# Brought Our Own Enterprise

## Lessons Integrating the IACD Framework

Anthony Ramos
Lead – Technology Security
AT&T Chief Security Office

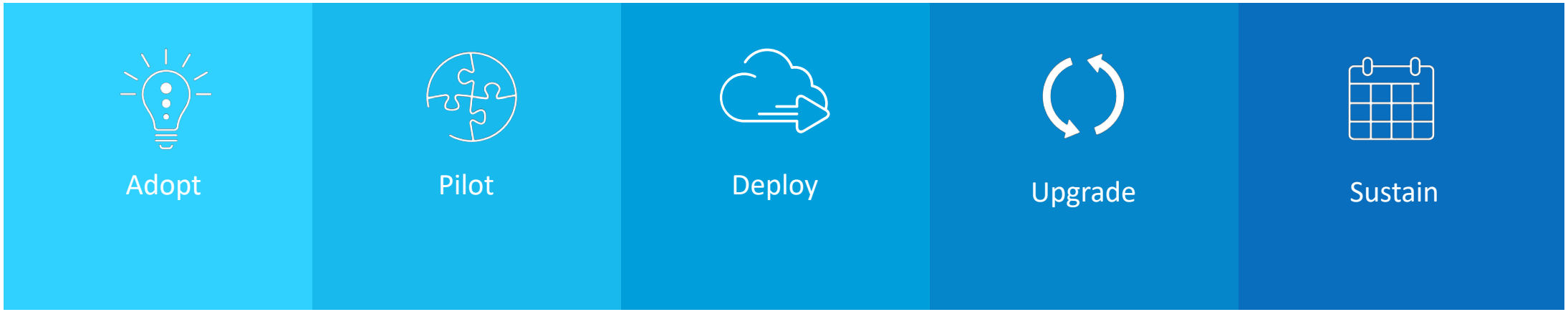
Michael Stair
Lead Member of Technical Staff
AT&T Chief Security Office

May 2, 2019



AT&T

# IACD Readiness Framework

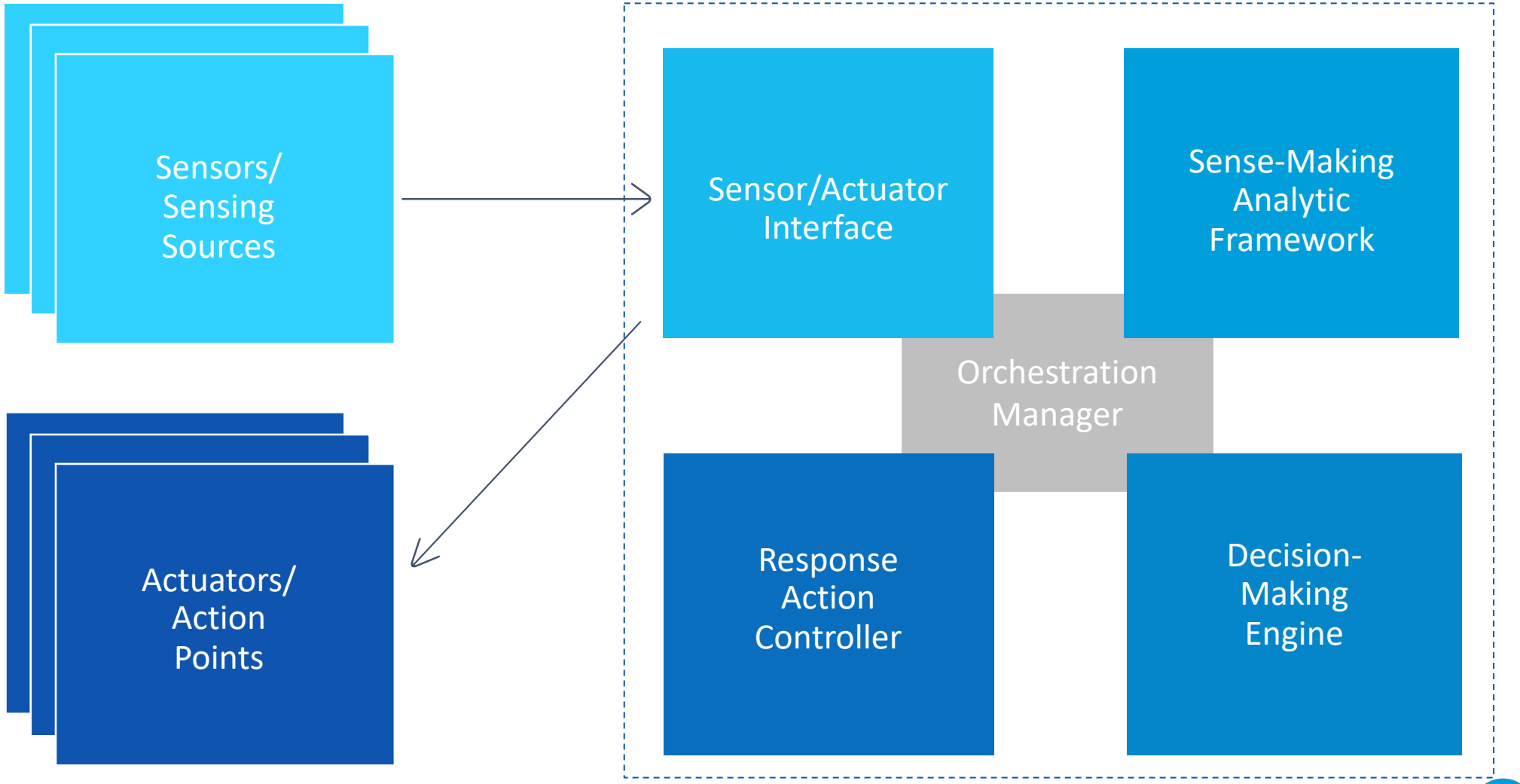






AT&T

# IACD Baseline Architecture

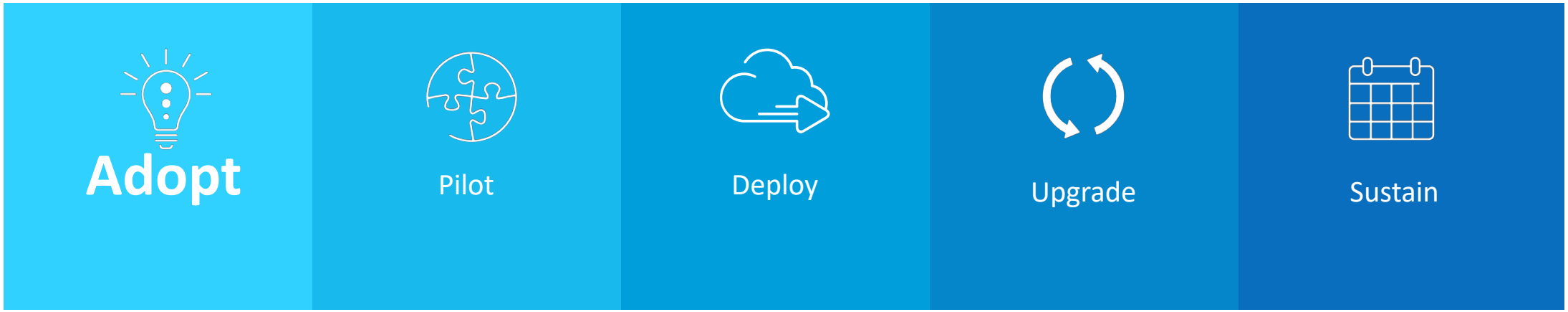






AT&T

# IACD Readiness Framework







AT&T

# Adoption

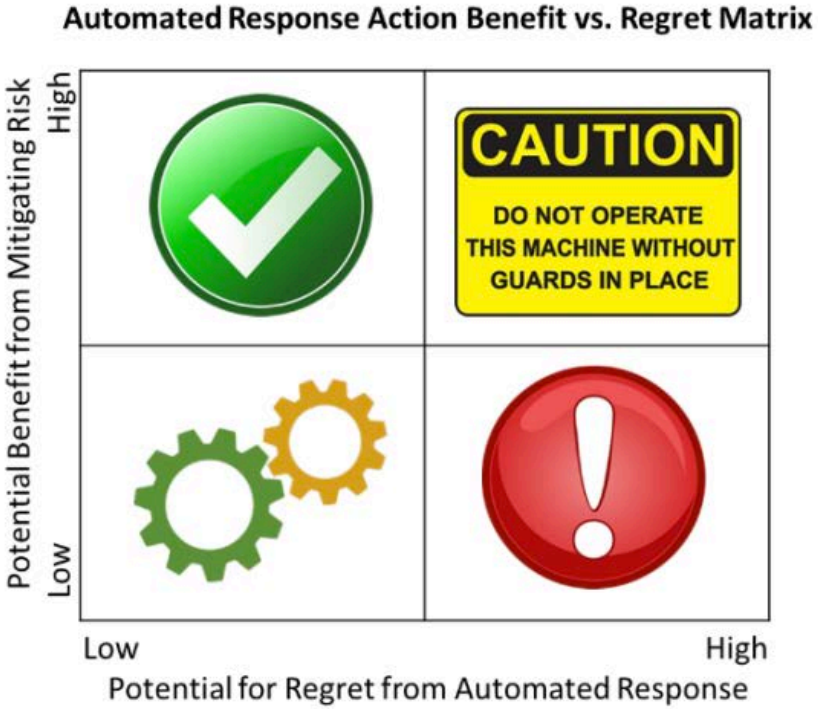
- Leadership Buy-in
  - Executive
  - Organizational
- Identify Candidate Business Cases
- Identify Adoption Strategy/Key Partners
  - Actuator Owners/Policy Management
  - Threat Analytics
    - Cyber Threat Information (CTI)
    - SOC/Incident Response
  - Operations Liaison




AT&T

# Candidate Business Case

- Low Regret/High Benefit
- Align with existing capabilities
- Utilize cross-organizational roles/expertise
- Malicious IP Address Blocking
  - Indicators of Compromise (IOC) from CTI
  - Multi-Vendor/Virtualized Actuators
  - Considerations for technology-based support/scale
    - Proactive/traditional inline blocking
    - Reactive/observation-based blocking
  - Ingress/Egress

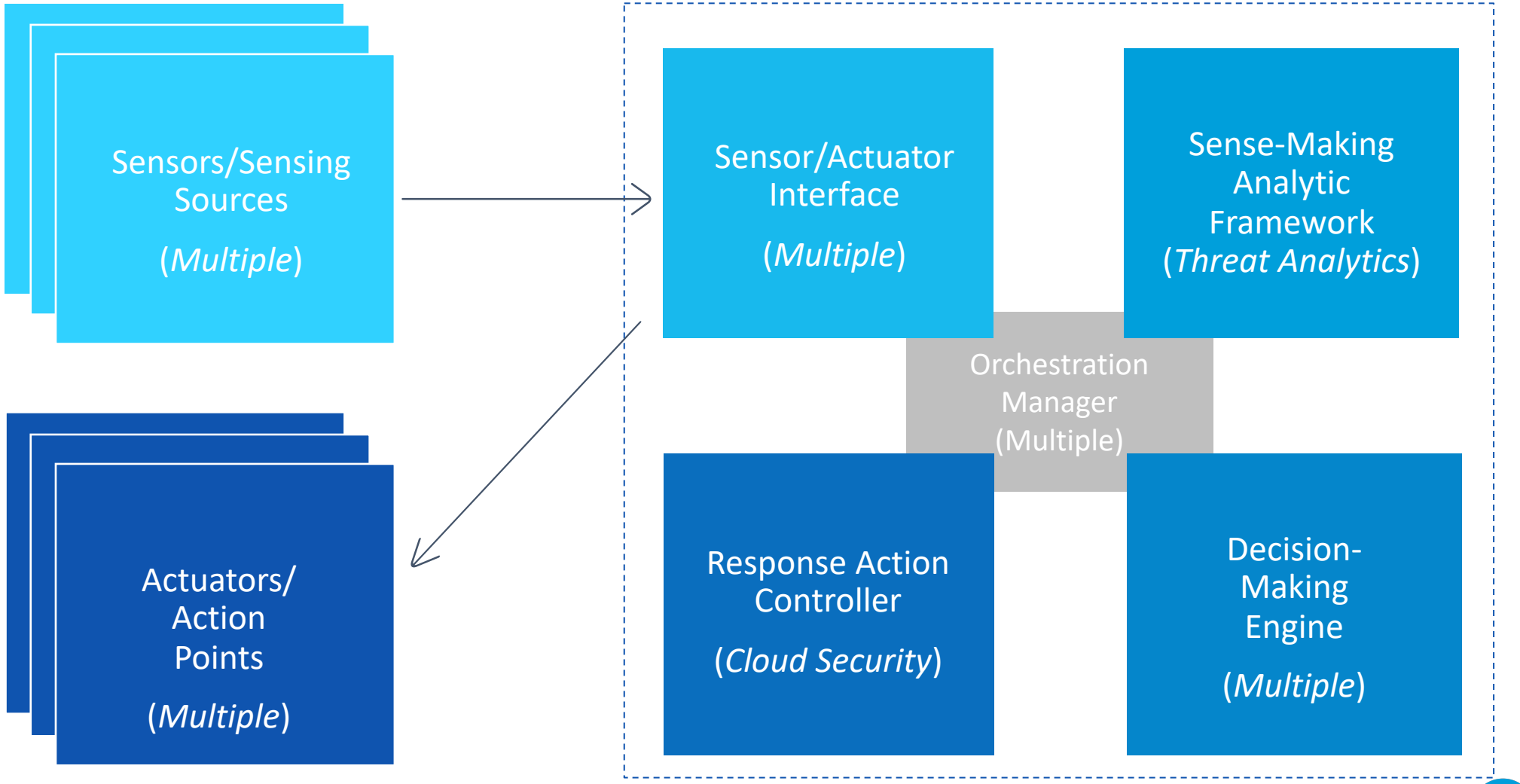



https://www.iacdautomate.org/orchestration




AT&T

# Functional Ownership

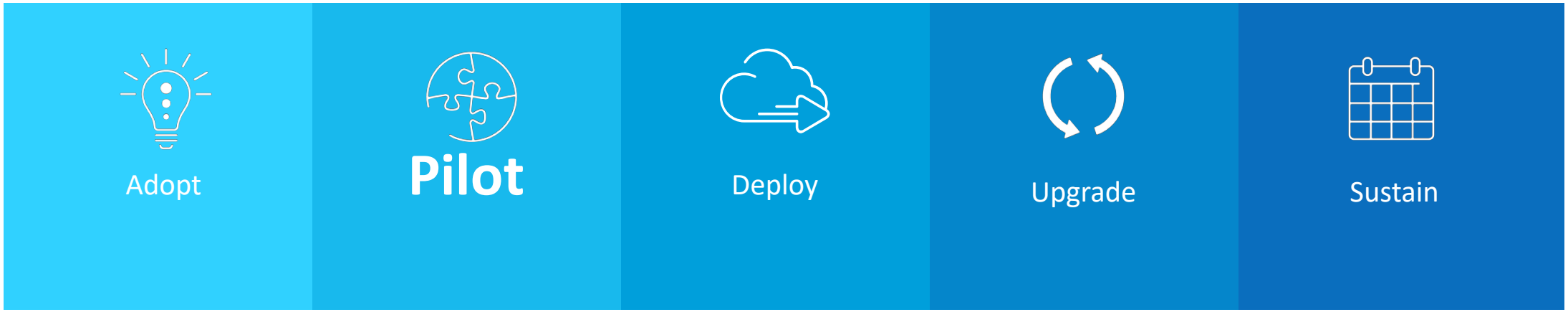






AT&T

# IACD Readiness Framework

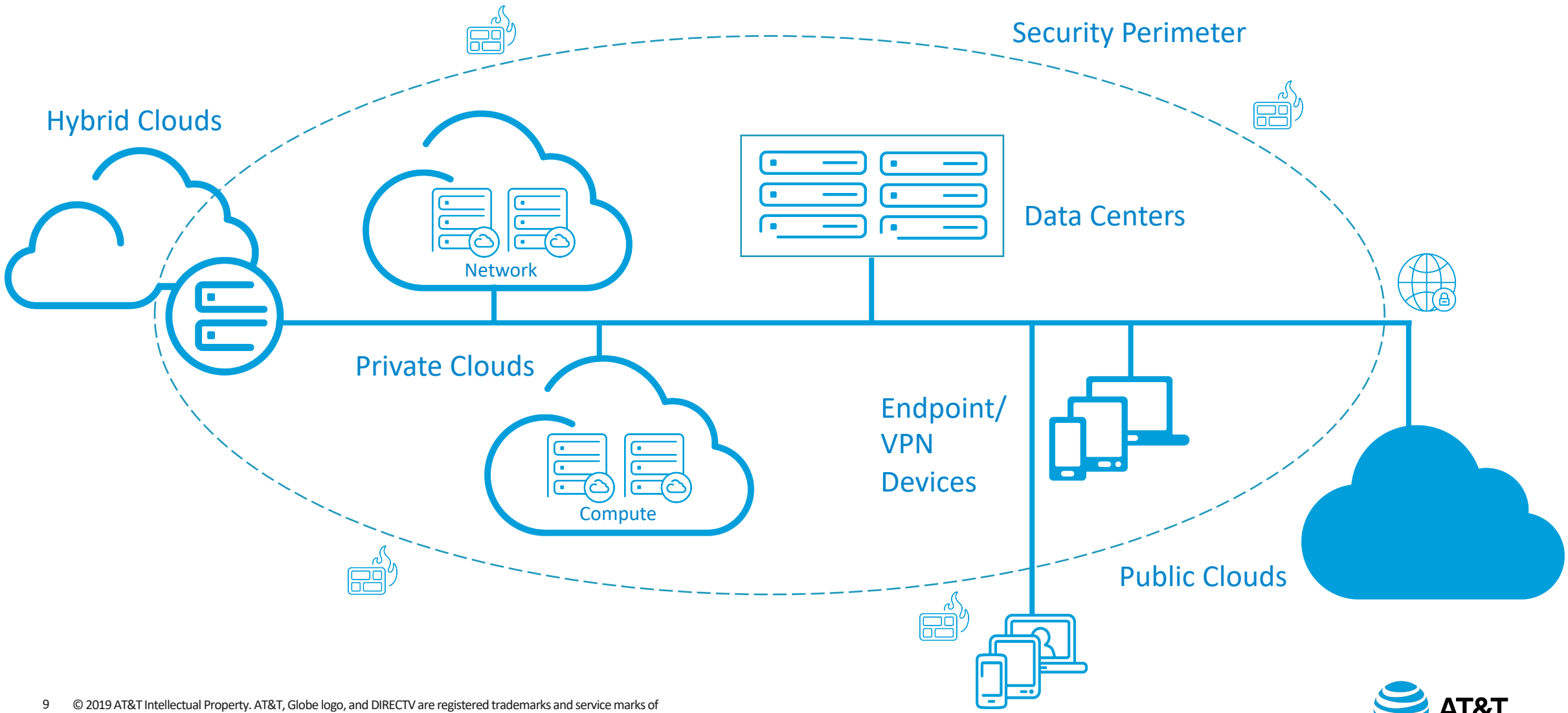






AT&T

# The New Enterprise

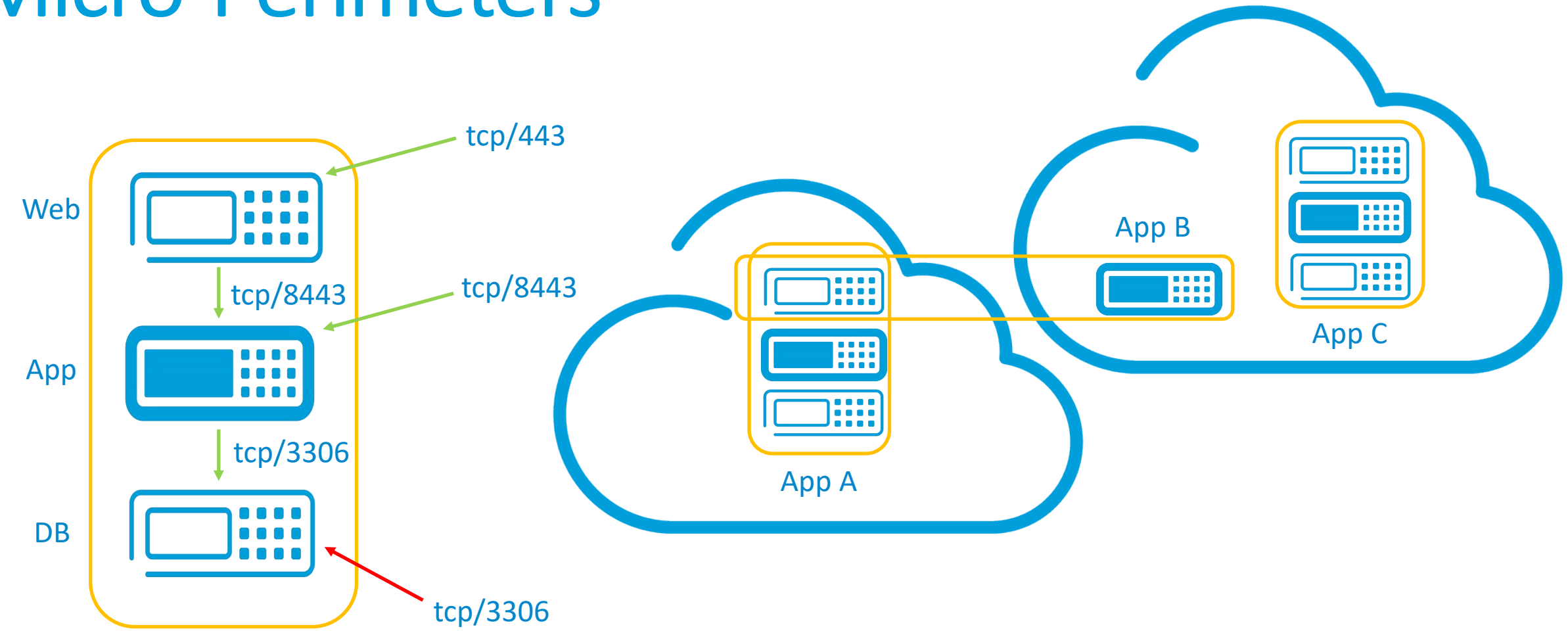






AT&T

# Micro-Perimeters







AT&T

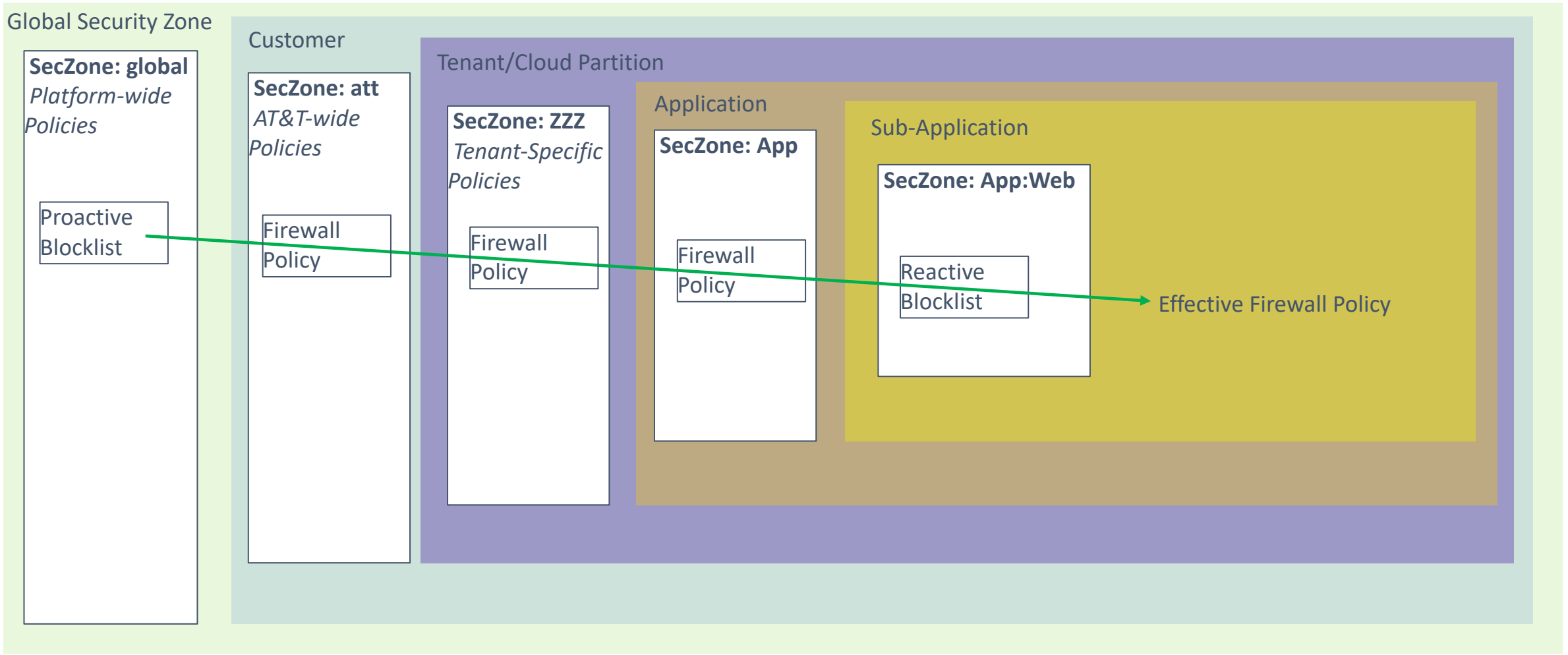
# Platforms and Interface Standards

- SOAR
  - Already evaluated/identified by earlier PoC efforts
  - Decision-Making/CoA Function
- In-House Response Orchestrator
  - Focus on virtualized security technologies
  - Hierarchical security policy engine
- OpenC2 – Open Command and Control
  - Vendor agnostic response action
- STIX 2 – Structured Threat Information eXpression
  - IOC Sightings/Observations




AT&T

# Policy Hierarchy - Security Zones

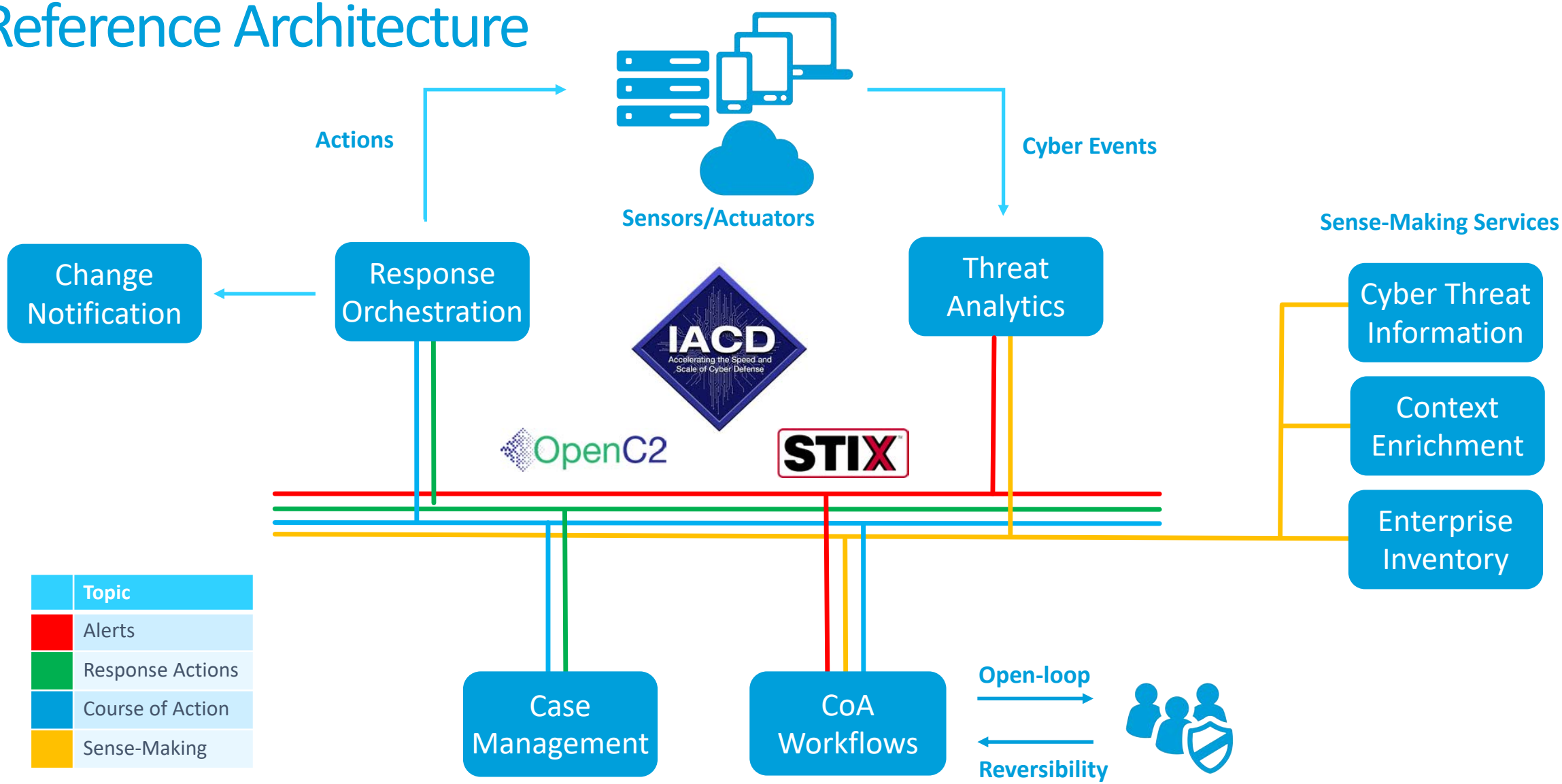






AT&T

# Reference Architecture

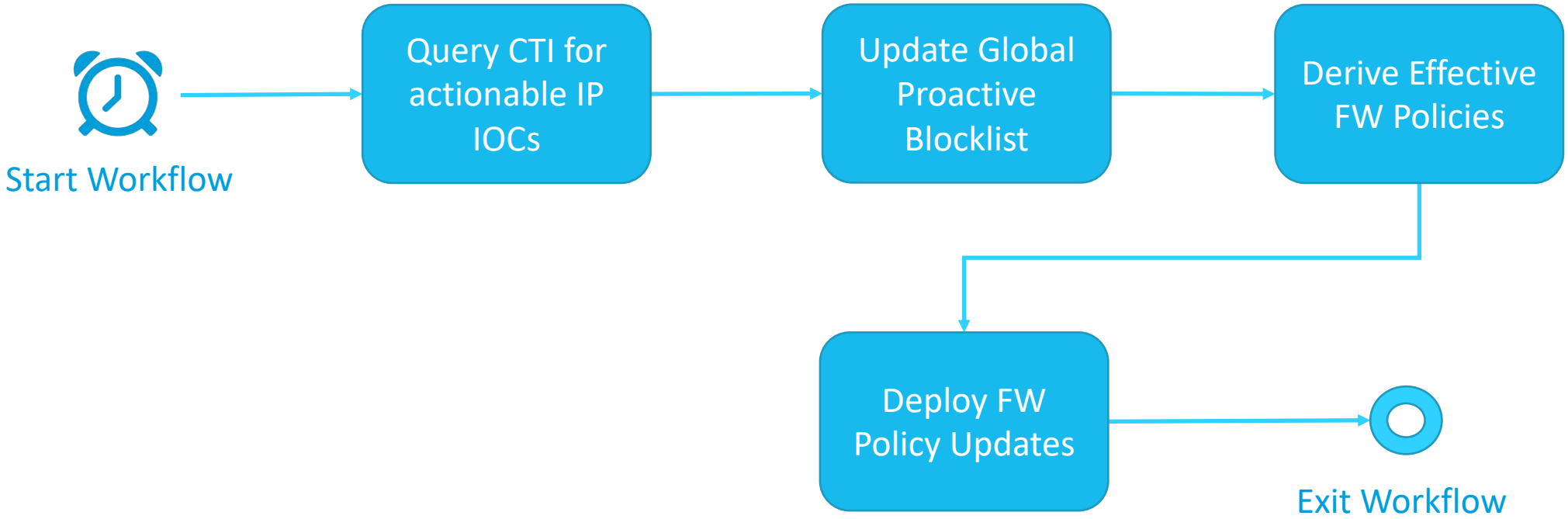






AT&T

# Workflow – Proactive Blocks

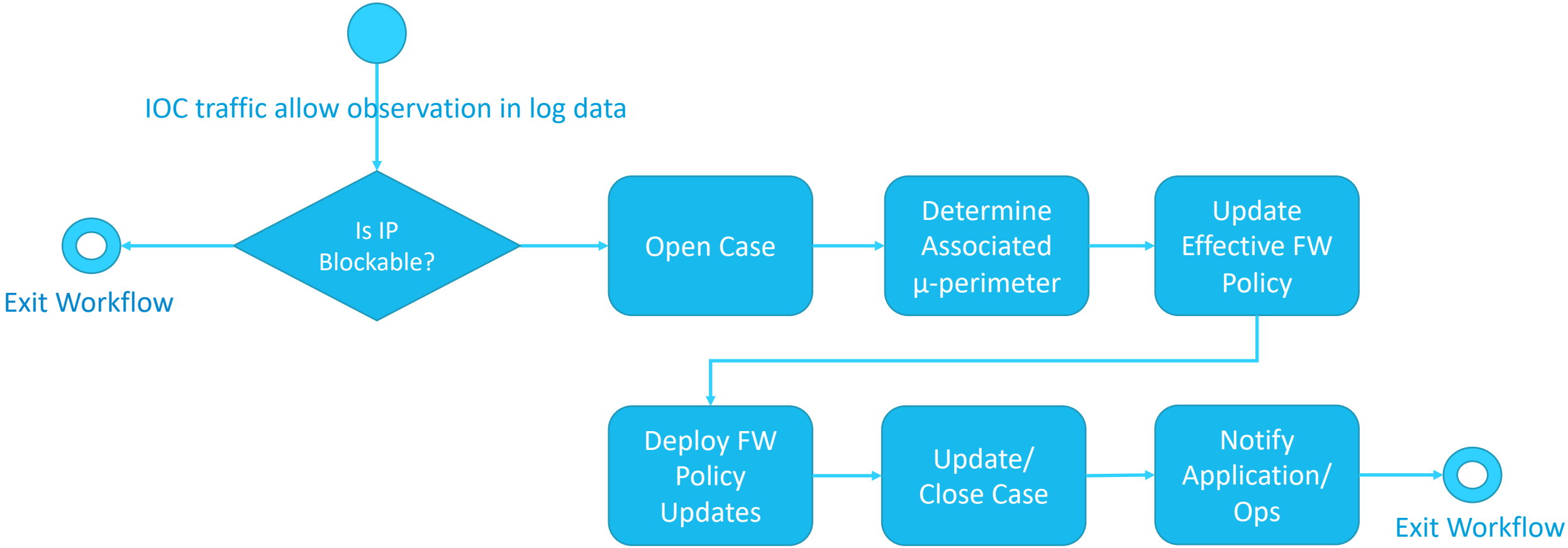






AT&T

# Workflow – Reactive Blocks







AT&T

# Reversibility

- False positives are inevitable
- Exception requests are inevitable
- Autoimmunity – Malicious CTI
- Restrictive CTI queries
  - Require IOC corroboration from multiple sources
- Extended workflows to support removal trigger




AT&T

# IACD Readiness Framework





AT&T

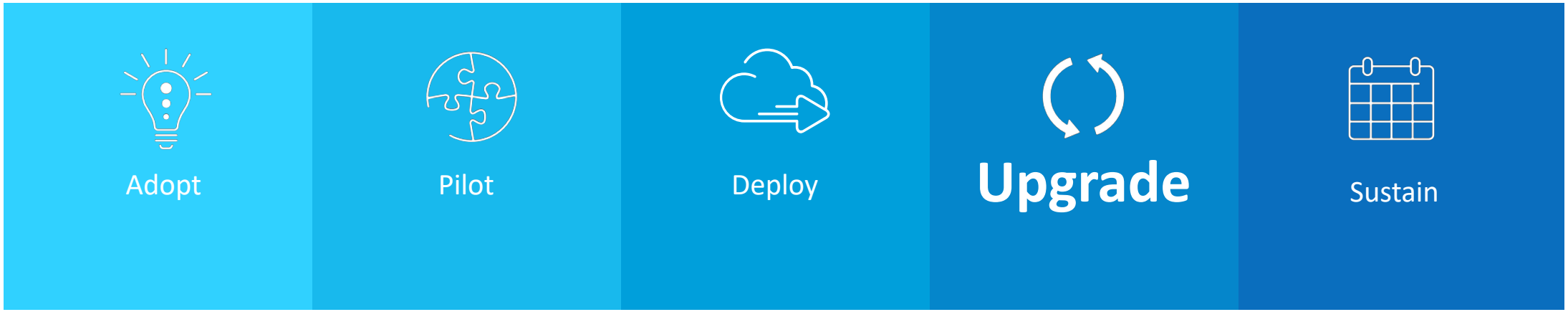
# Deploy

- Embed in SDLC
- Audit
  - SOC/IR Teams
    - Case Management
  - Operations/Application Owners
    - Change Notifications
- Metrics
  - Number of Security Policy Updates
  - Number of Reverse Workflows Executed
  - Reactive MTTR
  - Allows -> Denies




AT&T

# IACD Readiness Framework







AT&T

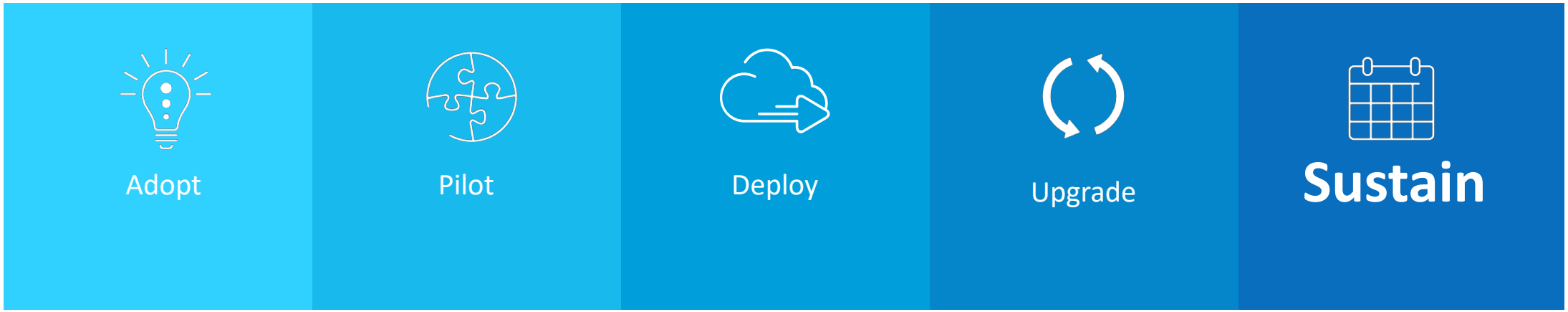
# Upgrade

- E2E Performance
- Iterative improvements to Business Case
  - Effectiveness
  - Expand coverage
  - ML/AI opportunities
- Additional Use/Business Cases
  - Champion in other environments/business units




AT&T

# IACD Readiness Framework







AT&T

# Sustain

- Funding/Budget Plans
- Platform Upgrades
- Revisit SOAR Capabilities/Options
- New/Evolved Standards




AT&T


AT&T