



November 13-15, Oslo Spektrum

Sami Laiho

Zero Trust – Dope or Nope?

Sami Laiho

Chief Research Officer / MVP

- IT Admin since 1995 / MCT since 2001
- MVP in Windows OS since 2011
- "100 Most Influencial people in IT in Finland" – TiVi'2019 →
- Specializes in and trains:
 - Troubleshooting
 - Windows Internals
 - Security, Social Engineering, Auditing
- Trophies:
 - Best Session at Advanced Threat Summit 2020
 - Best Speaker at NIC, Oslo 2016, 2017, 2019, 2020, 2022 and 2023
 - Ignite 2018 – Session #1 and #2 (out of 1708) !
 - TechEd Europe and North America 2014 - Best session, Best speaker
 - TechEd Australia 2013 - Best session, Best speaker

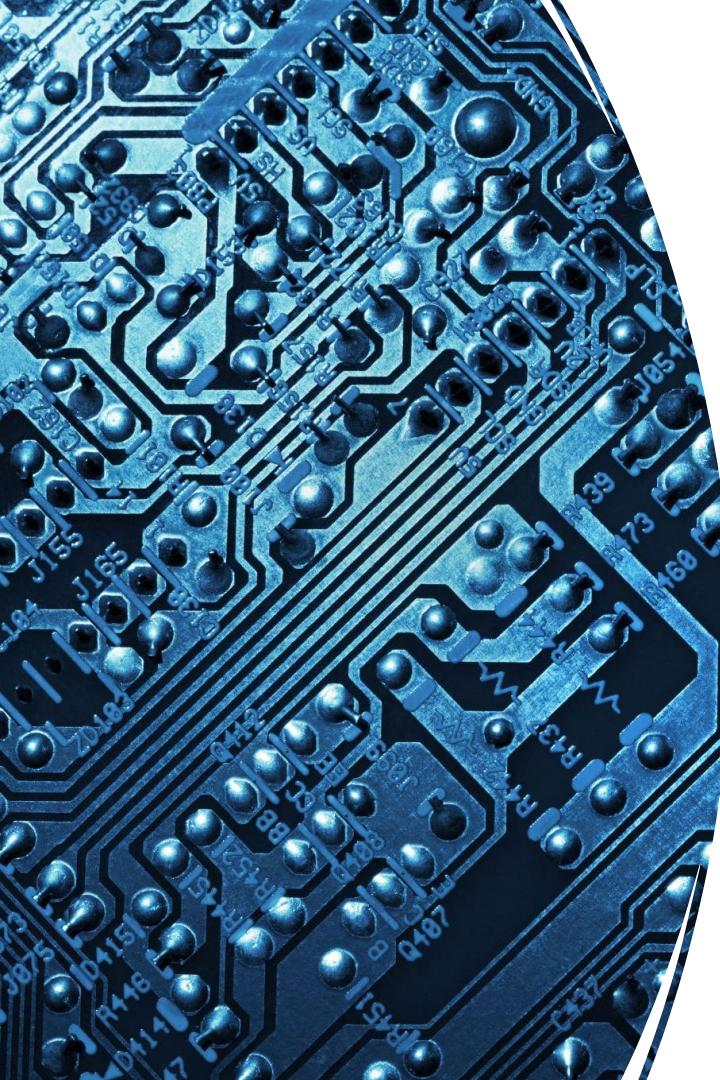




X (ex-Twitter): @samilaiho
Bluesky: @samilaiho.com
LinkedIn



Zero Trust Principles



In April 1994, the term "zero trust" was coined by Stephen Paul Marsh

- Wikipedia: There are several ways to implement all the tenets of ZT; a full ZTA solution will include elements of all three:
 - Using enhanced identity governance and policy-based access controls.
 - Using micro-segmentation
 - Using overlay networks and software-defined perimeters
- NCSC
 - Single strong source of user identity
 - User authentication
 - Machine authentication
 - Additional context, such as policy compliance and device health
 - Authorization policies to access an application
 - Access control policies within an application



ZeroTrust is the worst name ever...



Zero Trust principles



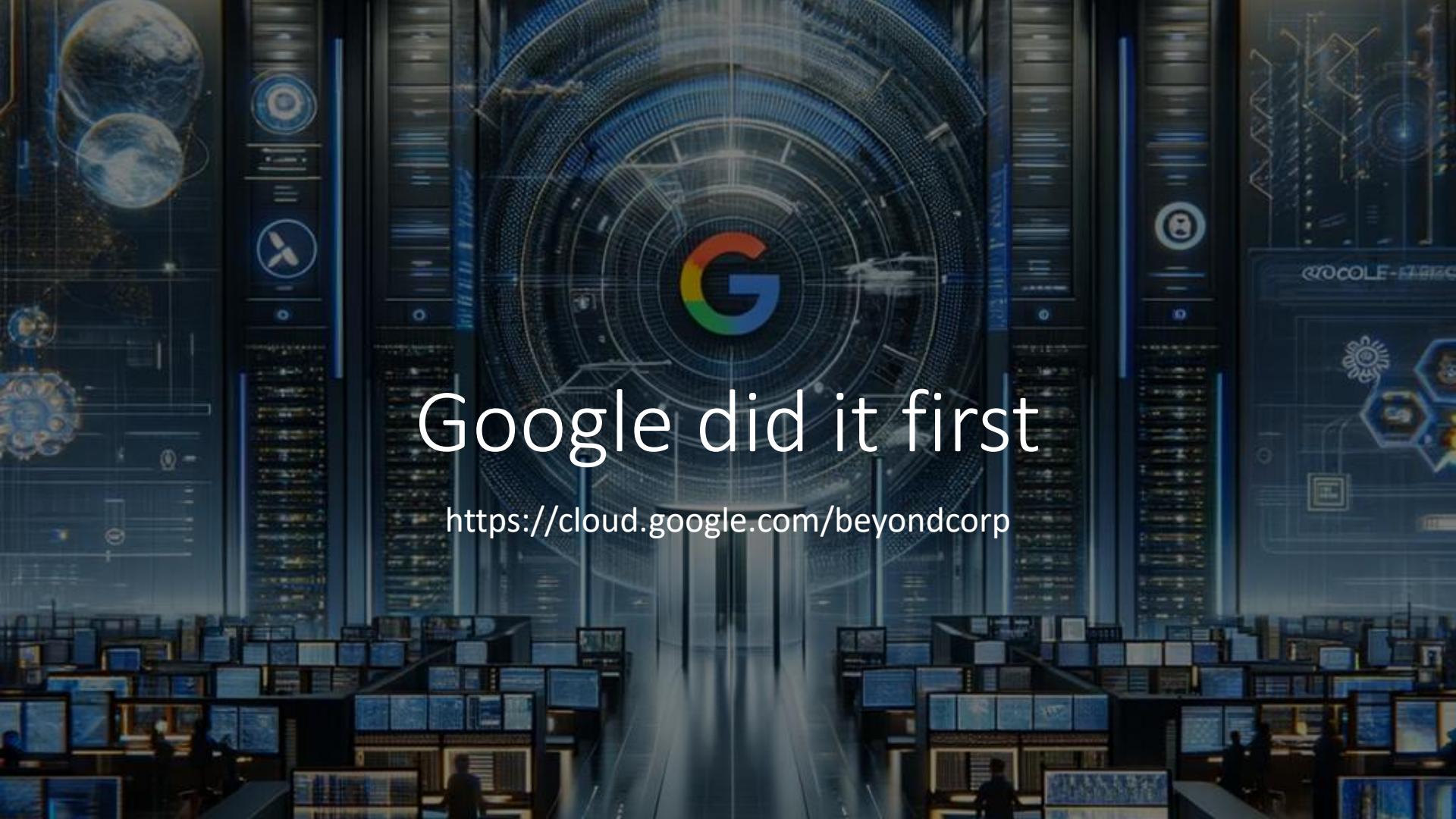
Verify explicitly



Use least privileged
access



Assume breach



Google did it first

<https://cloud.google.com/beyondcorp>



MFA

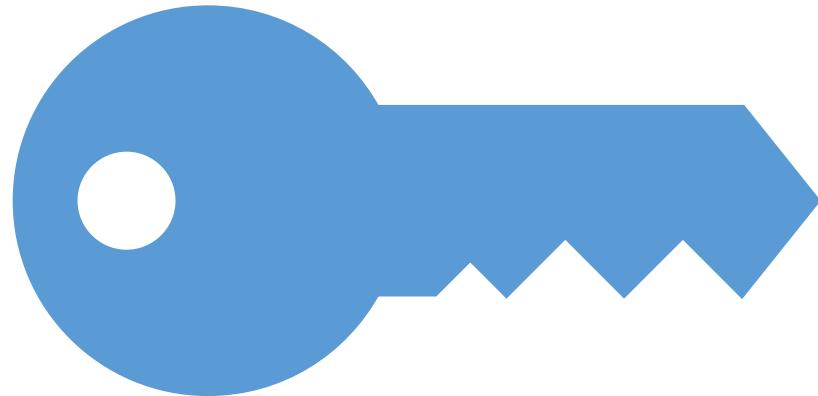
Verify Explicitly



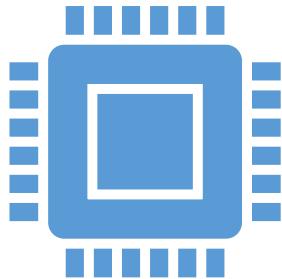
MFA

- Always verify → MFA everywhere
- Has changed the most used attack vector from Phishing → Unpatched Vulnerabilities
- Can be made accessible and easy enough to use
- Passwordless / Passkeys are the future but we can't wait

Factors



PIN-codes

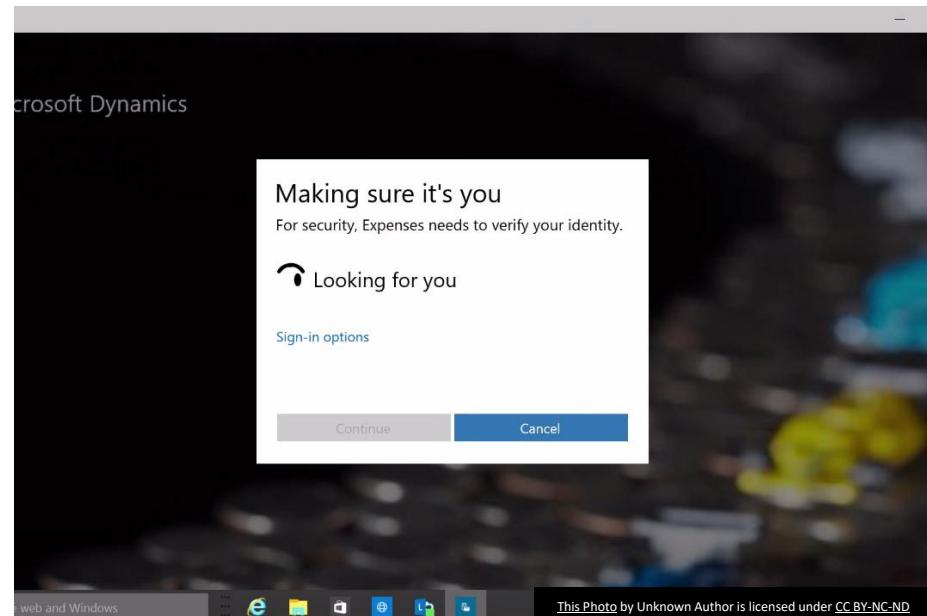


Windows with PIN is MFA!

Why a PIN is more secure
than a password



Biometrics



2 Factor Authentication!

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

Name: Token

Token Type: Live, Hedgehog

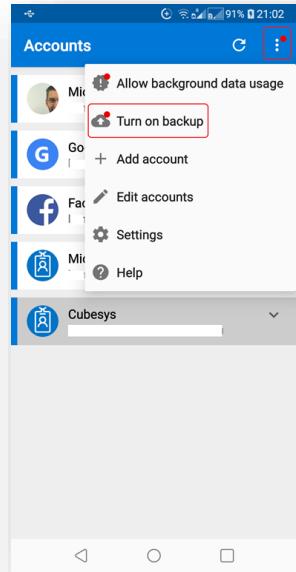
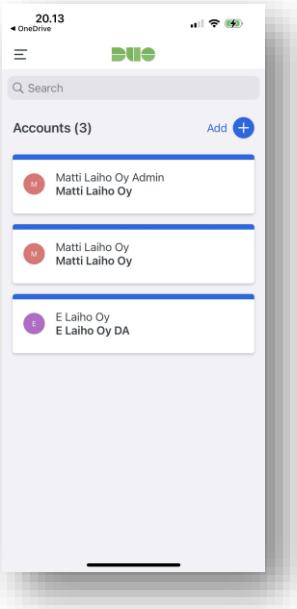
Token lifetime: 5-8 years

Tamper Protection: Yes



Authenticator Apps

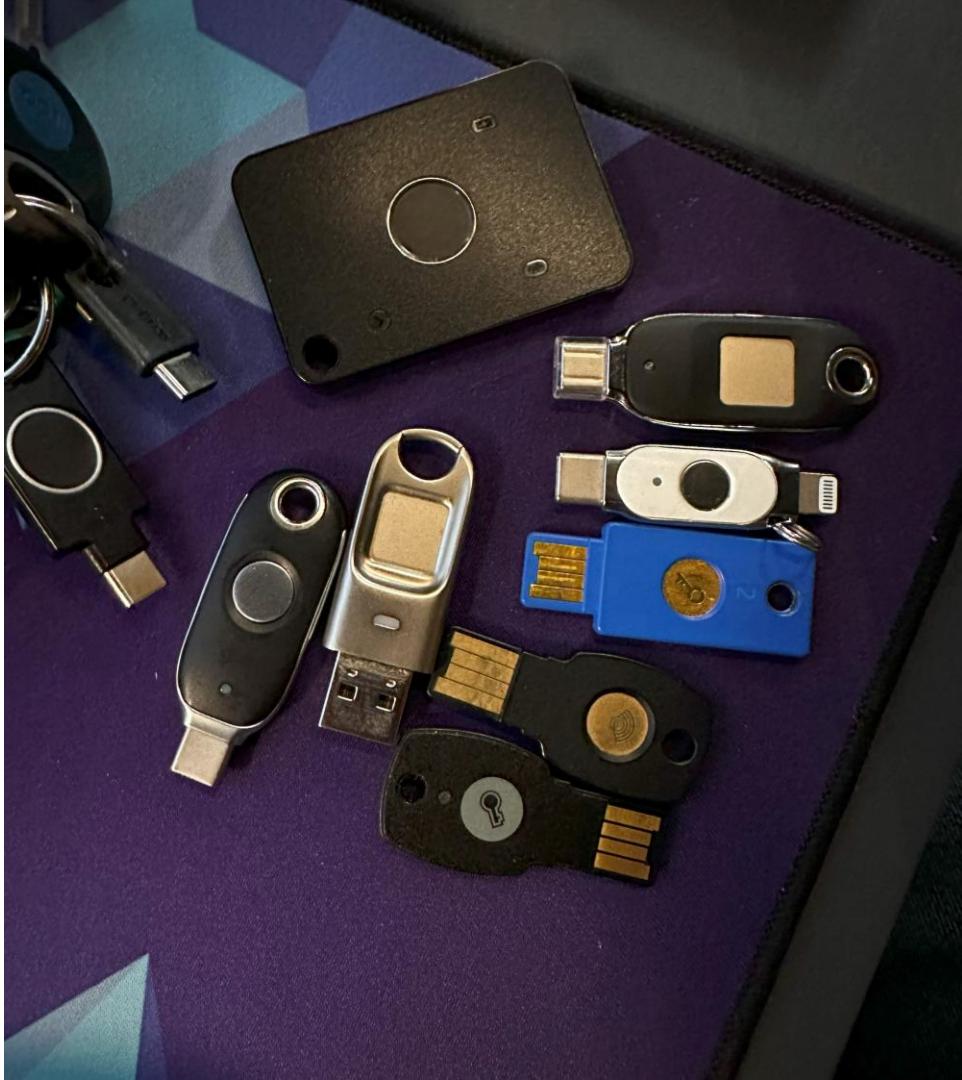
Requires a Smartphone



ADMINIZE

Physical Tokens

- Smartcards?
 - Phishing resistant MFA
 - Plug in or NFC
 - Biometrics or PIN



If Nothing Else //

RDP



182

Vendors Log into a Typical
Org each Week¹

76%

of Cloud Accounts Sold on
Dark Web = RDP²

80%

of Ransomware Attacks
Exploit RDP³



Ransomware Deployment Protocol

*“The two connections that are available with Terminal Services in Remote Administration mode are intended for administrative purposes only. You can use these connections for **emergency administration**”*

The statement is from the chapter titled “Terminal Services in Remote Administration Mode” in the Microsoft Windows 2000 Server Resource Kit1. The chapter number is 14 and the page number is 14-2.



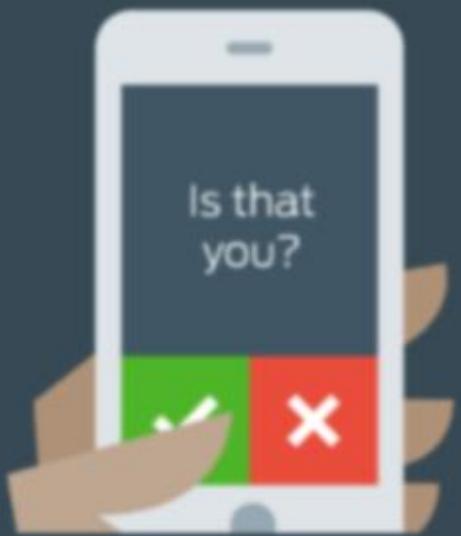
PASSWORD

PROOF

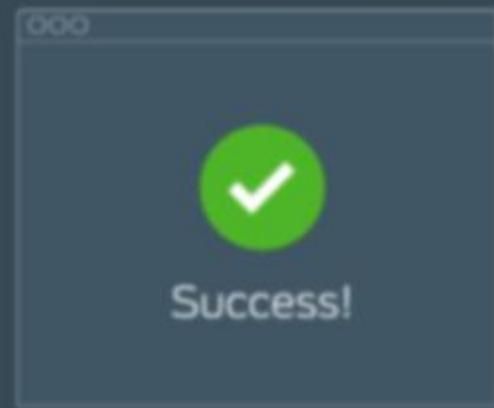
ACCESS



+



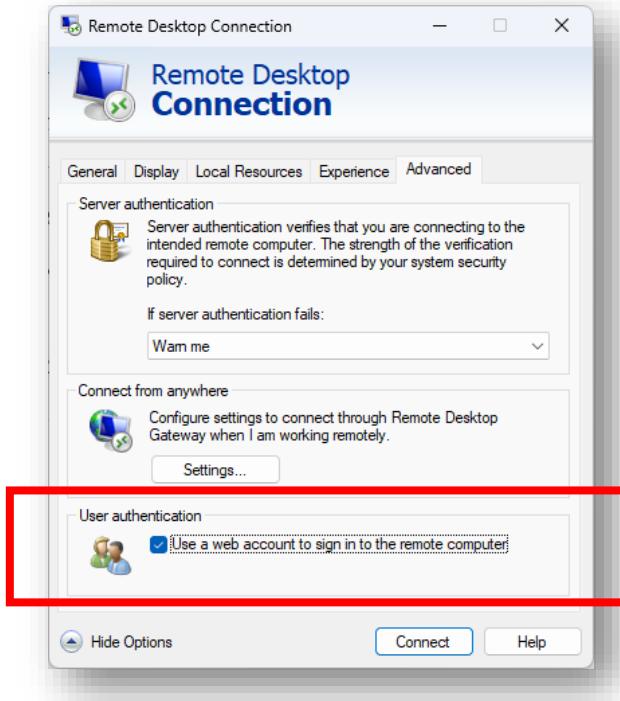
=



“If you RDP, you MFA”



Yubikeys

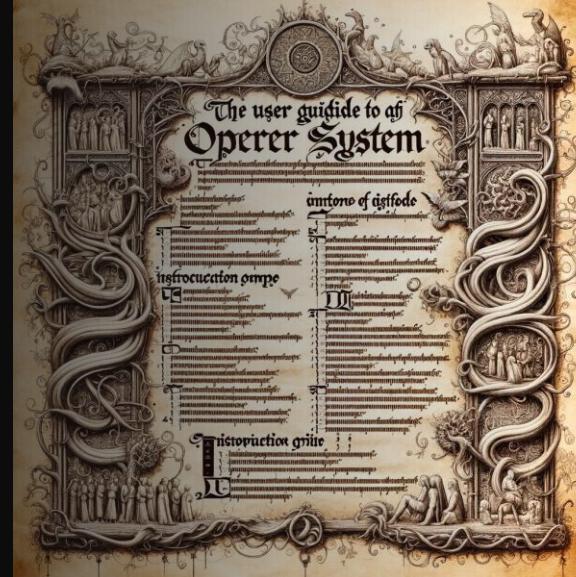


<https://swjm.blog/the-complete-guide-to-rdp-with-yubikeys-fido2-cba-1bfc50f39b43>



Least Privilege

NT 3.1 Security Guide



States that local admins have full access to the computer. FULL STOP.

Administrators Properties



General



Administrators

Description:

Administrators have complete and unrestricted access to the computer/domain

Critical risks of Administrative Rights



The risk increases dramatically from loss of one user's assets, to losing the whole company operations.



It allows the malicious tools to operate on Windows deeper and at hardware levels.



It prevents the company from controlling the computer settings and data, therefore managing risk.



It allows for identity theft.



Shadow IT is rampant as the end user controls the device



The Principle of Least Privilege is a Core Component of Zero Trust

Why Shouldn't Users Want to Have Administrative Rights?

Performance of systems is improved without local administrator rights

Installation of various software causes slowdowns and reliability issues.

SSD lifespan increases

Decreases the need for reinstallations.

Due to more reliable systems productivity is increased

The attack surface of malware is greatly reduced and helps limit propagation

Because it decreases the amount of money needed in extra security solutions

Because it mitigates more vulnerabilities than patching

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”

ADMINIZE
ADMINIZE

Admin Rights are not Human Rights

<https://www.zazzle.com/store/adminize/products>



Stop endusers from hurting their computers

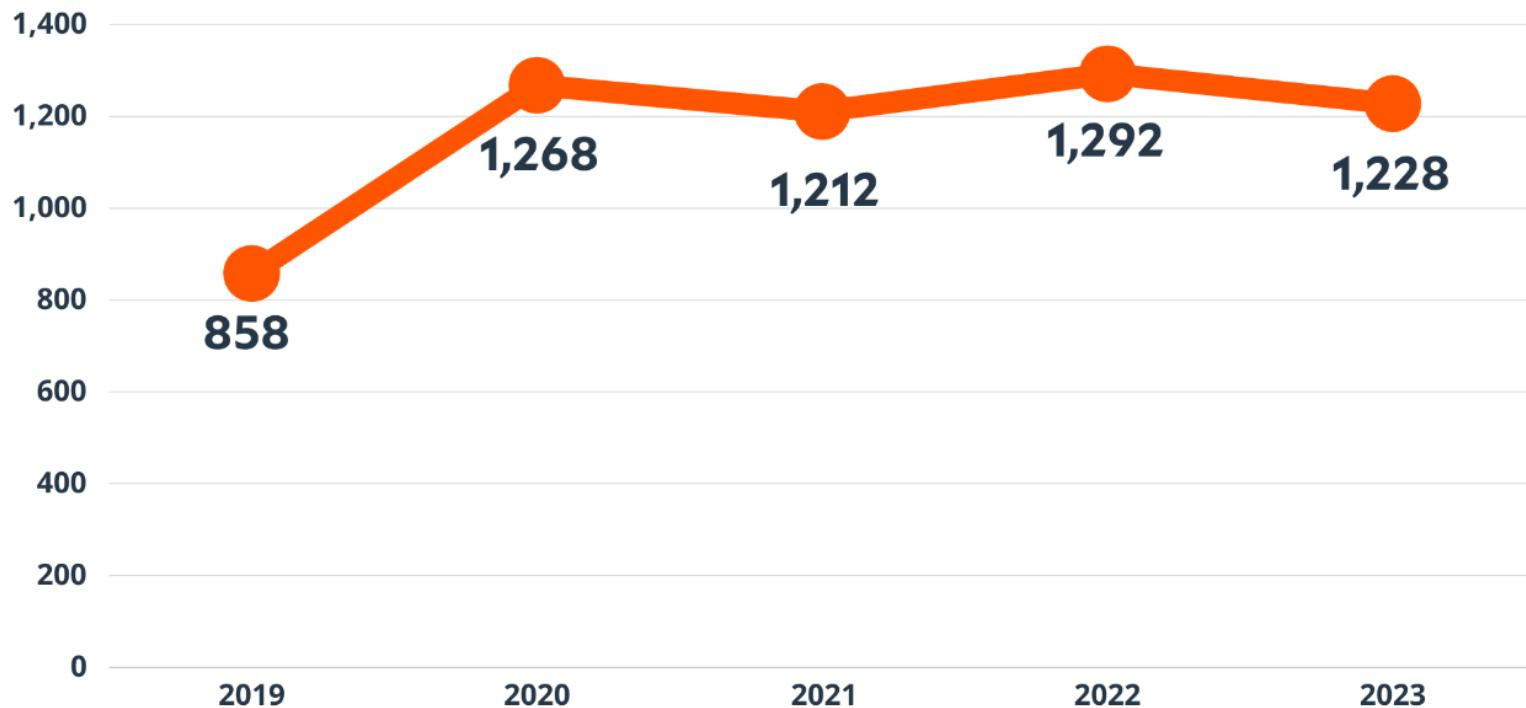
Jannik [REDACTED]

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

A scene from the TV show 'The Office' set in a busy office environment. In the foreground, two male employees are playing ping pong on a desk. One is wearing a white shirt and tie, and the other is wearing a blue shirt and tie. In the background, several other employees are working at their desks or participating in a ping pong game. The office is filled with cubicles, computer monitors displaying code, and various office equipment. A whiteboard in the background is covered with notes and diagrams.

US Customer: 65% less
reinstallations

Total Number of Microsoft Vulnerabilities (2019-2023)

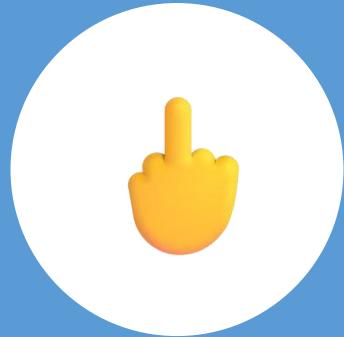


A man with brown hair and a mustache, wearing a light blue button-down shirt, is kneeling in front of an open computer case. He is holding a large, metallic adjustable wrench in his right hand, which is raised towards the top of the case. His left hand rests on the side panel of the case. He has a serious, focused expression on his face. The background shows a workshop or office environment with other computer equipment and a lamp. The overall lighting is dramatic, with strong highlights on the wrench and the man's face.

How do we fix this?

You Need a PAM!

Privileged Access Management



How I've lived without
admin rights for 22 years?

Microsegmentation

Software Defined Networking

Micro-Segmentation



Controlling flow between
every node or every app



Controlling “East-West”,
instead of “North-South”

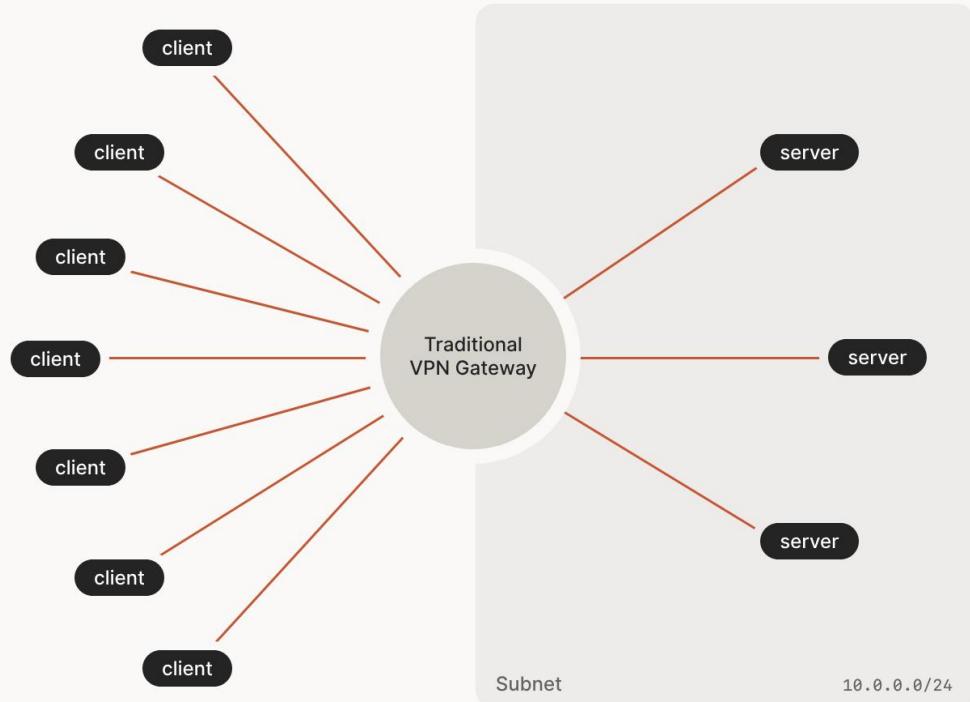


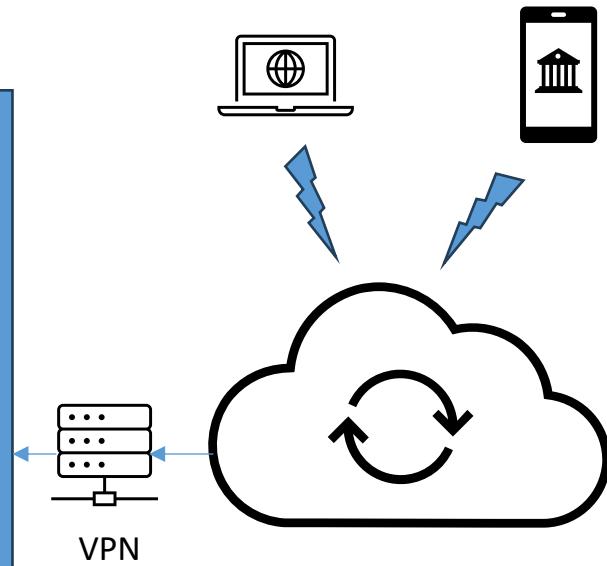
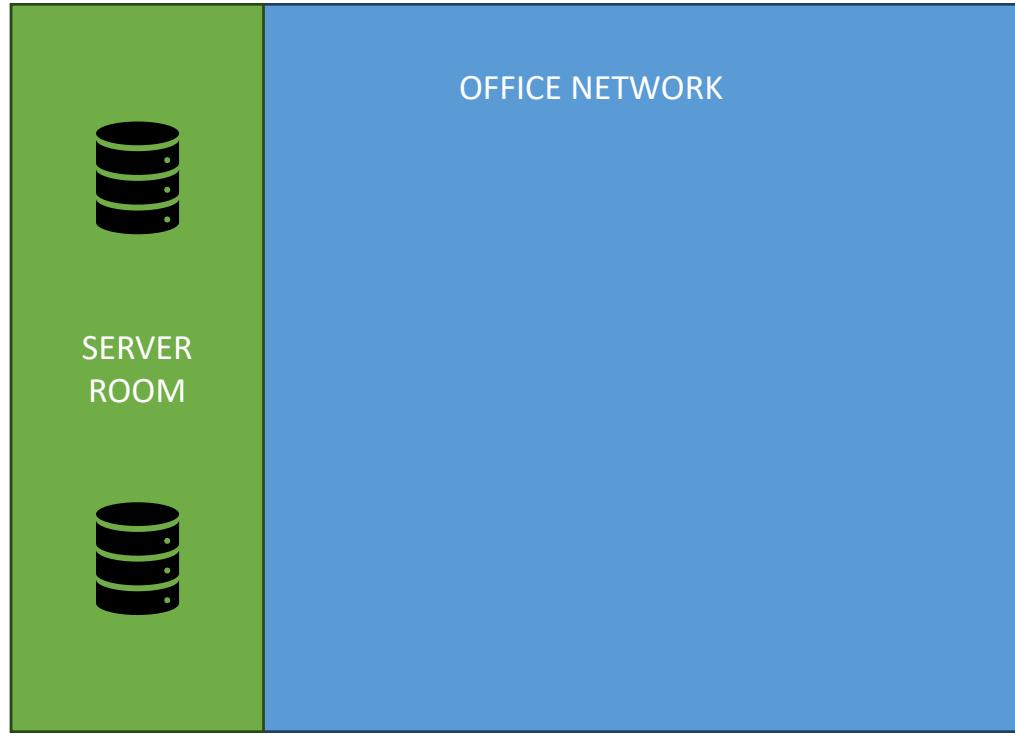
What are we Being Offered?

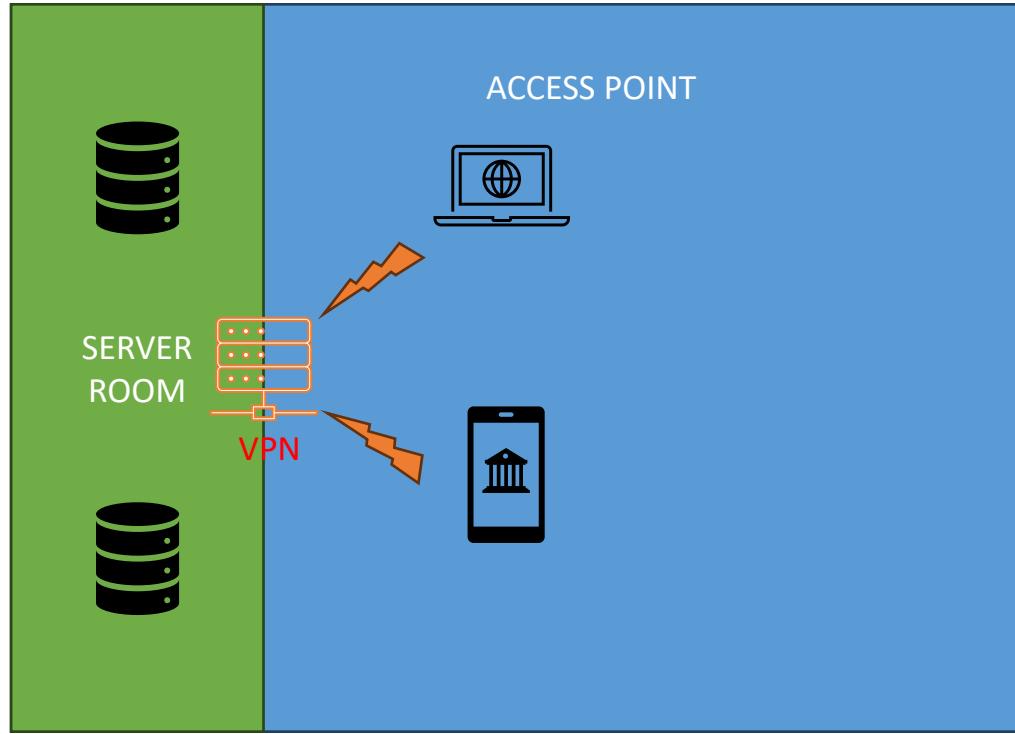
Move the VPN-
border



Traditional VPN







The screenshot shows the 'New Inbound Rule Wizard' interface across three steps:

- Step 1: Users**

Specify the users that are allowed to make the connection specified by this rule.

Steps:

 - Rule Type
 - Program
 - Protocol and Ports
 - Scope
 - Action
 - Users**
 - Computers
 - Profile
 - Name

Authorized users
Only allow connections from these users
[Empty list box]

Exceptions
Skip this rule for connections from these users
[Empty list box]

Note: user identities can only be verified if an authentication method that carries user identity is used.
- Step 2: Computers**

Specify the computers that are allowed to make the connection specified by this rule.

Steps:

 - Rule Type
 - Program
 - Protocol and Ports
 - Scope
 - Action
 - Users
 - Computers**
 - Profile
 - Name

Authorized computers
Only allow connections from these computers:
[Empty list box]

Exceptions
Skip this rule for connections from these computers:
[Empty list box]

Note: computer identities can only be verified if an authentication method that carries computer identity is used.
- Step 3: Action**

What action should be taken when a connection matches the conditions specified in the rule?

Allow the connection
This includes connections that are protected with IPsec as well as those are not.

Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

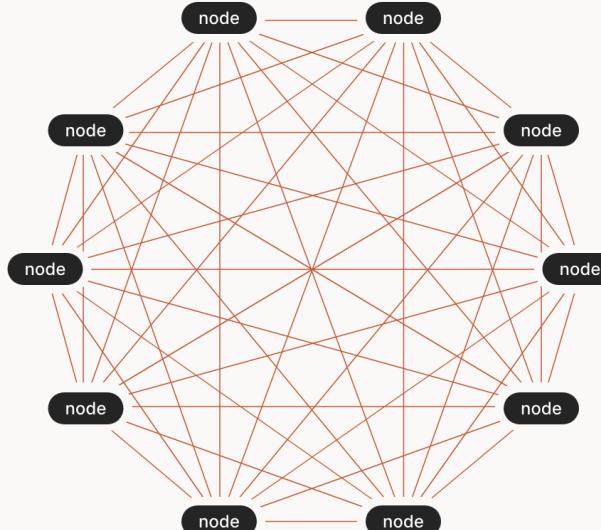
Block the connection

Firewall and IPsec together

- Identity is the new Black

WireGuard

MESH



$n(n-1) = 90$ WireGuard endpoints (for 10 connections)

A vibrant, multi-colored photograph of a group of nine children of various ages gathered around a long wooden table in a room decorated with video game posters on the wall. They are all focused on playing video games on multiple computer monitors and keyboards. The room is filled with colorful lighting from the screens and ambient light, creating a lively and energetic atmosphere.

Zero Trust with my Children

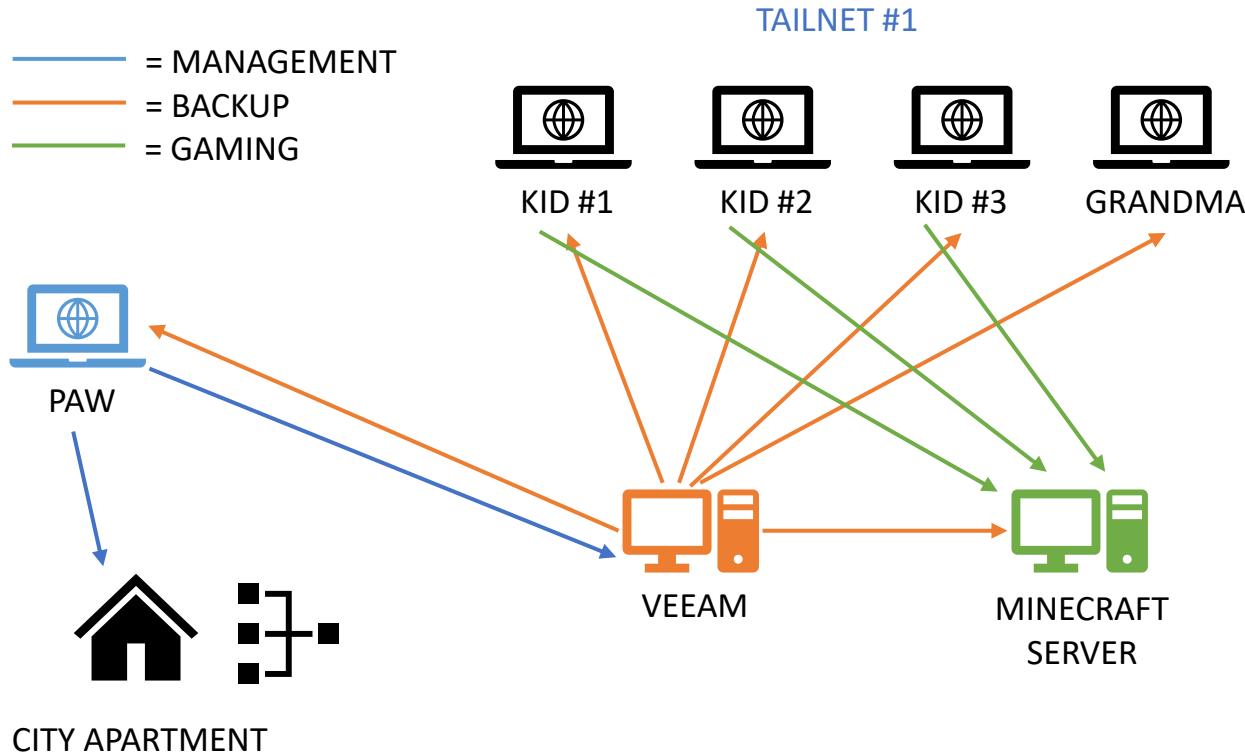
Just proves how bad the name is...



What has an
SLA of 3.67s ?



— = MANAGEMENT
— = BACKUP
— = GAMING



— = TRUE ZERO TRUST

TAILNET #2



WIFE

In ZeroTrust, don't
let Perfect be the
Enemy of Good

Thank you!
Remember the Evals



Contact

- sami@adminize.com
- Twitter: @samilaiho
- BlueSky: @samilaiho.com
- Free newsletter: <http://eepurl.com/F-Goj>
- Find me on LinkedIn – Please!
- My trainings:
 - Corellia (FIN)
 - ETC.at (ENG)
- <https://win-fu.com/dojo/>
 - Free for one month!!
 - Promo Code: TRIAL2023

