Let‘s talk about

Zero Trust

Revolution or Evolution?

March 2024

Reto Zeidler, Dipl. Inf | EMBA FH | CISSP | GSLC
Security Professional, Senior Executive & Guest Lecturer

https://www.linkedin.com/in/reto-zeidler/

What you will learn today..

1. A brief History of Zero-Trust
2. Problems we are going to solve (and those we don't)
3. The Key Principles and Models
4. How to address Zero-Trust in an organisation?

Once upon a time – A brief History of Zero-Trust

The term Zero Trust was born

NIST Special Publication 800-207

Zero Trust Architecture

NIST National Institute of Standards and Technology U.S. Department of Commerce

Zero Trust Maturity Guide

Zero Trust Maturity Model

Pre-2010 | 2010 | 2014 | 2020 | 2020+

„De-perimeterisation“

JERICHO FORUM

DEPARTMENT OF DEFENSE

DEFENSE INFORMATION SYSTEMS AGENCY

CSA cloud security alliance

Software Defined Perimeter

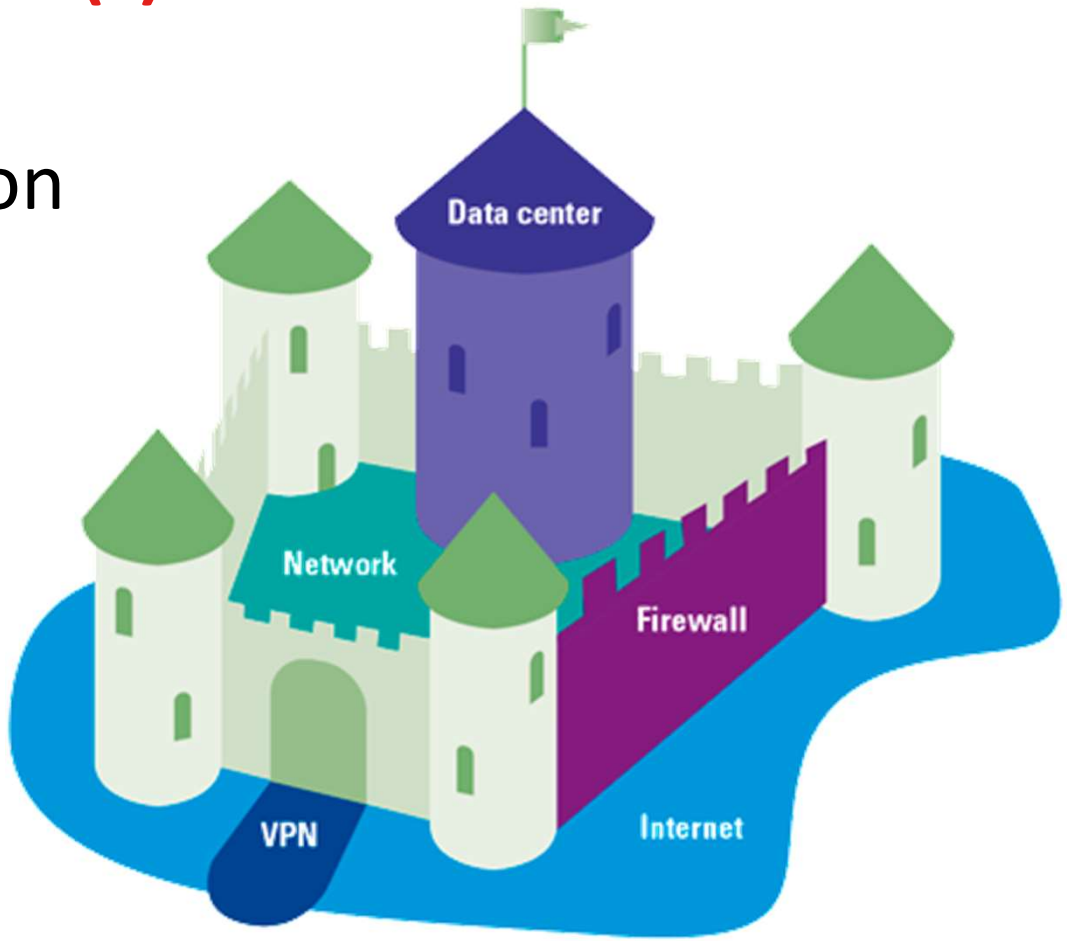
BeyondCorp Enterprise

Microsoft Zero Trust

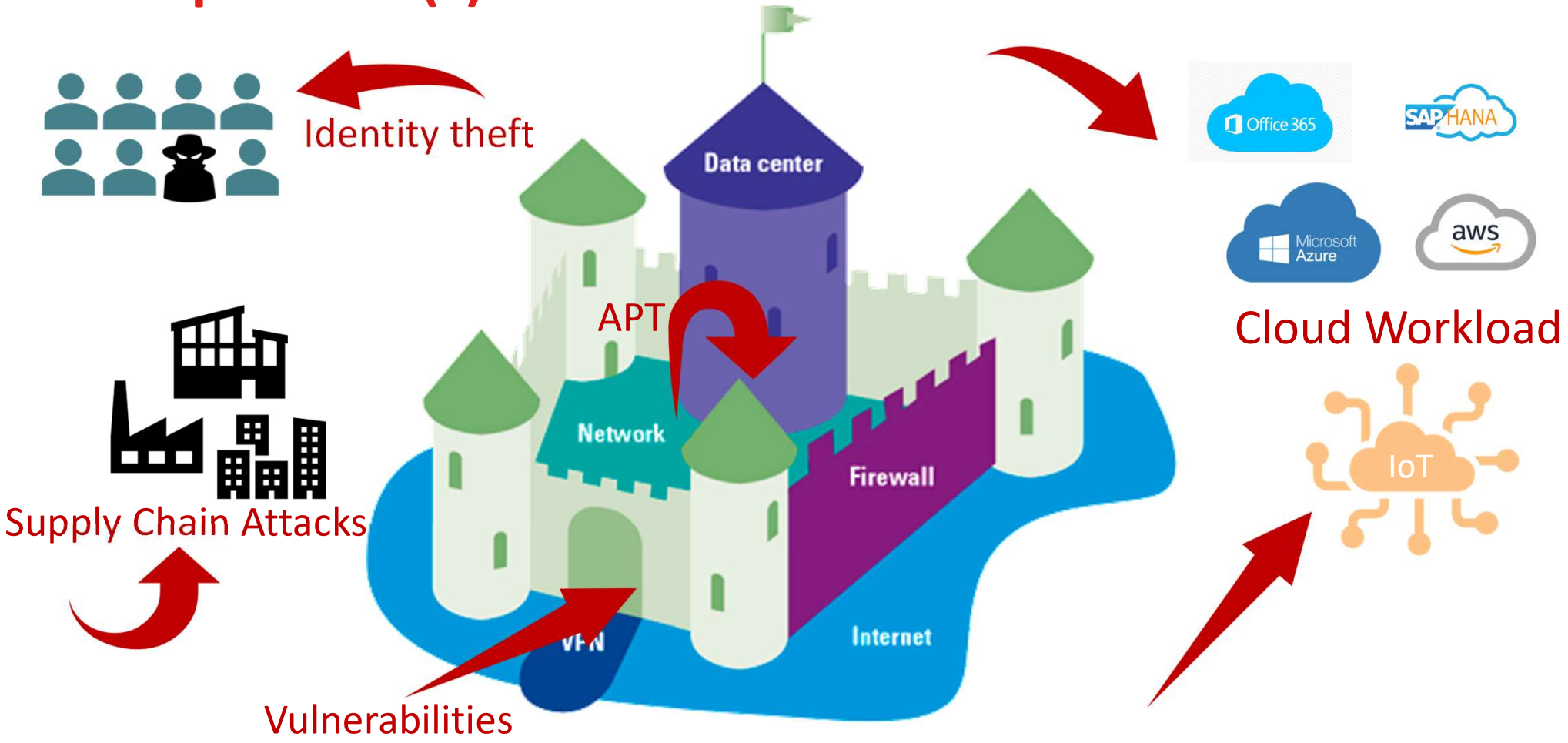
What is the problem to our solution?

What problem(s) does Zero-Trust address?

„Once upon a time..“



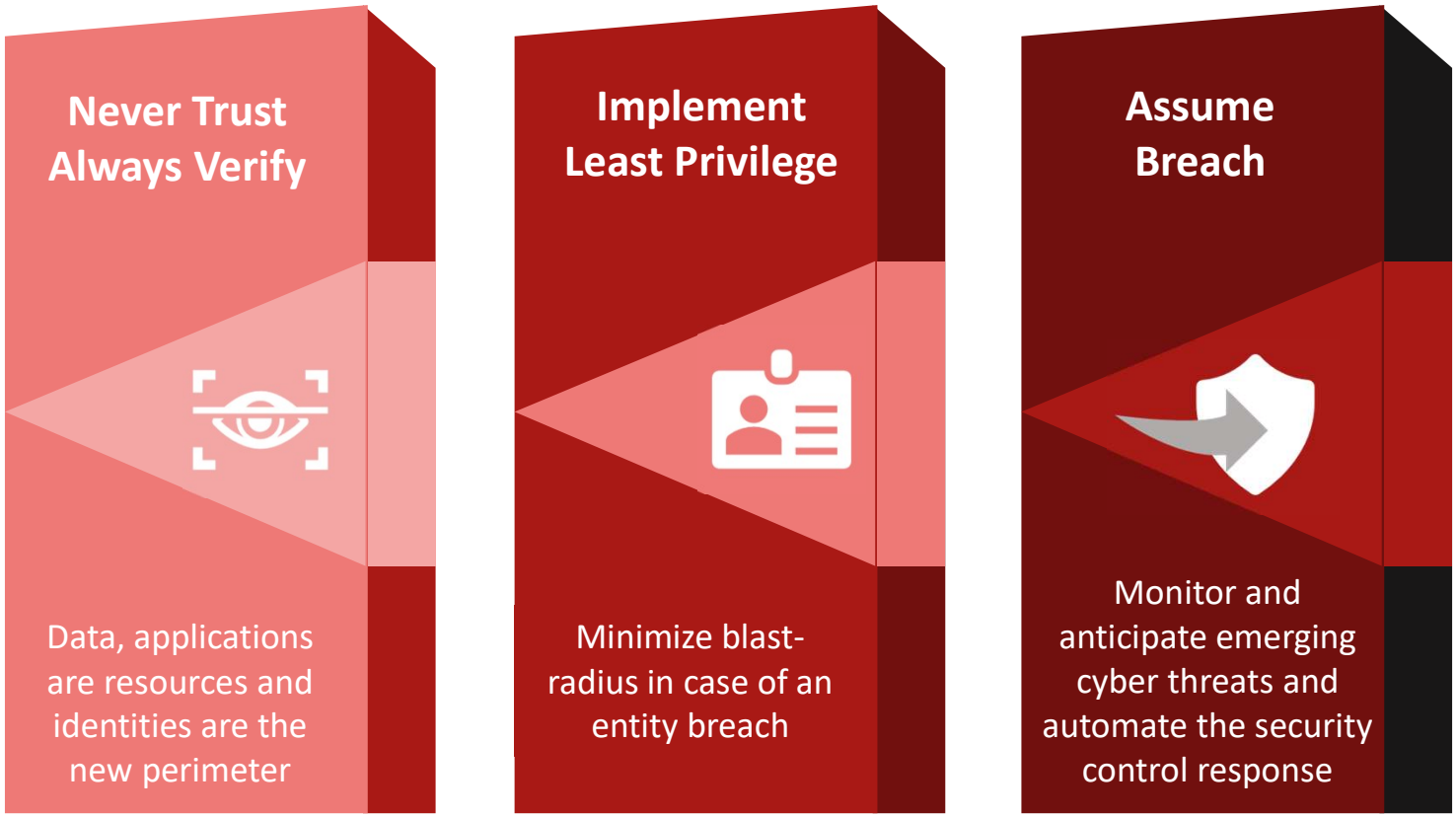
What problem(s) does Zero-Trust address?



From trust but verify to never trust

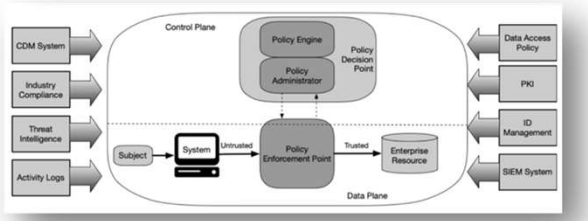
The Zero Trust Principles

Zero-Trust (Key-)Principles

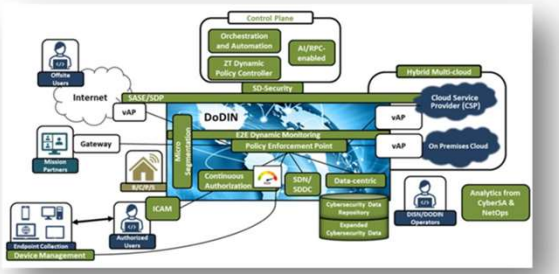


Zero Trust Reference Architecture Models..

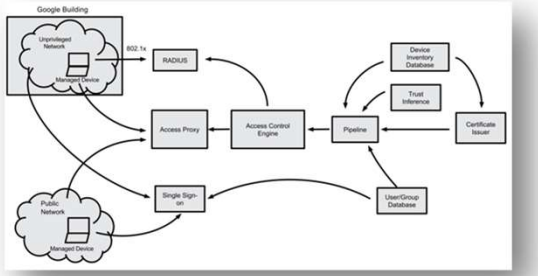
NIST SP 800-207 – Zero Trust Architecture (2020)



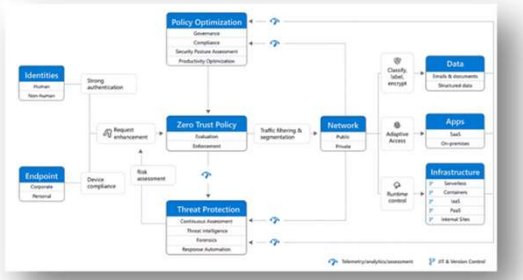
DoD Zero Trust Target Architecture (2022)



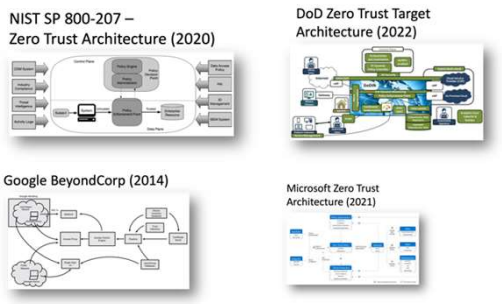
Google BeyondCorp (2014)



Microsoft Zero Trust Architecture (2021)



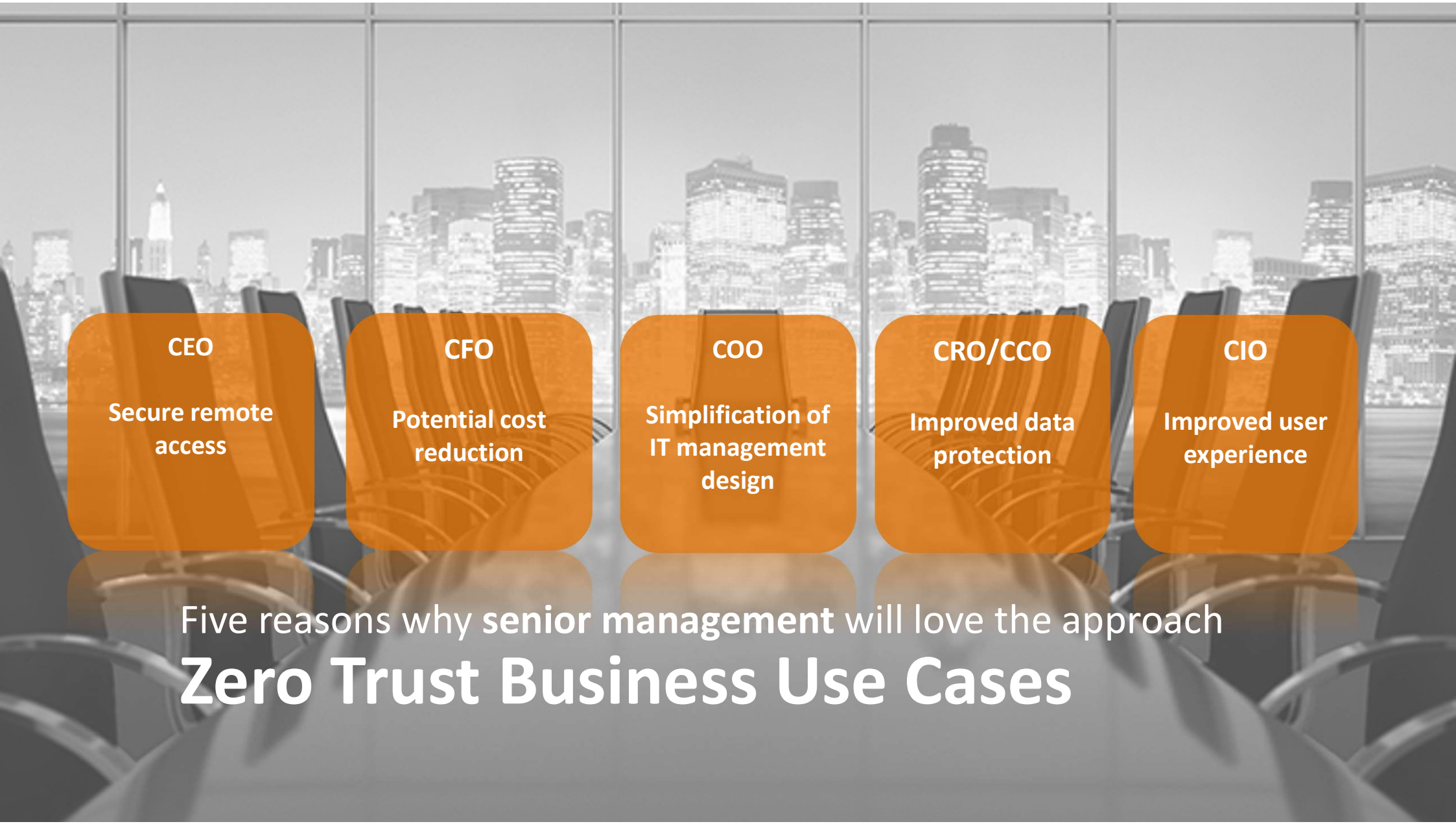
Zero Trust Reference Architecture Models..
..are probably not the best way to approach the topic.



„If you think technology solves your security problems, you did not understand the technology nor your security problems.. „ Bruce Schneier

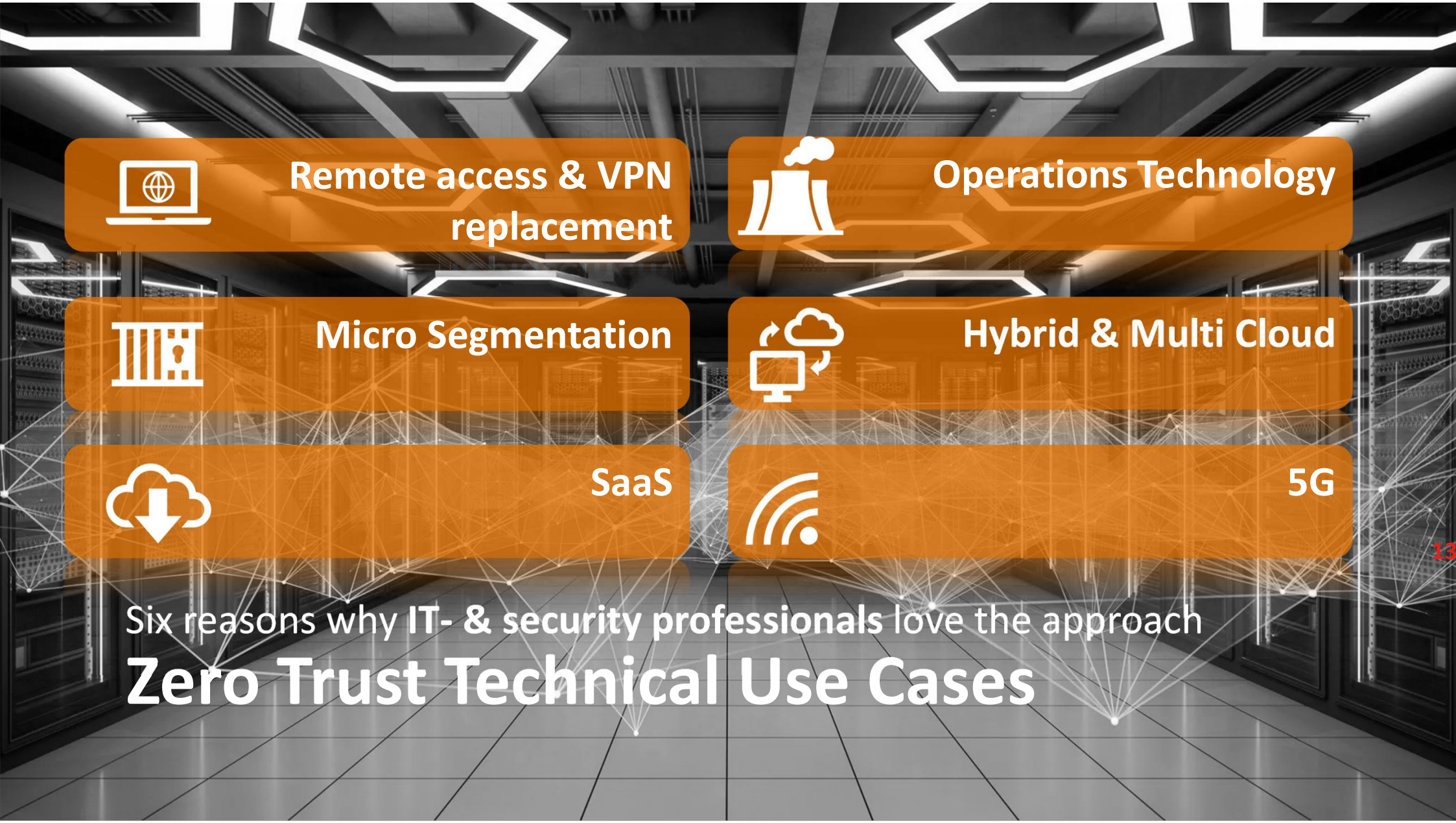
Don‘t try to eat the elephant at once

How to address Zero-Trust in an organisation?

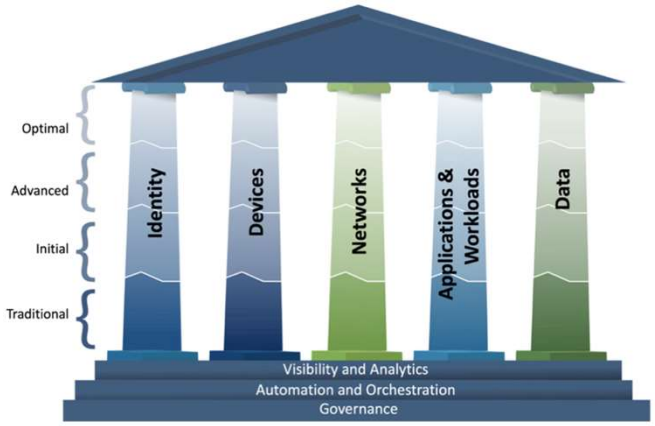


Five reasons why **senior management** will love the approach

Zero Trust Business Use Cases


Remote access & VPN replacement
Operations Technology
Micro Segmentation
Hybrid & Multi Cloud
SaaS
5G
Six reasons why IT- & security professionals love the approach
Zero Trust Technical Use Cases

Prepare your Zero Trust roadmap



Zero-Trust Maturity Model 2.0 by CISA

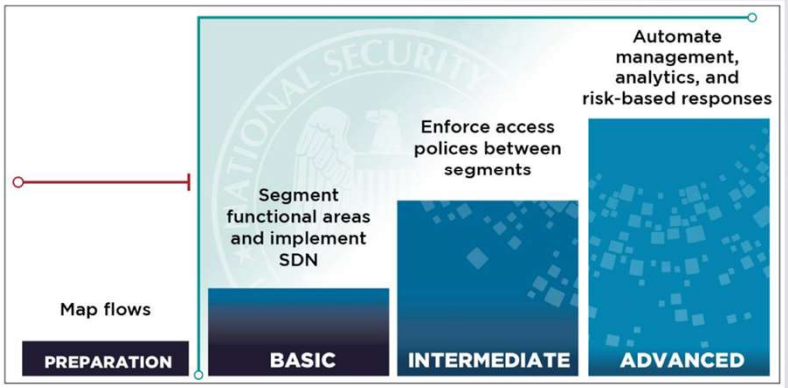
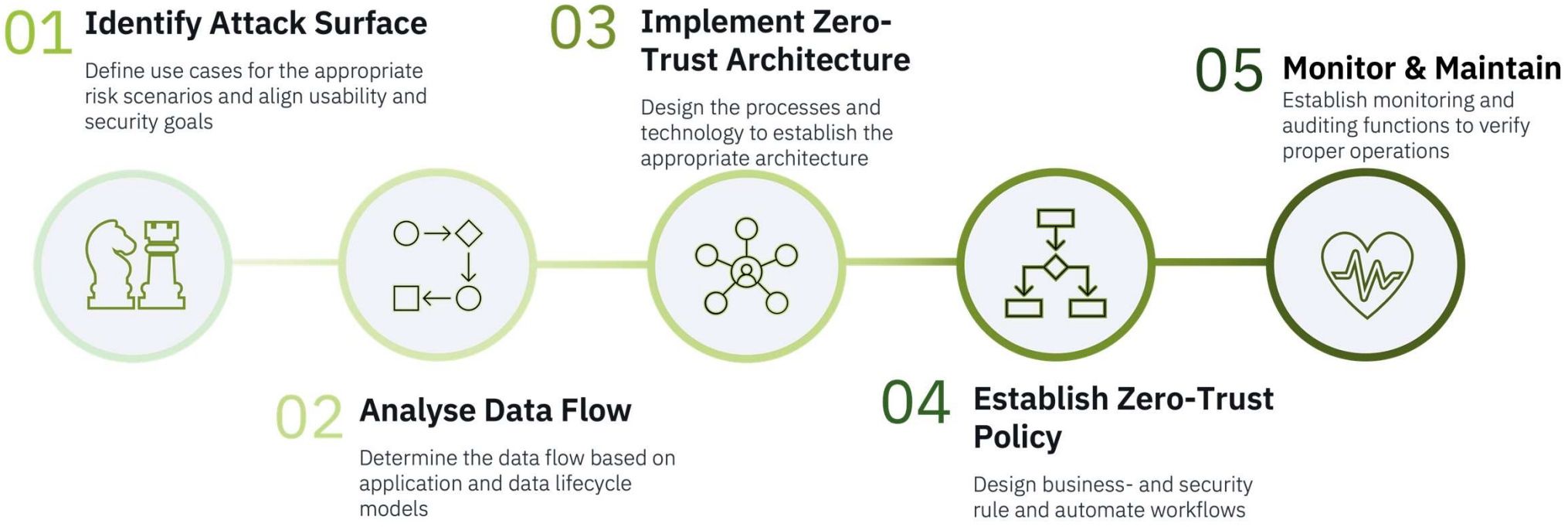


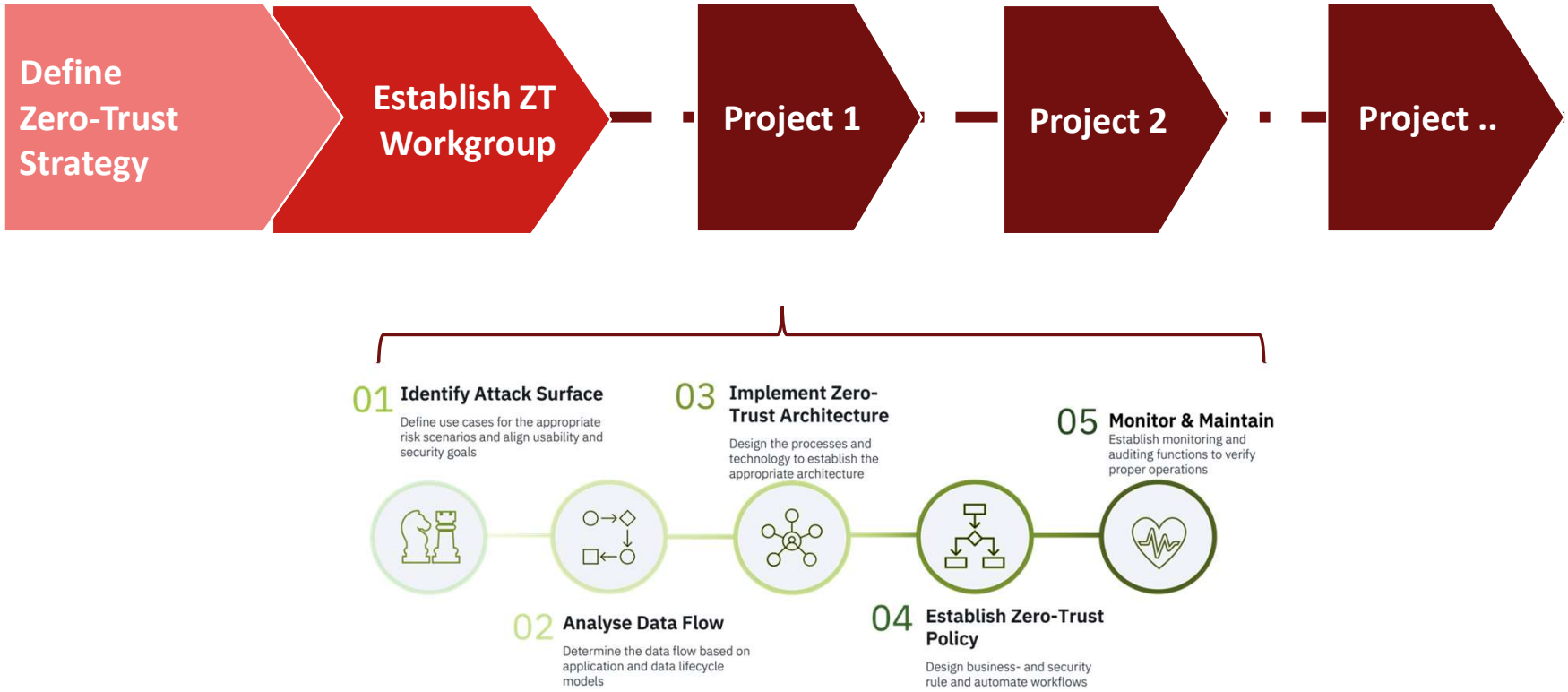
Figure 2: Zero Trust network and environment pillar maturity

The **maturity model** issued by CISA and the maturity guidelines by NSA are valuable tool tools to determine the transition roadmap from classic to a zero trust architecture

Addressing Zero Trust with the The-Five-Step-Implementation-Model

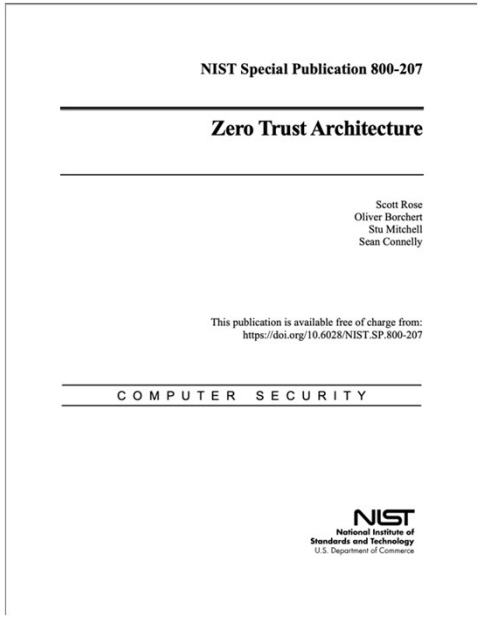


Embedding your implementation into the strategy

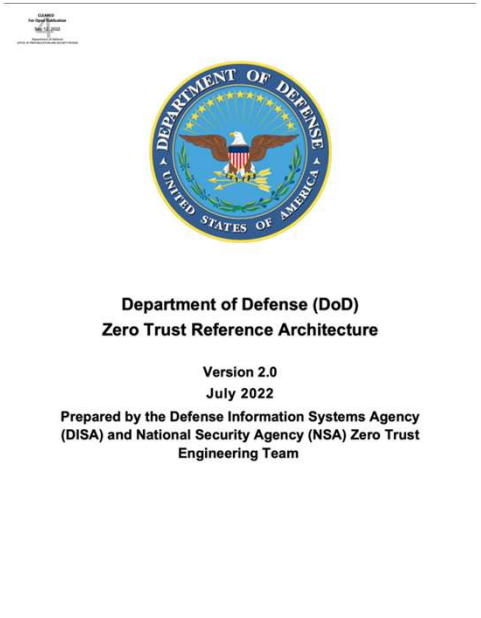


Intern

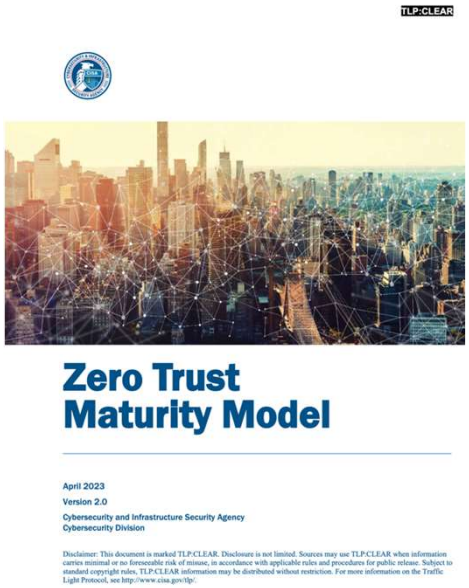
My favorites for practitioners



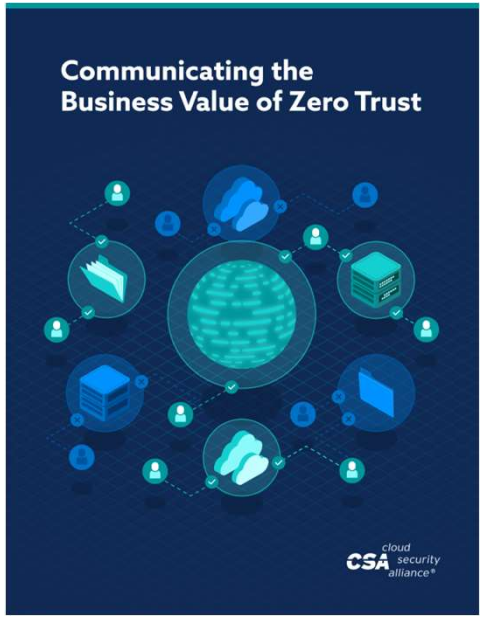
https://csrc.nist.gov/publications/detail/sp/800-207/final



https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf



https://www.cisa.gov/sites/default/files/202304/zero_trust_maturity_model_v2_508.pdf



https://cloudsecurityalliance.org/artifacts/communicating-the-business-value-of-zero-trust

Wrapping Up

Zero Trust..

..is a strategy, expressed in architecture models, supported by technology

..don’t approach Zero Trust from a pure technological viewpoint – it’s a mindshift

..adds security **AND** improves usability, (what is rare)

Links & Resources

BeyondCorp: A new approach to enterprise security
https://cloud.google.com/beyondcorp

NIST SP800-07 / Zero-Trust Model
https://csrc.nist.gov/publications/detail/sp/800-207/final

Microsoft Zero-Trust Model
https://www.microsoft.com/en-us/security/business/zero-trust

CISA Maturity Model 2.0
https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

NSA - Embracing a Zero Trust Security Model
https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

CSA – Defining the Zero Trust protect Surface
https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface

The Future of Directory Services Is Domainless
https://learn.g2.com/directory-services

Passwordless Authentication: What It Is and How It Works
https://www.beyondidentity.com/resources/passwordless-authentication

Modern Bastion Hosts
https://eng.sigmacomputing.com/modern-bastion-hosts-abed8c7c7c63

Immutable Container Images
https://thenewstack.io/how-zero-trust-models-work-in-container-security/