RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: CMI-W05V

A Simplified and Practical Approach to Pursuing a Zero Trust Architecture

Soumen Bhattacharya

Technical Director, Security Architecture
Delta Dental of California

Dr. Lynette Qu

Director of Security Architecture
Zendesk

The **CARE** Ethos

Reimagining the perimeter security model to deliver achievable and risk appropriate design principles and components that distribute enforcement responsibilities while promoting engaging experiences.

Two concepts, one approach

Conditional Access

Access adapts to suit risk and applicable policies in real-time.

Responsible Enforcement

Provide risk-appropriate access leveraging intelligence that minimizes user friction.

The Evolution of Zero Trust

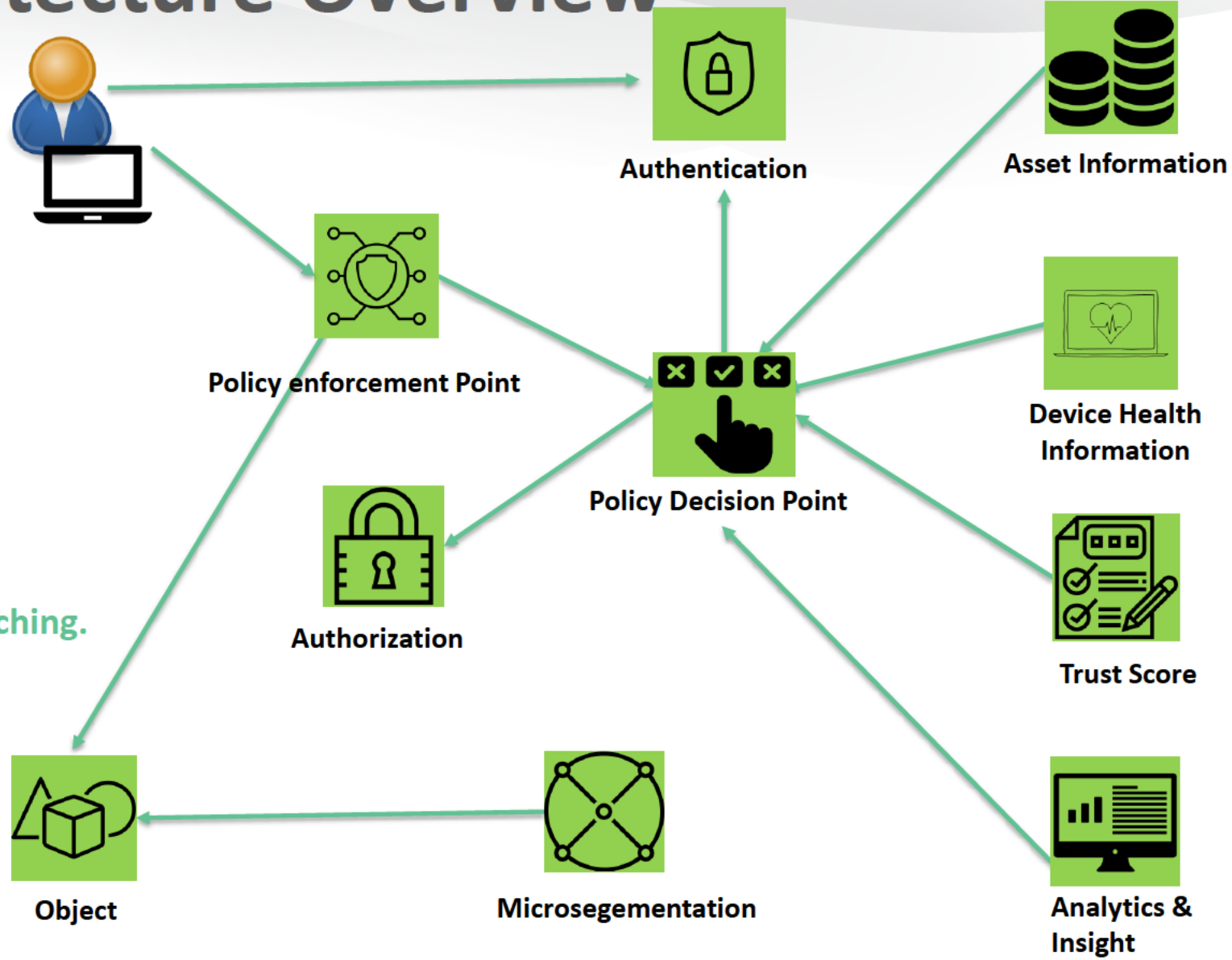
Forrester Research
Security framework coined by analyst John Kindervag in 2009

Gartner CARTA Framework
Trust is not absolute, but continuous.

Google BeyondCorp
Understand the context, authenticate, authorize and encrypt.

DELTA DENTAL

C.A.R.E. Architecture Overview



Design Principles

Practice good object awareness.

Apply boundless trust verification.

Promote central decision making.

Think macro but apply micro.

Treat data flows like everyone is watching.

Be mindful of dark defaults.

DELTA DENTAL

Unpacking CARE

DELTA DENTAL

Unpacking CARE

DELTA DENTAL

Unpacking CARE

DELTA DENTAL

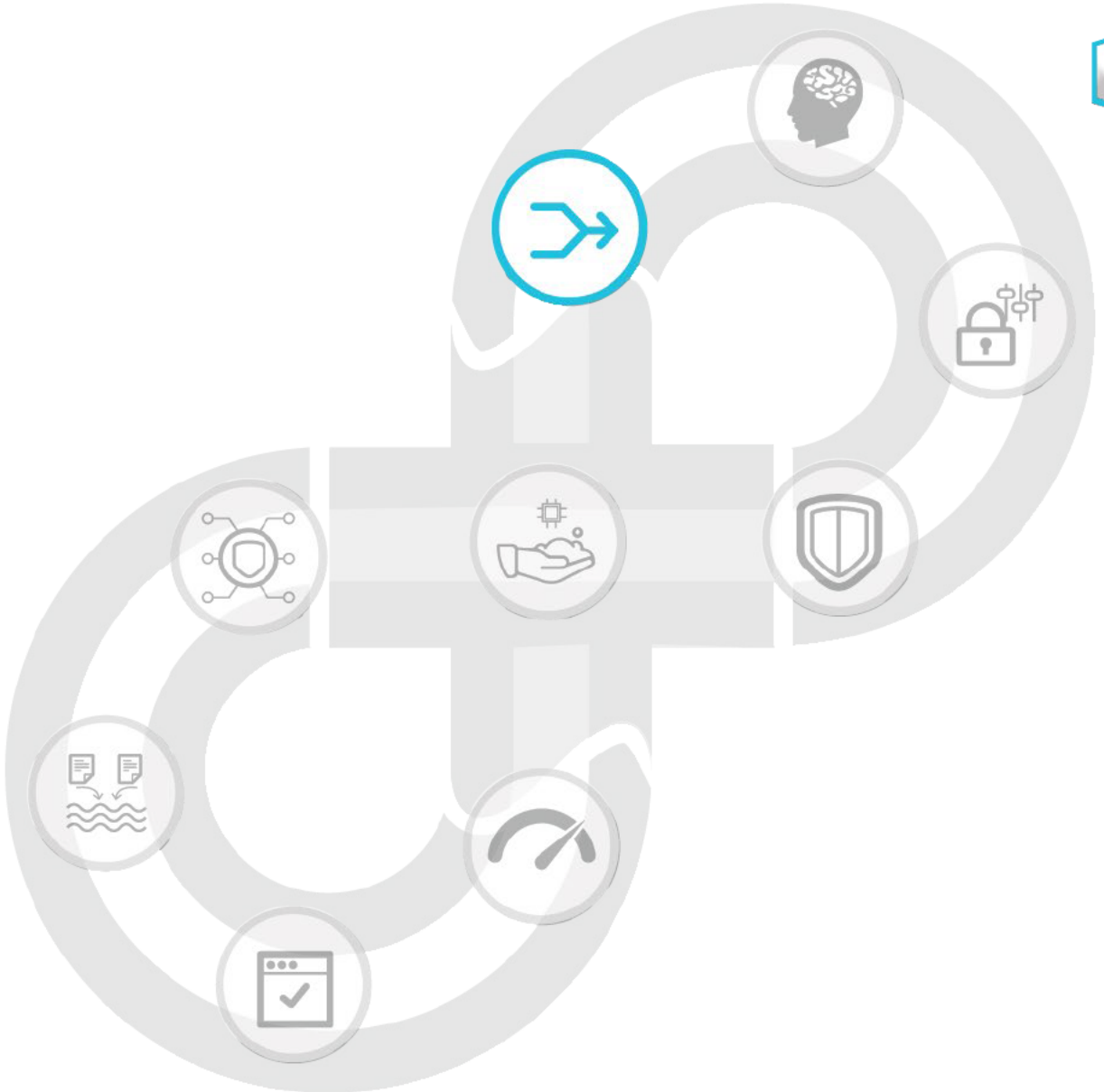
Unpacking CARE

Identity
is the foundation

Policies
are your boundary

People
are your trust universe

DELTA DENTAL



Identity

Unified Directory and Access Decisioning

Federation is not enough

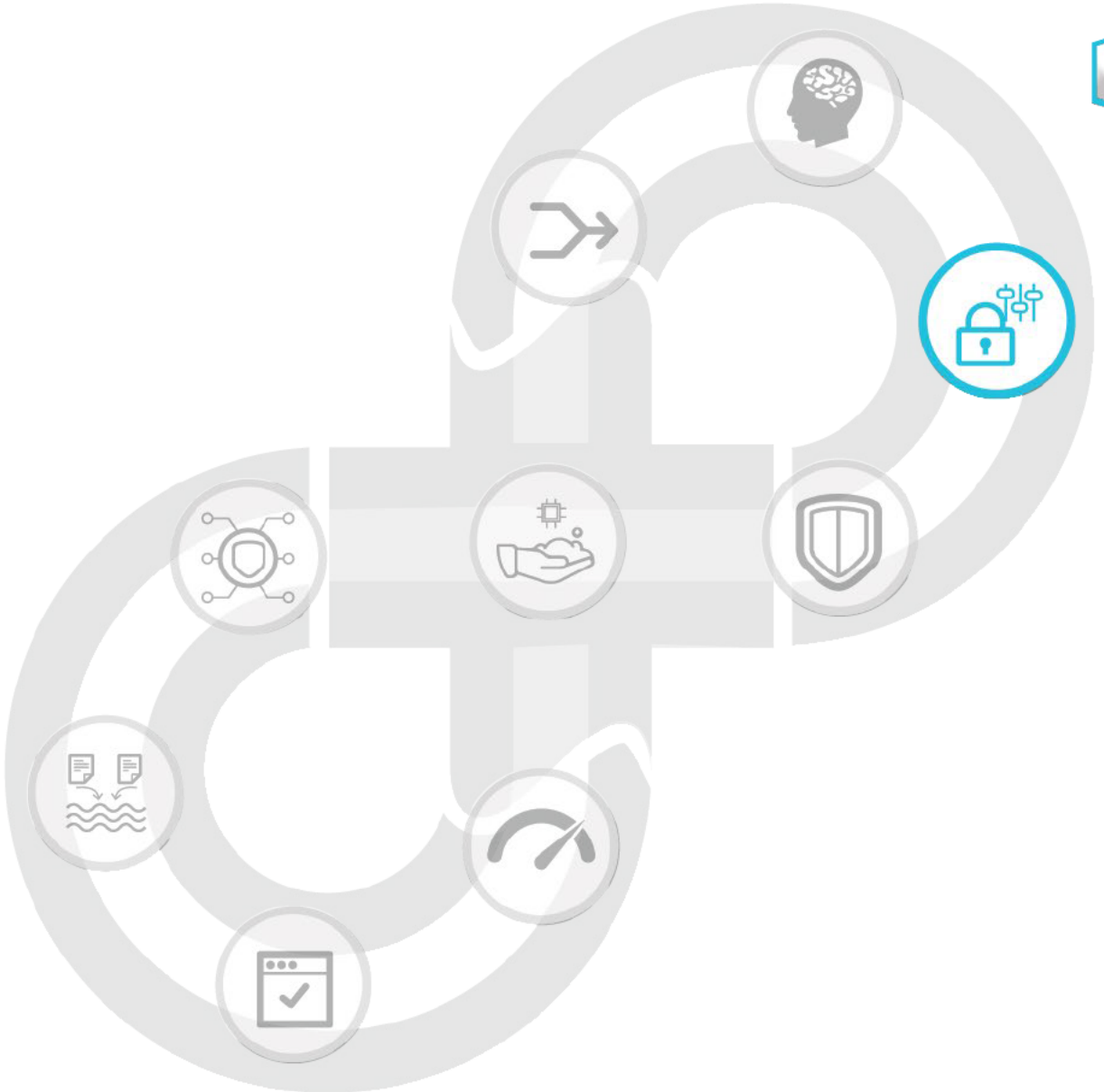
Consolidate directories : True Directory and True SSO. Support for LDAP, SCIM, REST, SQL.

Leverage Schema flexibility. Establish flexible and global management

Define contextual and intelligent policies. Build efficient governance

Automate feedback and centralize monitoring

DELTA DENTAL



Identity

Flexible Access Management

Smart, context aware access

- Stronger authentication & multi-factor support
- Detect anomalies. Reduce IT support costs
- Unify privilege access management & policy-based access management
- Support diversified protocols for different services

DELTA DENTAL

Identity as Foundation Example

Previous

- Multiple disparate directories
- Heterogenous authentication schemes
- Legacy inline MFA
- VPN Access to trusted internal network
- Legacy apps (custom + on-prem software)
- Disparate and Diverse AD groups
- Limited Authorization management
- Limited privileged access management
- Limited Monitoring
- Missing insider threat detection

Now

- Consolidated directories
- Standard authentication schemes
- Adaptive MFA
- Open access from external network
- Cloud deployed apps
- Centrally administered groups
- Unified Authorization management
- Conditional Access Policies
- Active Privileged access management
- Centralized User Behavior Monitoring

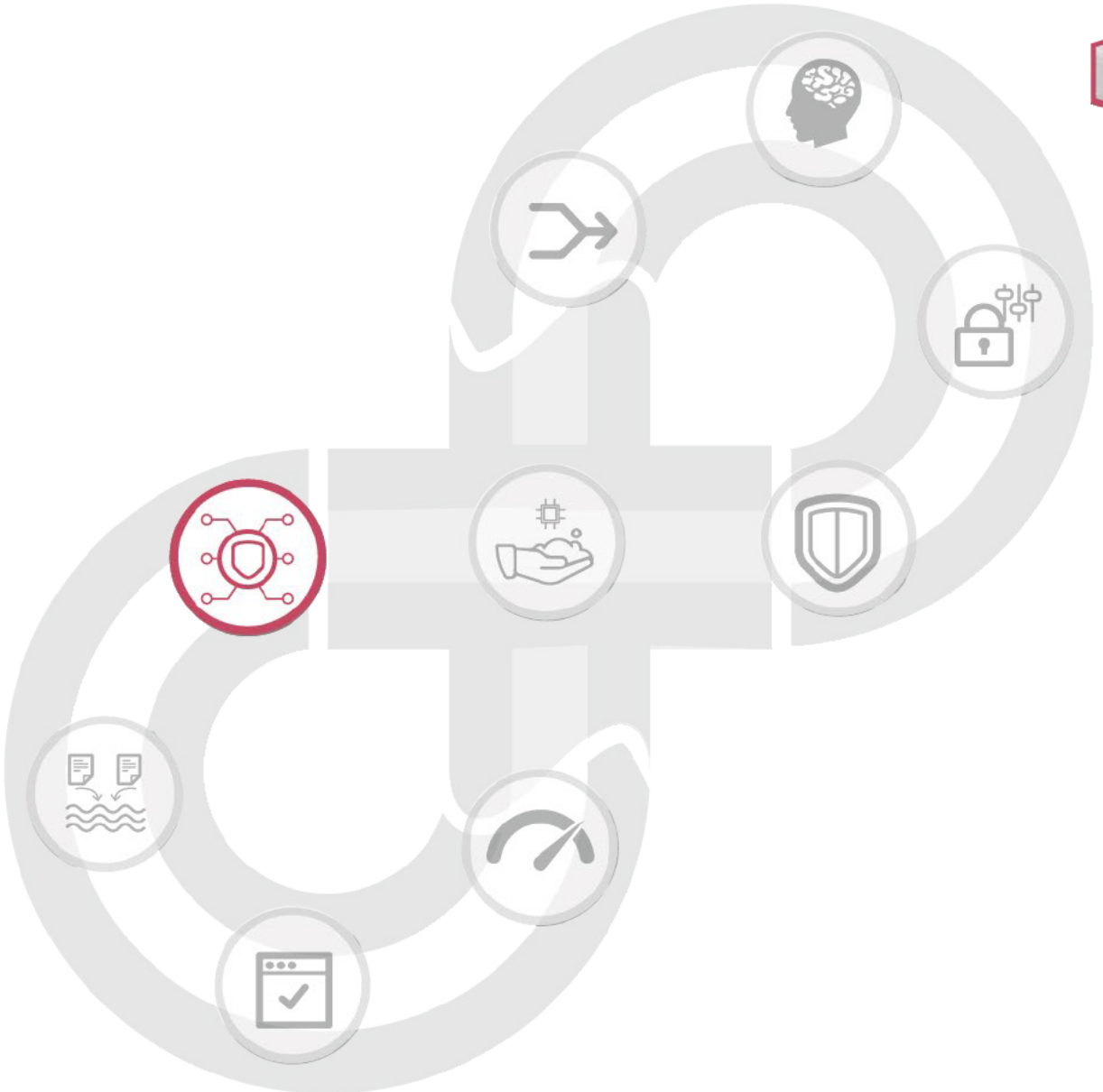
Policies

Confined Trust Boundary

Tailored security setting

- Renovate flawed traditional Defense-in-Depth
- Define network security policies based on workflows
- Create logical segregation
- Apply granular controls to limit network and application flows

DELTA DENTAL



Policies

Attached Enforcement Proxy

Protected resources

- Attach as a gatekeeper to the protected resources
- Enforce based on unified decision
- Apply least privileged policies
- Maintain user experience without rigid policies

DELTA DENTAL

Policy as Boundary Example

Previous

- Flat and open networks
- Limited and patchy asset awareness
- Redundant and numerous network policies
- Loose Network Access controls
- Access through VPN network
- Decentralized and inconsistent enforcement
- Undetected and ungoverned shadow IT
- Access from non-managed devices

Now

- Zero Trust Segmented Networks
- Completed asset inventory
- Granular network policies
- Localized Network Access controls
- Access from anywhere
- Protected internet exposure
- Allow sanctioned apps only
- Allow managed devices only
- Improved network monitoring

DELTA DENTAL

People

People Data

Data is backbone for access decisions

Store data in one enormous data lake

Collect behavior, technology and physical proximity data

Buy and build IT systems with APIs in mind

DELTA DENTAL

People

Engagement Portal

Personalized security feed & tips

Provide actionable information to improve security posture

Verify suspicious activities to reduce false positives

Provide a single pane for overall trust profile visibility

DELTA DENTAL

People

Confidence Score

Assess risk based on behavior

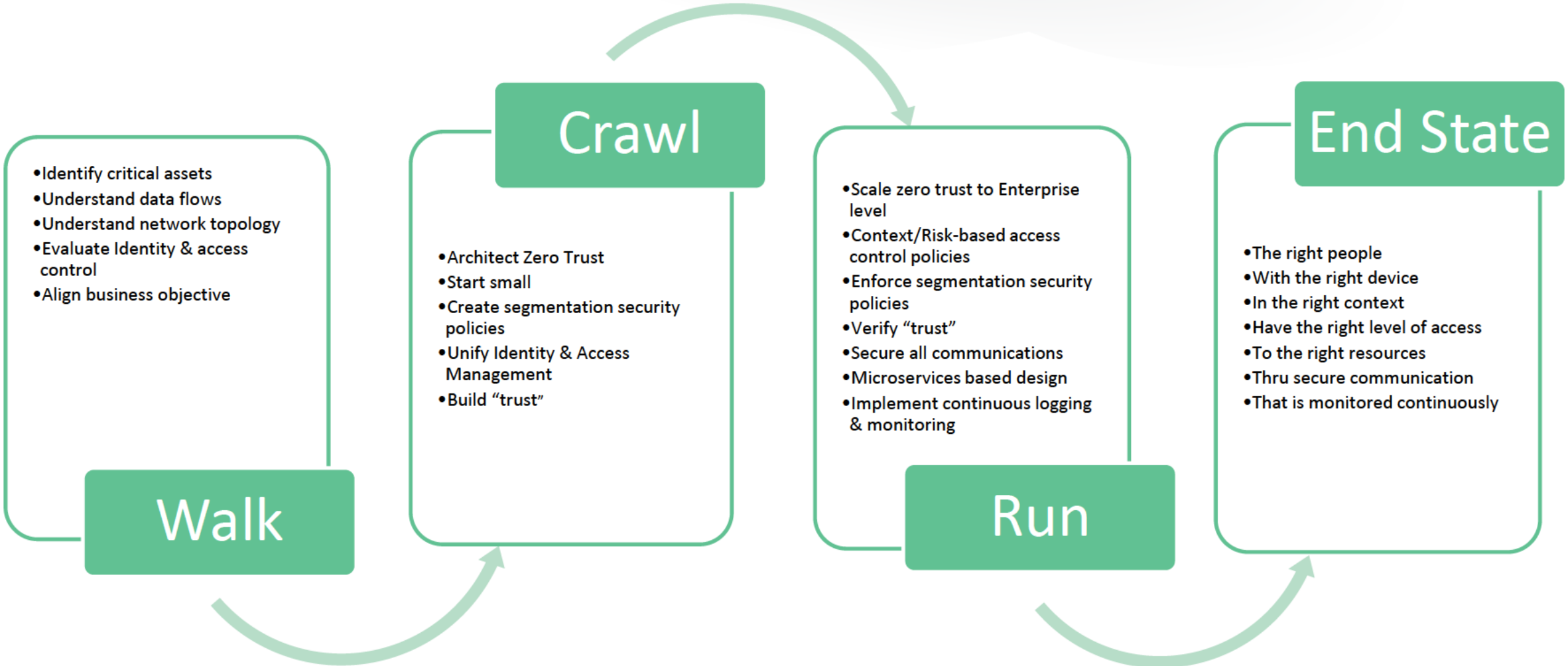
Represent an employee's trust profile

Reflect an employee’s responsible behavior towards improving their trust profile

Apply access control to protected resources

DELTA DENTAL

Journey To Zero Trust



DELTA DENTAL

Apply Take-Away

Next week you should

- Understand current state and identify critical assets.
- Identify distributed identity and distributed access policy stores.

In the first three months you should

- Unify identity and policy stores.
- Block insecure protocols.
- Segment environment.
- Build trust score mechanism.

Within six months you should

- Adopt localized and responsive policy design.
- Provide risk-based access based on real-time employee trust score.

Appendix

Design Principles

Practice good object awareness.
Cataloging assets and data enriches trust intelligence.

Be mindful of dark defaults.
Policy failures must protect the resource & minimize disruption.

Treat data flows like everyone is watching.
Removing insecure protocols ensures confidentiality.

Apply boundless trust verification.
Performing frequent access checks discourages dormant threat actors.

Promote central decision making.
Applying policies in one place allows for easy management.

Think macro but apply micro.
Focusing on the resource improves control effectiveness.