Zero Trust Security - 5G & Beyond

Dr. Sheeba Backia Mary B.,
Advisory Researcher
Lenovo, Motorola Mobility | 28 August 2023

Smarter technology for all

Outline

- What is Zero Trust?
- Core ZTS Principle & the need for ZTS
- ZTS Tenets - A NIST View
- ZTS Relationship with Telecommunication network
  - A Standardization Perspective
- Global ZTS Initiatives
- Future Directions

What is Zero Trust?

Make Sure everybody in the boat is rowing and not drilling holes when you aren‘t looking!!!

- An evolving set of cybersecurity paradigms

Static and network based perimeters → **Moves defense** → **Focus on users, assets, and resources**

- Once attackers breach the perimeter security, further lateral movement is unhindered.
- Defense-in-depth strategy to protect from external and internal threats
- Assumes:
  - No implicit trust granted to assets/user accounts
    - E.g., based solely on their physical/network location/asset ownership
  - An attacker is present in the environment
    - An enterprise-owned environment is no different—or no more trustworthy—than any nonenterprise-owned environment.

Core ZTS Principle

Assume no Implicit Trust

Continuously analyze and evaluate the risk (to assets, resources & services)

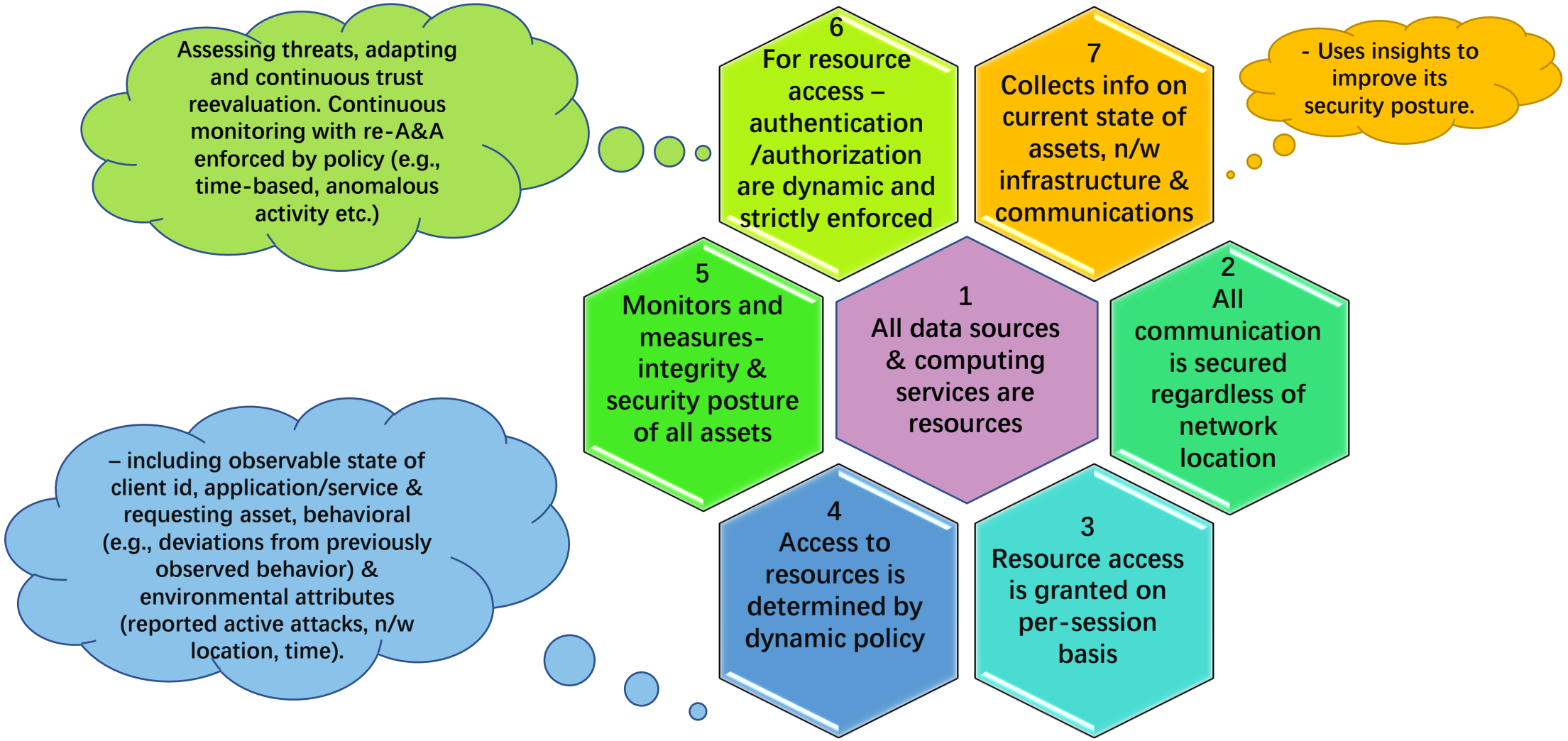
Enact protections to mitigate these risks

Need for ZTS

- ZTS Principles prevents data breaches and limit internal lateral movement.
- A Zero Trust Architecture (ZTA) - A cybersecurity architecture that is designed based on zero trust principles.

ZTS Tenets – A NIST View

NIST Special Publication 800-207: Zero Trust Architecture



A standardization Perspective

ZTS Relationship with Telecom Network

Future directions:
What can facilitate Security evaluation and monitoring

2-3

UE to Network Security

UE – N/W: Mutual authentication (EAP-AKA'/5G AKA/ or any EAP methods.
NAS, AS - RRC & UP protection using keys resulting from mutual authentication.
Subscription based service access control

2-3

Core Network - Service Based Interfaces Security:

- Mutual Authentication
TLS - Transport layer protection (or)
NDS/IP - Network layer protection
- Authorization
Static Authorization – local authorization policy
Token based Authorization (e.g., Oauth 2.0 access token)

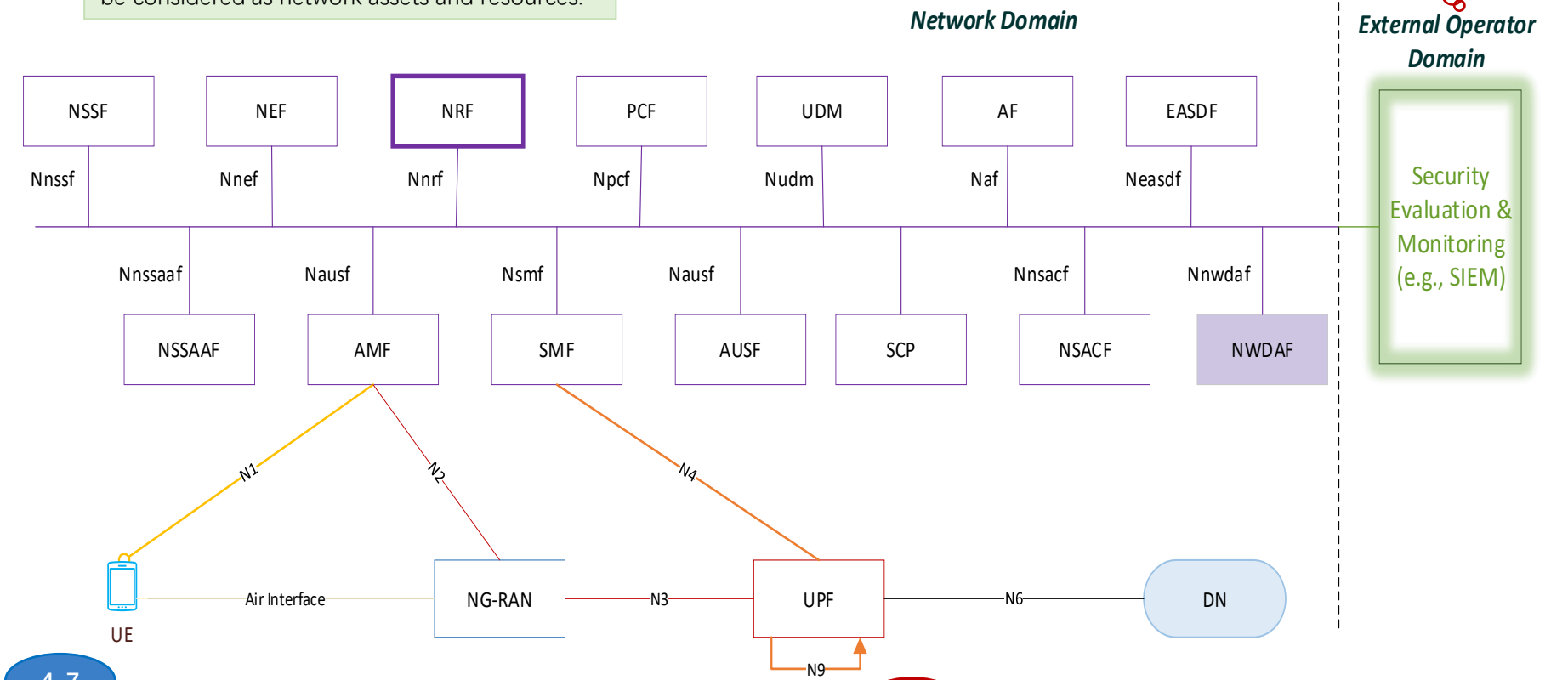
2-3

5G Core and Access Network Non-Service Based Interfaces Security:

- IP based interfaces
NDS/IP - Network layer protection
- Implements IPsec ESP and IKEv2 certificates-based authentication
In addition DTLS (Transport layer security) is supported for mutual authentication
Non-SBA Interfaces internal to Core: N4 and N9.
Other Non-SBA Interfaces: N2, N3, Xn

1

All Network functions, devices and services can be considered as network assets and resources.



4-7

Based on TS 23.288 - Limited effort exist for UE related usecases:
Example: **NWDAF** detects following risk:

- Suspicion of DDoS attack
  - PCF requests SMF for PDU session release.
- Too frequent Service Access
  - AF releases AF session; PCF requests SMF for PDU session release.

4-7

Gap Exists for Network related usecases:
Initiated 3GPP Rel.18 SA3 TR 33.894 - Study on applicability of the Zero Trust Security principles in mobile networks.

Some Global ZTS Initiatives

National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

MITRE

Achieving mission assurance for enterprises

Department of Defense (DoD)

Zero Trust Reference Architecture

National Cyber Security Centre

Zero trust architecture design principles

NIST Special Publication 800-207

Zero Trust Architecture

O-RAN Alliance

WG11 Security Work Group

O-RAN Study on Security for Non-Real-Time RIC

O-RAN Security Requirements Specifications

3GPP SA3 Work Group (Rel-18)

TR 33.894 - Study on applicability of the Zero Trust Security principles in mobile networks

ITU Study

Group 17: Guidelines for ZT based access control platform in telecom. networks

Group 13: Assessing trust evaluation models for telecom. networks

ATIS

Enhanced Zero Trust and 5G Whitepaper

Future Directions

Identification of data points

(per domain)

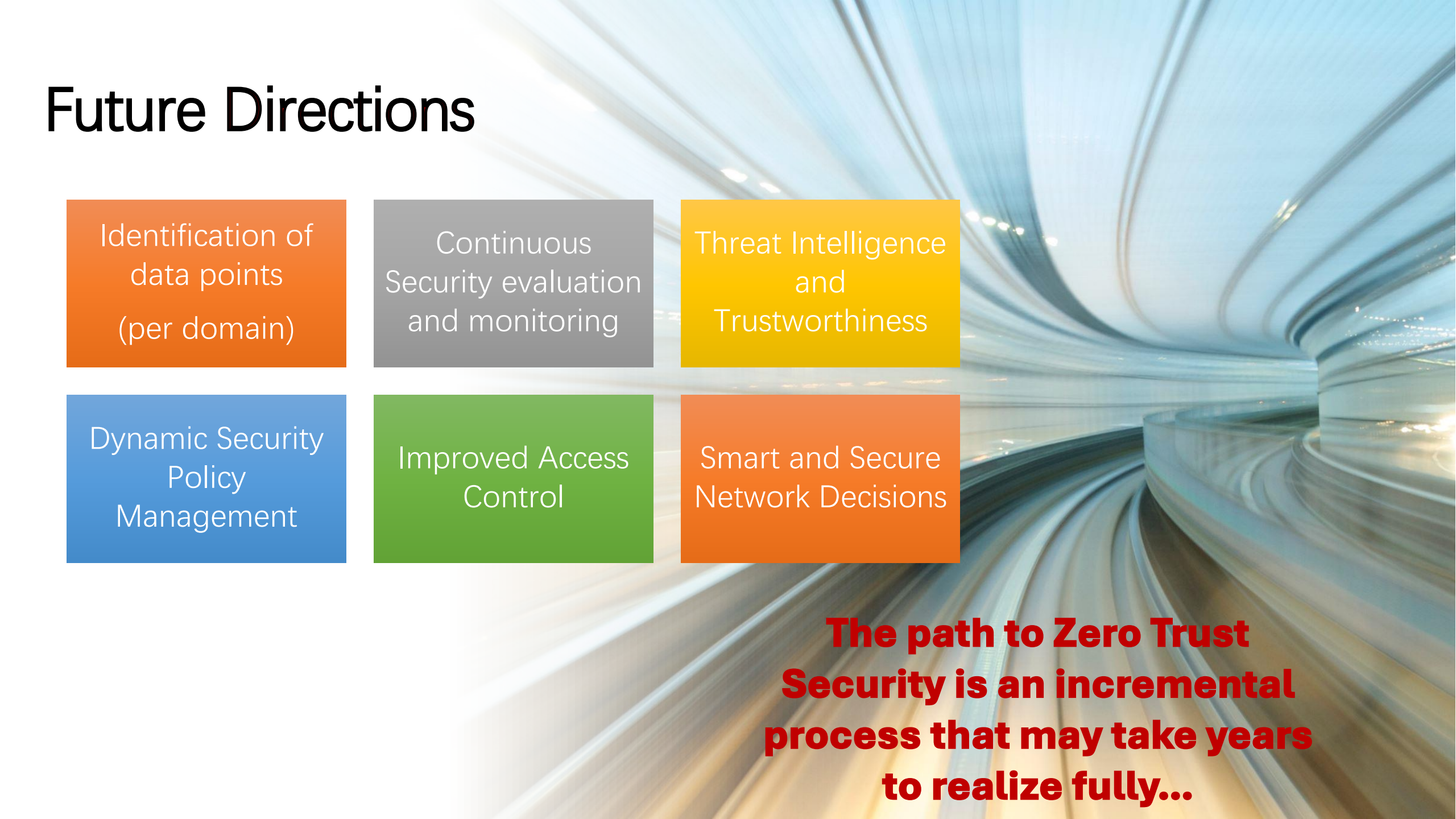
Continuous Security evaluation and monitoring

Threat Intelligence and Trustworthiness

Dynamic Security Policy Management

Improved Access Control

Smart and Secure Network Decisions



The path to Zero Trust Security is an incremental process that may take years to realize fully…

thanks.