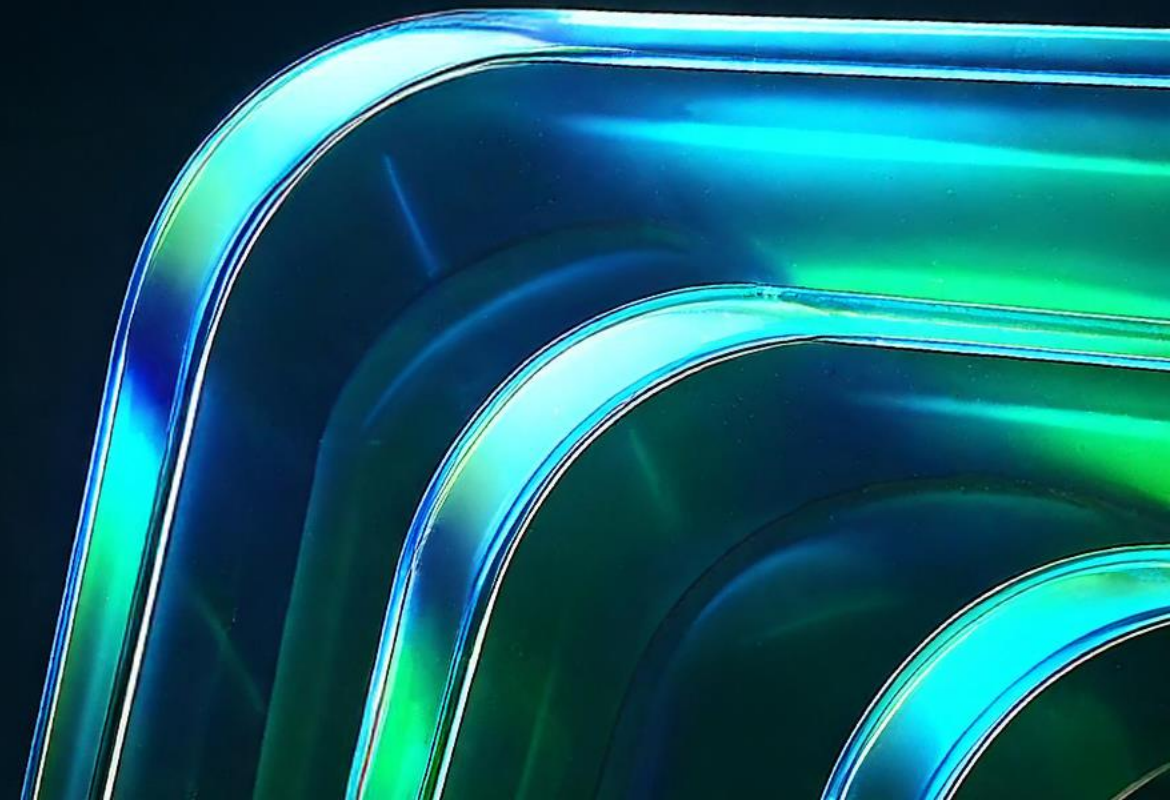
Check-In & Earn Points!

- Already got the **Cvent App**? Tap **CHECK IN** and enter the session code “ZeroTrust1”
- Prefer a faster option? Just scan the QR code to check in directly!

TECH CON

Zero Trust Security Models for Modern Businesses



TECH CON

HI, I'M NATE SCHMITT

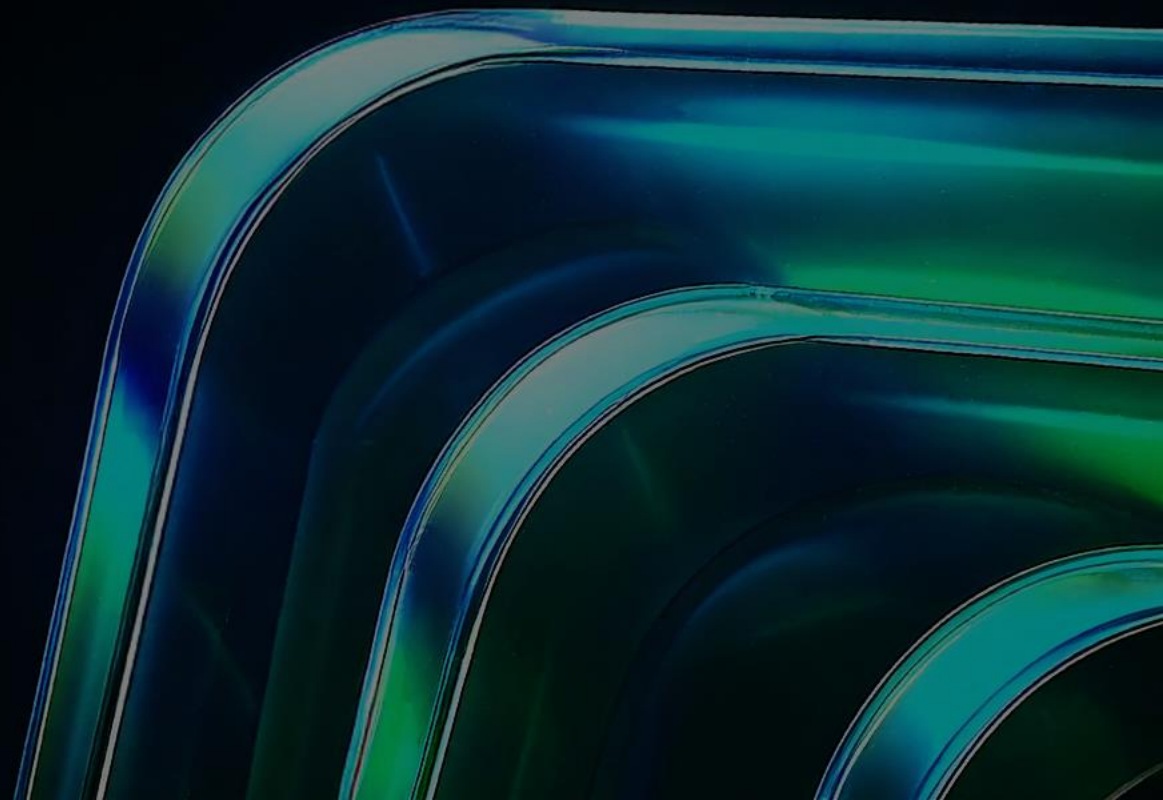
- Lead CIT's Cybersecurity team/vCISO
- Instructor
- 30+ ransomware engagements
- 250+ business email compromises
- Own two classic cars

TECH CON

Zero Trust Security Models for Modern Businesses

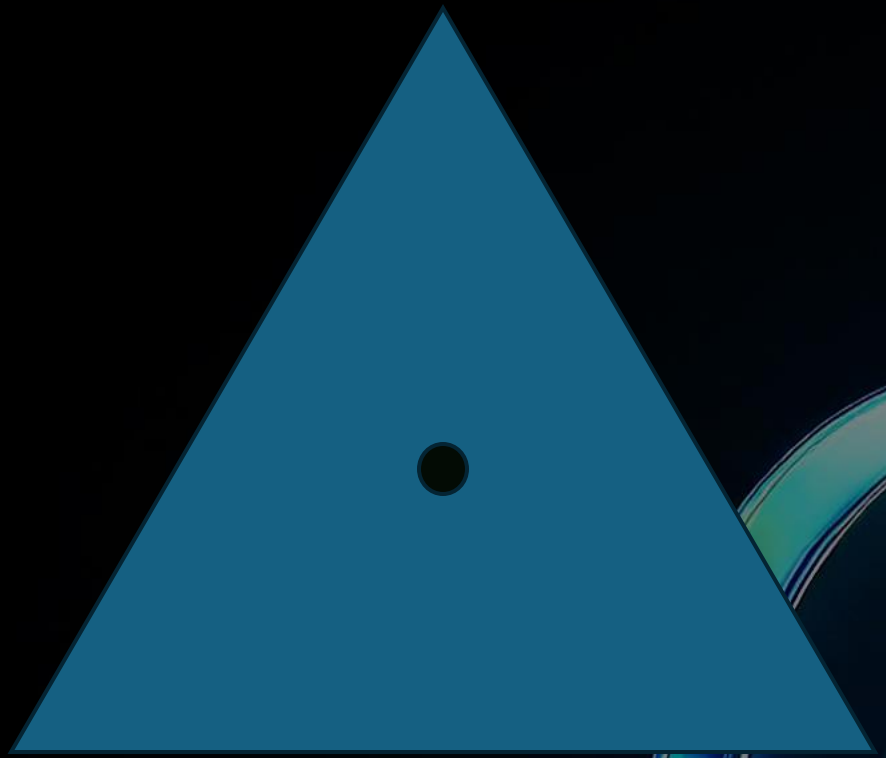
Takeaways:

1. Defining Zero Trust
2. Practical Frameworks to apply
3. Key Recommendations



Laying the Foundation

Security

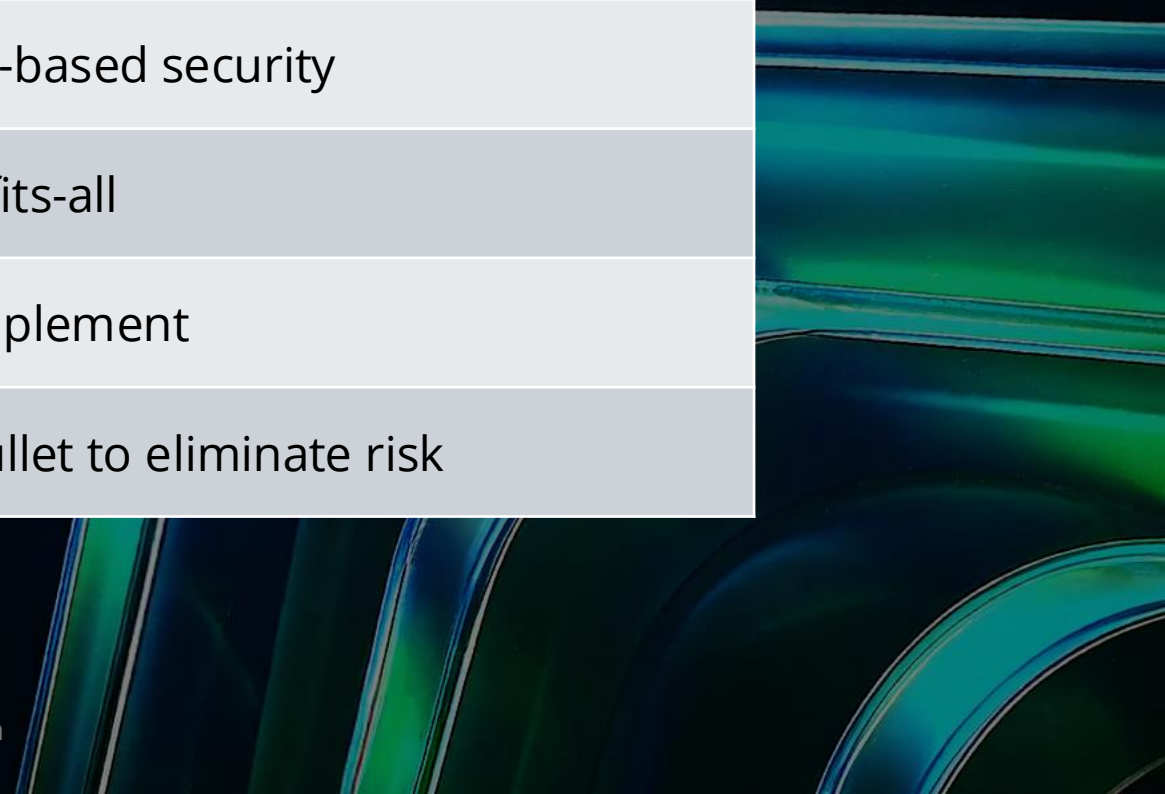


Functionality

Usability

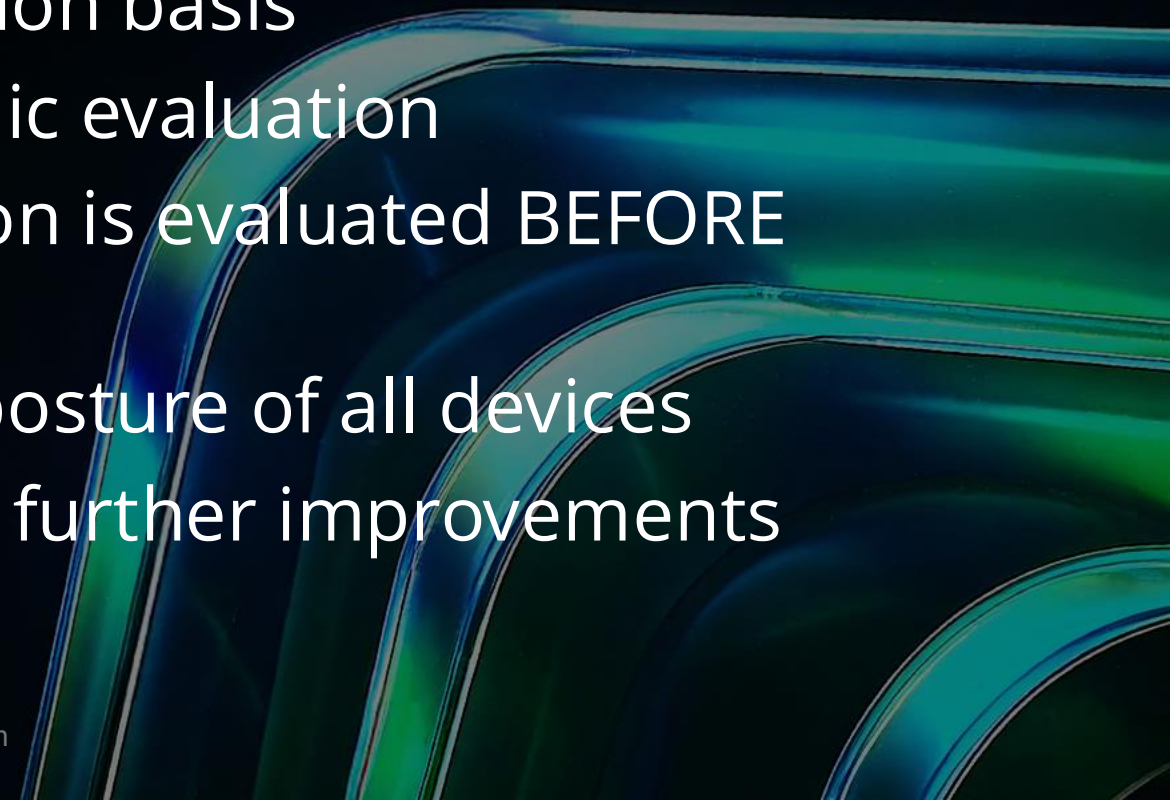
Defining Zero Trust

IS	IS NOT
A mentality/framework	A single product or technology
Data-focused	Perimeter-based security
Proactive	One-size-fits-all
Identity-centric	Easy to implement
Dynamic	A silver bullet to eliminate risk



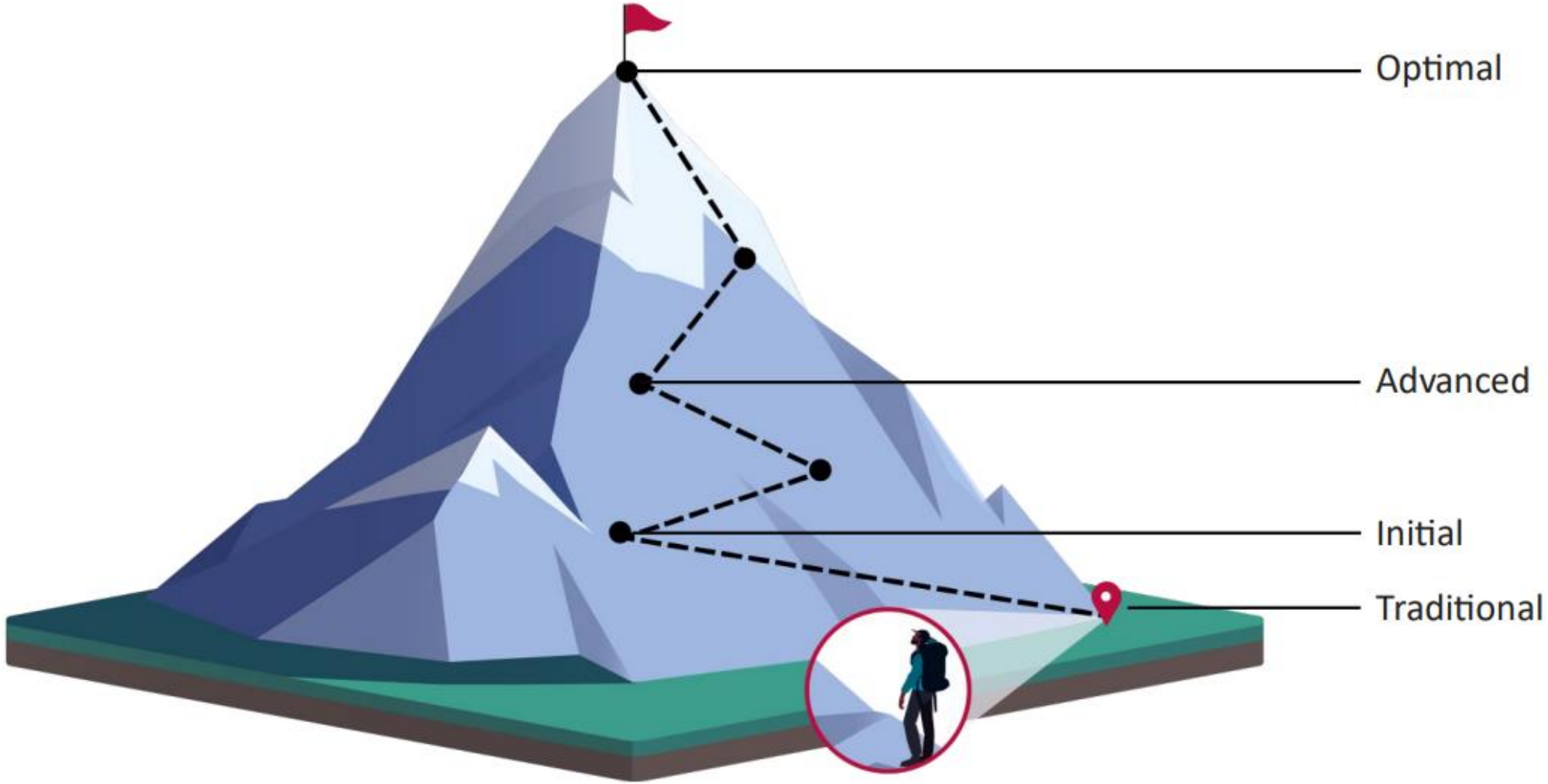
Zero Trust Tenets

1. All resources must be considered
2. Location should be considered irrelevant
3. Access is granted on a per-session basis
4. Access is determined by dynamic evaluation
5. Authentication and authorization is evaluated BEFORE access is allowed
6. Monitor integrity and security posture of all devices
7. Develop baseline of network to further improvements

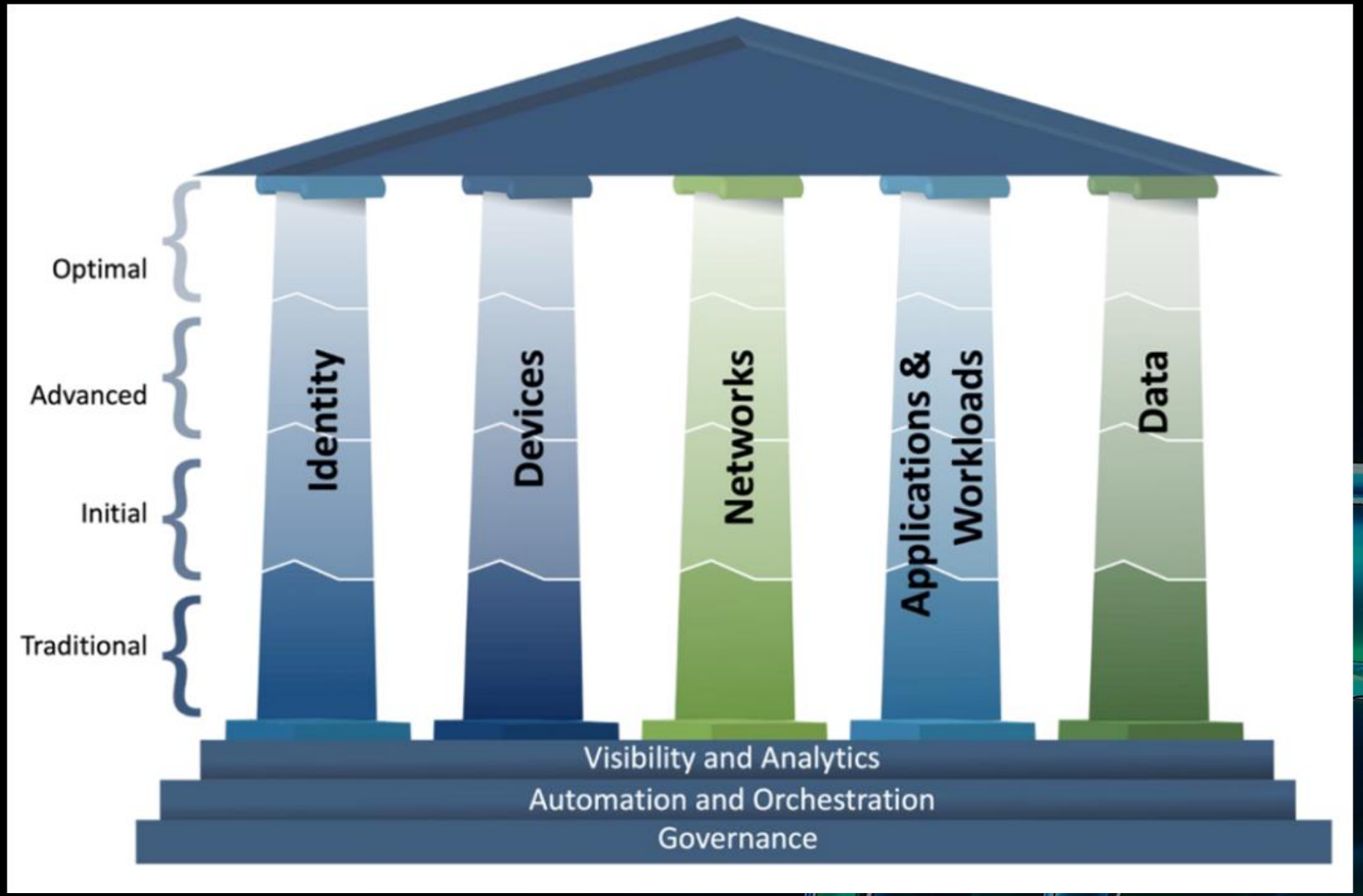


The Climb to Success

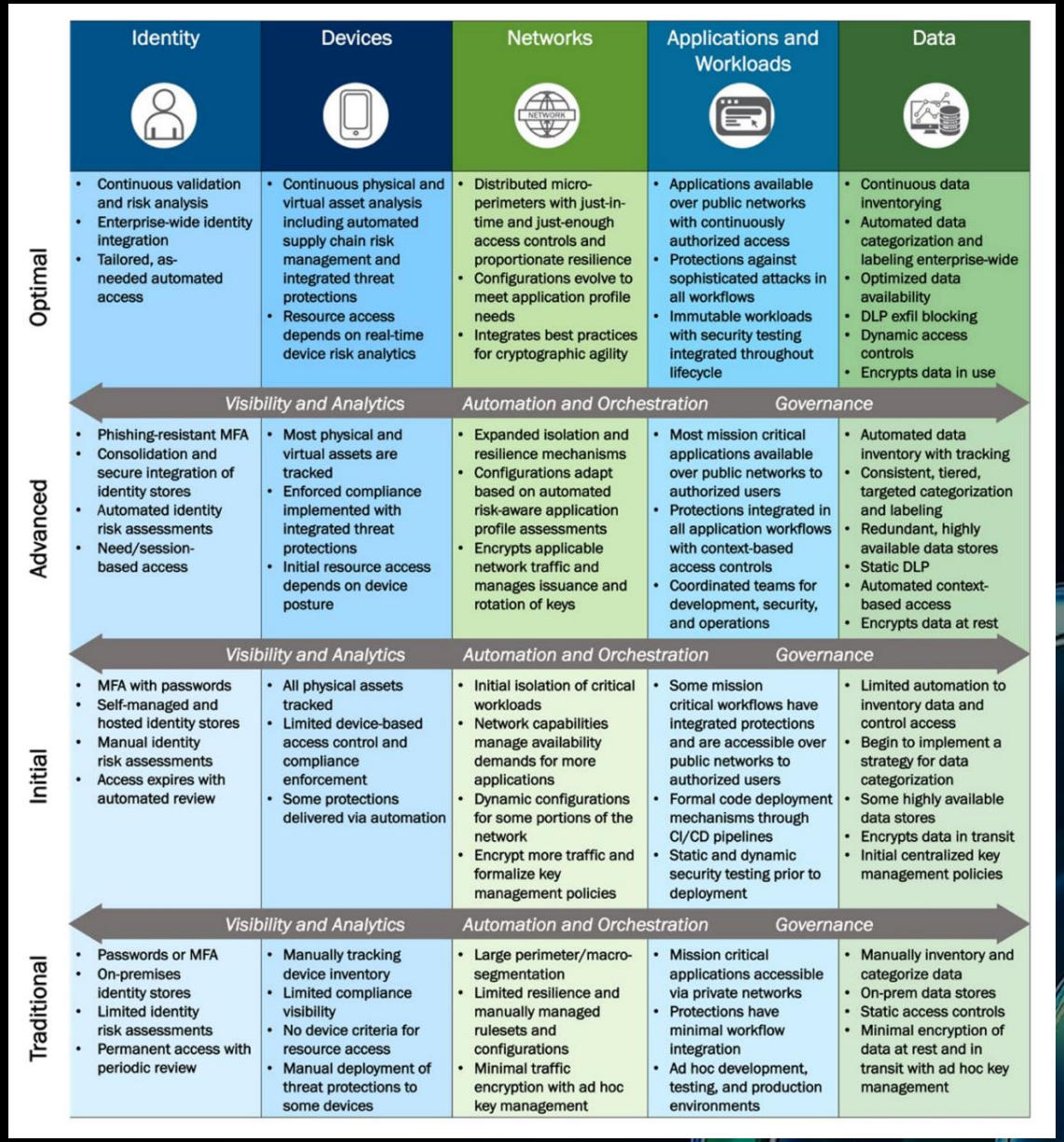
Zero Trust Maturity Journey



Cybersecurity and Infrastructure Security Agency, 2023)



(Cybersecurity and Infrastructure Security Agency, 2023)

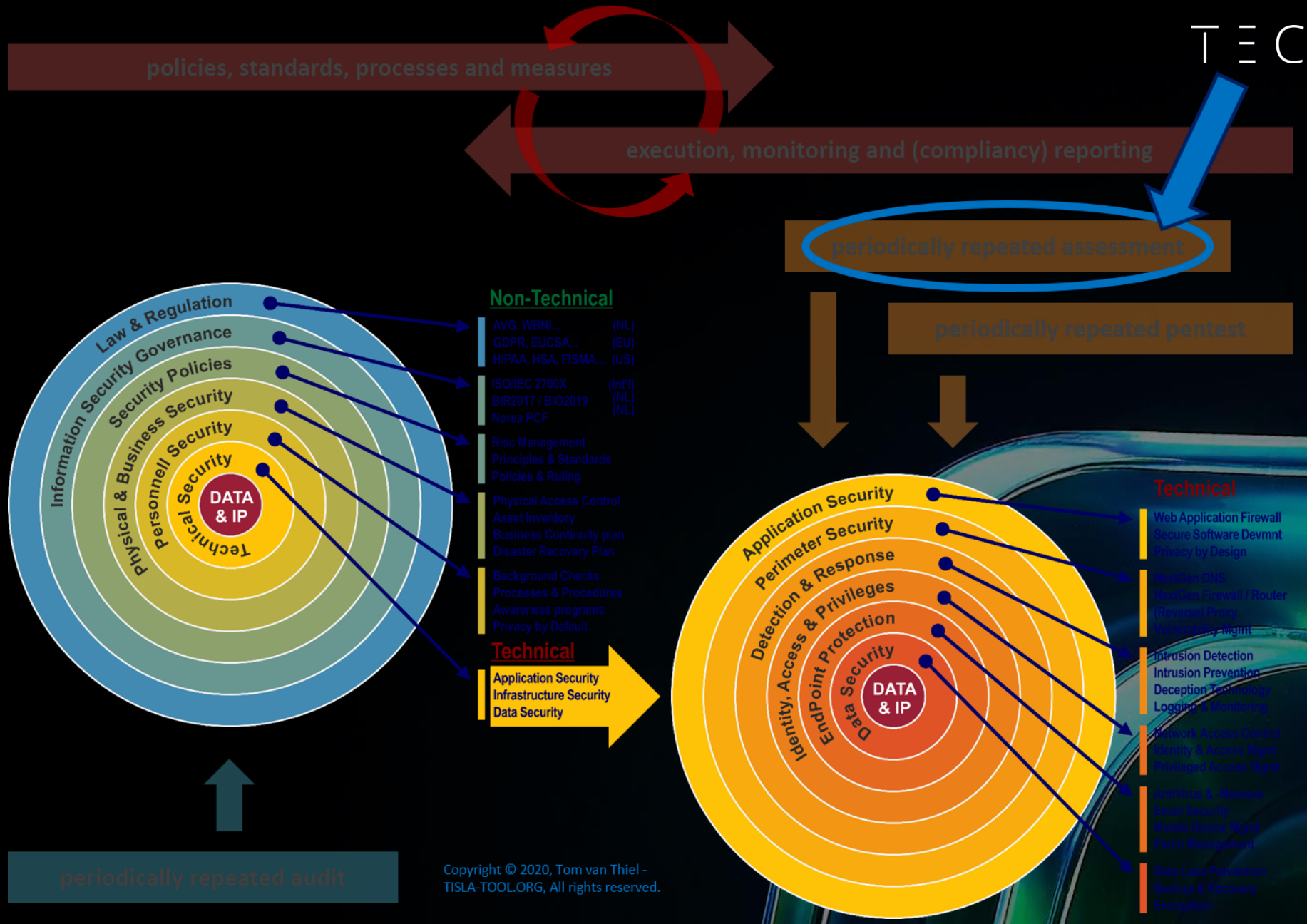


	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

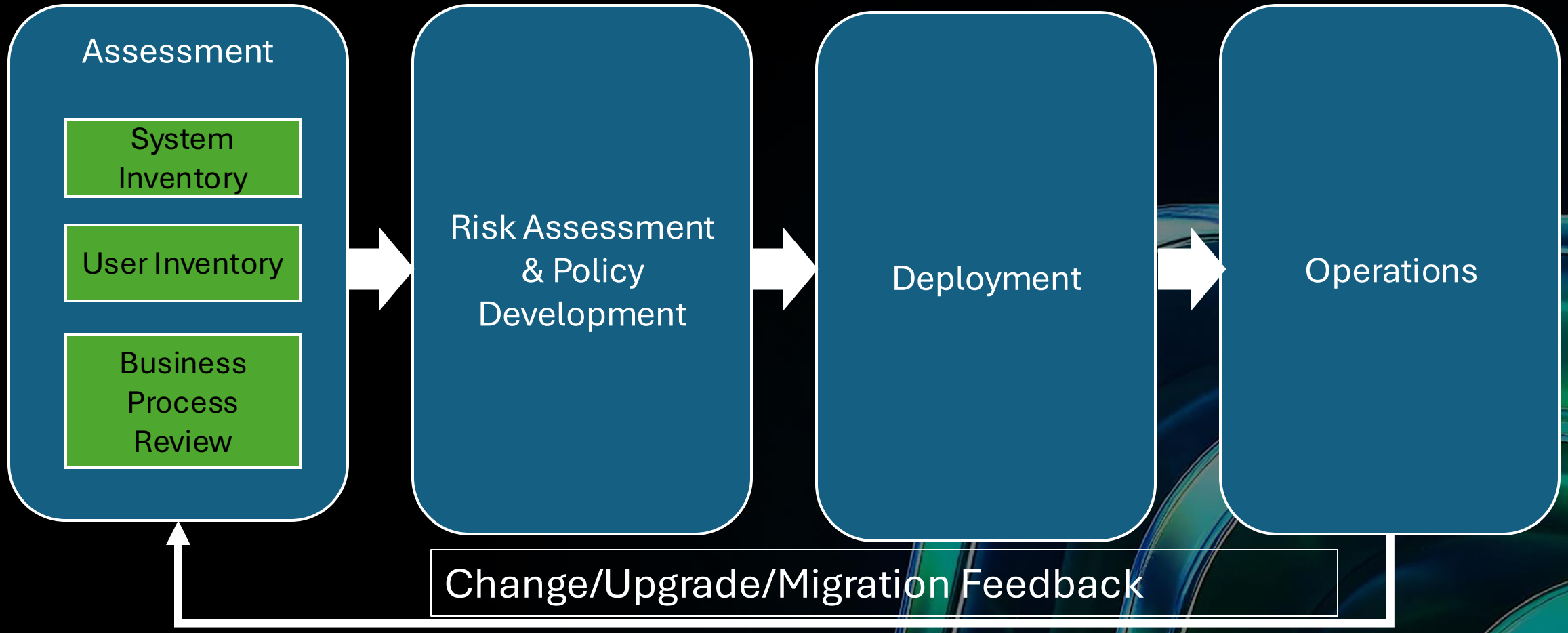
(Cybersecurity and Infrastructure Security Agency, 2023)

Structural Support

TECH CON



NIST SP 800-207 Deployment Cycle



CIT's Practical Implementation Plan

TECH CON

1. Define Strategy
2. Inventory Resources
3. Define Scope

4. Enhance Device Security
5. Network Segmentation
6. Implement IAM

7. Implement SIEM
8. Deploy DLP
9. Automate Processes

10. Monitor & Adapt

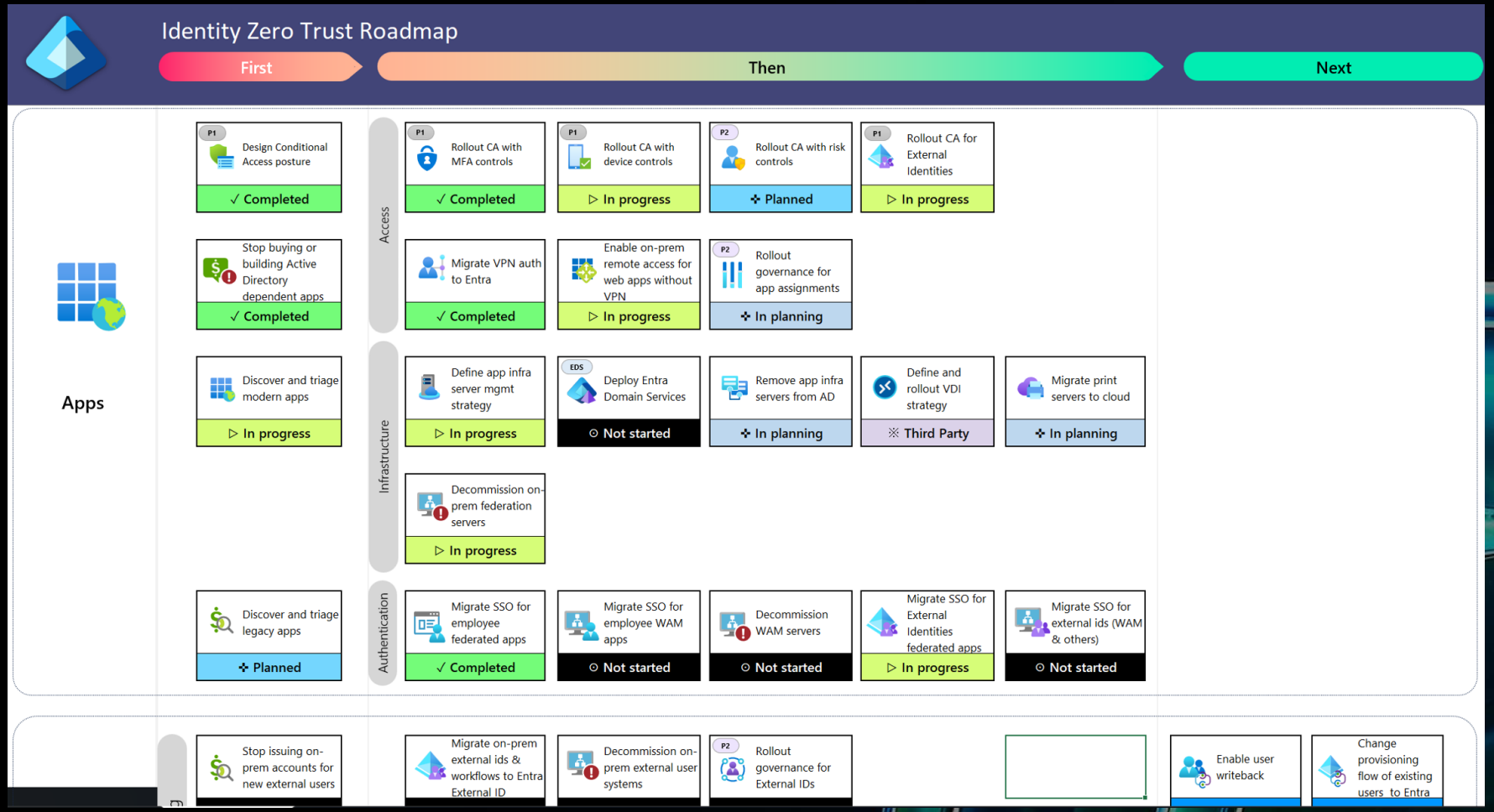
Foundation & Strategy → Core Security Infrastructure → Advanced Capabilities → Continuous Improvement

What's Next?

Core Security Recommendations

- Phishing Resistant MFA
- Endpoint Detection & Response (EDR)
- Application Allowlisting
- Privileged Access Management
- Zero Trust Network Access (ZTNA)
- Network Access Control (NAC)
- Security Awareness Training
- BCDR Review

Free Microsoft Resource



TECH CON

LET’S CONNECT

Nate Schmitt

www.cit-net.com

nate.schmitt@citsolutions.net

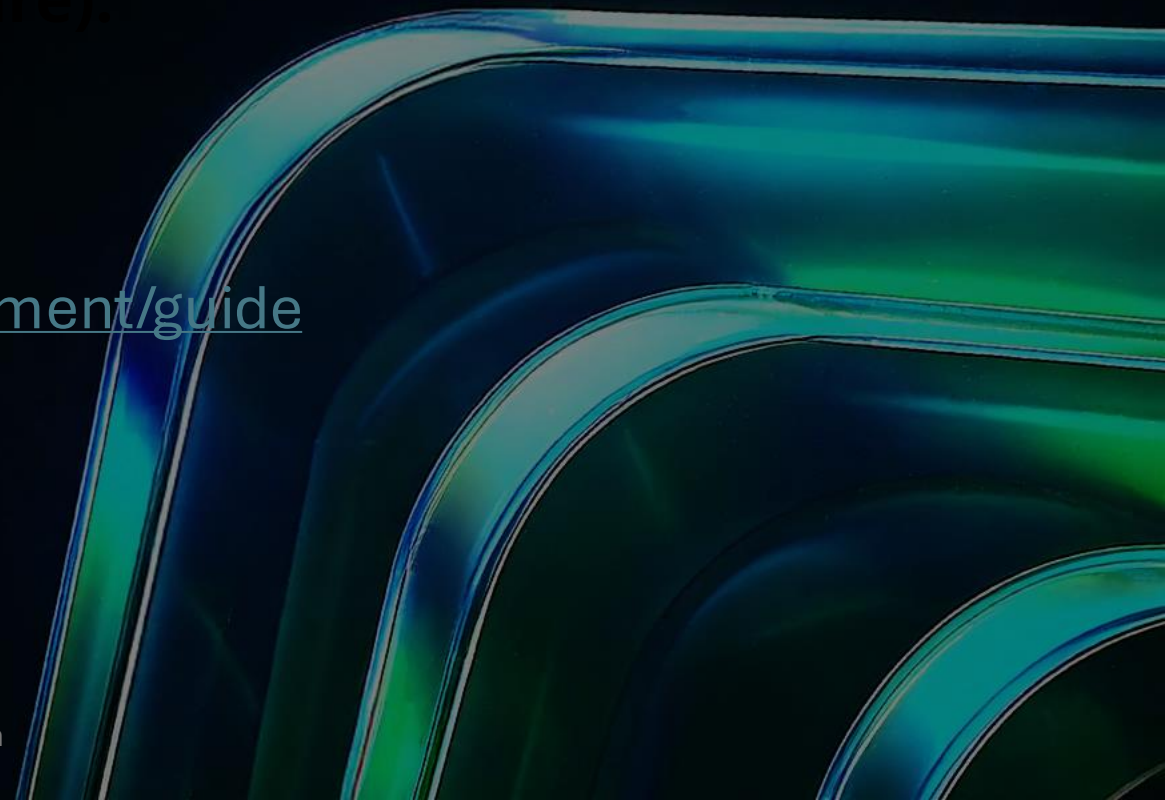
651.255.5773

Resources

https://www.cisa.gov/zero-trust-maturity-model

https://csrc.nist.gov/pubs/sp/800/207/final

https://microsoft.github.io/zerotrustassessment/guide



Grand Ballroom

Lunch

Grab food in the Grand Foyer & head on in!