

**Identity Security** Track

MS Zero Trust security model -Silver bullet or just another chase for the unicorn?

Dr. Nestori Syynimaa (Secureworks)



#### Secureworks

### MS Zero Trust security model

### Silver bullet or just another chase for the unicorn?

@DrAzureAD

https://linkedin.com/in/nestori

#### Who?

Dr. Nestori Syynimaa

Senior Principal Security Researcher @Secureworks

Developer of AADInternals toolkit

Microsoft MVPx2 (Identity and Access, Intune)

Microsoft MVSR

#### Contact

- nsyynimaa@secureworks.com
- Twitter: <a>@DrAzureAD</a>
- <a href="https://linkedin.com/in/nestori">https://linkedin.com/in/nestori</a>
- https://o365blog.com













#### **Contents**

- Introduction to Zero Trust
- Zero Trust in Theory
- Zero Trust in Practice

## Introduction to Zero Trust

#### **Zero Trust principles**

Verify explicitly

Use least privileged access

Assume breach

Always authenticate and authorize based on all available data points Limit user access with just-in-time and just-enough-access (JIT/JEA)

Minimize blast radius and segment access

#### **Zero Trust defence areas**

Identities	Endpoints	Apps
Strong authentication	Ensure compliance and health	Gate access based on real-time analytics
Data	Infrastructure	Network
Move to data-driven protection	Use telemetry to detect attacks	Do not trust internal network

# Zero Trust in Theory

#### Verify explicitly

Identities **Endpoints** Apps Use strong Use only compliant Limit access to apps and healthy devices authentication Network Data Encrypt data Ip address Geo location

Secureworks

#### Use least privileged access

Identities	Endpoints	Apps
Limit # of admin users User PIM	Remove admin rights	Limit creation of apps Limit access to apps
Data	Infrastructure	Network
Limit access to data	Limit access to infrastructure	Limit access to network

#### **Assume breach**

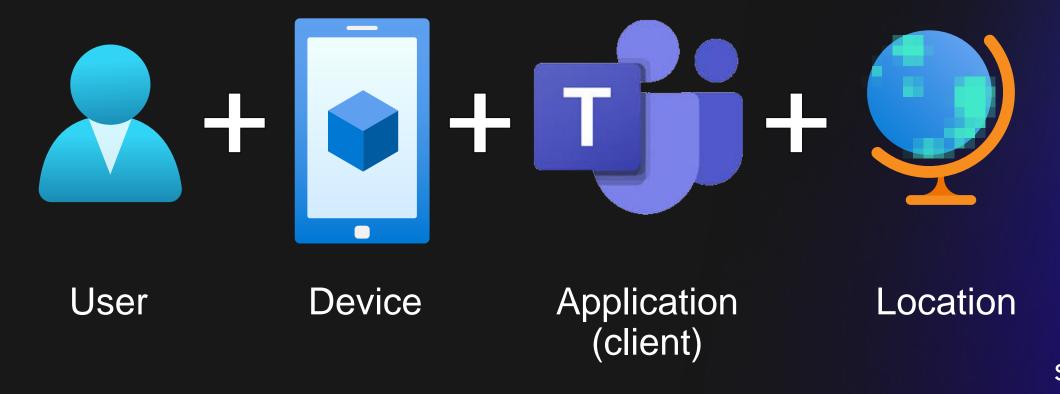
Identities	Endpoints	Apps
Use strong auth Review permissions	Manage all devices	Limit and review app permissions
Data	Infrastructure	Network
Encrypt the data	Monitor, detect, and response automatically	Do not give access based on location

Secureworks

## Zero Trust in Practice

#### **Conditional Access**

- Grant / block access based on conditions
- Outside signals:



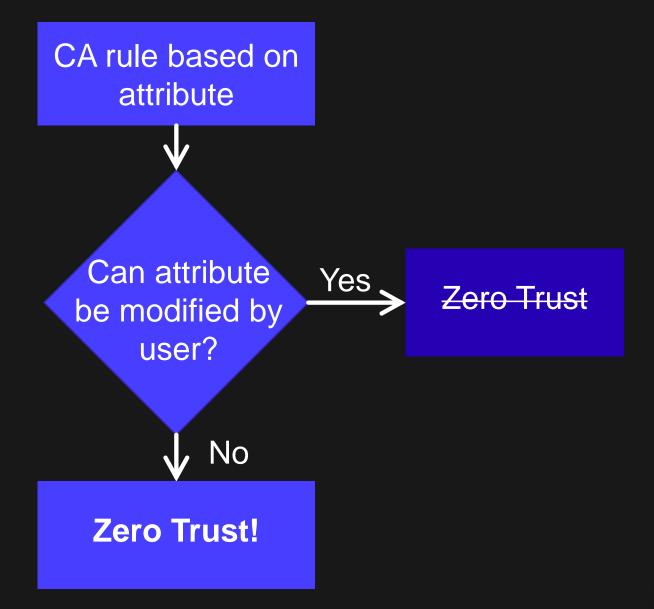
#### Ten Immutable Laws of Security 1/2

- 1. If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.
- 2. If a bad guy can alter the operating system on your computer, it's not your computer anymore.
- 3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
- 4. If you allow a bad guy to run active content in your website, it's not your website anymore.
- 5. Weak passwords trump strong security.

#### Ten Immutable Laws of Security 2/2

- 6. A computer is only as secure as the administrator is trustworthy.
- 7. Encrypted data is only as secure as its decryption key.
- 8. An out-of-date antimalware scanner is only marginally better than no scanner at all.
- 9. Absolute anonymity isn't practically achievable, online or offline.
- 10. Technology is not a panacea.

#### **Zero Trust flowchart for Conditional Access**



#### **Identities**

- Use strong authentication:
  - MFA
  - Passwordless authentication (WH4B, FIDO, Authenticator)
- Use Privileged Identity Management (PIM) for admins
- Protect hybrid environment components (Azure AD Connect, ADFS)
- Allow only admins to add users
- Allow only admins or users to invite guests
- Allow Global Administrator access only from Privileged Access Workstations (PAW)
- Allow DirSync account access only from named location(s)

#### **Devices**

- Allow access only from trusted/compliant devices
- Allow only (named) admins to register/join devices
- Use Intune/MDM
- Use property-based rules to limit access
  - PAWs
  - Specific apps
- CA rules based on Device platform do not work!
- CA rules based on OS & OS version do not work!

#### **Applications**

- Block sign-in to unused applications
- Allow only admins to register applications
- Assign applications to specific users or groups
- Always review requested access!
- CA rules based on apps do not work!
  - MS please, we need rules based on used API!

#### Locations

- Treat all locations untrusted
- Define locations for
  - PAWs
  - Azure AD Connect (DirSync) servers

### Thank you!



JOIN THE CLOUD IDENTITY LOUNGE AT 8:00 PM (CEST)

Roundtable discussion and Q&A on experiences from the field, current trends and more! Interactive session to bring your questions and use the opportunity to meet the speakers or exchange with members of the community!

