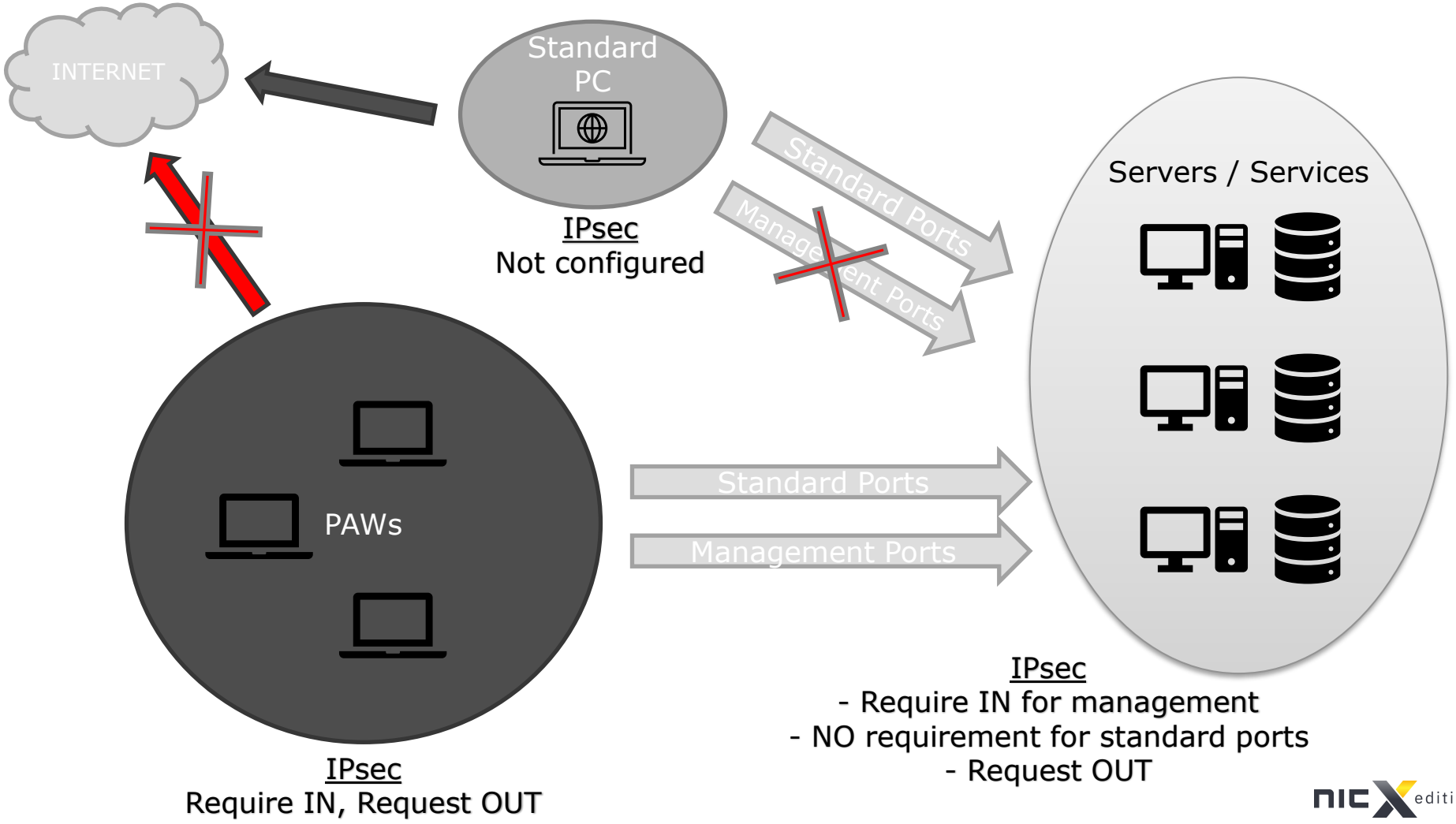
- In Windows there is no Security if you logon as an admin
- The security subsystem was not built to withstand the use of admin rights
- With “No-Admin” approach
  - We get better performance
  - We get less tickets
  - We get less reinstallation
  - We get more productive users!
  - We get less malware
  - We get to be lazier as admins!

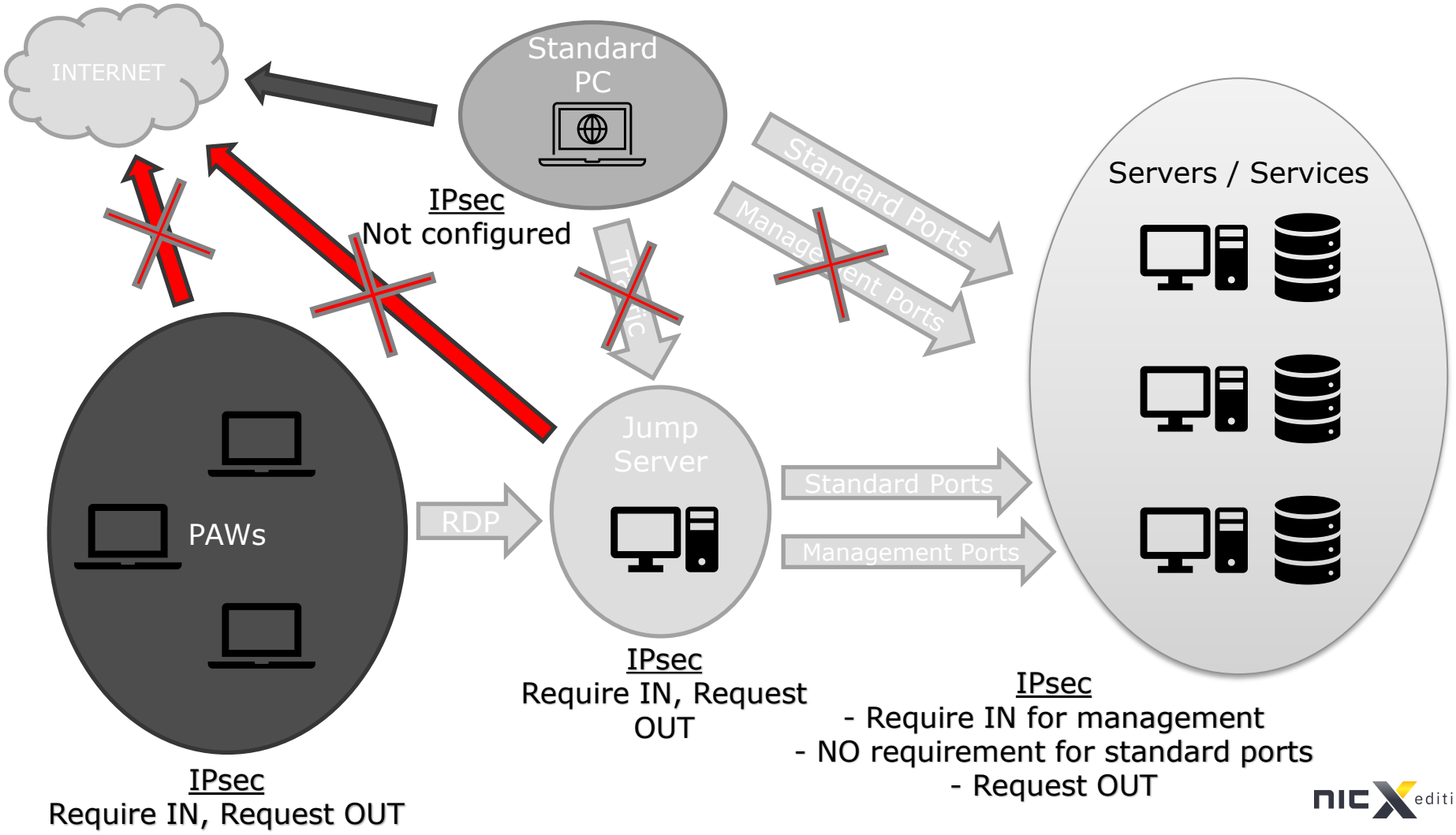
If you can use a device to take down the company, you should not be able to Facebook on it...

Privileged Access Workstation (PAW)

PAW-workstations

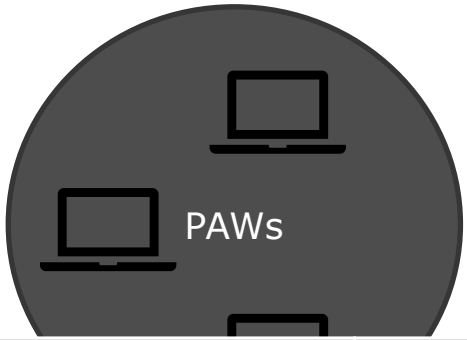
- Management WS
  - RSAT installed
  - Allowed to use Windows Admin Center
  - Allowed to logon with administrative users (and usually only by them)
    - Hopefully not interactively though
- https://blogs.technet.microsoft.com/datacentersecurity/2017/10/13/privileged-access-workstationpaw/


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

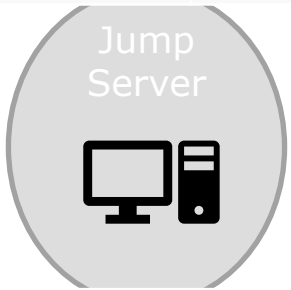

INTERNET
Standard PC
IPsec
Not configured
Standard Ports
Management Ports
Traffic
Servers / Services
PAWs
RDP
Jump Server
Standard Ports
Management Ports
IPsec
Require IN, Request OUT
IPsec
Require IN, Request OUT
IPsec
- Require IN for management
- NO requirement for standard ports
- Request OUT

Administrators-group members

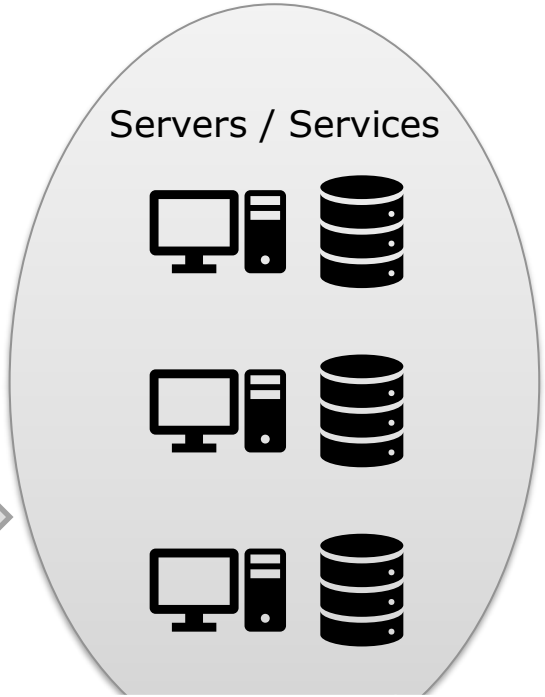
Administrators	
Domain Admins	YES
Workstations Admins	YES
Server Admins	NO
Builtin Administrator (used via LAPS)	YES



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

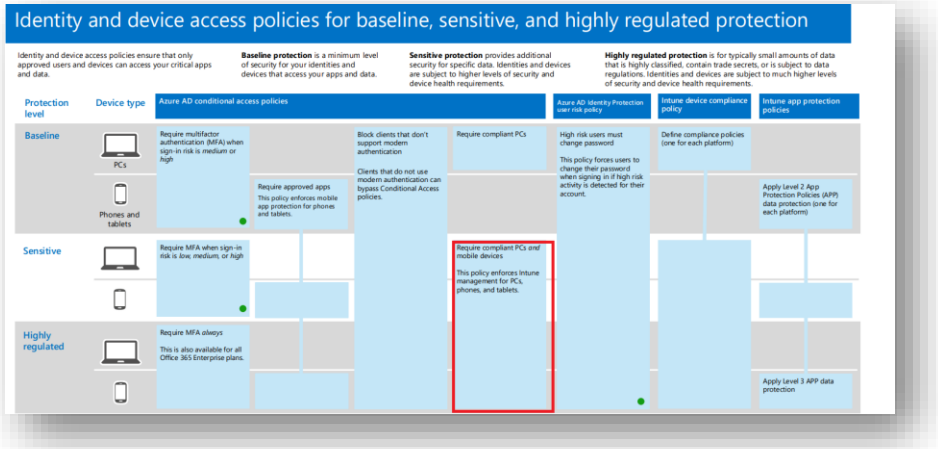


Administrators	
Domain Admins	YES
Workstations Admins	NO
Server Admins	YES
Builtin Administrator (used via LAPS)	YES

dition

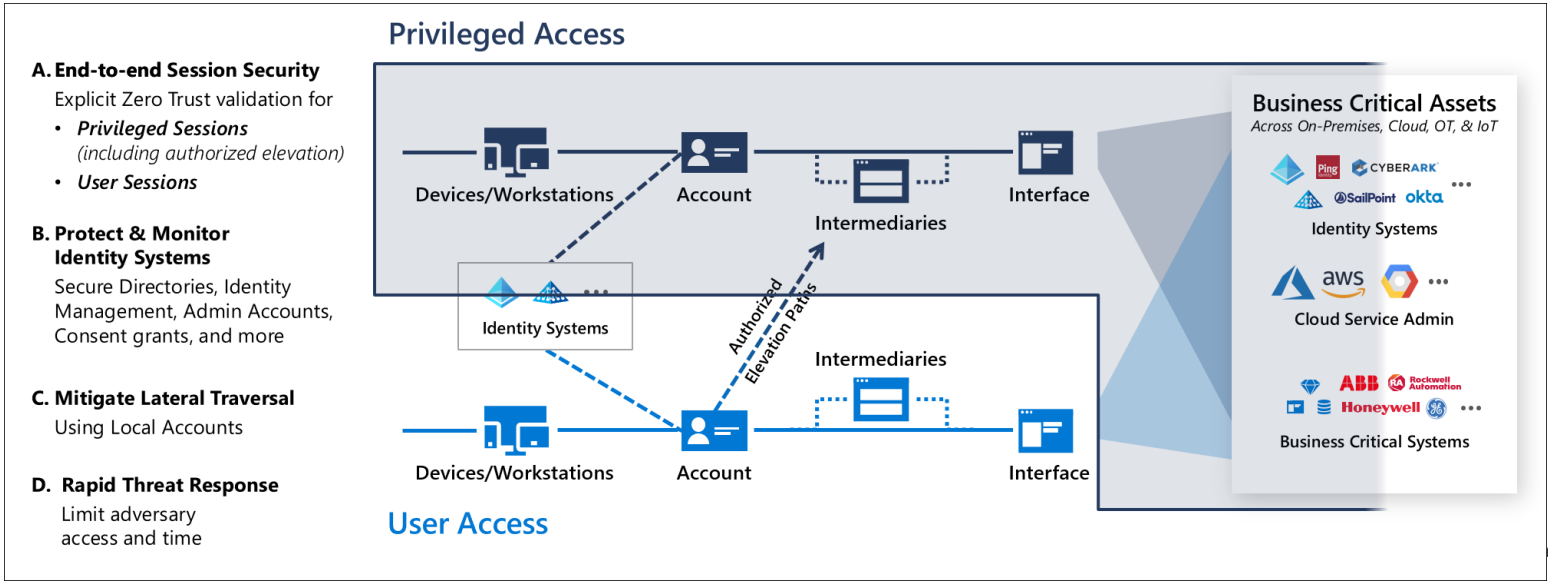
Native Azure PAW

- Good instruction on how to do it with Conditional Access Policies!
  - https://call4cloud.nl/2021/11/paw-love-and-thunder/
- Microsoft's own doc: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices



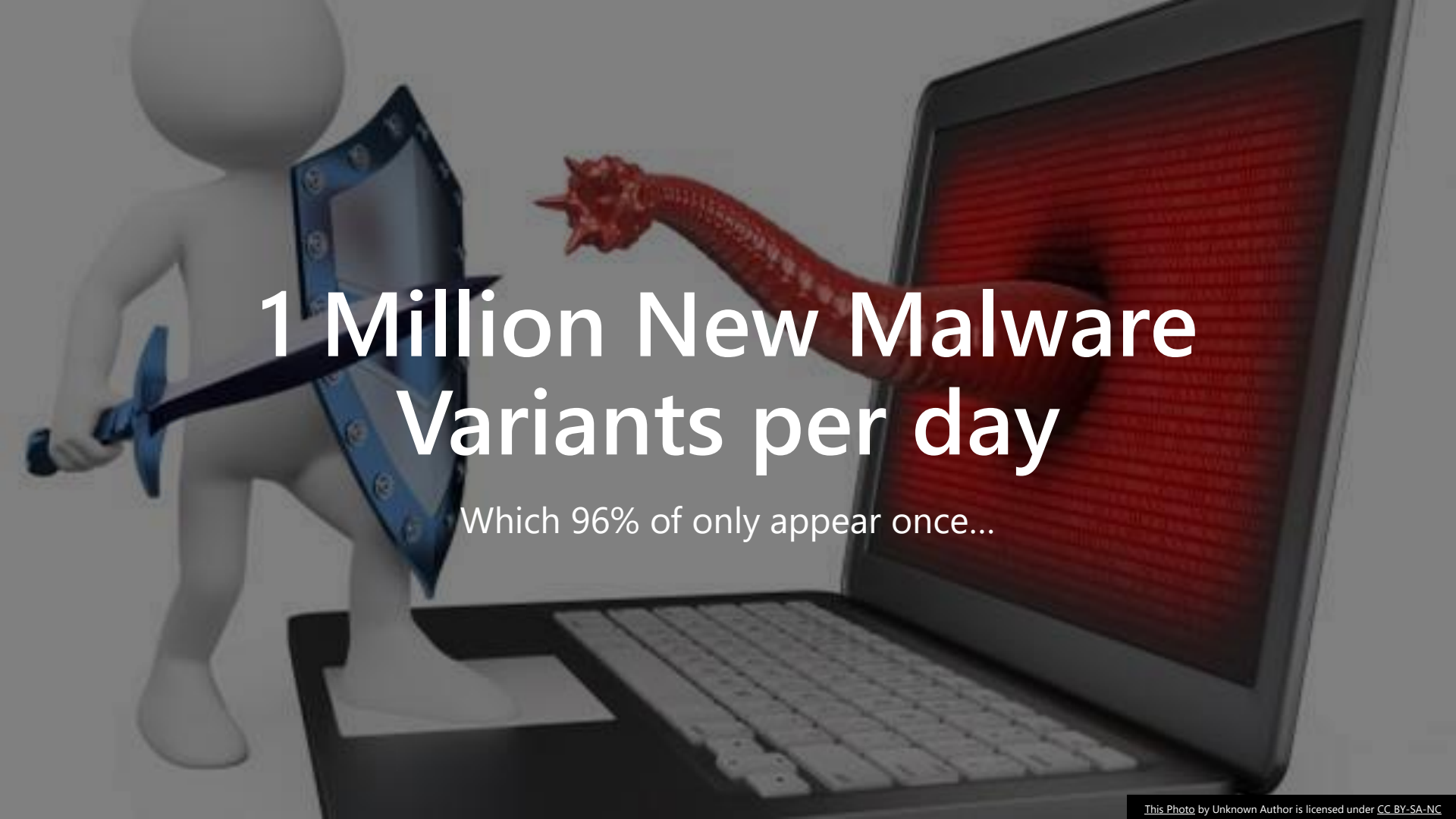
Microsoft RAMP

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



DEMO - PAW

Allow-Listing

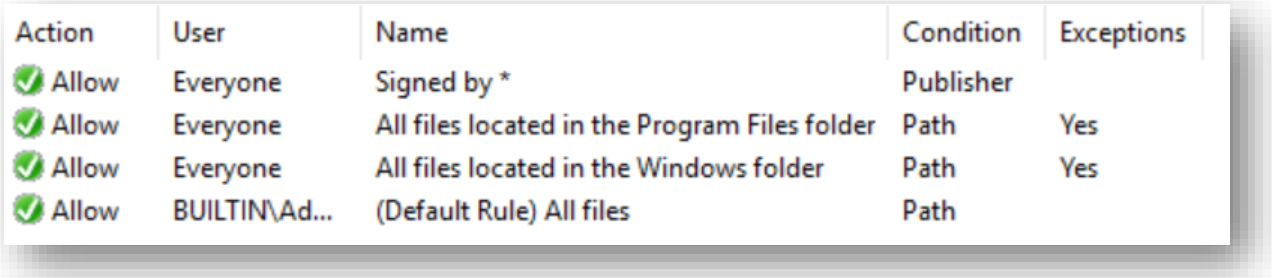


1 Million New Malware Variants per day

Which 96% of only appear once…

Simplest AppLocker

- THIS KILLS 950000+ PIECES OF MALWARE PER DAY!! With no Anti-Malware ☺

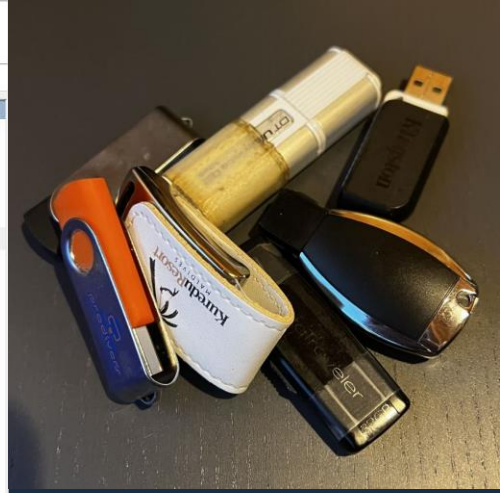


Action	User	Name	Condition	Exceptions
Allow	Everyone	Signed by *	Publisher	
Allow	Everyone	All files located in the Program Files folder	Path	Yes
Allow	Everyone	All files located in the Windows folder	Path	Yes
Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

DEMO

Apps Required to Have Earned Trust – Aka Allow-Listing

Control Devices



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 GUIDs appear in the list you create. If you enable this policy

Show Contents

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

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

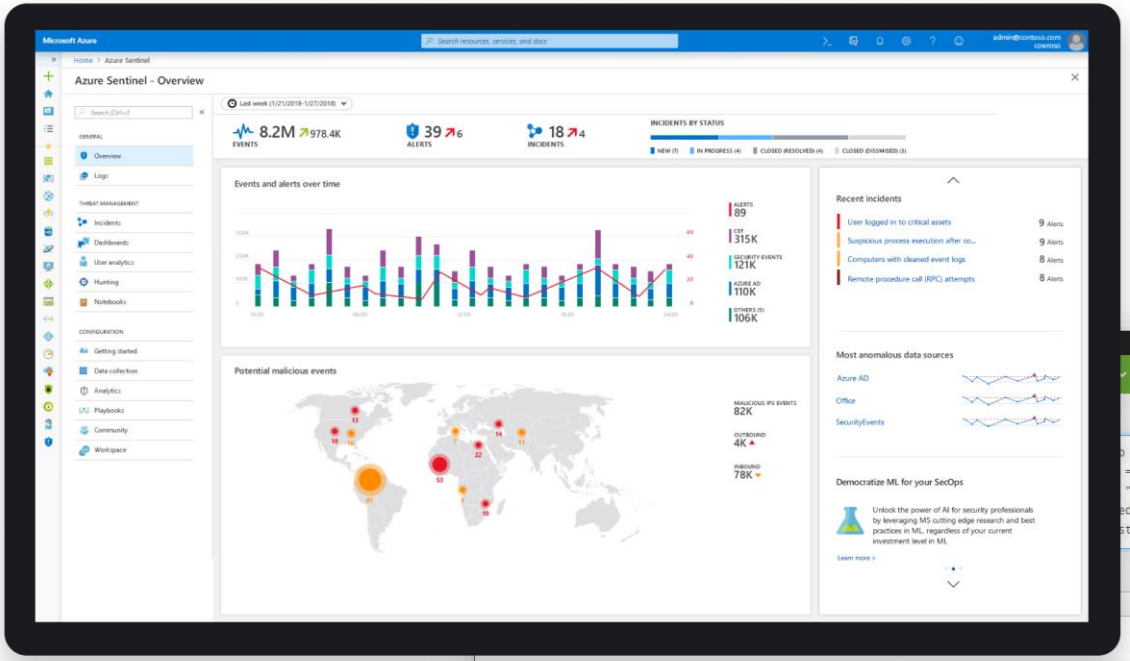
OK

Settings

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

2°C Pilvistä ENG 11.55 8.3.2022

Monitoring



Function1 System Acct | 3 Messages | Settings | Activity | Help | Find

Settings | Run a Search | Monitoring Console

Save As | Close

```
= if (status == "missing", "N/A", sum_kb) | eval avg_tcp_kbps_sparkline = if
== "missing", "N/A", avg_tcp_kbps) | eval avg_tcp_eps = if (status ==
"Heavy Forwarder", forwarder_type == "uf", "Universal Forwarder",
ed = strftime(last_connected, "%m/%d/%Y %H:%M:%S %z") | search NOT [|
stname] status=missing | replace * WITH "<hostname-IP>" IN hostname
```

Last 60 minutes

Job | Smart Mode

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

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