MONET +

Zero Trust

Radomír Pravda
Sales Manager


access
Trust
Policy
Security
Zero
Continuous
verify
Device
Risk
User
Compliance
Posture
detection
check
time
Telemetry
Credential
resistant
theft
Conditional
breach
Never
always
explicitly
Unmanaged
Phishing
auth
Federation
verification
Endpoint
Explicit
privilege
control
Least
SSO
Identity
Assume
Passwordless
Provider
MFA
EDR
ABAC
Patch
Application
XDR
Microsegmentation
management
BYOD
hardening
MDM
Perimeterless
SIEM
classification
SASE
Model
West
enforcement
Approval
ZTX
level
depth
Analytics
policies
Maturity
workflow
CISA
logs
Intelligence
Defense
Microsoft
Forrester
gateway
VPN
Monitoring
BeyondCorp
RBAC
engine
ZTNA
Segmentation
East
algorithm
Framework
Threat
Proxy
replacement
Audit
traffic
Behavior
evaluation
based
Google
Adaptive
request
SDP
Real
Design
Dynamic
boundary
NIST
SOAR
Remote
Data
Anomaly
context
point
correlation

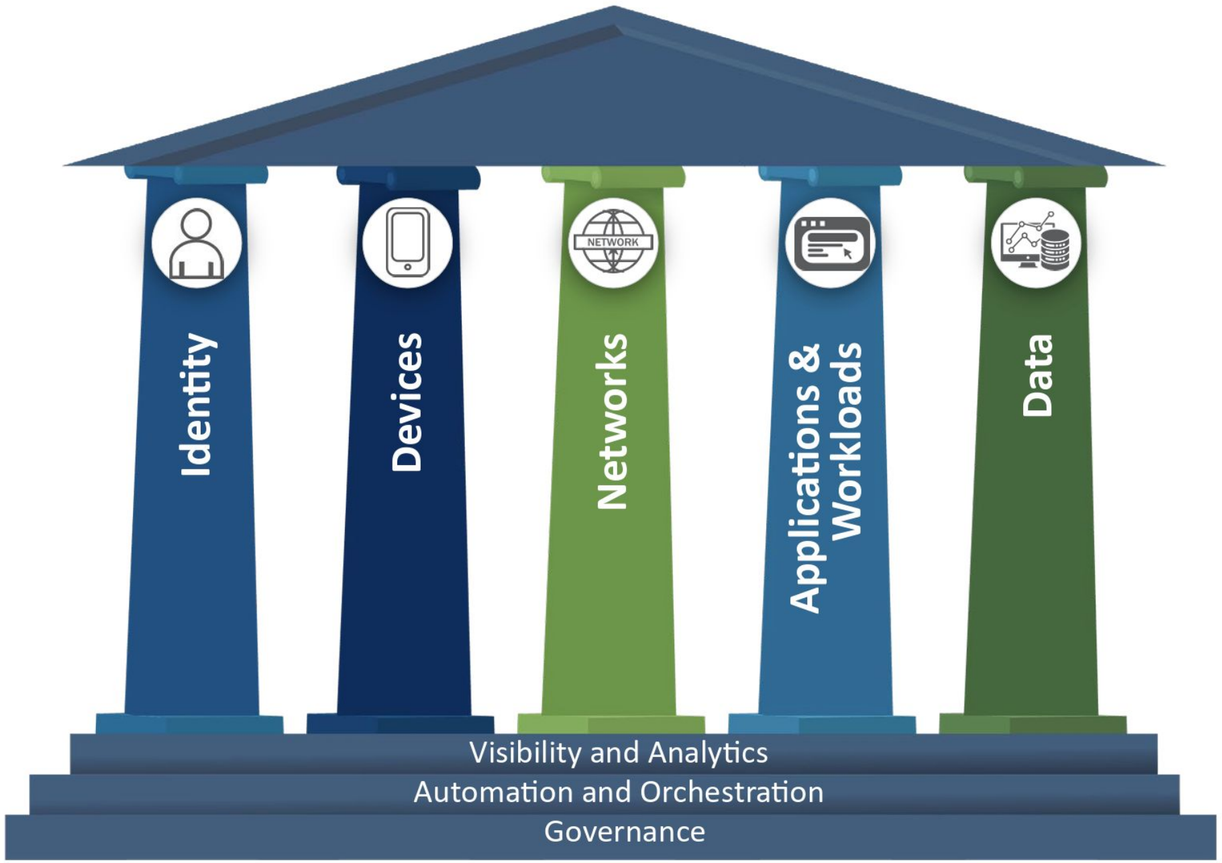
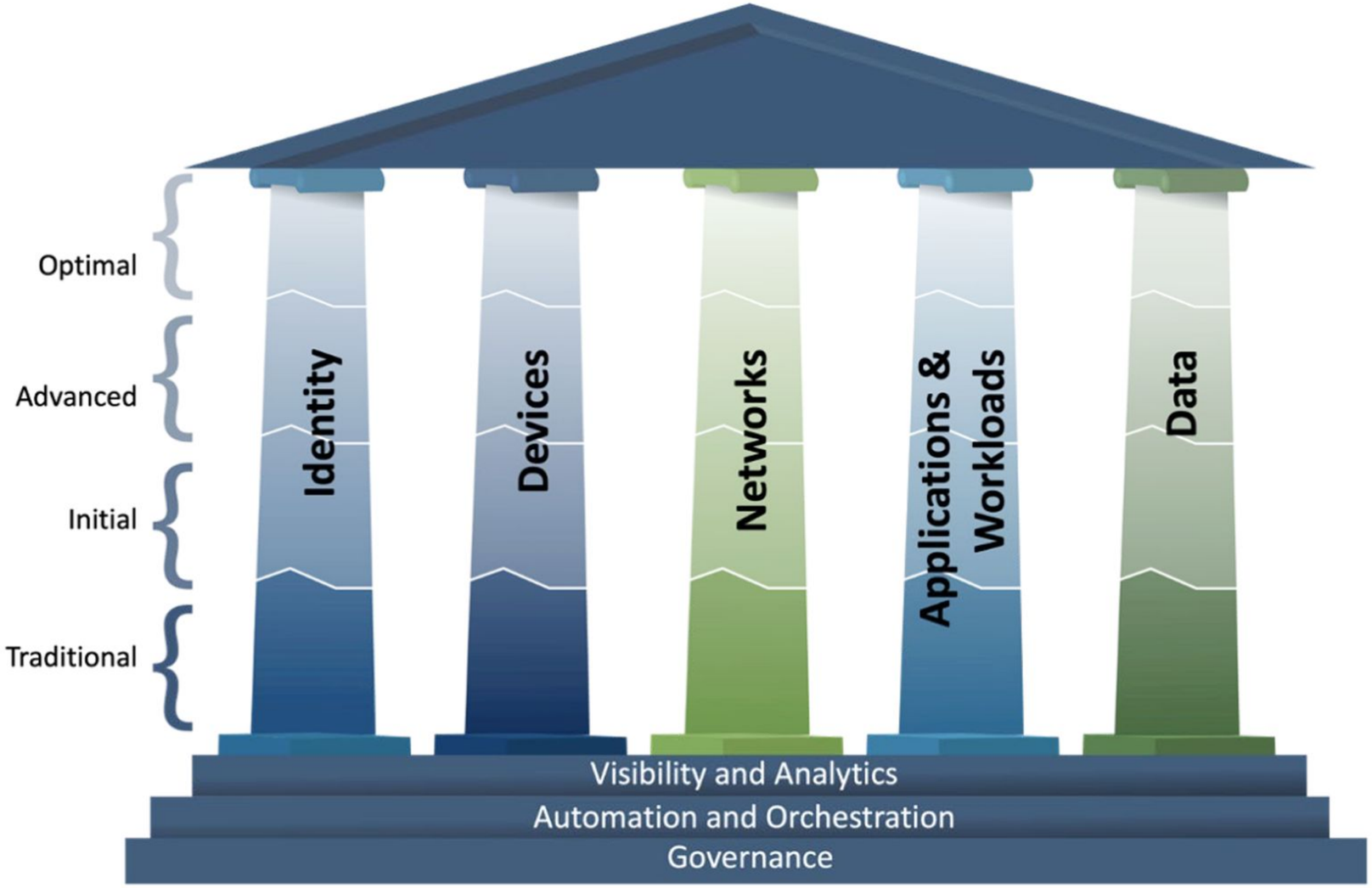


Figure 1: Zero Trust Maturity Model Pillars[8]

CISA's ZTMM is one of many paths to support the transition to zero trust.

Zero Trust Maturity Model



Zero Trust Maturity Evolution

Support

MONET +

Bezpečnostní konzultace

- Požadavek: „máme zájem o Zero Trust, pomůžete nám?”

- Dohodnutý postup:
  - představíme **teoretický** pohled na Zero Trust Architekturu
  - rozdělíme na oblasti
  - na vybraném podoblasti navrhneme konkrétní **technologie**
  - připravíme **ukázku** použití

1. Teoretický pohled na Zero Trust Architekturu

- Explicitně zájem zákazníka o naplnění standardu NIST SP 800-207
  - “praktická” část konzultace by měla být v souladu s tímto zdrojem
  - “mapování”

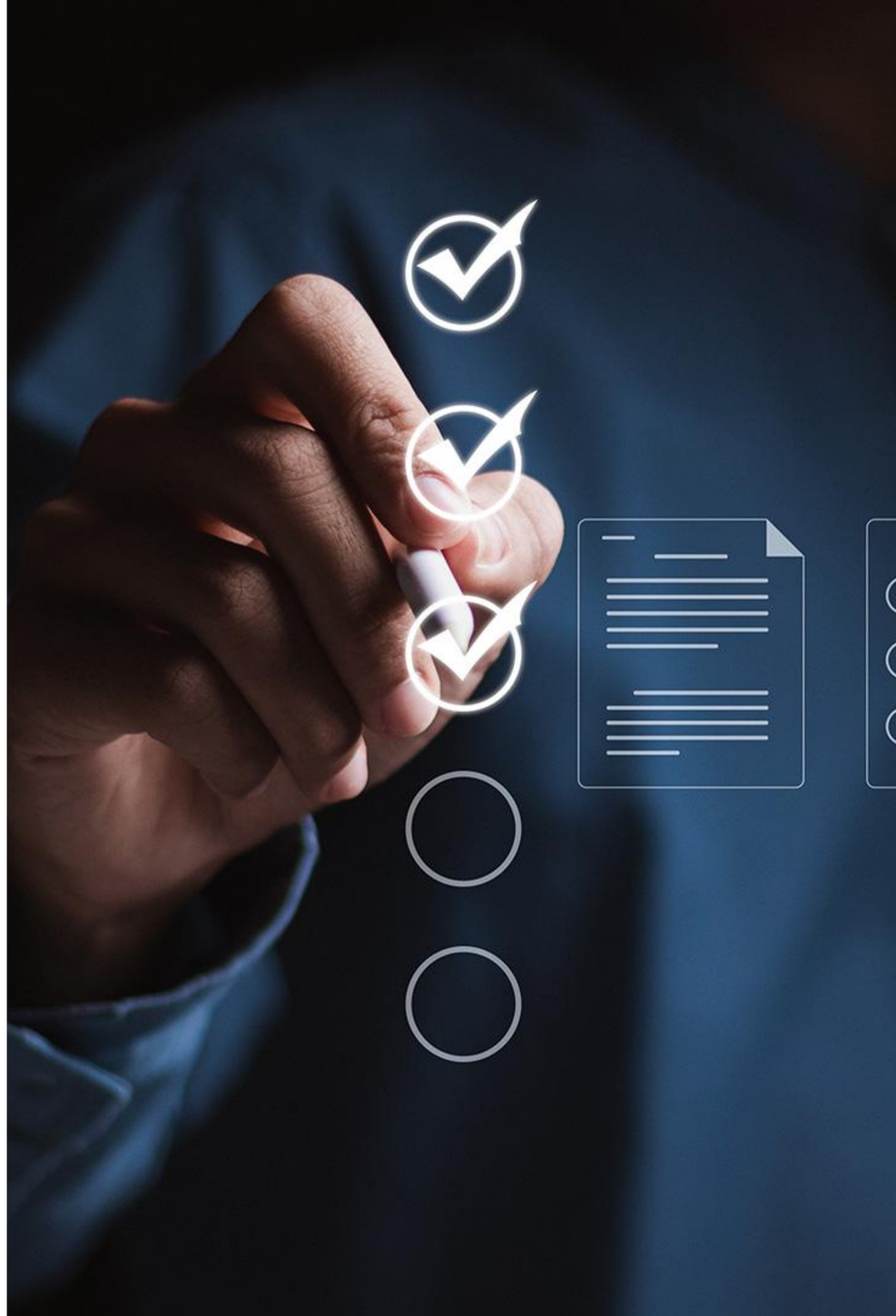
- Mantra: *“start with protect surface”*

2. Vymezení podproblému a návrh technologií

- Vybraná oblast: Application-to-Application
  - se zaměřením na Kubernetes

- Jiné identifikované podoblasti:
  - Employee-to-Asset
    (např. přihlášení do počítače) (✨ ProID ✨)
  - Employee-to-Service
    (např. správa Kubernetes klustru)
  - Employee-to-Application
    (např. přístup do Jira)

- *“see the big picture”*



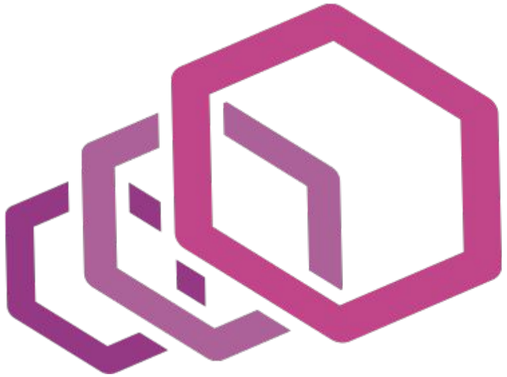
3. Návrh technologií - Application-to-Application

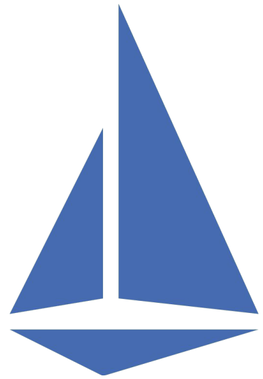
Jedno z dvou:

- Proxy
  - **Envoy**
- Service mesh
  - **Istio**
  - Linkerd
  - Consul
  - Kuma

a

- Policy engine
  - **Open Policy Agent**
  - Kyverno





Takeaway...

MONET +

Možné *Quick wins*

Obecné principy Zero Trust	S čím začít
Zmapuj identity, zařízení a systémy	IdP pro jednotnou identitu, CA pro vydání certifikátů, MDM pro správu zařízení
Zaveď silné dvoufaktorové ověřování (MFA)	Smart Card nebo mobilní autentizace pro přihlášení do počítače Alternativní metody - využití biometrie, FIDO2, passwordless login
Unifikuj a centralizuj	SSO pro co nejvíc aplikací, KMS a secret management
Sleduj a loguj všechny přístupy	Centralizovaný sběr logů a auditních udalostí Anomaly detection a notifikace
Omezuj přístup na základě rizika	MFA také u SSO pro klíčové aplikace a systémy
Automatizuj životní cyklus	CLM, CI/CD

Thank you for your attention!

Contact me

Radomír Pravda

rpravda@monetplus.cz