Understanding Zero Trust through the Cyber Defense Matrix

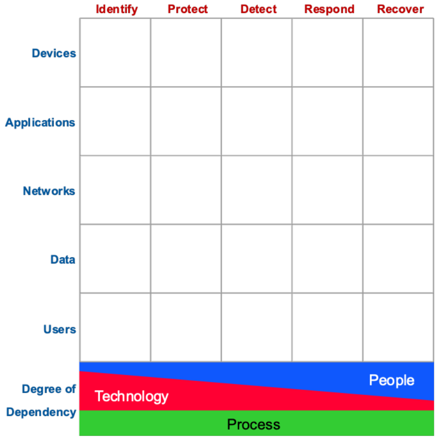
Sounil Yu

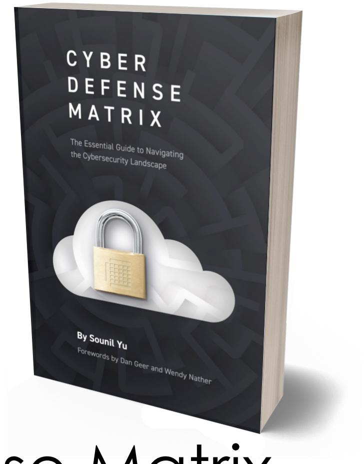
$whoami

Currently: Security Ambassador at JupiterOne

Formerly: Chief Security Scientist at BANK OF AMERICA

Creator of:

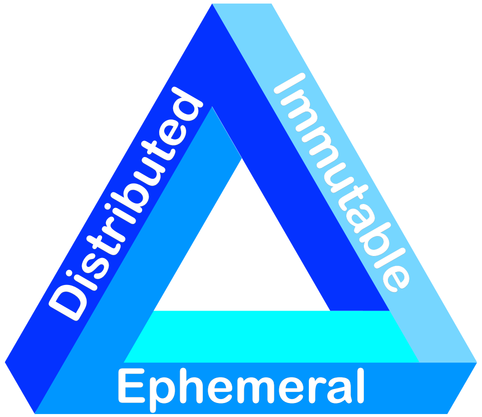




CYBER DEFENSE MATRIX
The Essential Guide to Navigating the Cybersecurity Landscape
By Sounil Yu
Forewords by Dan Geer and Wendy Nather

Cyber Defense Matrix

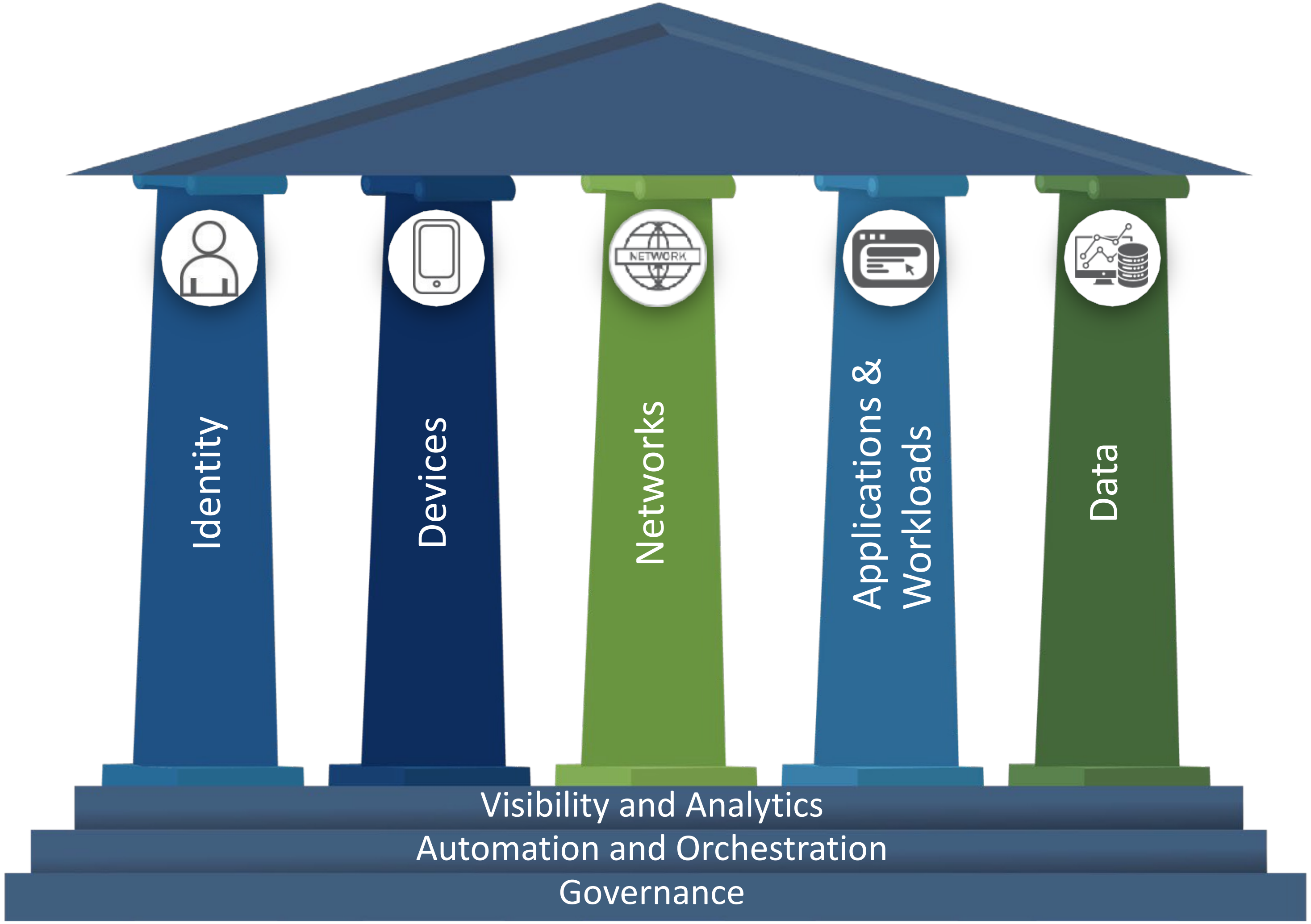
https://cyberdefensematrix.com



DIE Triad

https://dietriad.com

CISA’s Zero Trust Maturity Model Framework
(August 2021)



Visibility and Analytics

Automation and Orchestration

Governance

Cyber Defense Matrix
(February 2016)

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect **to** Protect

SESSION ID: PDIL-W02F

Understanding the Security Vendor Landscape Using the Cyber Defense Matrix

Sounil Yu
sounil@gmail.com
@sounilyu

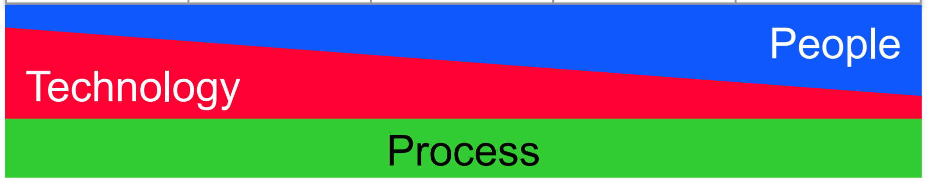
Model Shortfalls: Where is analytics? GRC? Orchestration?

#RSAC

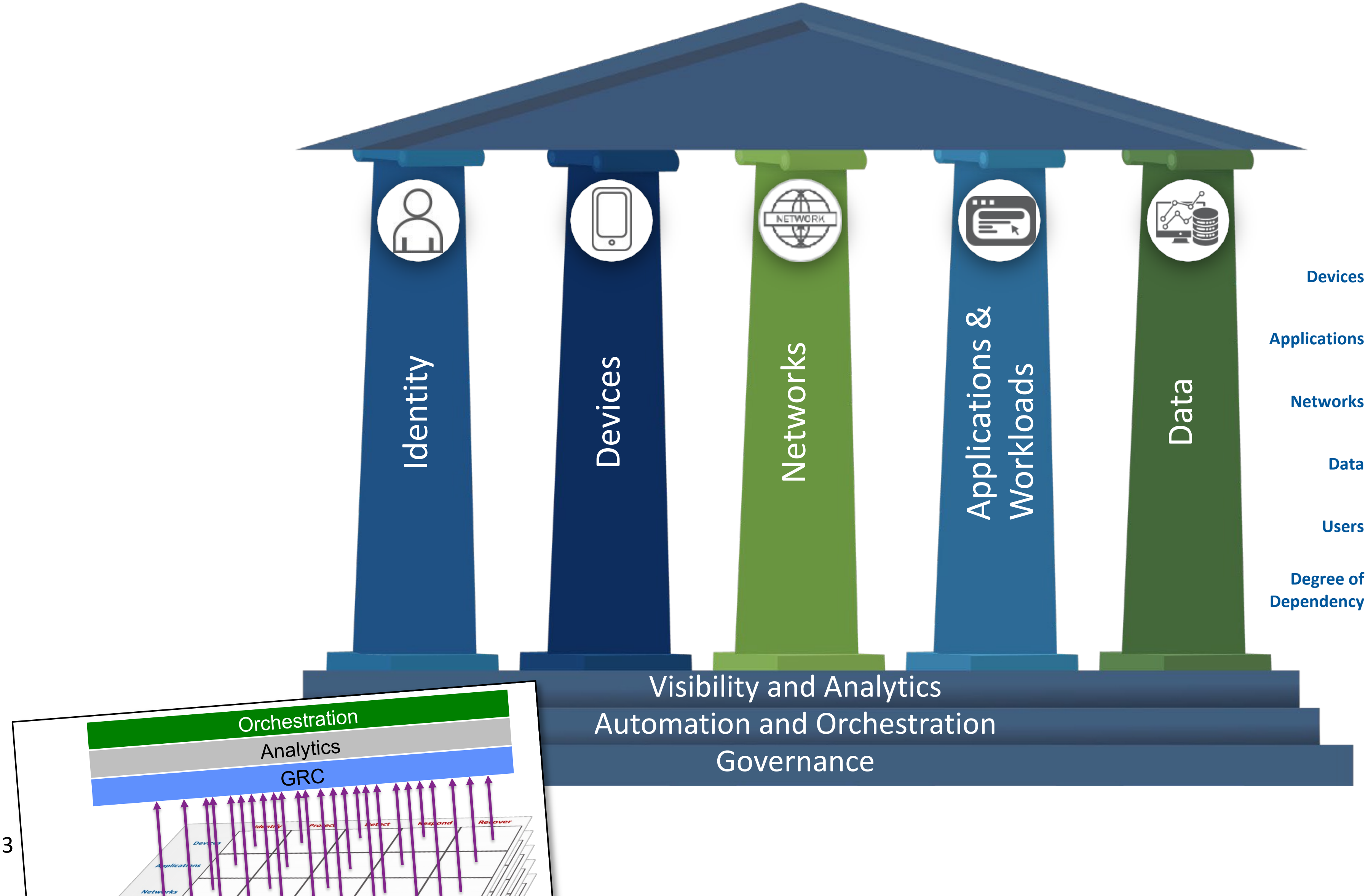
This framework supports the higher level functions of orchestration, analytics, and governance/risk/compliance, but they are represented on a different dimension

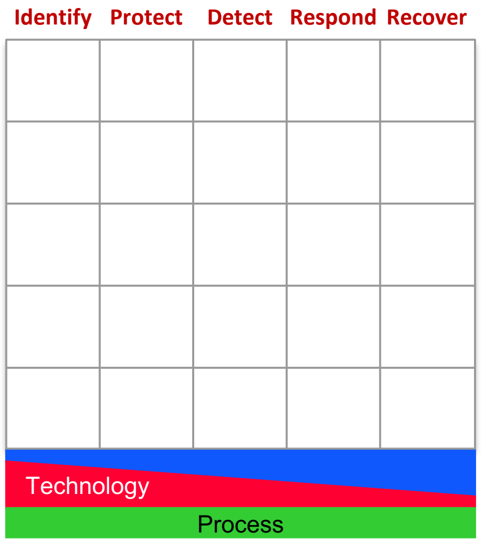
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

Degree of Dependency



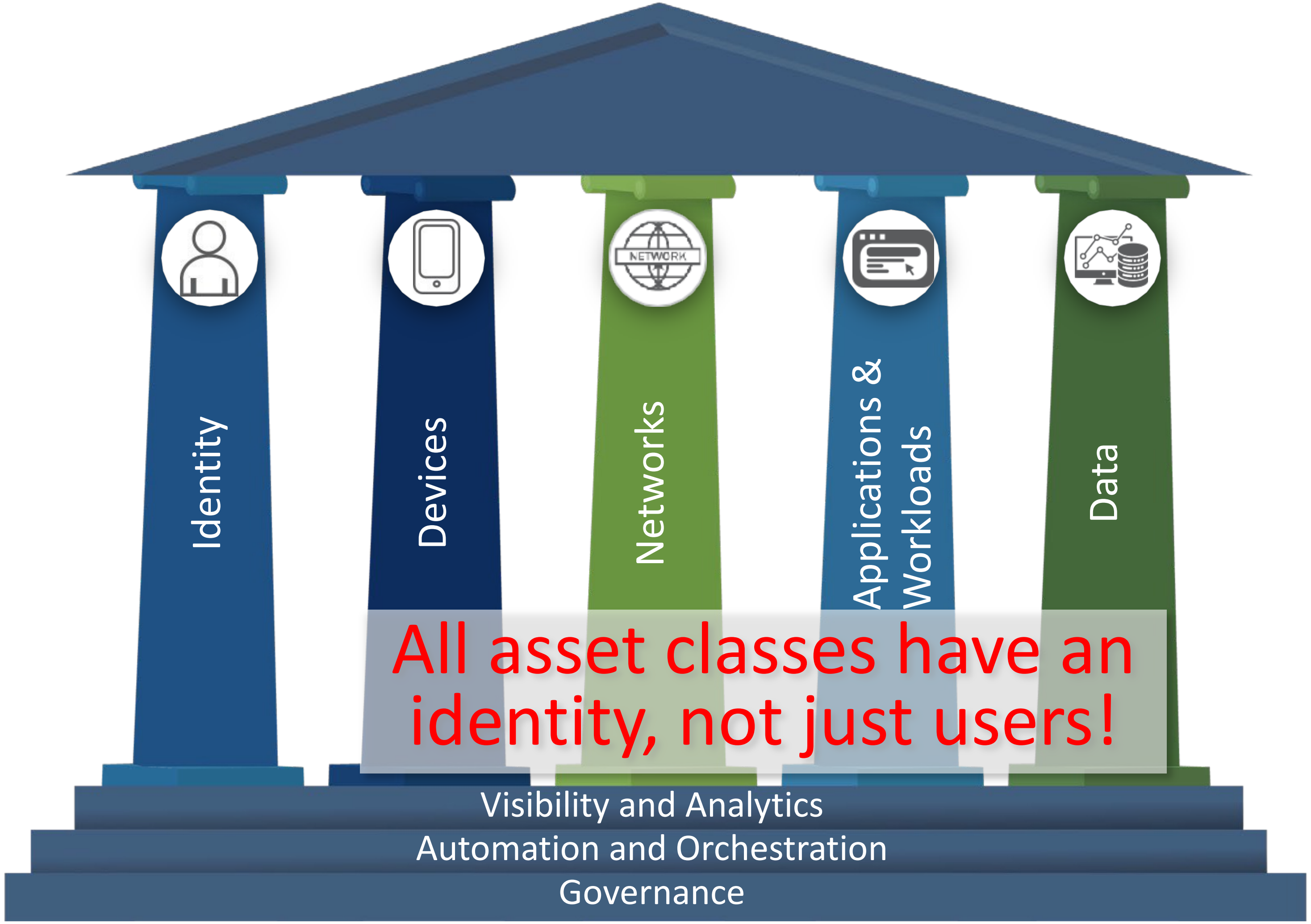
CISA's Zero Trust Maturity Model Framework





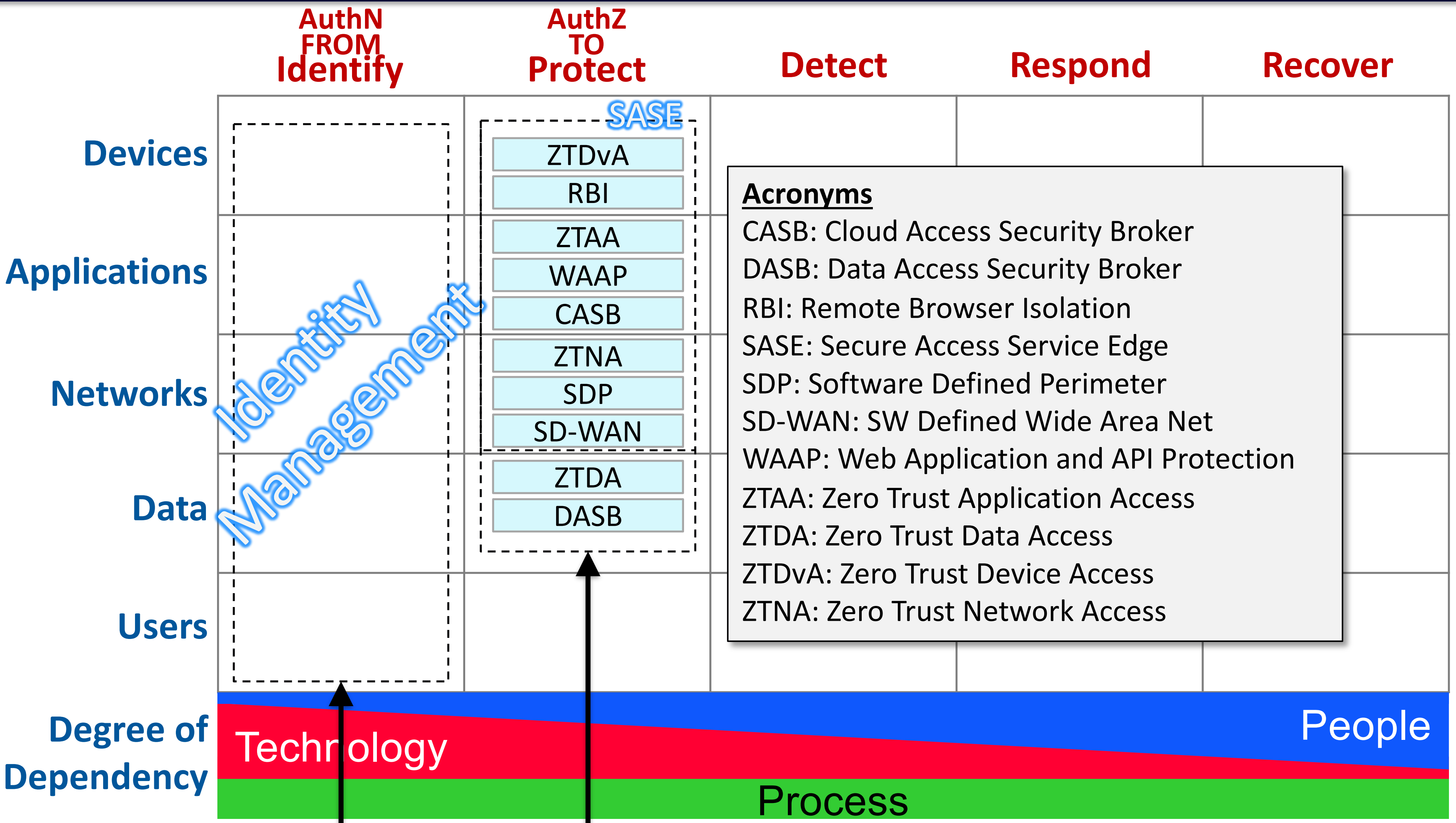
	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

All assets have an identity



All asset classes have an identity, not just users!

How Zero Trust fits into the Matrix



	AuthN FROM Identify	AuthZ TO Protect	Detect	Respond	Recover
Devices	Identity Management	SASE ZTDvA RBI			
Applications		ZTAA WAAP CASB			
Networks		ZTNA SDP SD-WAN			
Data		ZTDA DASB			
Users					
Degree of Dependency	Technology		People		

Acronyms

CASB: Cloud Access Security Broker

DASB: Data Access Security Broker

RBI: Remote Browser Isolation

SASE: Secure Access Service Edge

SDP: Software Defined Perimeter

SD-WAN: SW Defined Wide Area Net

WAAP: Web Application and API Protection

ZTAA: Zero Trust Application Access

ZTDA: Zero Trust Data Access

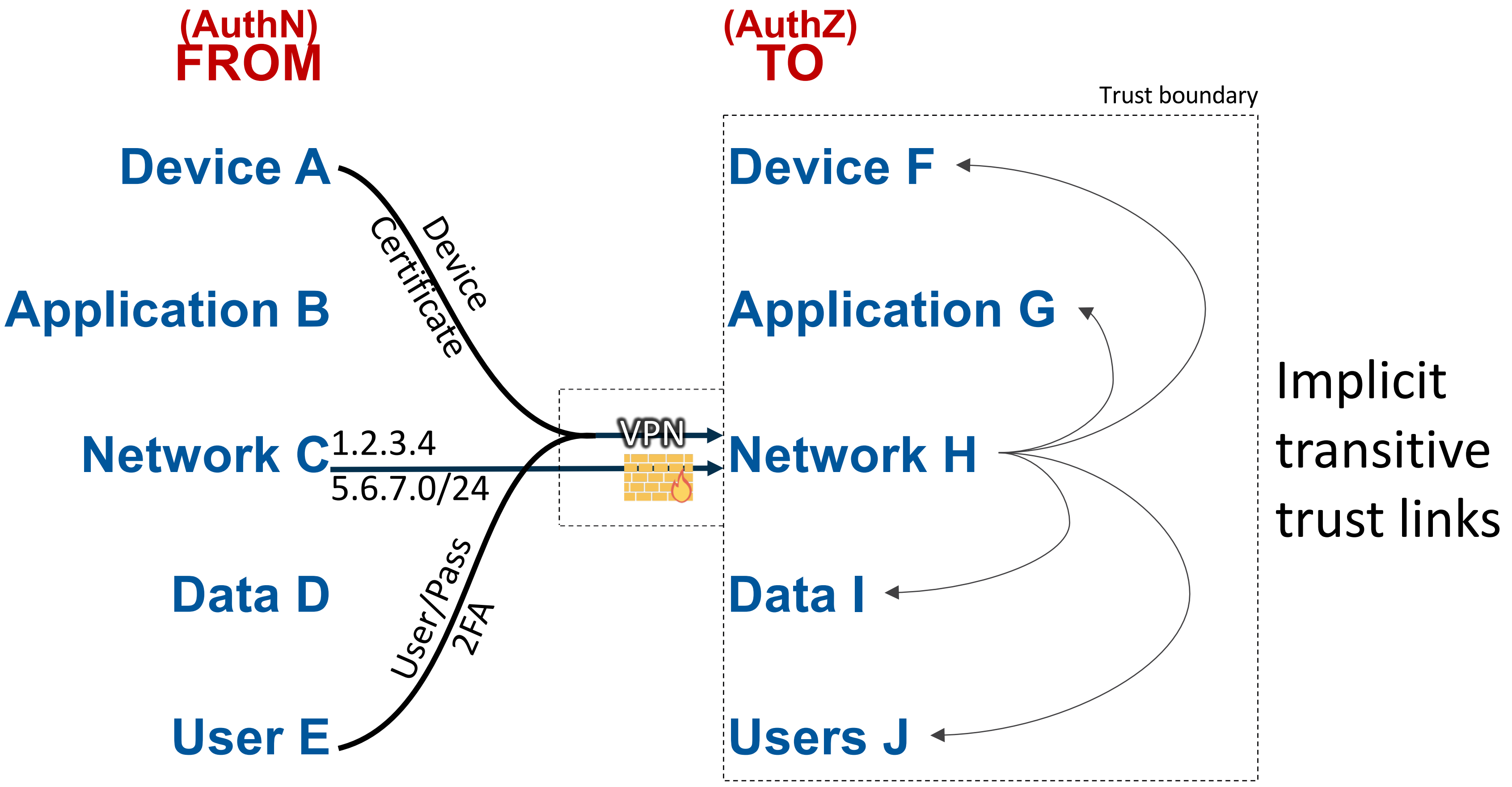
ZTDvA: Zero Trust Device Access

ZTNA: Zero Trust Network Access

Establishes trustworthiness
of the requestor

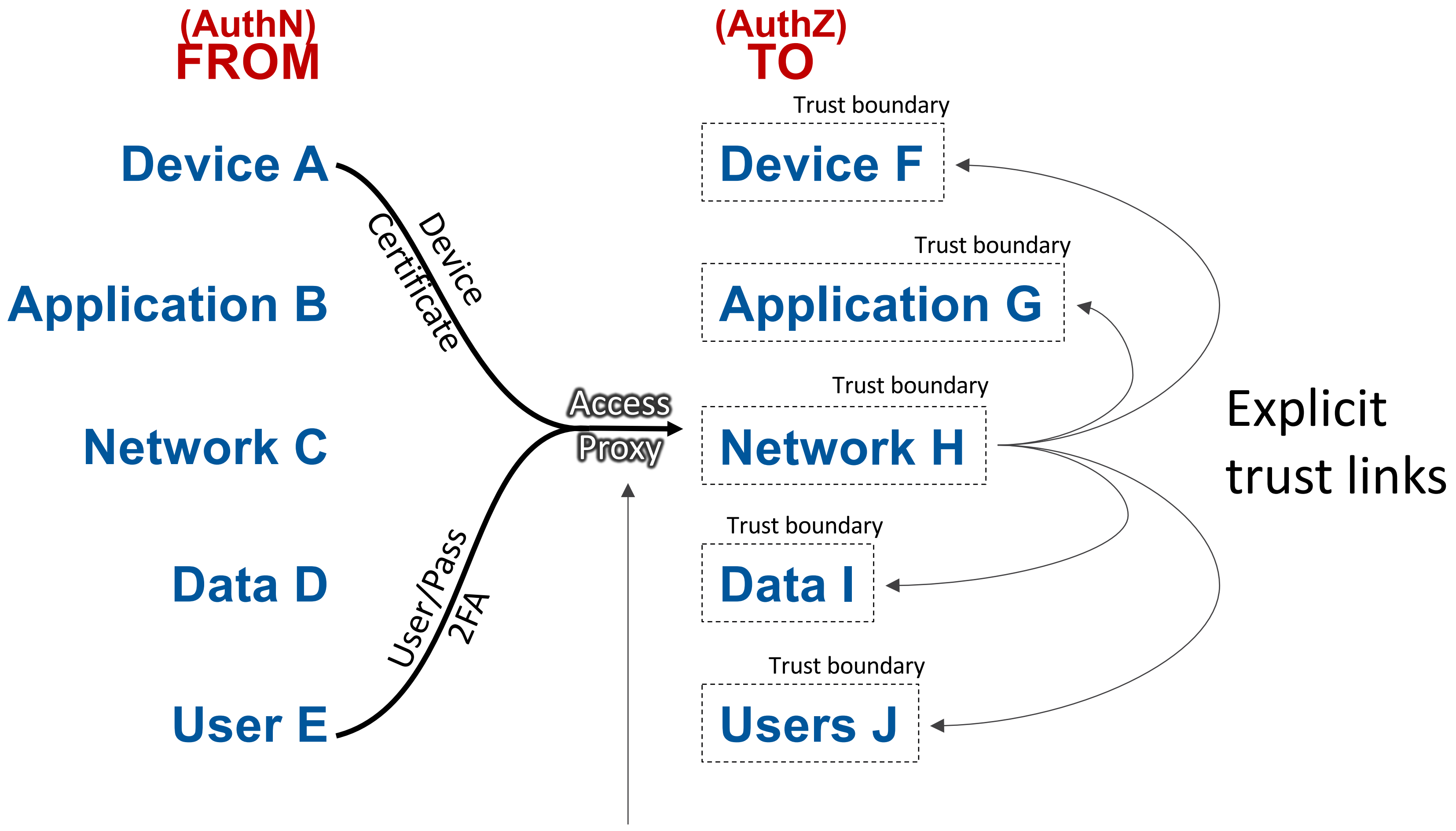
Enforces access policy based on trustworthiness
and other environmental and behavioral factors

The network perimeter is dead! Love live the perimeter!



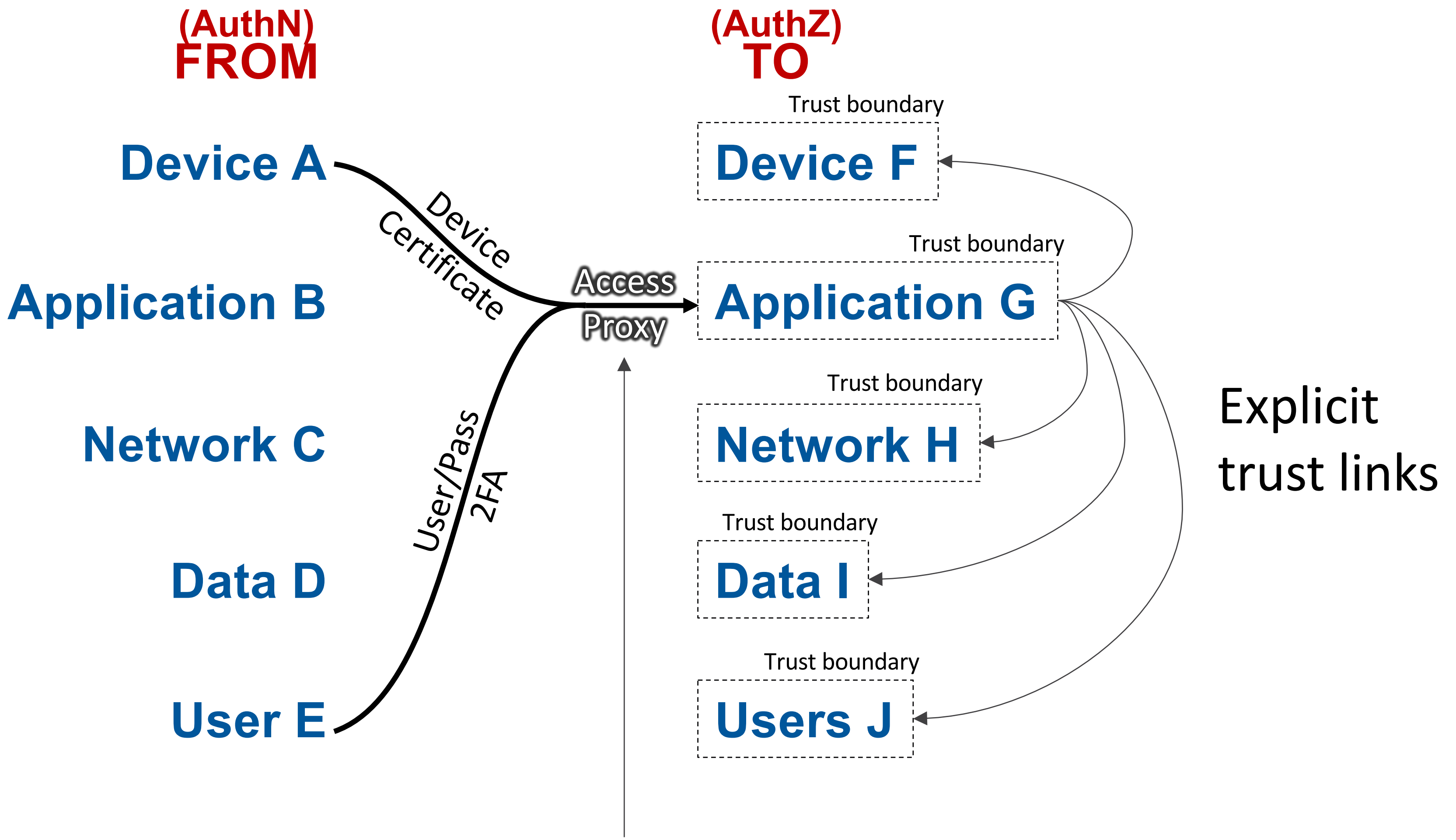
Implicit transitive trust links

The network perimeter is dead! Love live the microsegmented perimeter!



Zero Trust Network Access (ZTNA)

The network perimeter is dead! Love live the microsegmented perimeter!



(AuthN)
FROM

(AuthZ)
TO

Device A

Application B

Network C

Data D

User E

Device Certificate

User/Pass 2FA

Access Proxy

Trust boundary
Device F

Trust boundary
Application G

Trust boundary
Network H

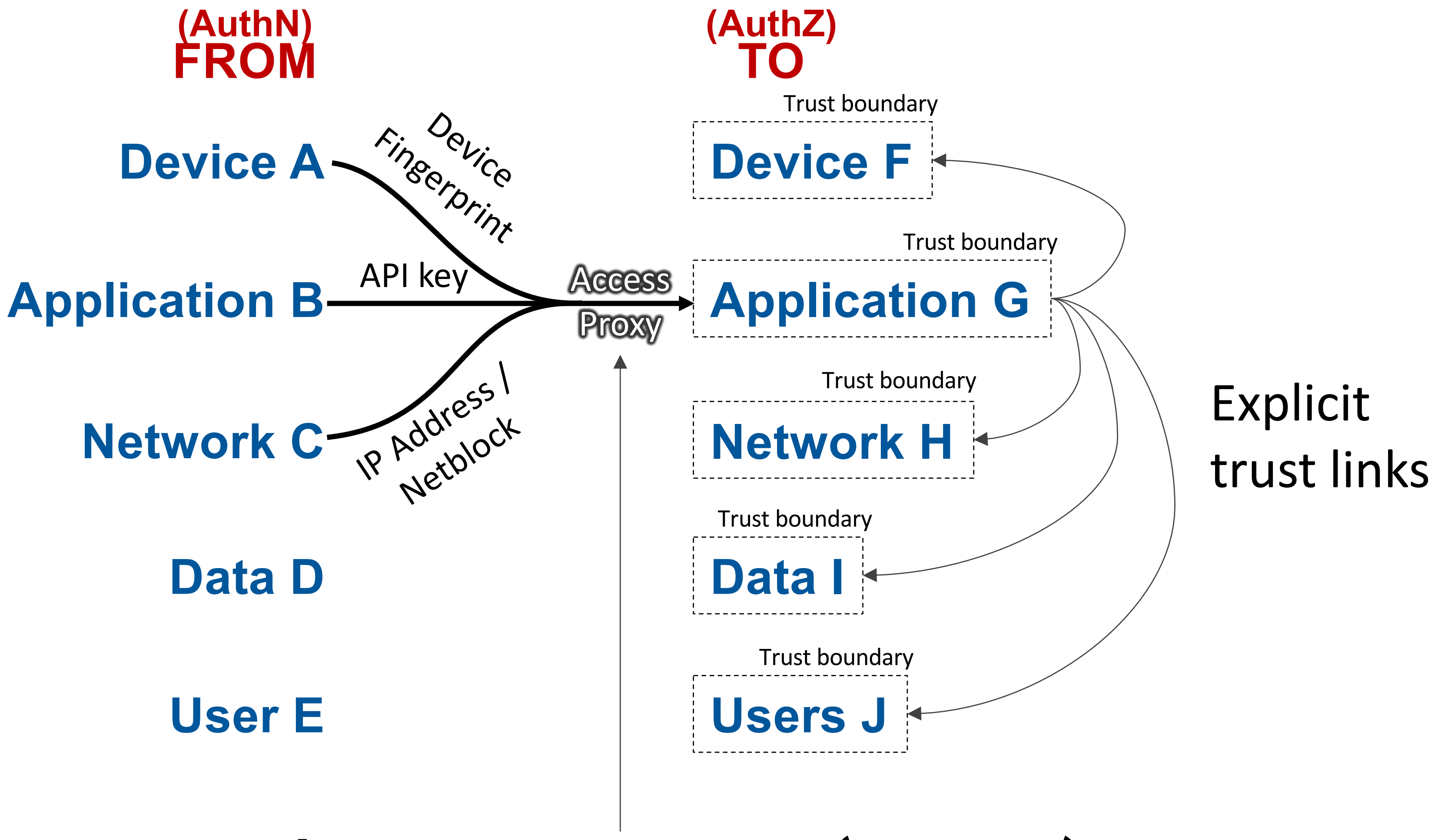
Trust boundary
Data I

Trust boundary
Users J

Explicit trust links

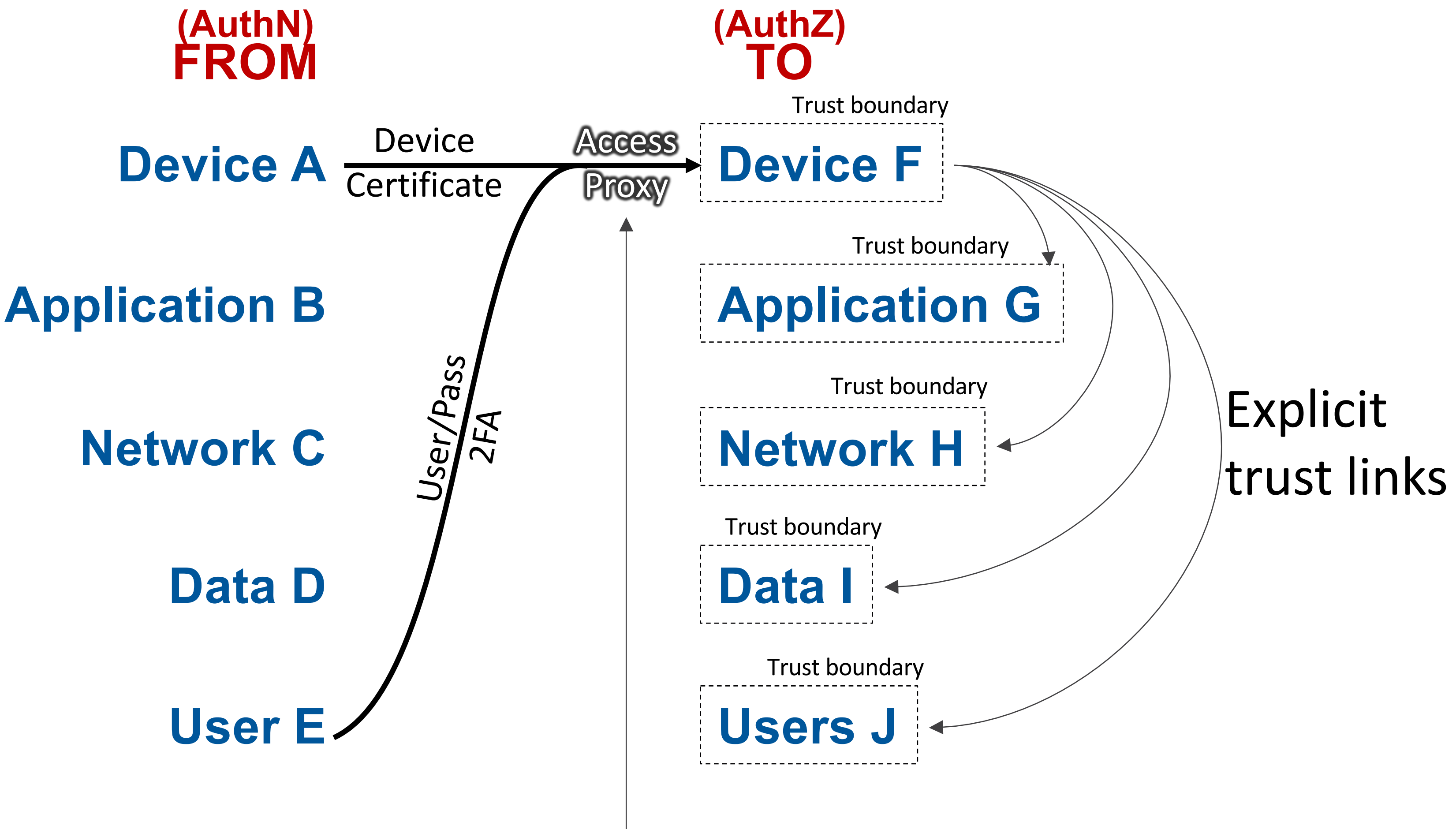
Zero Trust Application Access (ZTAA) – Web App focused

The ^network perimeter is ^not dead! Love live the ^microsegmented perimeter!



Web Application and API protection (WAAP)

The ^network^ perimeter is dead! Love live the ^microsegmented^ perimeter!



Zero Trust Device Access (ZTDvA) – SSH, RDP, VNC, telnet
Remote Browser Isolation

The perimeter is not dead! Love live the perimeter!

Device Certs, Fingerprint, Security status

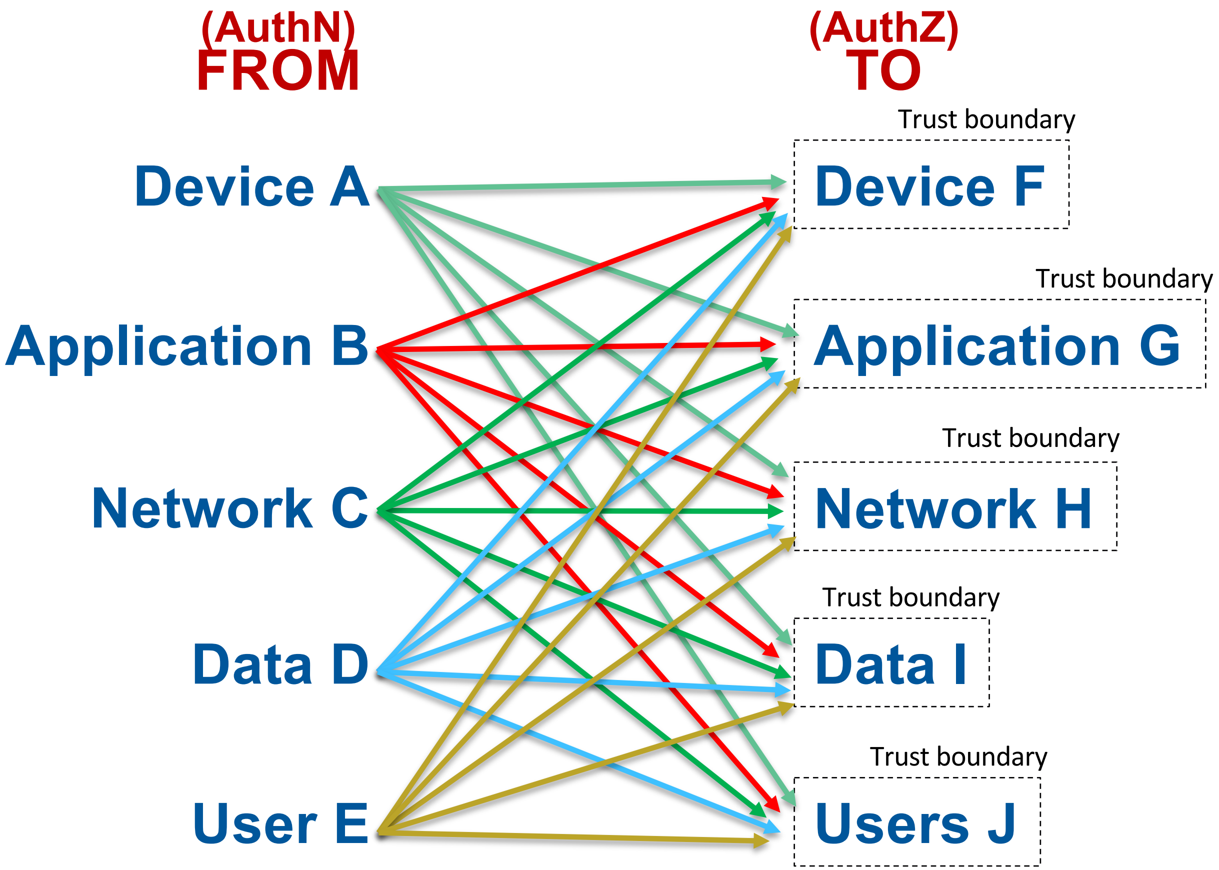
Mutual TLS Certs, API Keys, Browser Headers

IP Address, Identity-Based IP

Hashes, Checksums, Data Classification

PWs, Tokens, 2FA, Location, Employment status

Example Identity Attributes to Establish Trustworthiness



An identity-centric perimeter is more than just a user-centric perimeter

Device-centric ZTDA Proxy, RBI, VDI, Host-based FW

Webapp-centric ZTAA Proxy, API Gateway

ZTNA, Microseg, Firewall, VPN, Single Packet AuthN

Data Access Security Broker, Data Access Proxy

Executive Assistant, Skeptical Brain

Example Access Policy Enforcement Mechanisms

Defining acceptable trustworthiness

(How “zero” is your Zero Trust?)

	Trustworthiness Scale*	
Any Device	**0** 1 2	Devices fully controlled and configured by enterprise
Any Software	0 **1** 2	Only authorized software signed by trusted entities
Any Network	**0** 1 2	Private, fully authenticated network
Any Data	0 1 **2**	Trusted Execution Environment
Any User	0 1 **2**	Fully vetted individuals w/Polygraph and DNA samples

Relative Cost to Implement = $10^{(\text{trustworthiness value})}$

The level of trustworthiness varies for each use case

	Bank Account Login Page	**Outlook Web Access**	**Virtual Desktop Infrastructure**	**PII Database**
Device	[✓ 0] 1 2 Any device	0 [✓ 1] 2 Device cert	0 [✓ 1] 2 Device cert	0 1 [✓ 2] Gold image machine
Apps	[✓ 0] 1 2 Any browser	[✓ 0] 1 2 Any browser	0 [✓ 1] 2 VDI app	0 1 [✓ 2] Whitelisted, signed apps
Network	0 [✓ 1] 2 Any non-blacklisted net	[✓ 0] 1 2 Any network	[✓ 0] 1 2 Any network	0 [✓ 1] 2 Corporate intranet
Data	[✓ 0] 1 2 Can save data locally	[✓ 0] 1 2 Can save data locally	0 [✓ 1] 2 No ability to save data	0 1 [✓ 2] Trusted Execution Env
User	0 [✓ 1] 2 User authenticated with correct username/pw	0 1 [✓ 2] User authenticated with MFA	0 1 [✓ 2] User authenticated with MFA	0 1 [✓ 2] User authenticated with MFA

Summary

- Study the Cyber Defense Matrix since it serves as the foundation for CISA's Zero Trust Maturity Model
- Leverage the fact that all types of requesting entities (e.g., devices, applications, networks, data, users) have an identity
- Determine the level of trustworthiness based on the strength of the identity attributes
- Implement "zero trust" access proxies that can consume the broader set of identity attributes for access decisions
- Calibrate what is an acceptable amount of trustworthiness (how "zero" is your zero trust?) for each use case

Questions?

@sounilyu

https://cyberdefensematrix.com

https://www.linkedin.com/in/sounil

https://www.slideshare.net/sounilyu/presentations