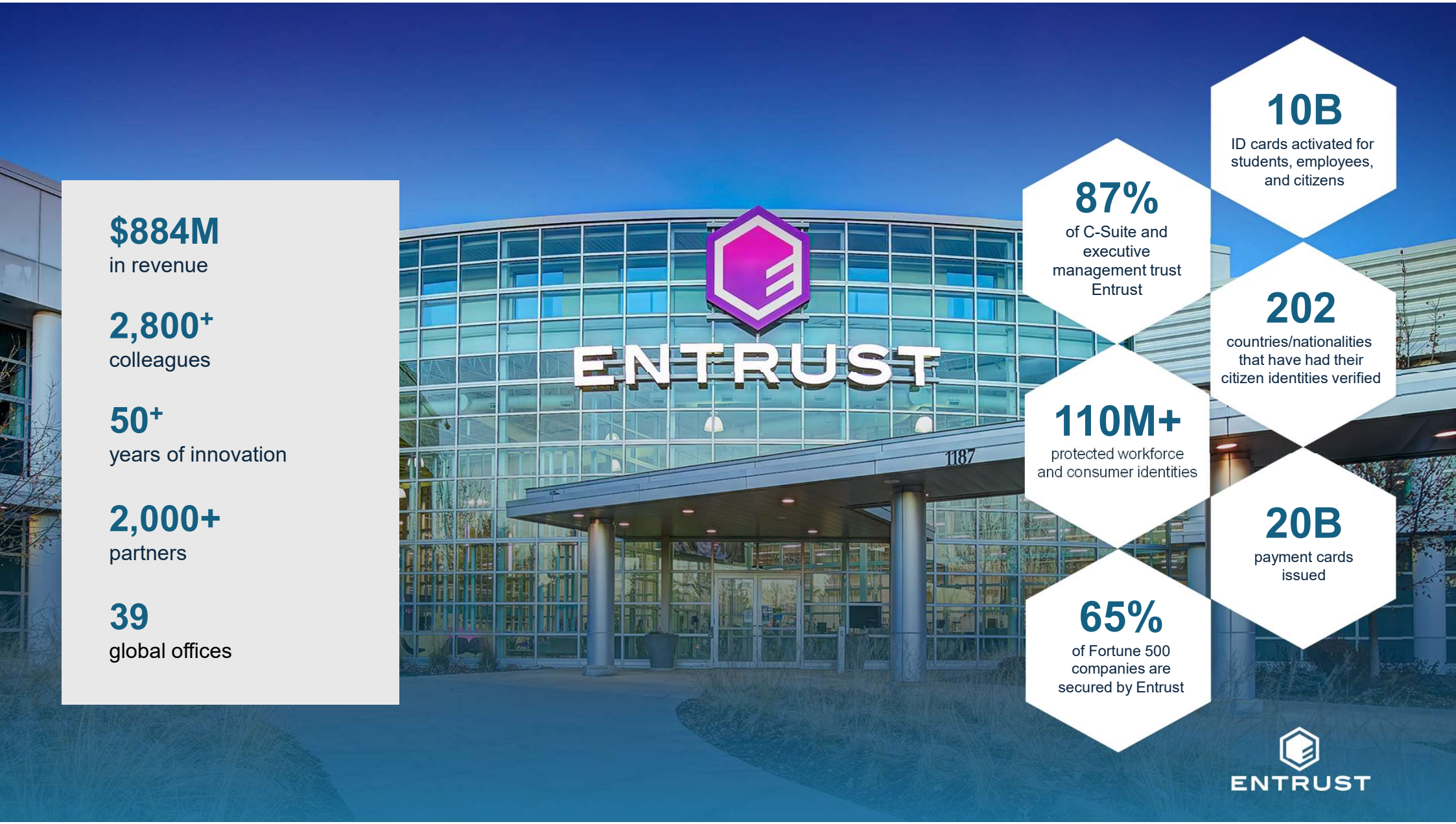
ENTRUST
Authentication/Identity



$884M
in revenue

2,800+
colleagues

50+
years of innovation

2,000+
partners

39
global offices

10B
ID cards activated for students, employees, and citizens

87%
of C-Suite and executive management trust Entrust

202
countries/nationalities that have had their citizen identities verified

110M+
protected workforce and consumer identities

20B
payment cards issued

65%
of Fortune 500 companies are secured by Entrust

ENTRUST

People, Process, Technology

CISA – ZERO TRUST MATURITY MODEL (V2.0)

Cybersecurity and infrastructure security agency (CISA)

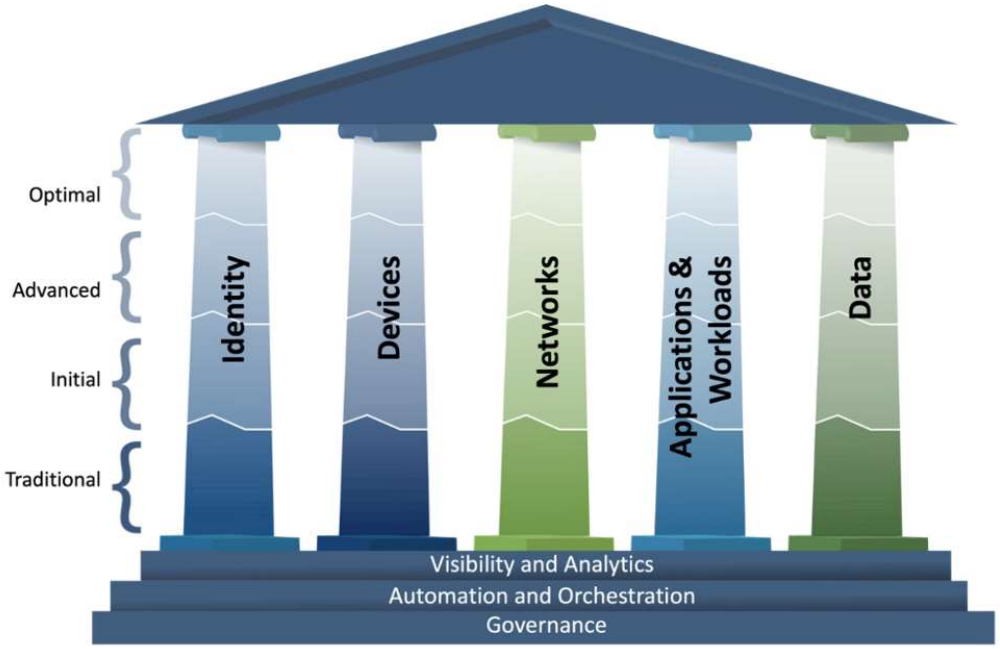
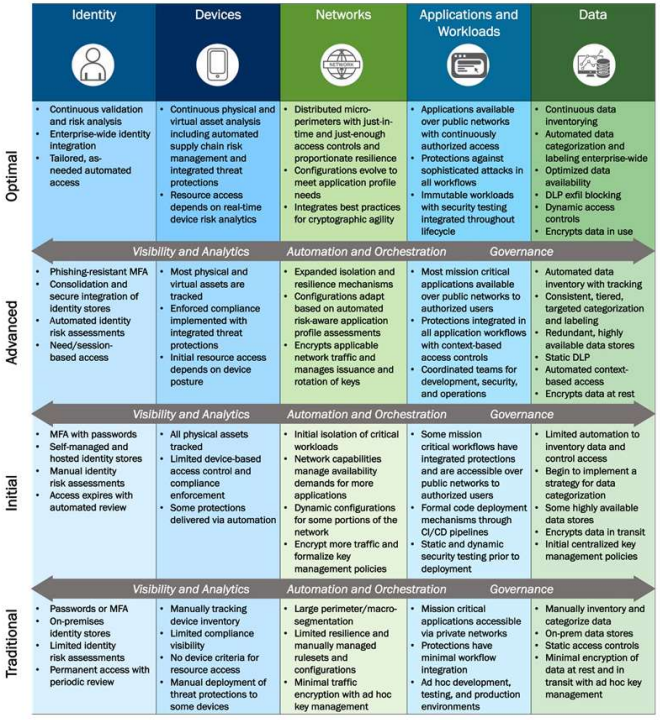


Figure 3: Zero Trust Maturity Evolution



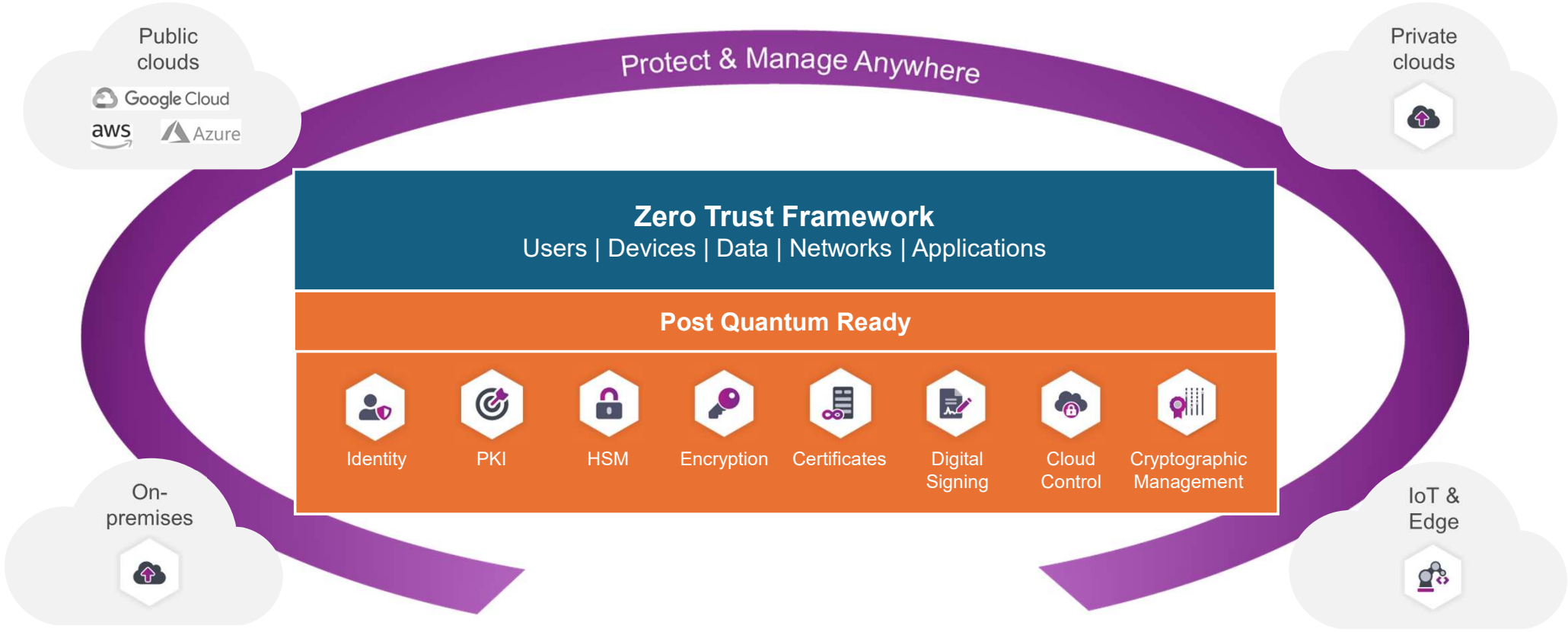
	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat 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

Figure 4: High-Level Zero Trust Maturity Model Overview

https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

JM0

ENTRUST ZERO TRUST SOLUTION



Folie 5

JM0 [@Rohan Ramesh] [@Samantha Mabey] [@Juan Asenjo] focus should be on ZT, but do we include a slide on PQ Ready and MC Sec? We'll cover PQ more in Q2.
John Metzger; 2023-05-04T12:52:38.688

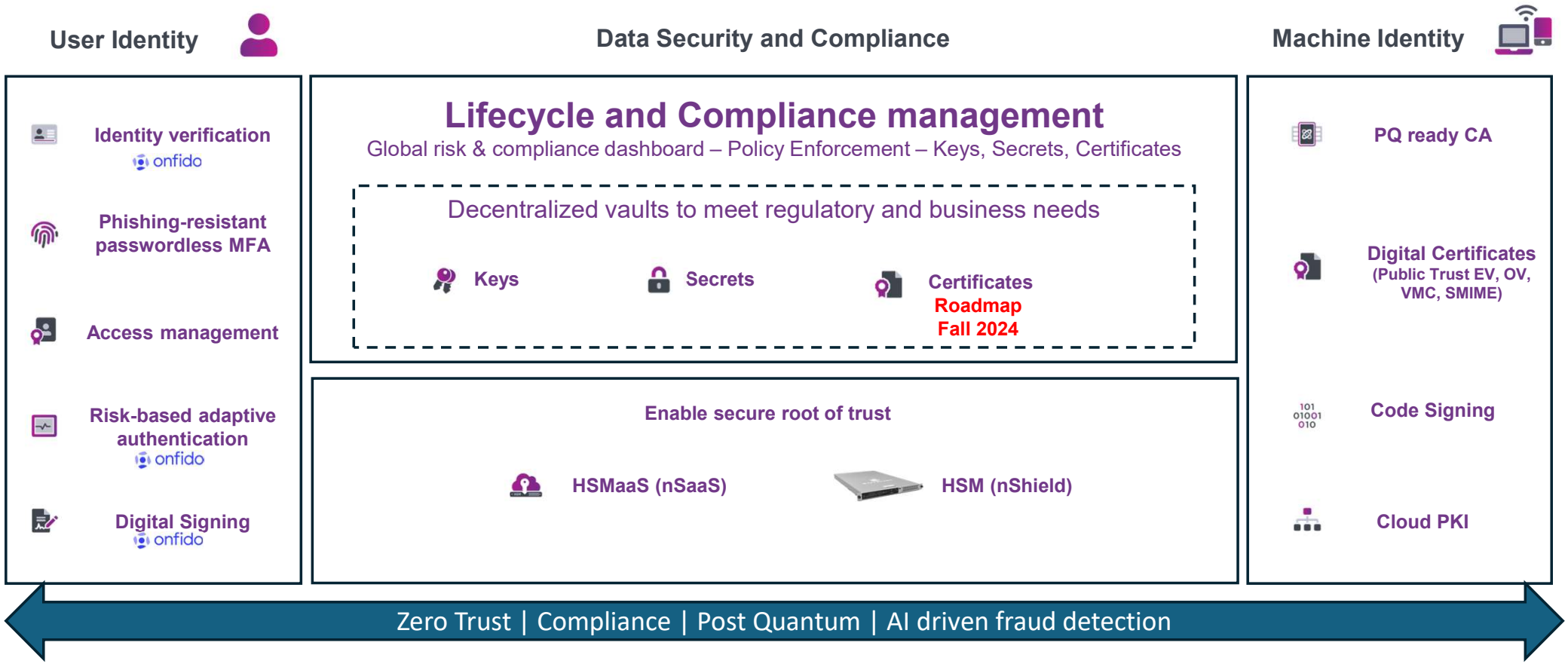
RR0 0 Robert was going to add a teaser at the end for PQ in Q2
Rohan Ramesh; 2023-05-04T14:07:23.002

JA0 1 [@John Metzger] Please note that the slide title still says Data and Networks. I suppose that changes to the new statement that Karen sent out?
Juan Asenjo; 2023-05-04T16:56:56.438

JM0 2 Thanks for catching. It looks like someone (you?) fixed the headline.
John Metzger; 2023-05-04T17:58:15.221

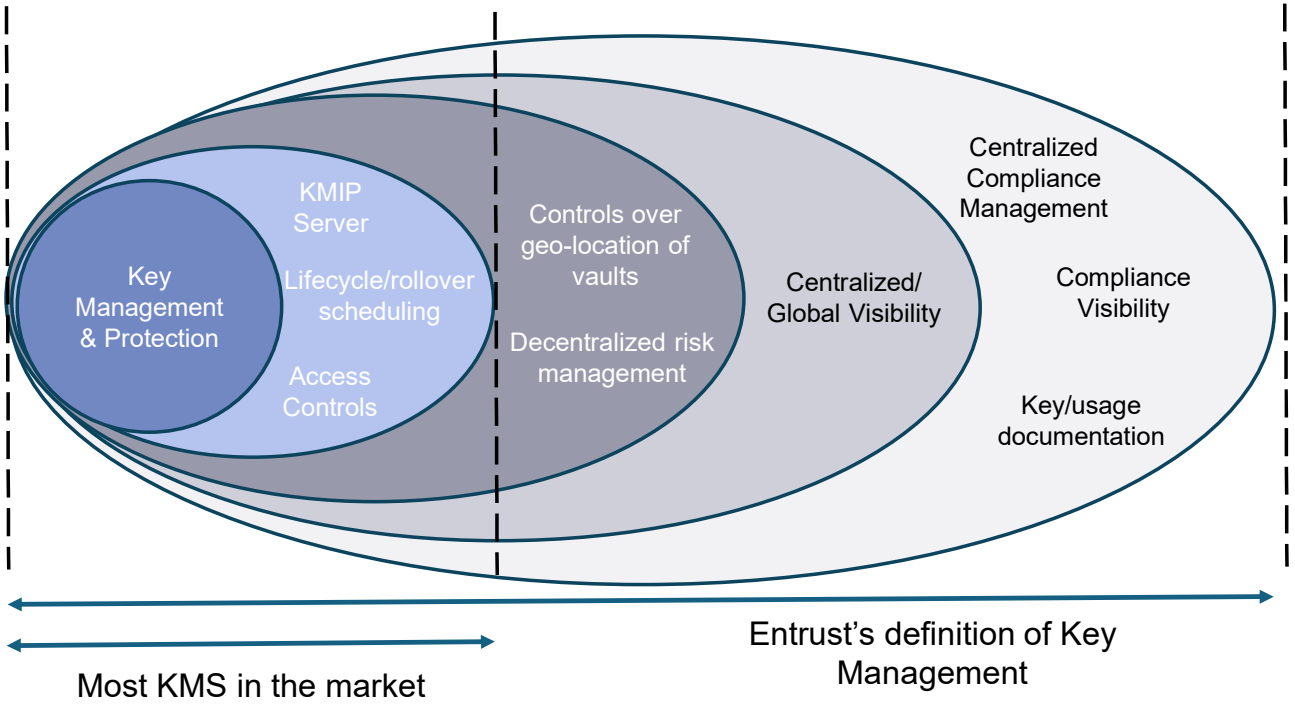
JA0 3 [@Rohan Ramesh] [@John Metzger] the 7th hex on the illustration should really be "VM Security"
Juan Asenjo; 2023-05-06T04:29:55.323

Identity centric security



Entrust's Vision on Key Management

Redefining Key and Secrets Lifecycle Management



- Traditional Lifecycle Management
- Decentralized Vault-Based Architecture
- Comprehensive Central Policy
- Compliance Management Dashboard

ENTRUST

Hardware security modules provide a foundation of trust

A hardware security module (HSM) is a certified, trusted platform for generating cryptographic keys and protecting them during use and at rest

Highest level of protection for encryption or signing keys

Implement and enforce customer-defined policy

“Harden” applications that use cryptography

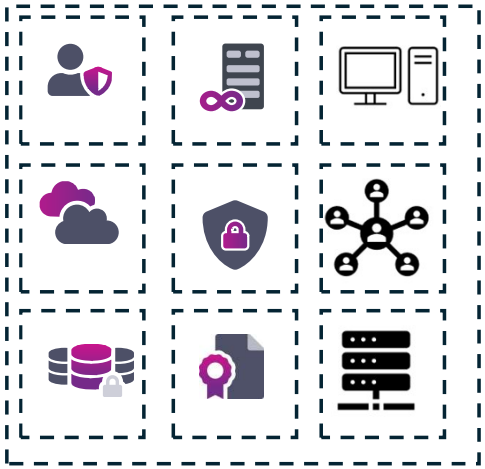
Source of high quality random numbers for keys

ENTRUST

A Practical and Operational Approach To Implementing Zero Trust Model: Identity-Centric Security

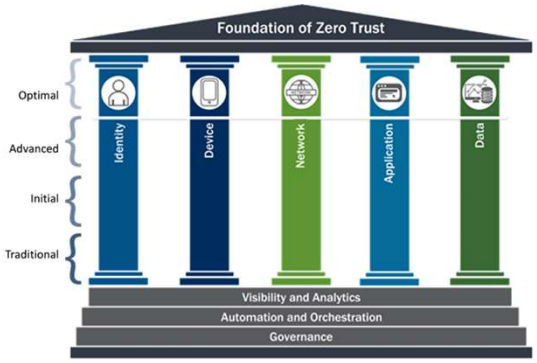
Traditional Security

"Secure the Perimeter"



Zero Trust

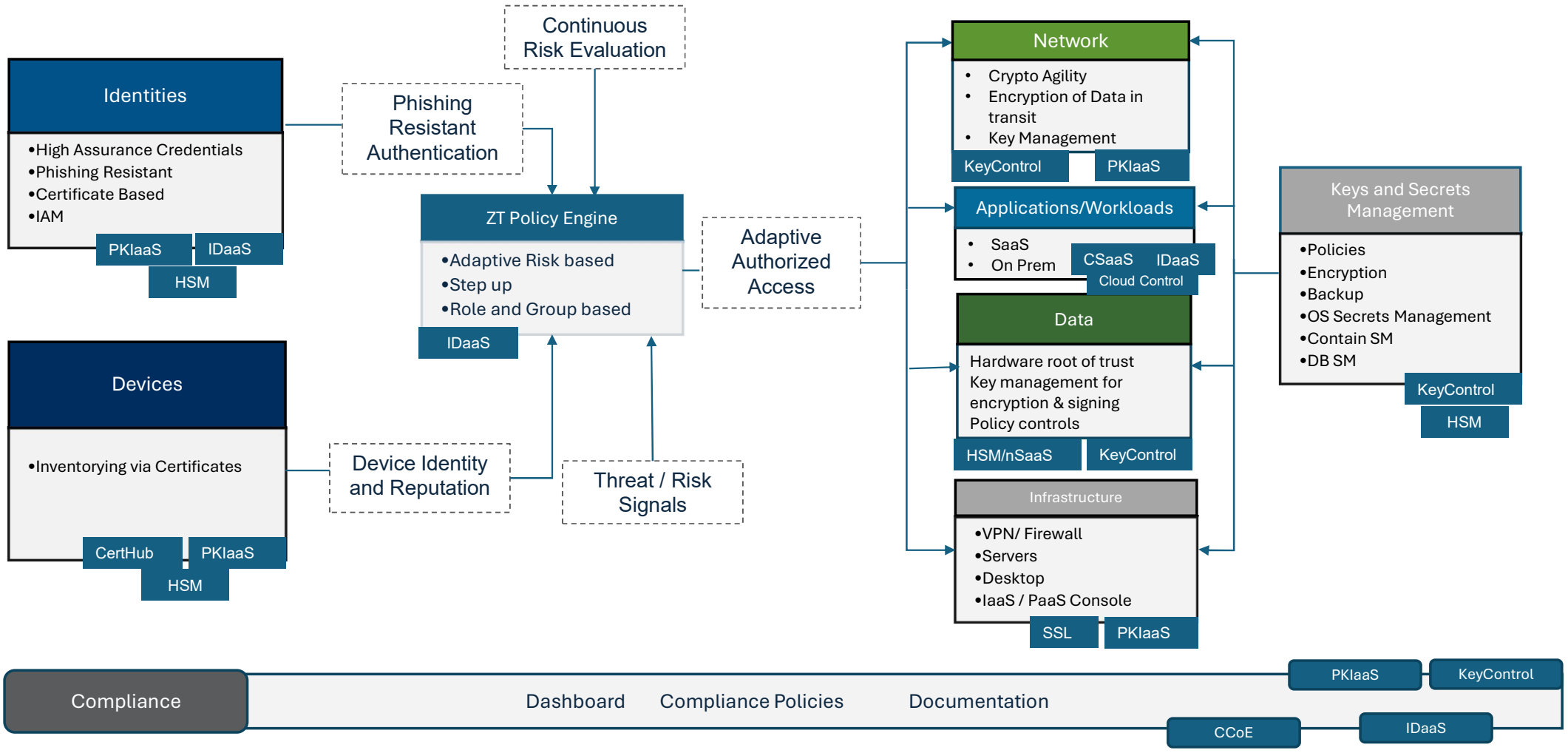
"There is no Perimeter"



Identity-Centric Security

"Identity as foundational control"

ENTRUST ZERO TRUST FOUNDATIONS REF. ARCHITECTURE Based on CISA



10

HOW?

High assurance phishing resistant Identity

- FIDO2 and Passkeys

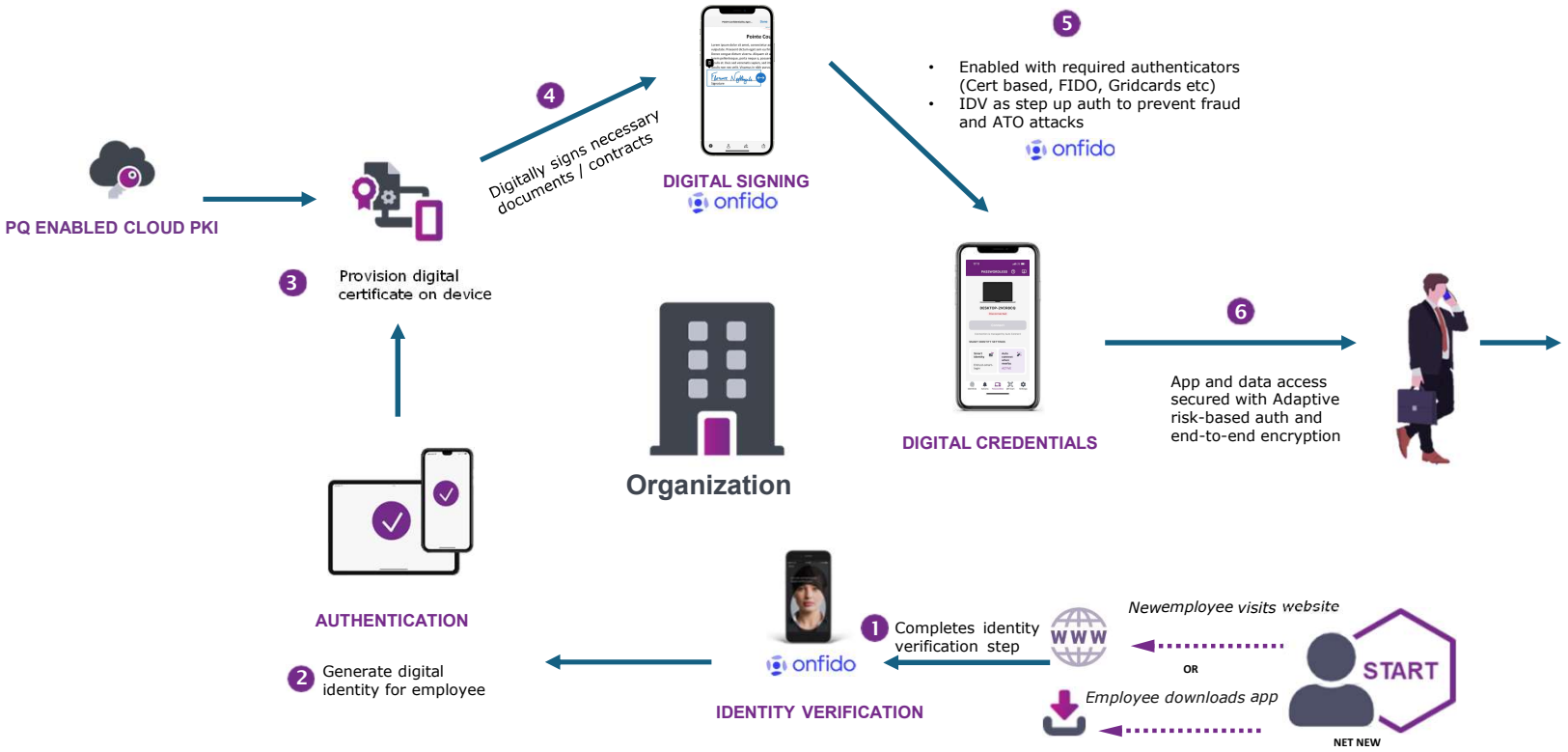
Risk-based adaptive step-up authentication

- Flexible risk engine to analyze contextual information
- Adaptive to dynamically issue 2FA request or deny access

AI – driven Facial Biometric Identity verification

- AI / ML based facial biometrics to prevent phishing, credential compromise and other remote based attacks
- Prevent fraud and secure high value transactions and privileged access

Entrust Identity for Organisations



Identity centric security to secure your workforce

Use Cases

- Workforce Onboarding
- Phishing-resistant passwordless MFA
- IDV as step up for out of compliance and high value transactions
- Configurable Risk based Adaptive Auth
- User Self Service Portal
- User and app provisioning
- Low code / no code orchestration workflows

Fighting fraud throughout the identity journey

Why Entrust

- Shut down phishing and credential compromise to prevent breaches and mitigate damage with a layered defense across the entire identity lifecycle
- Configurable risk-based adaptive engine to dynamically verify authenticity of user
- Step up with AI-driven biometrics to secure against ATO attacks
- Certificate-based authentication for both users and devices

THANK YOU

Visit entrust.com

SECURING A WORLD IN MOTION