Trust, No Trust or Zero Trust - Myth Demystifying

Vandana Verma Sehgal

@Infosecvandana

About Me

Vandana Verma Sehgal

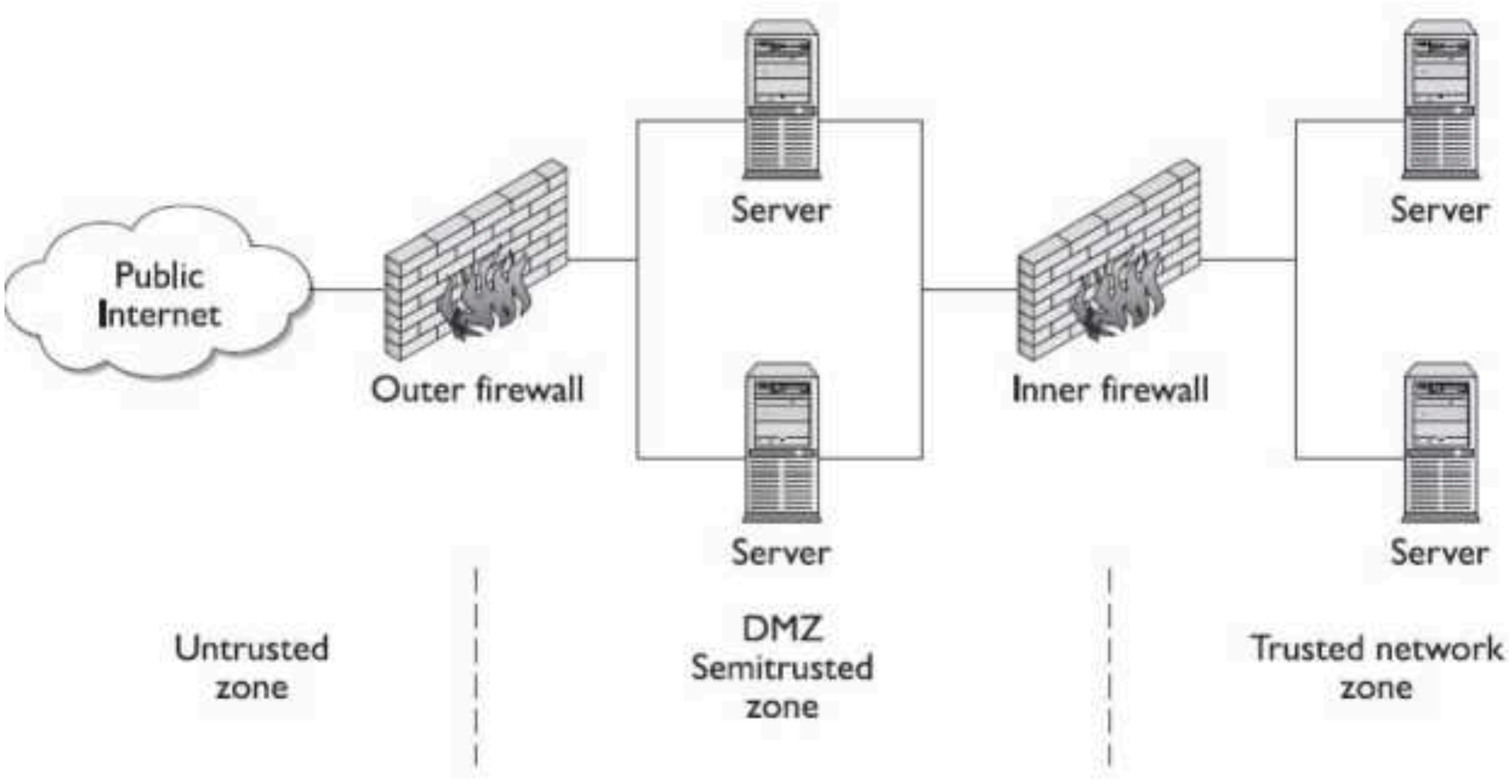
- OWASP Global Board of Directors
- President of Infosec Girls
- Award-winning Cybersecurity Professional
- Keynote Speaker, Inclusion Advocate
- Member of Review Board at Grace Hopper, BSides Conferences, Global AppSec, etc.

OWASP
Open Web Application Security Project

InfosecGirls

Traditional Security Model

Conventional Security Model



http://www.vce-download.net/study-guide/comptia-securityplus-2.3.4-security-topologies-tunneling.html

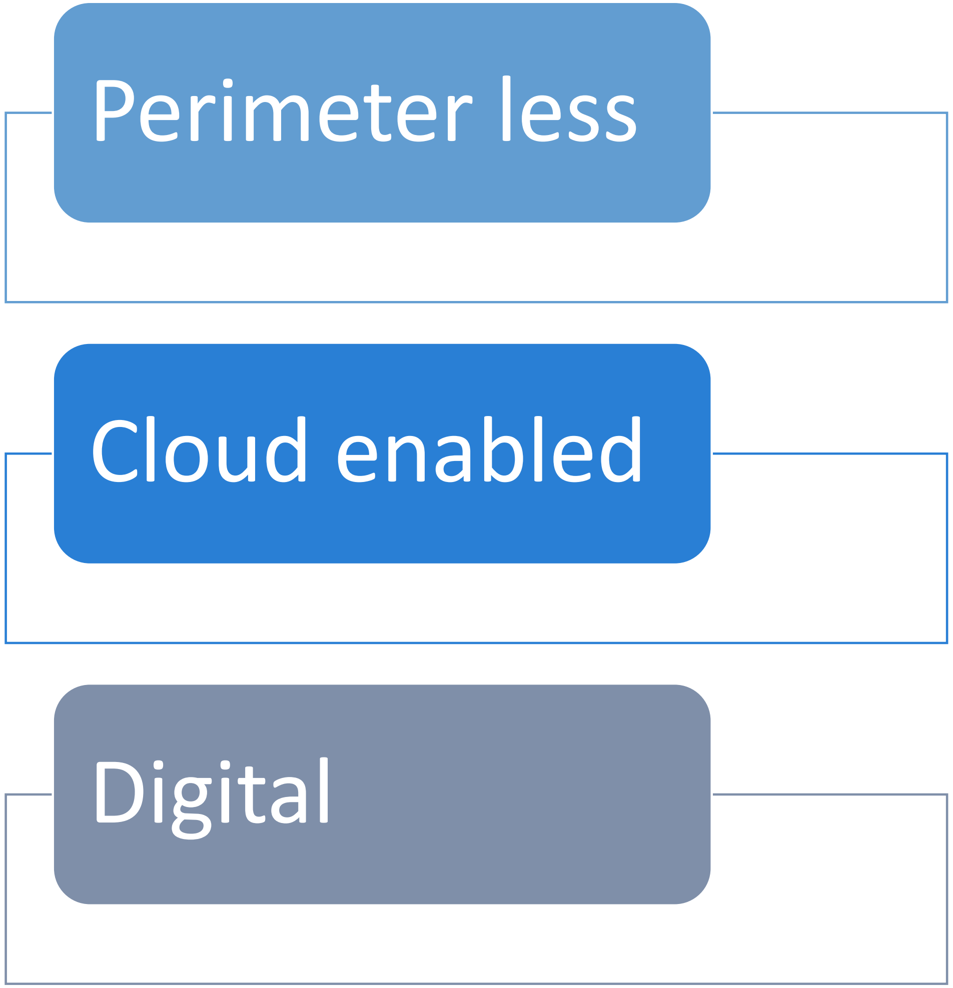
Does the Traditional Security Model really work?

TRUST INSIDERS; WHAT ABOUT INSIDER THREAT?

ONLY ONE DOOR; IS IT PRACTICAL?

PROTECT EVERYTHING FROM OUTSIDERS, WHAT ABOUT COST OF PROTECTING NON-CRITICAL INFORMATION?

Current landscape



Perimeter less

Cloud enabled

Digital

Breach statistics - Past years

$6 trillion

Cybercrime cost by 2021,
Src:- Cybersecurity Ventures

$3.62 million

Average cost of data breach
Src:- Ponemon institute
(sponsored by IBM)

80% Data breaches

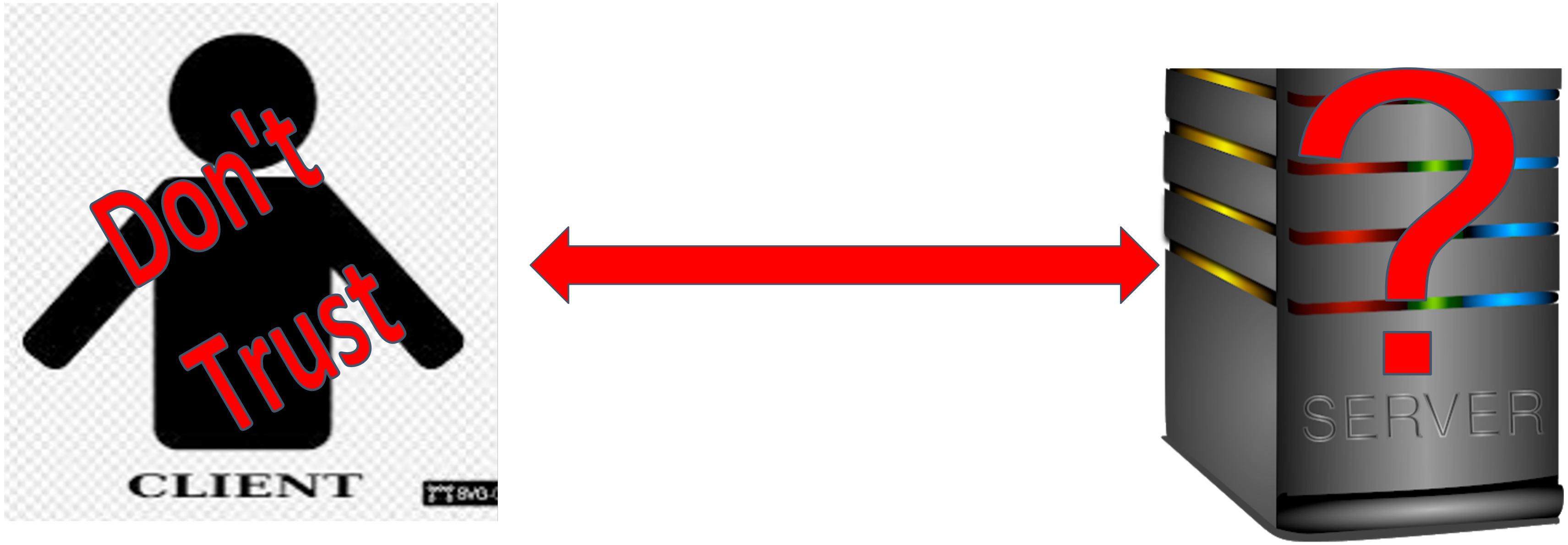
Privileged access abuse
Src:- Forrester estimates

Can we trust?............

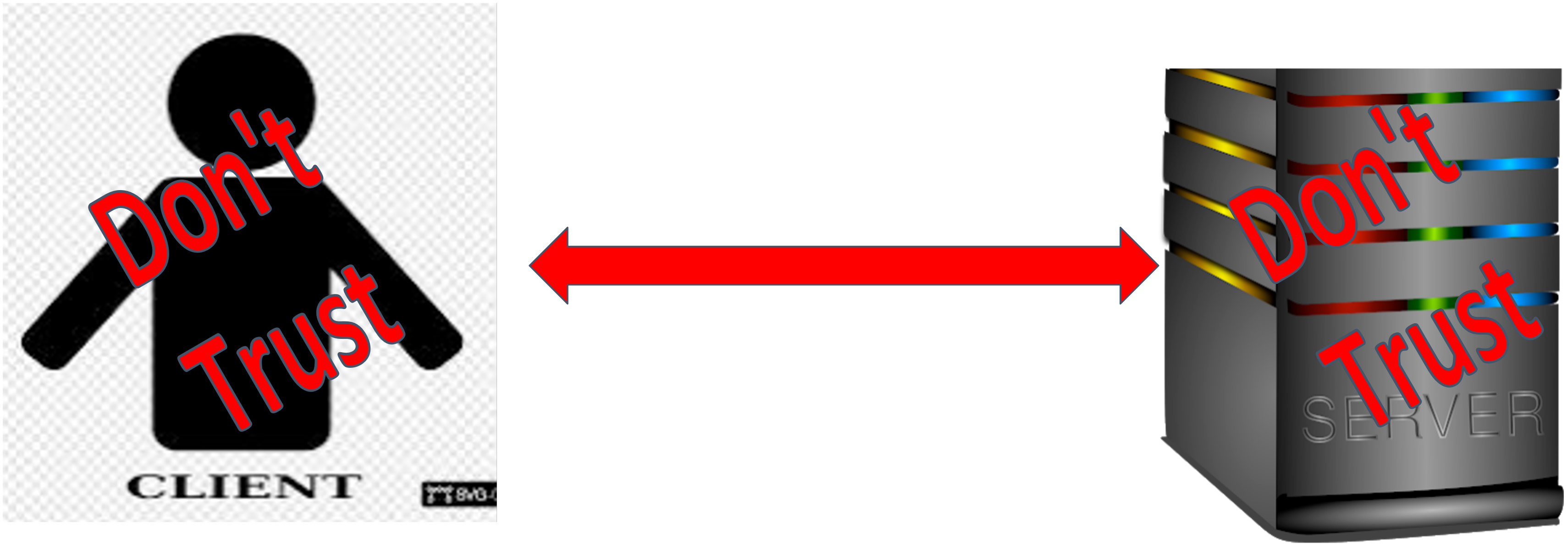
Can we trust?............

Can we trust?............

Server

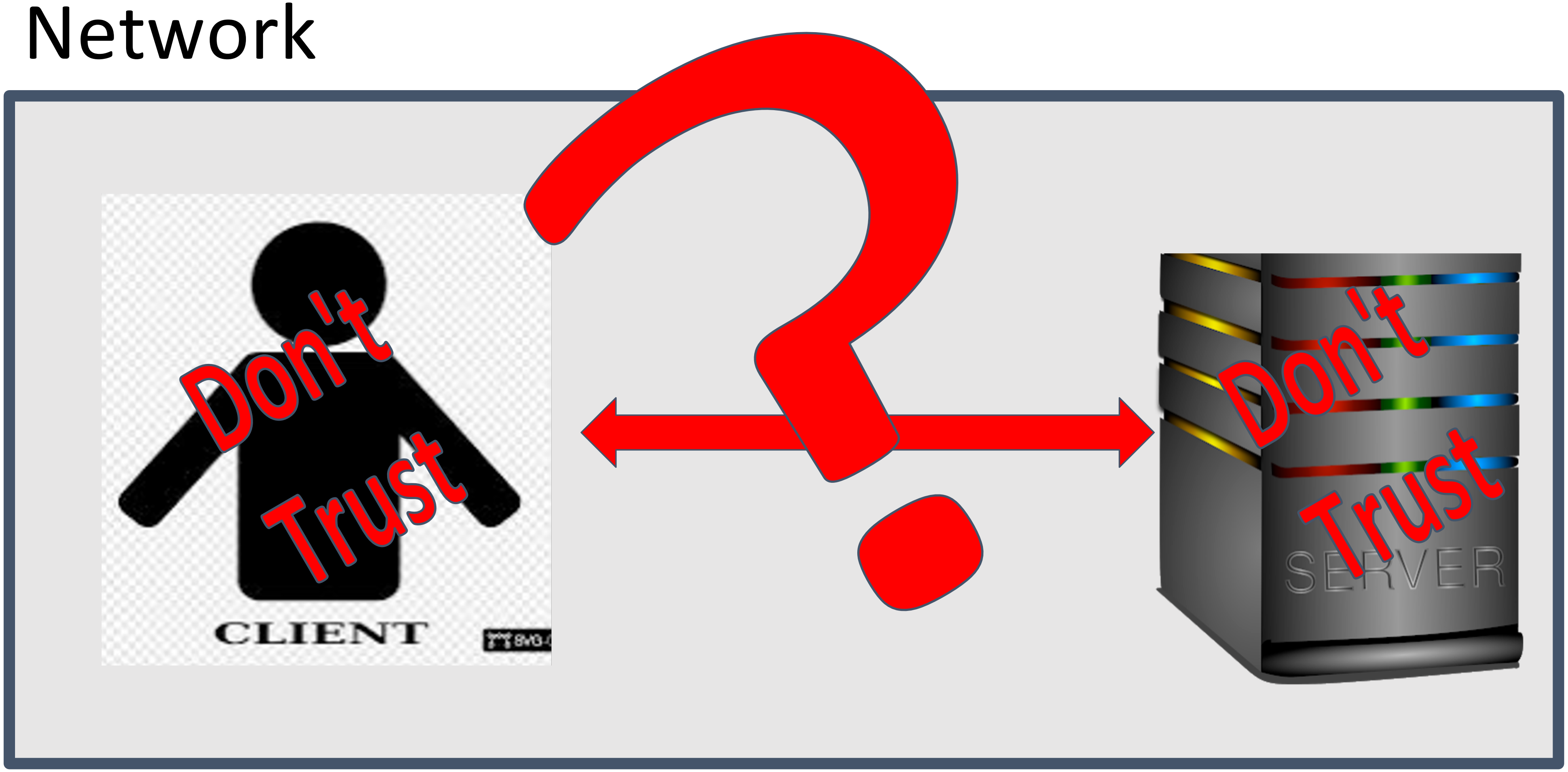


Can we trust?............



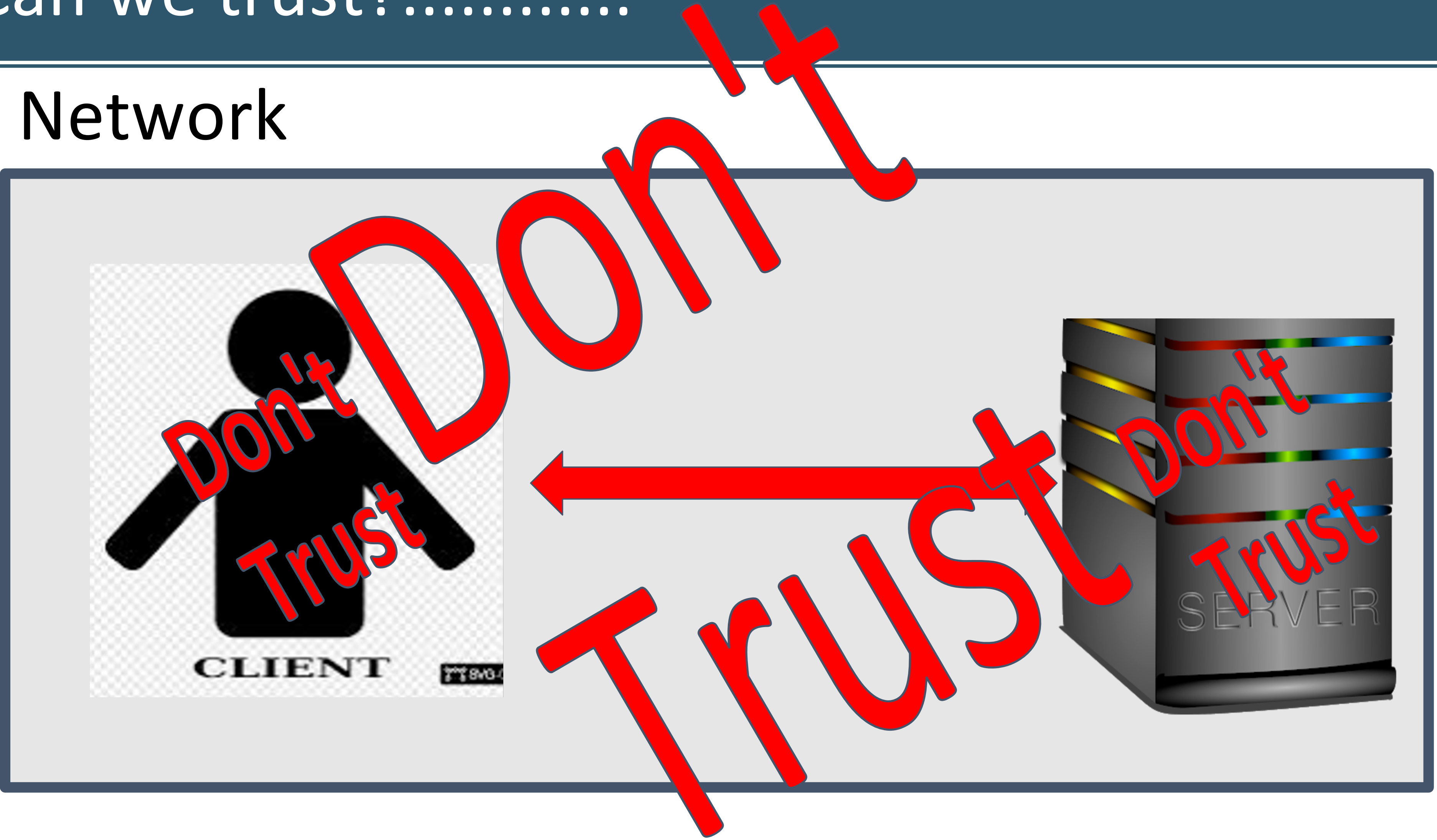
Can we trust?............

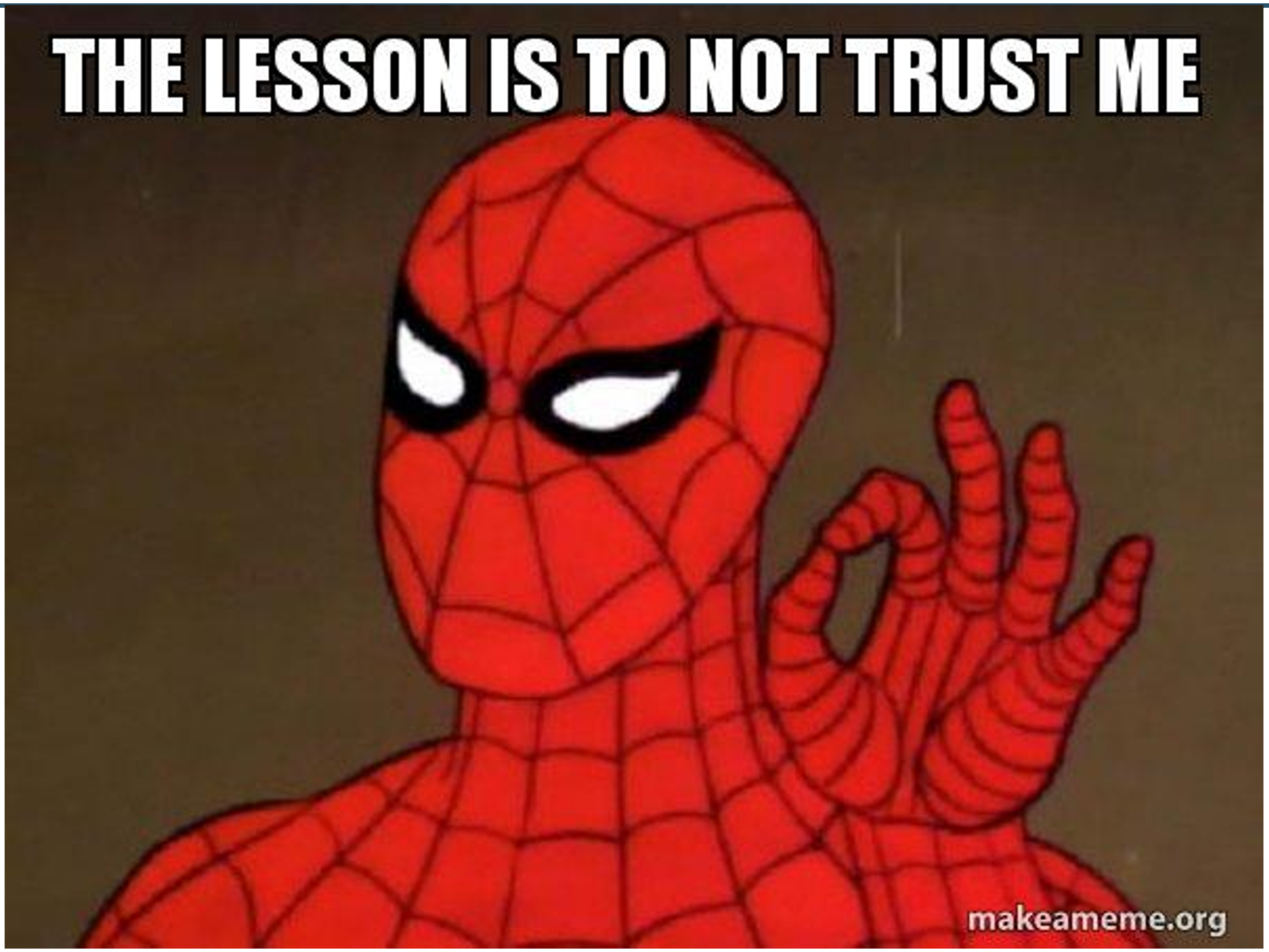
Network



Can we trust?............

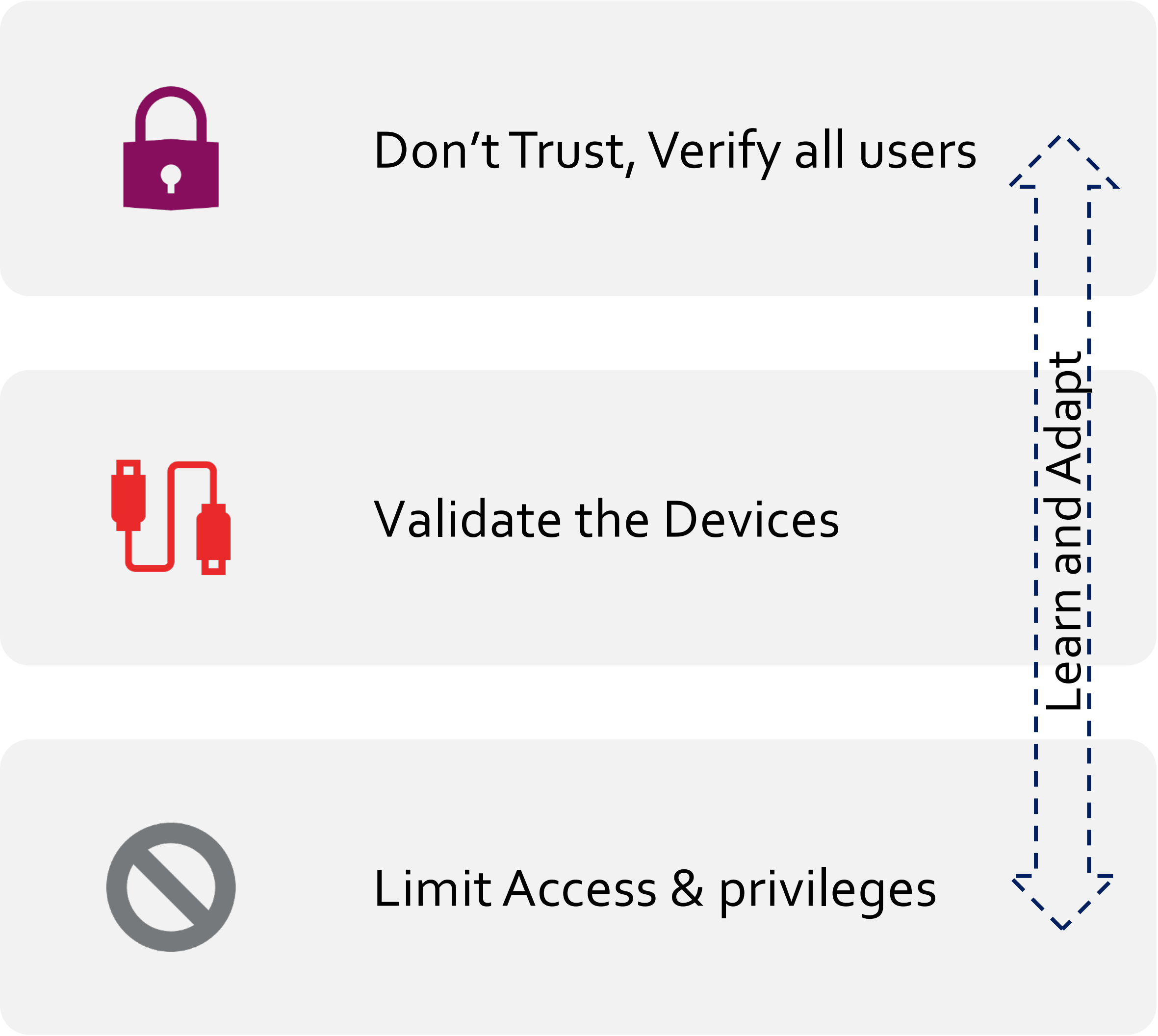
Network




THE LESSON IS TO NOT TRUST ME
makeameme.org

I DON'T ALWAYS TRUST
BUT WHEN I TRUST, I VERIFY
memegenerator.net

Zero Trust



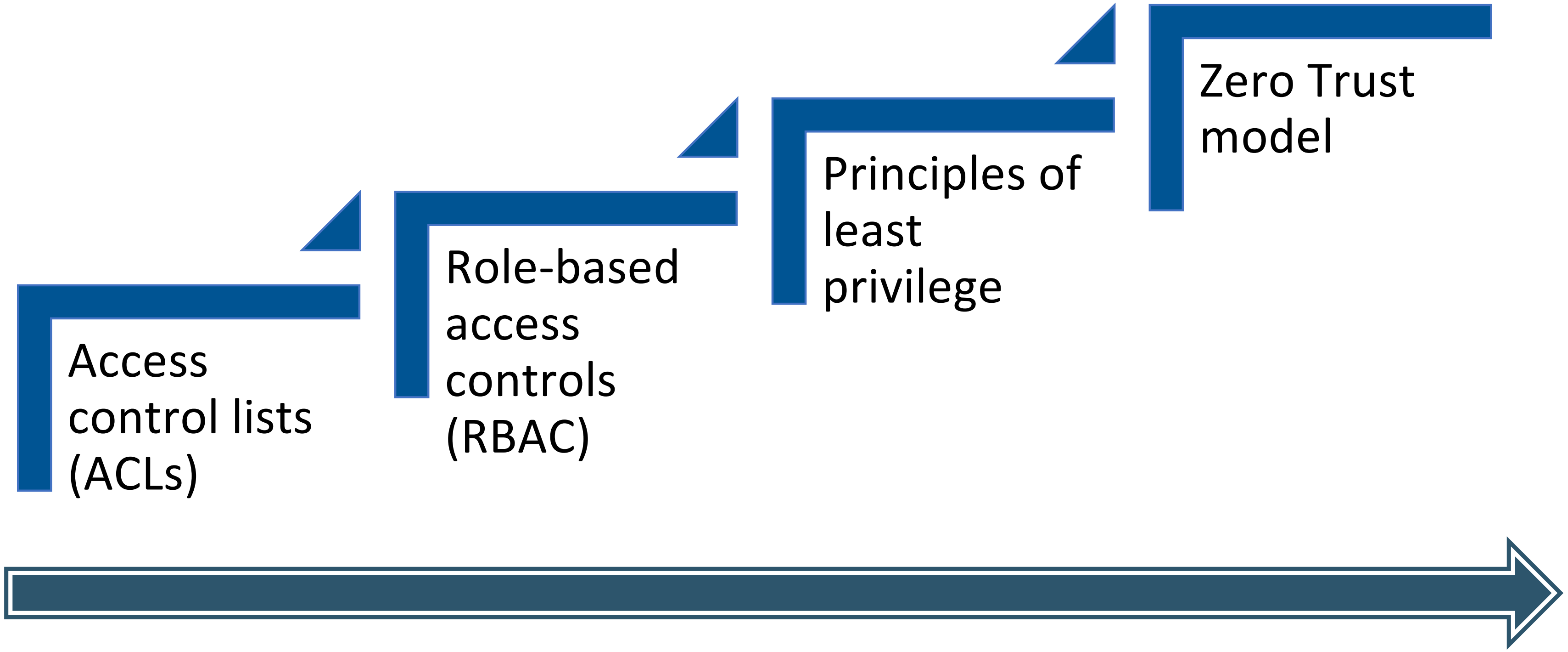
Don’t Trust, Verify all users

Validate the Devices

Limit Access & privileges

Learn and Adapt

Advancements in Security Model

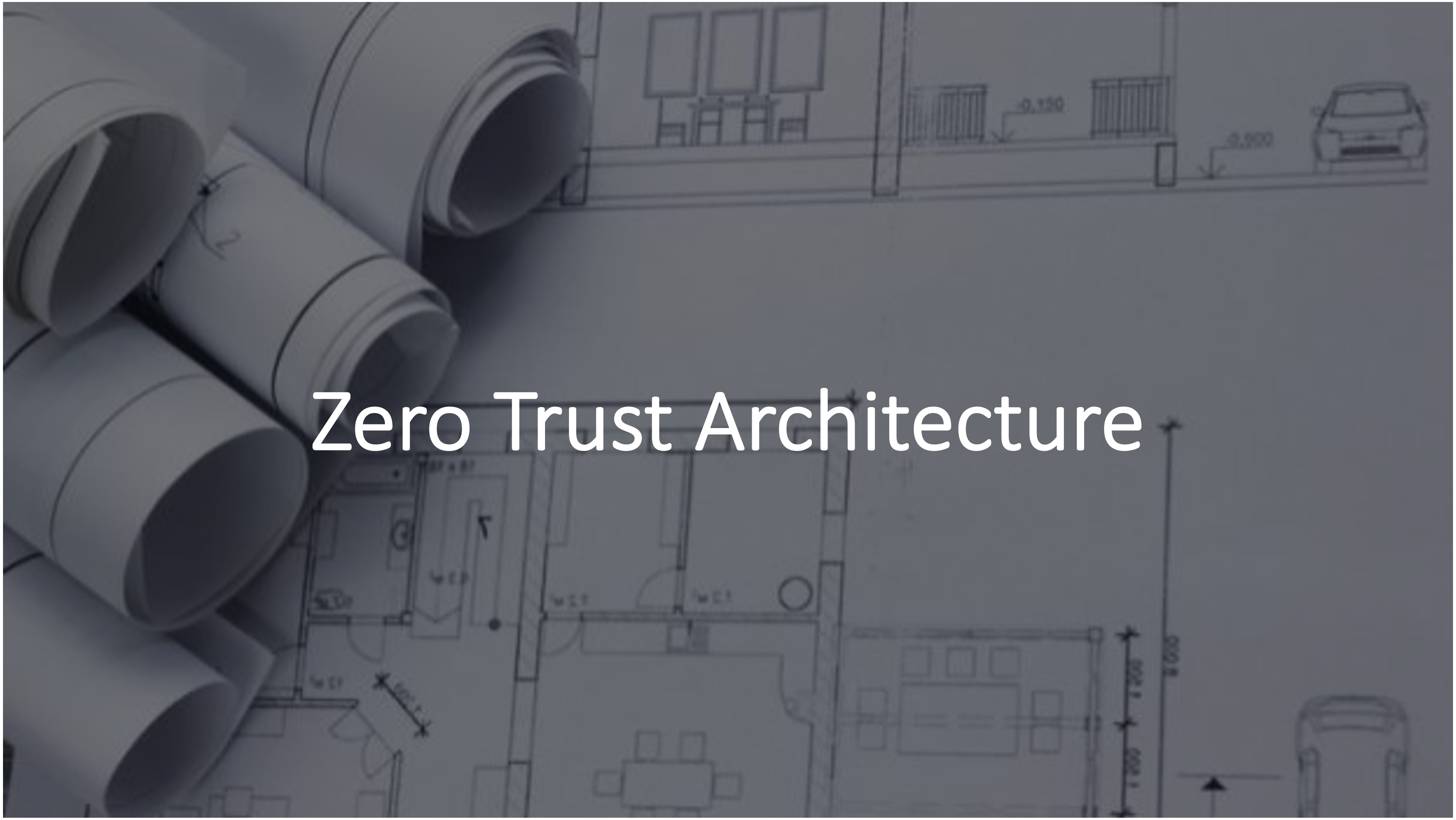


Access control lists (ACLs)

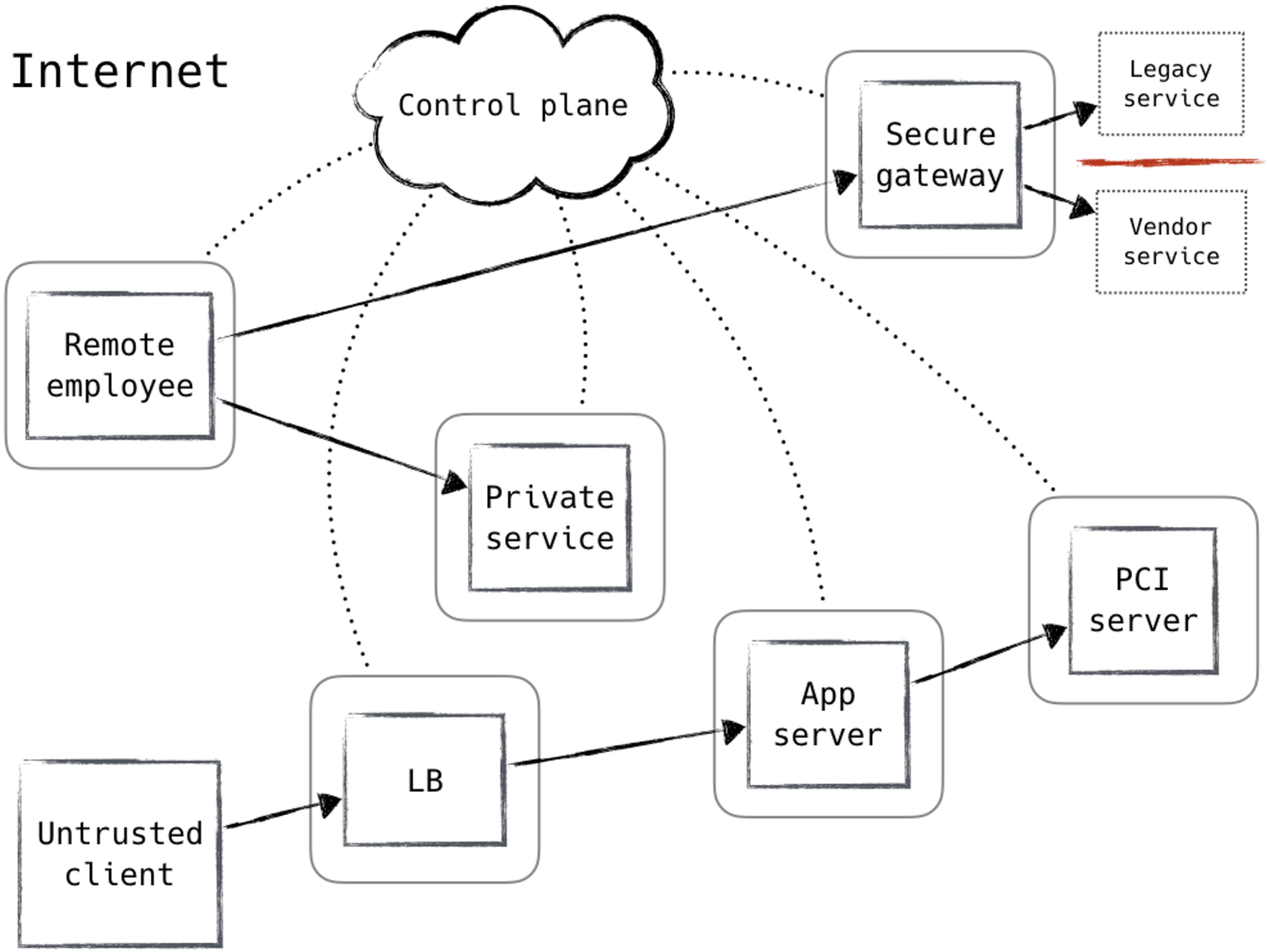
Role-based access controls (RBAC)

Principles of least privilege

Zero Trust model



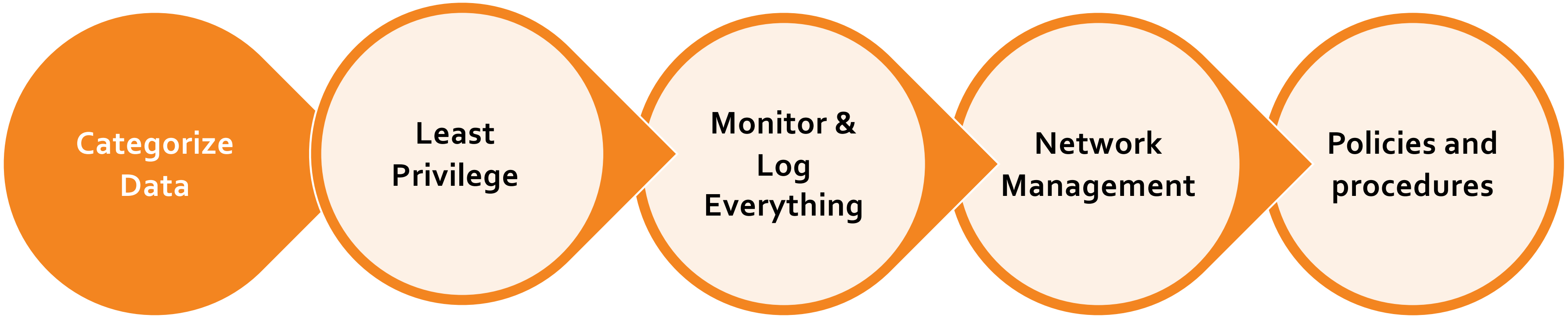
Zero Trust Architecture



https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/assets/ztnw_0102.png

Perfect fit for the Cloud

Zero Trust can be implemented with..



Categorize Data

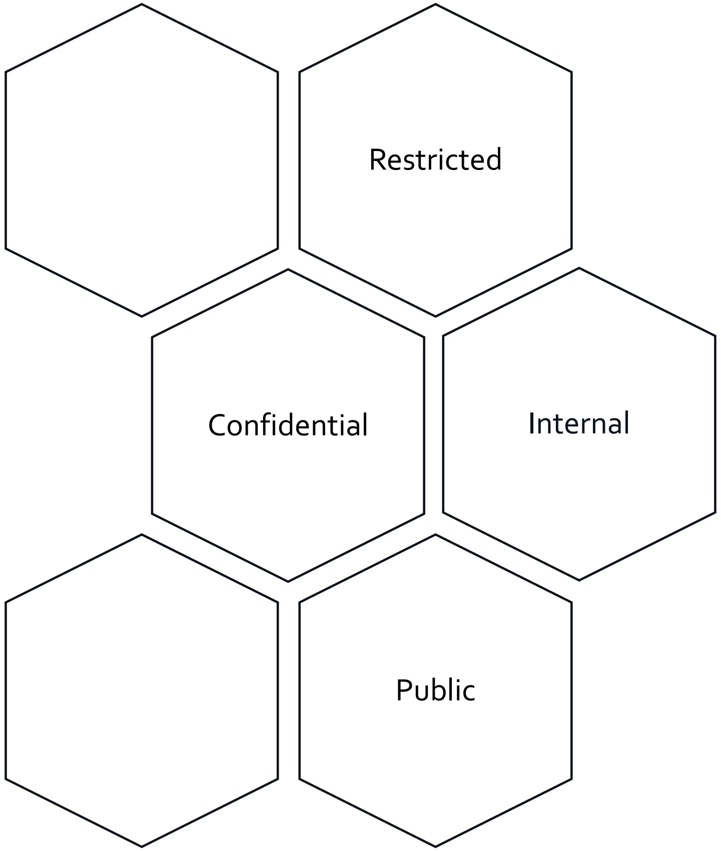
Least Privilege

Monitor & Log Everything

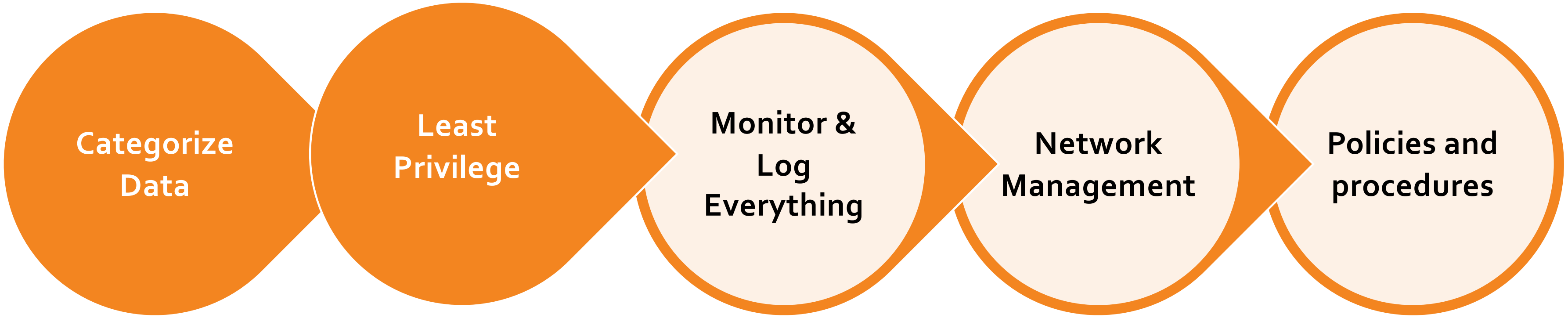
Network Management

Policies and procedures

https://www.doxnet.com/2019/12/data-classification-what-it-is-why-its-important-and-how-to-make-it-happen/



Zero Trust can be implemented with..

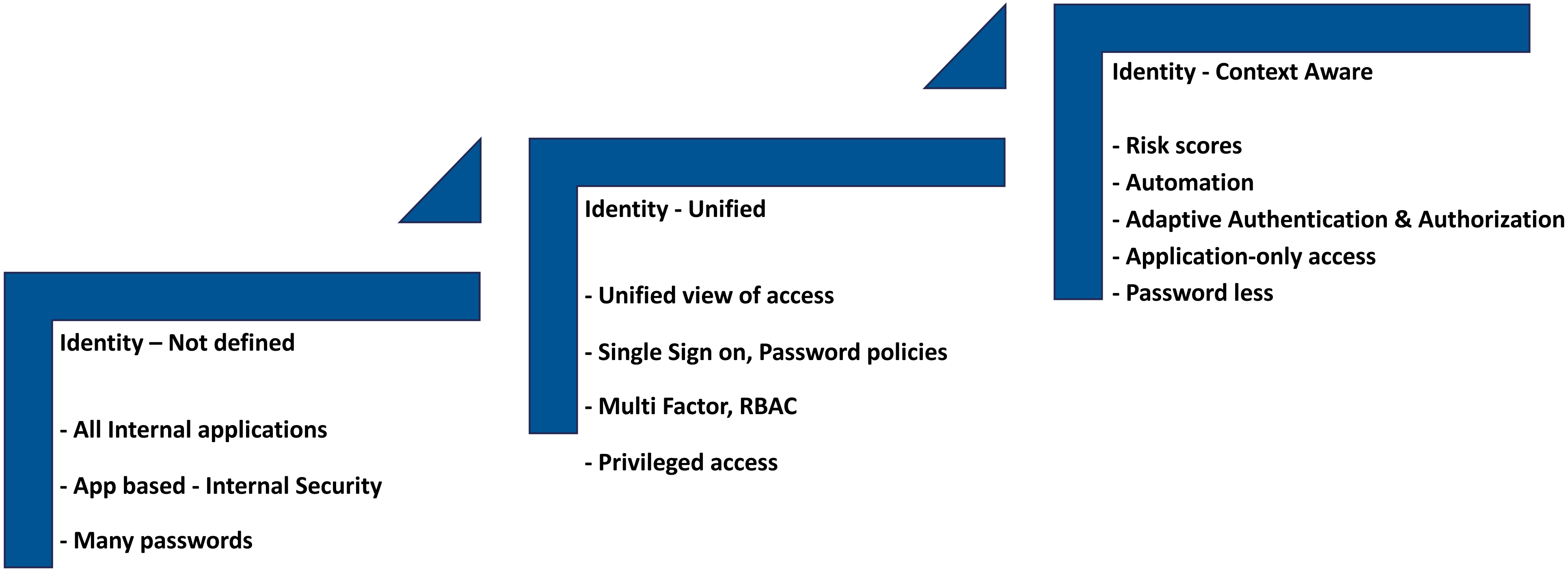


Principles of Least Privilege

- Authenticating and verifying on all access
- Automate rule and access policy baselines
- Granular Role-Based Access,
- Using Just in Time Least Privilege
- Access Requests for App/Endpoint/Infrastructure,

Raise your hands if you have multiple accounts with multiple passwords

Stages of IAM Maturity



Identity – Not defined

- All Internal applications

- App based - Internal Security

- Many passwords

Identity - Unified

- Unified view of access

- Single Sign on, Password policies

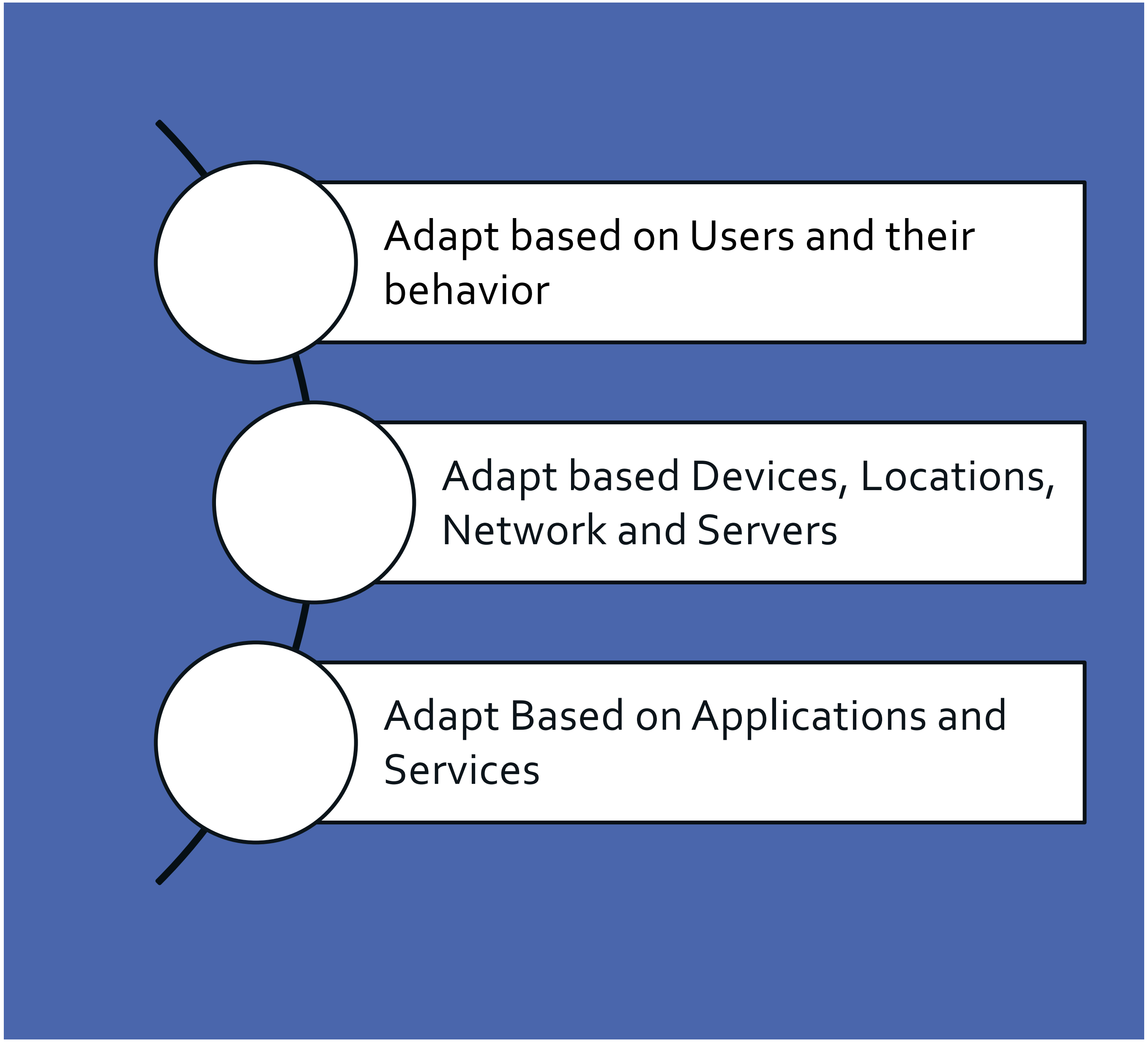
- Multi Factor, RBAC

- Privileged access

Identity - Context Aware

- Risk scores
- Automation
- Adaptive Authentication & Authorization
- Application-only access
- Password less

Context aware Access

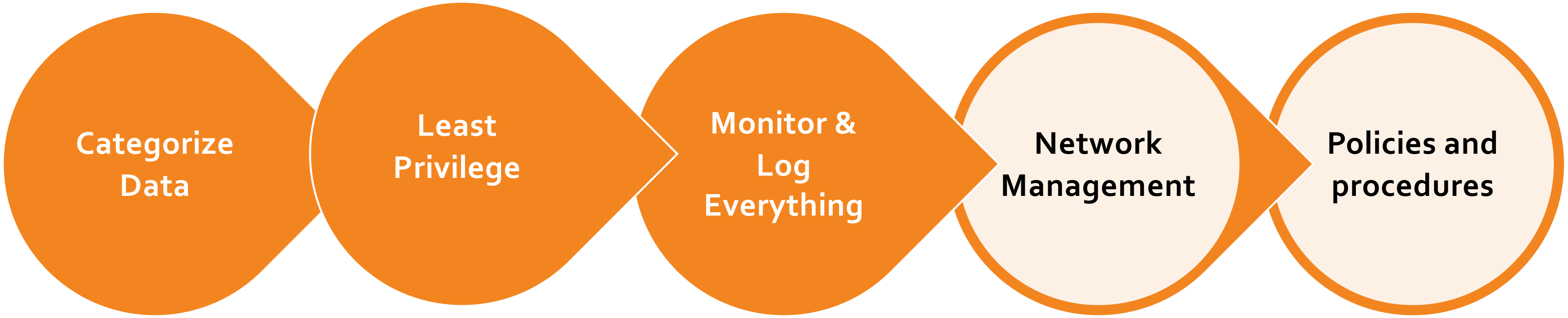


Adapt based on Users and their behavior

Adapt based Devices, Locations, Network and Servers

Adapt Based on Applications and Services

Zero Trust can be implemented with..



Categorize Data

Least Privilege

Monitor & Log Everything

Network Management

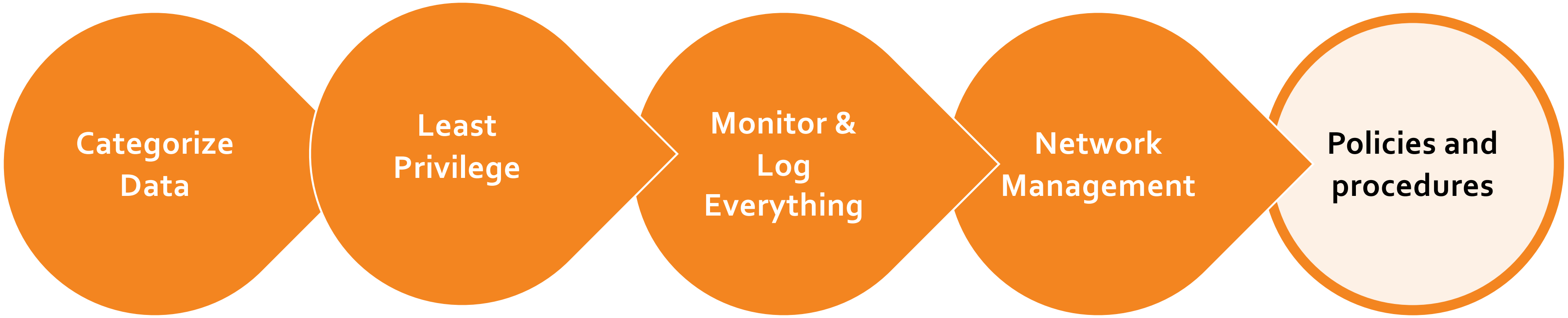
Policies and procedures

Good logging and monitoring

Do you think your enterprise's logging and monitoring is up to mark?

- All accesses to sensitive data logged and monitored?
- All access attempts and its actions are recorded?
- Authentication and Authorization of all identities are monitored?
- How is the network is being analyzed and monitored?
- Will you be able to demonstrate an audit trail for access, data and actions
- How much of automation is in place, to detect incidents?
- How are alerts and events managed?

Zero Trust can be implemented with..



Categorize Data

Least Privilege

Monitor & Log Everything

Network Management

Policies and procedures

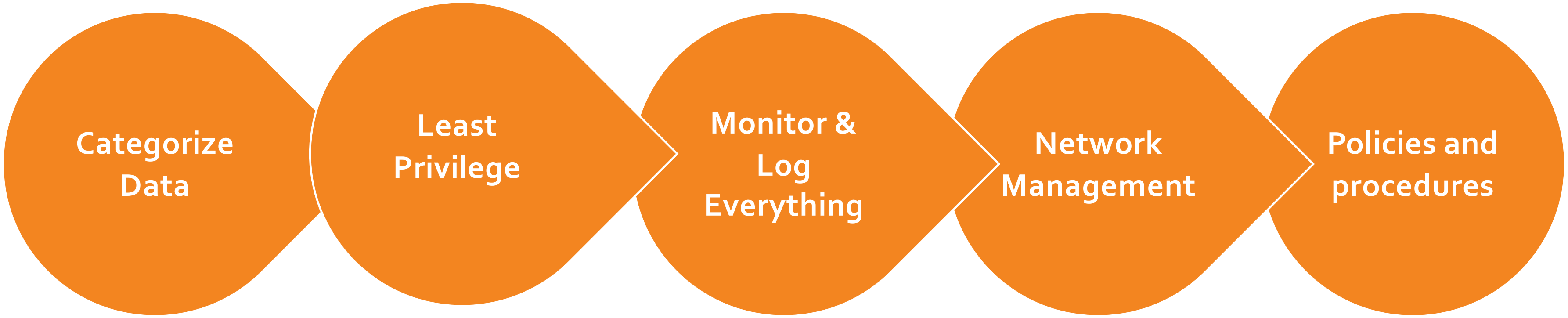
Network Management –
Demise of perimeters, rise of security

MICRO SEGMENTATION – BASED ON CONTEXT AND APPLICATION

SOFTWARE-DEFINED PERIMETER

ORCHESTRATION AND AUTOMATION

Zero Trust can be implemented with..



Categorize Data

Least Privilege

Monitor & Log Everything

Network Management

Policies and procedures

Polices and Procedures

REMOTE ACCESS

BYOD

PASSWORDS POLICIES

LEAST PRIVILEGE

DEFAULT DENY

CONTINUOUS CHANGES

Implementation

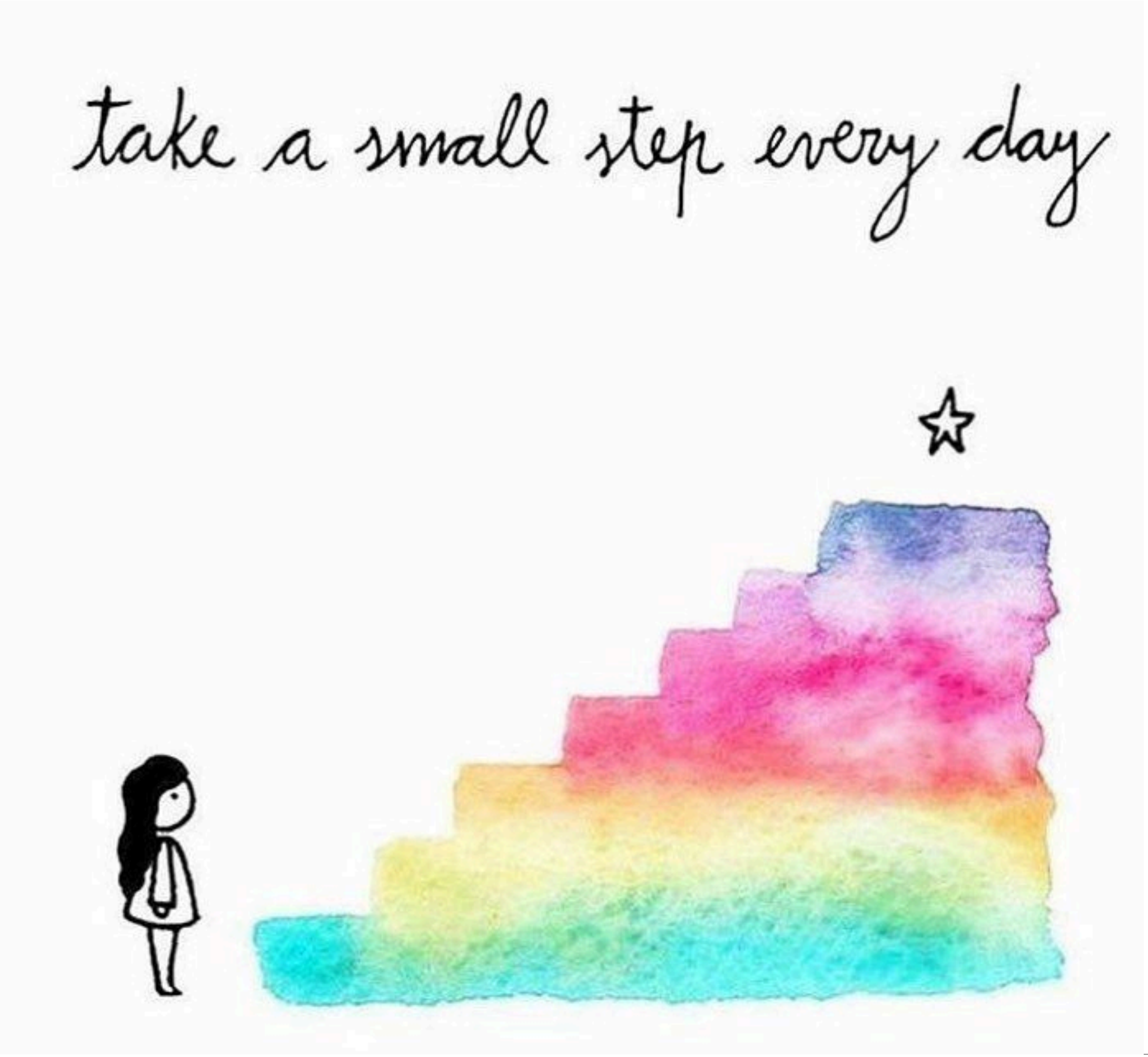
Identify	Identify what type of applications
Understand	Understand how the organisation’s applications work
Create	Create boundaries between users and applications
Deploy	Deploy Zero Trust policies
Monitor and maintain	Monitor and maintain your Zero Trust environment

Watch your back.
Don't trust anyone.
Do you trust me?
Yes.
I just said,
don't trust anyone.
ORGANIS
ATION
ZERO
TRUST

Zero trust is Not a product but a "perspective"

Do you agree?...............

Identity is becoming the new security perimeter



Take small Steps in the journey of Zero Trust!

References

- https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
- https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf
- https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/
- https://ldapwiki.com/wiki/Zero%20Trust
- https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-for-the-cloud
- https://www.youtube.com/watch?v=-Why_ZjJUhg
- https://www.forbes.com/sites/louiscolumbus/2019/02/07/digital-transformations-missing-link-is-zero-trust/#6be166fe727f
- https://www.akamai.com/us/en/multimedia/documents/white-paper/how-to-guide-zero-trust-security-transformation.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft.pdf
- https://heimdalsecurity.com/blog/what-is-the-zero-trust-model/

Reach Me!

Twitter: @InfosecVandana

LinkedIn: vandana-verma

Thank You