

Zero Admins – Zero Problems

- Sami Laiho
- Senior Technical Fellow @adminize.com
- Twitter @samilaiho
- MVP



NORDIC

– VIRTUAL SUMMIT –

Sami Laiho

Senior Technical Fellow
adminize.com / Sulava

- IT Admin since 1996
- MVP in Windows OS since 2011
- **"100 Most Influential people in IT in Finland" – TiVi'2019, 2020**
- 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



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

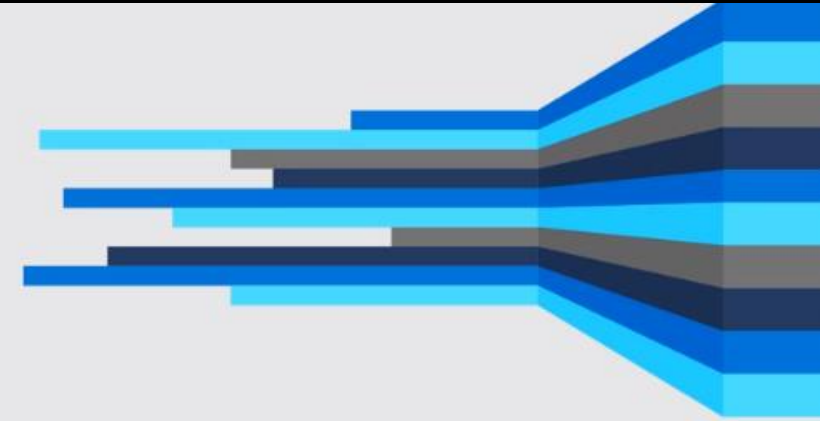


Use least privileged access



Assume breach

Trust



Admin Epoch

1985 - 2005

Users run as local admin
Users install their own software
Apps trusted by default



Non-Admin Epoch

2005 - 2025

Users run as standard user
Admins install software
Apps trusted by default



App Control Epoch

2025 - ?


Users run as standard user
Admins install software
Apps trusted when trust is earned



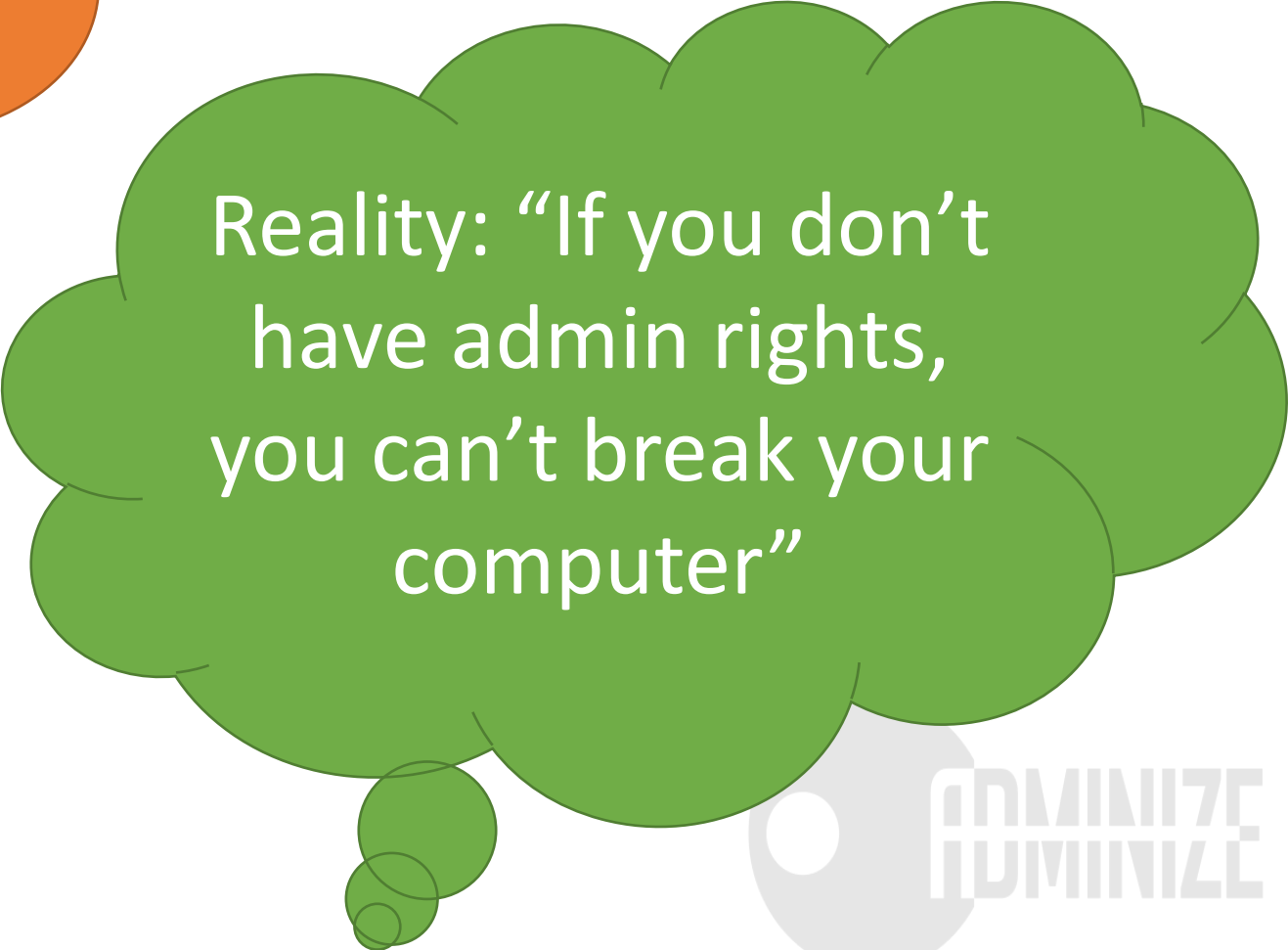
Principle of Least Privilege

- Windows can't guarantee 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



An orange thought bubble with a black outline and three smaller circles trailing from its bottom left.

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

A green thought bubble with a black outline and three smaller circles trailing from its bottom left.

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

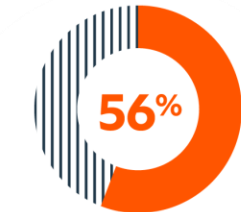
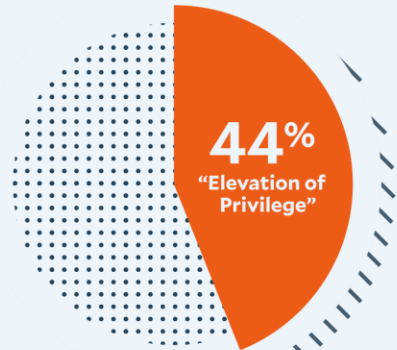
Attackers gain access to accounts and **increase the level of privileges** to compromise other IT assets.

Controlling Admin Rights Mitigates the Risk

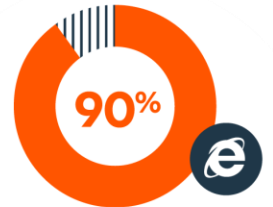
Enforcing least privilege is the **fastest & most effective measure** to address this problem.

1,268
vulnerabilities
a record
HIGH

48%
↑
compared to 2019



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



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

**ADMINIMIZE
ADMINIMIZE**

A collage of four icons: a blue envelope icon in a circle at the top; a compass with a blue face and silver rim on the bottom left; a globe with a blue and orange color scheme on the bottom center; and a Chrome logo with its characteristic red, yellow, and green segments and a blue center on the bottom right.

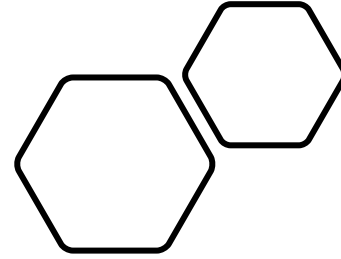
How does malware
get into a computer?

95%+ of Attacks Happen Through Email or the Browser

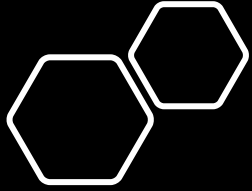
- 90% of Critical vulnerabilities in internet explorer would have been mitigated through the removal of admin rights
- 85% of Critical Vulnerabilities in Microsoft edge would have been mitigated through the removal of admin rights.
- 100% of all critical vulnerabilities in Microsoft outlook would have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

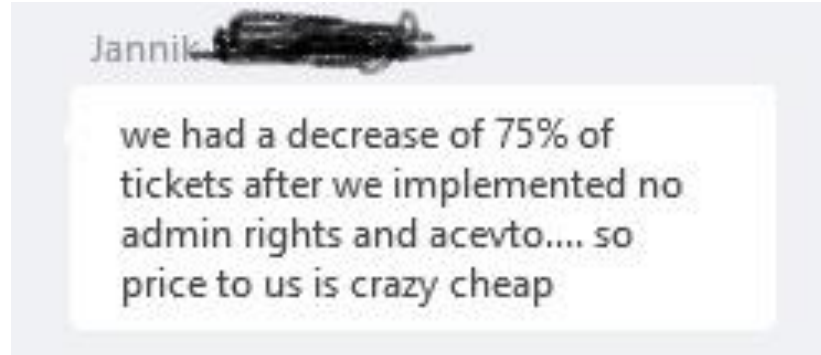


Success!

This autumn!



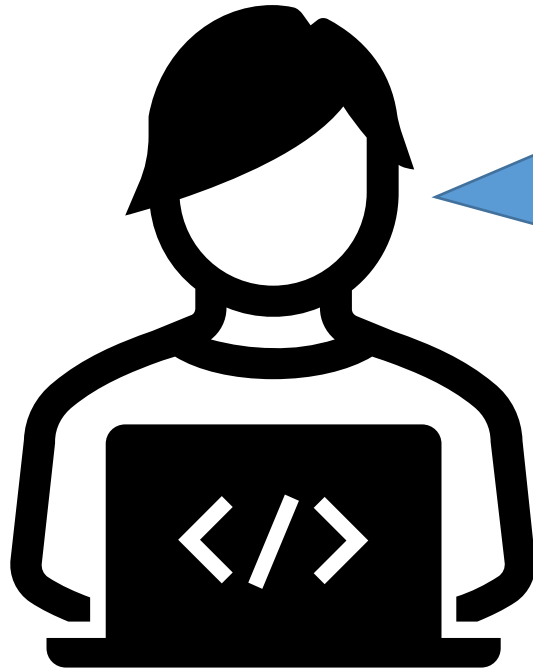
Stop end-users from hurting their computers



US Customer: 65% less
reinstallations







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

The diagram features a large, solid black hexagon on the left containing the word 'DEMO'. To its right is a smaller, solid black hexagon containing the text 'Shit'o'Meter'. This smaller hexagon is connected by a black line to a larger, hollow hexagon on the right. Above the 'Shit'o'Meter' hexagon are two small, hollow hexagons, one slightly overlapping the other.

DEMO



No BitLocker...

The diagram features a large dark grey shape on the left containing the word 'DEMO'. To its right is a cluster of hexagons: two small white hexagons at the top, a solid black hexagon in the middle containing the text 'No BitLocker...', and a large white hexagon with a black outline at the bottom. A black line connects the bottom of the solid black hexagon to the top of the large white hexagon.

DEMO



Permissions
don't protect...

The diagram features a large dark grey shape on the left containing the word 'DEMO'. To its right, there are two small white hexagons at the top. Below them is a solid black hexagon containing the text 'Permissions don't protect...'. A line extends from the bottom of this black hexagon and connects to a larger, empty white hexagon on the right.

DEMO



Permissions can
be bypassed

The diagram features a large dark grey shape on the left containing the word 'DEMO'. To its right, there are three hexagons: two small white ones at the top left and one large white one on the right. A black callout box with the text 'Permissions can be bypassed' is connected to the large white hexagon by a black line.


DEMO



Group Policy /
MDM can't
protect you...

The diagram features a large dark grey shape on the left containing the word 'DEMO'. To its right, there are two small white hexagons at the top. Below them is a solid black hexagon containing the text 'Group Policy / MDM can't protect you...'. A line extends from the bottom of this black hexagon and connects to a larger, empty white hexagon on the right.


DEMO



The diagram features a large, dark gray, rounded shape on the left side of the slide. To its right, there is a cluster of hexagons. At the top left of this cluster are two small, white-outlined hexagons. Below them is a solid black hexagon containing the text "Identities are not private". To the right of this black hexagon is a large, white-outlined hexagon. A thin black line connects the bottom of the black hexagon to the left side of the large white-outlined hexagon.

Identities are
not private

DEMO



Sessions are not private...

The diagram features a large dark grey shape on the left containing the word 'DEMO'. To its right, there is a cluster of hexagons. At the top left of this cluster are two small, empty hexagons. Below them is a solid black hexagon containing the text 'Sessions are not private...'. To the right of this solid hexagon is a large, empty hexagon with a black outline. A black line connects the bottom of the solid hexagon to the bottom-left corner of the large empty hexagon.



Have do we fix this?

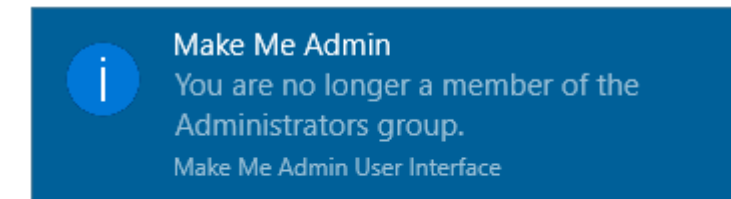
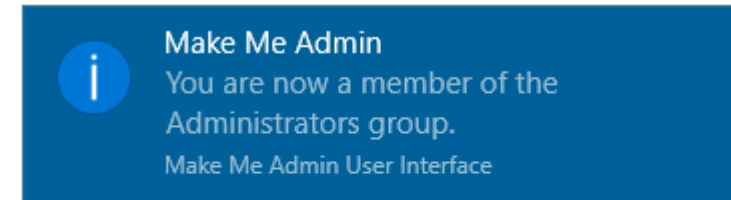
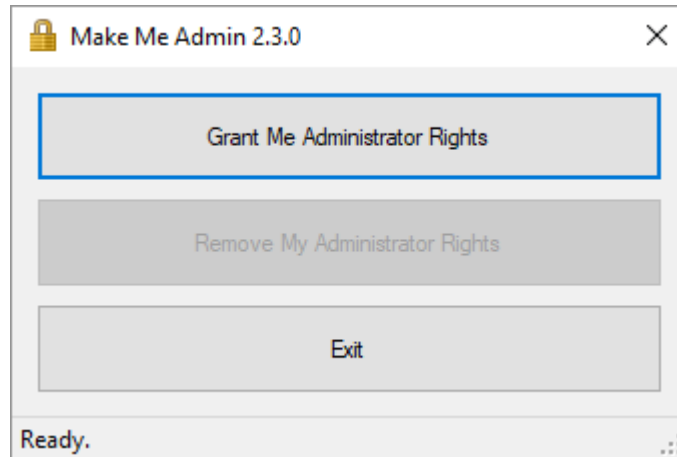
RunAs-solutions...

- Don't really work
 - Erunas
 - Sudowin
 - Etc...
 - All use "CreateProcessWithLogonW"
- Except maybe for PowerShell JITJEA solutions for servers

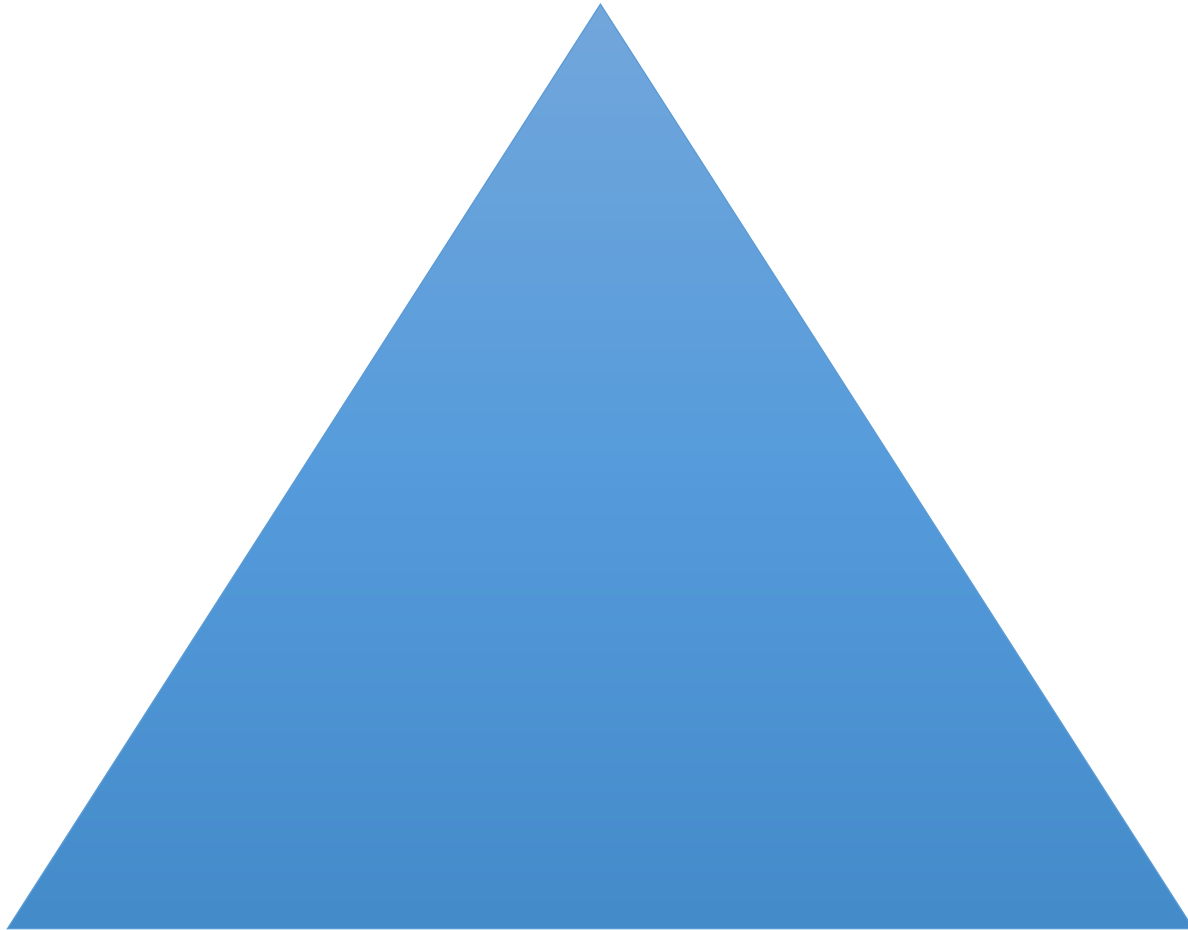


MakeMeAdmin

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



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
 - Adminizer
 - Always a separate account
 - 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)
 - Self-elevation possible
 - BeyondTrust
 - Can use the same account (with a network connection)
 - Self-elevation possible
 - More reporting



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

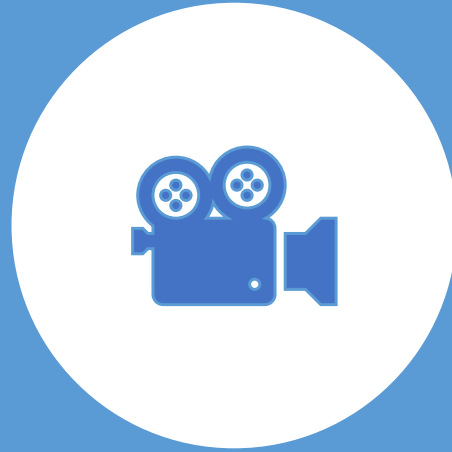
Log only

Visibility is the key

Reduce rights

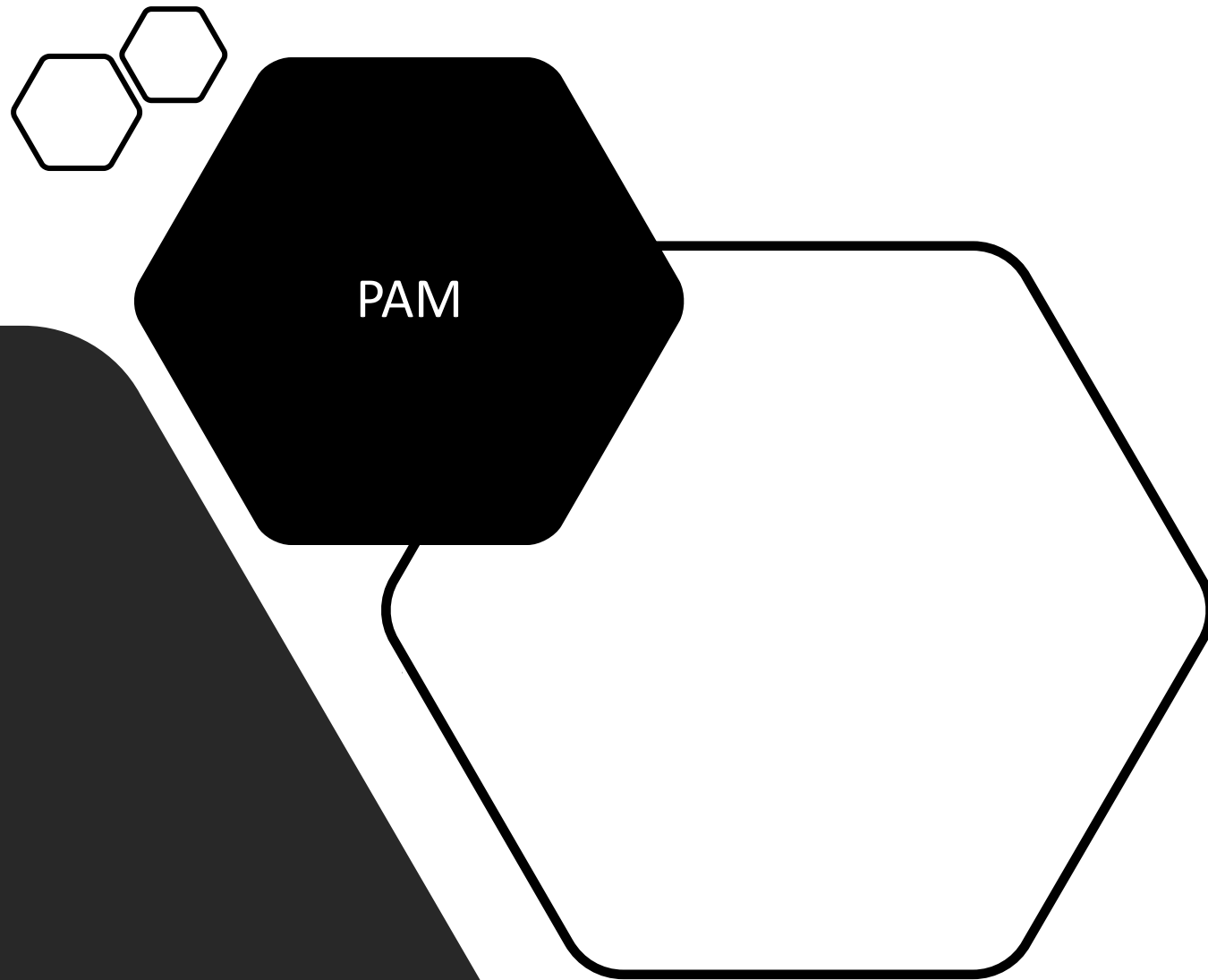
For enemy entry points





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

DEMO



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

Contact

- sami@adminize.com
- Twitter: @samilaiho
- Blog: <http://blog.win-fu.com/>
 - New on <https://4sysops.com/archives/author/sami-laiho/>
 - 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!

