



The bridge to possible

# A global view on Zero Trust

Mapping your business resilience requirements

Rolf Haas, Business Solutions Architect, CISSP, CCSP, S+  
@rolfhaas

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



Key Takeaways for this track

Business focus view on  
Zero Trust

Enrich, Empower & Secure  
your Business Resilience  
with Cisco





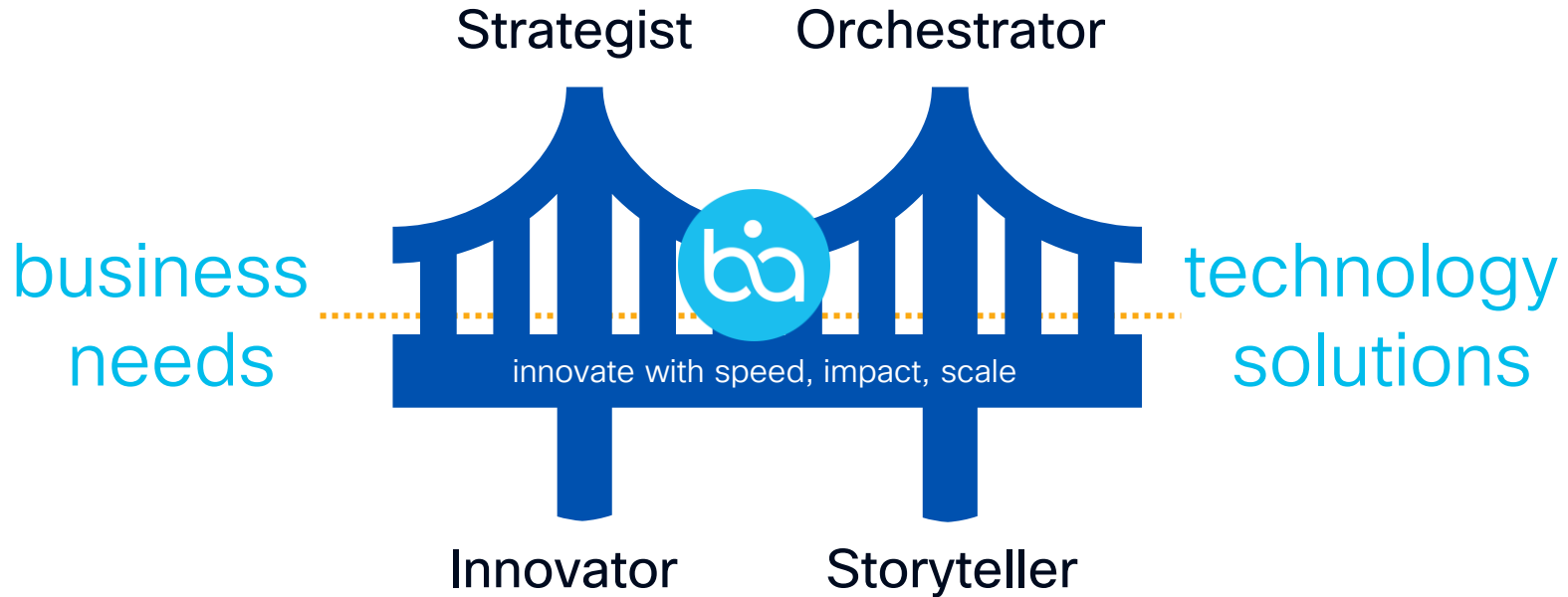
# Agenda

- Introduction and Methodology
- Why the Business Strategy must be on focus!
- Business \*and\* IT Resilience both key factors of success
- Cisco's Zero Trust - a Framework for the future
- Enrich your core-business in all IT areas
- Conclusion



Understanding the customers (business) language  
leads to process centric approach not system/network  
centric

# Business Architecture at Cisco



# Approaches Bottom-up / Top-Down

## Zero Trust Transformation achievement

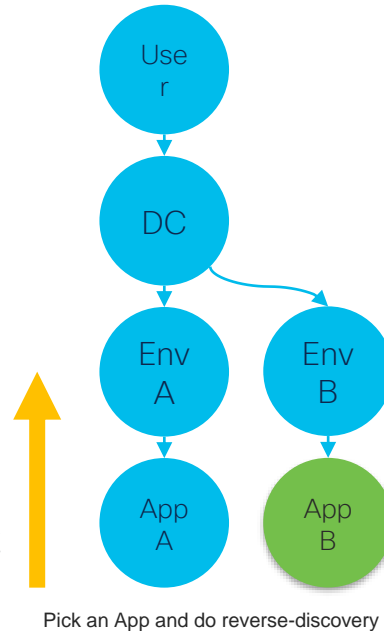
### Bottom-Up:

- Extensive time performing reverse discovery
- Dependency on existing inventory
- Complex approving process
- Continuous app owner engagement for changes

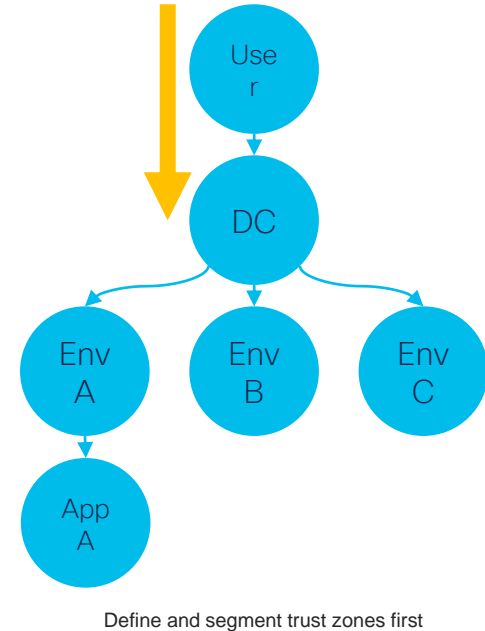
### Top-Down:

- Value realization starts faster paired with a [phased approach](#)
- Has less dependencies on customer data set maturity
- Provides a pathway to granular the Zero Trust transformation

#### Common Approach Bottom-Up



#### Top-Down



Why the  
Business  
Strategy must be  
on focus!

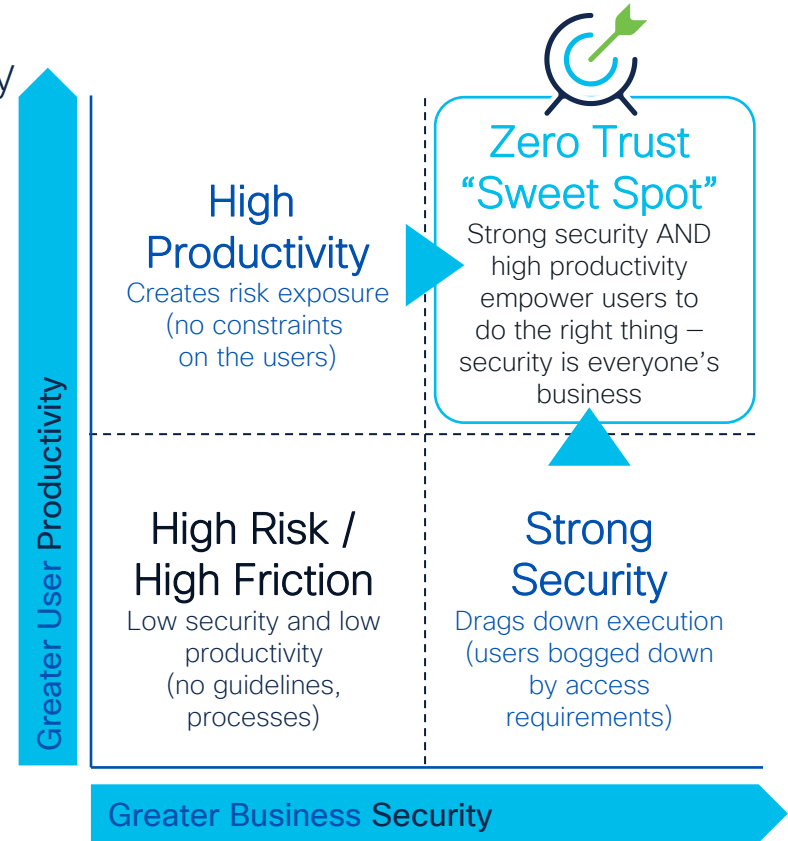




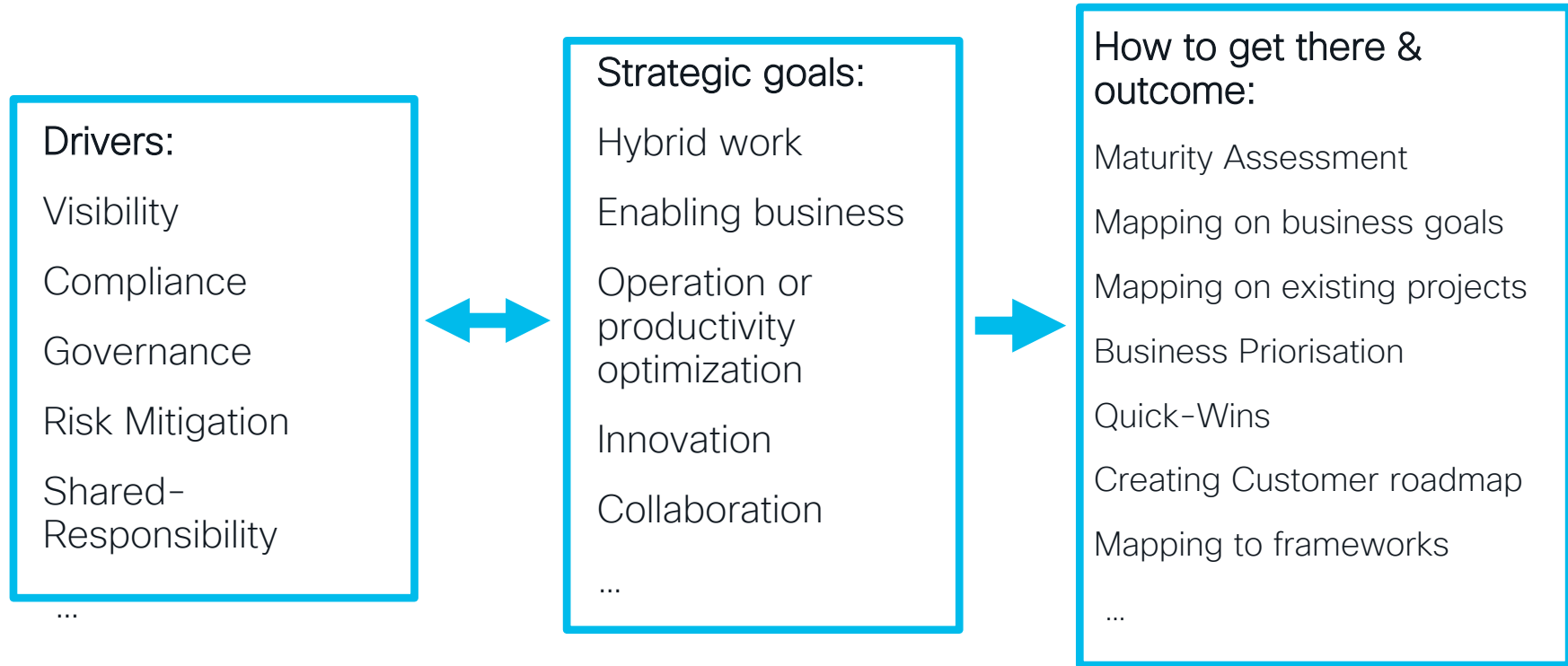
# Business goals on focus

Balance between productivity and security

- Empower the business (resilience)
- Empower the user
- Frictionless as possible
- Strong security in the backend
- **Business resilience** by capsulating and hardening the process
- **Goal:** Eliminate trade-off



# Motivation, Drivers and how to get an adaptable and open Zero Trust strategy



Business \*and\*  
IT Resilience  
both key factors  
of success

# Brownfield Zero Trust analysis view

- Start with a **Maturity Self Assessment** (what you have – what is good, what is bad)
- Do not start in a “green field view”. **Include the strength of your existing environment** (e.g. Data-Center and or Switching infrastructure – goal: investment protection)
- **Visibility is a key success** (before and after – TCO view)
- Identify **Quick-Wins** for optimization (e.g. Zero Trust Authentication which is more than just MFA)
- Keep your **business goals always on focus!**

# Self-Assessment (reflection from key stakeholder)

What are the drivers?

Where are you?

**Self Assessment**

## Customers Maturity

Each Person would set their own Maturity Level in different Domains for IT-Security in a Zero-Trust Context

What are the top customer's top **business** value drivers?

- Protect Intellectual Property (IP) and Assets
- Protection of Critical Business Infrastructure and Systems
- Reducing Costs and improve efficiency
- Reduce Risk of Advanced Cyber Threats and Data Breach
- Streamline other Verticals (e.g. CRM usage)
- Control to Cloud's Shared Responsibility Model
- Access Control
- Discovery and Visibility (Back, Front, SaaS, PaaS)
- Protect Company Reputation and Brand
- Secure Cloud Team Formation
- See Ops and Test Ops Viability
- Importance to multi-vendor integration
- Protect and control vendor integration of Cloud
- Cloud Incident Detection and Response
- Multi-Platform Coverage
- Data Protection per se

What are the top customer's top **cloud** value drivers?

What are the top **end-user** value drivers?

- Multi-Factor Authentication
- Posture Management of Users (Device and Location)
- Easy to use (e.g. minimize granular applications)
- Avoidance of security issues from untrusted devices (social, device)
- Micro-Segmentation (Granular Security)
- DevOps with SaaS-Like Approach (Performance, Data, etc.)
- Visibility in different clouds (cloud, shared, AWS, Azure, etc.)
- Secure infrastructure to ensure security in cloud environment
- Access to cloud resources (e.g. SaaS, PaaS, IaaS)
- User Behavior Analytics (UBA)
- Secure Cloud (e.g. SaaS, PaaS, IaaS)
- SASE Alignment

What are the top **end-point** protection value drivers?

- Using Windows embedded Security
- On-premise Hybrid or Cloud Management approach
- Advanced threat protection and security (e.g. endpoint protection)
- Data Protection
- Overall Security Management and Visibility
- Mobile Security
- Integration with other Vendors
- BYOD

What are the top customer's top **data protection** value drivers?

- Privacy and Compliance Regulations
- Physical Location of the data (on-premise and cloud)
- Content Protection (DLP functionality)
- Classification & Encryption
- Reducing Risk to a Regulatory Breach
- User Awareness and Training
- Visibility and Discovery
- Unified Policy Management

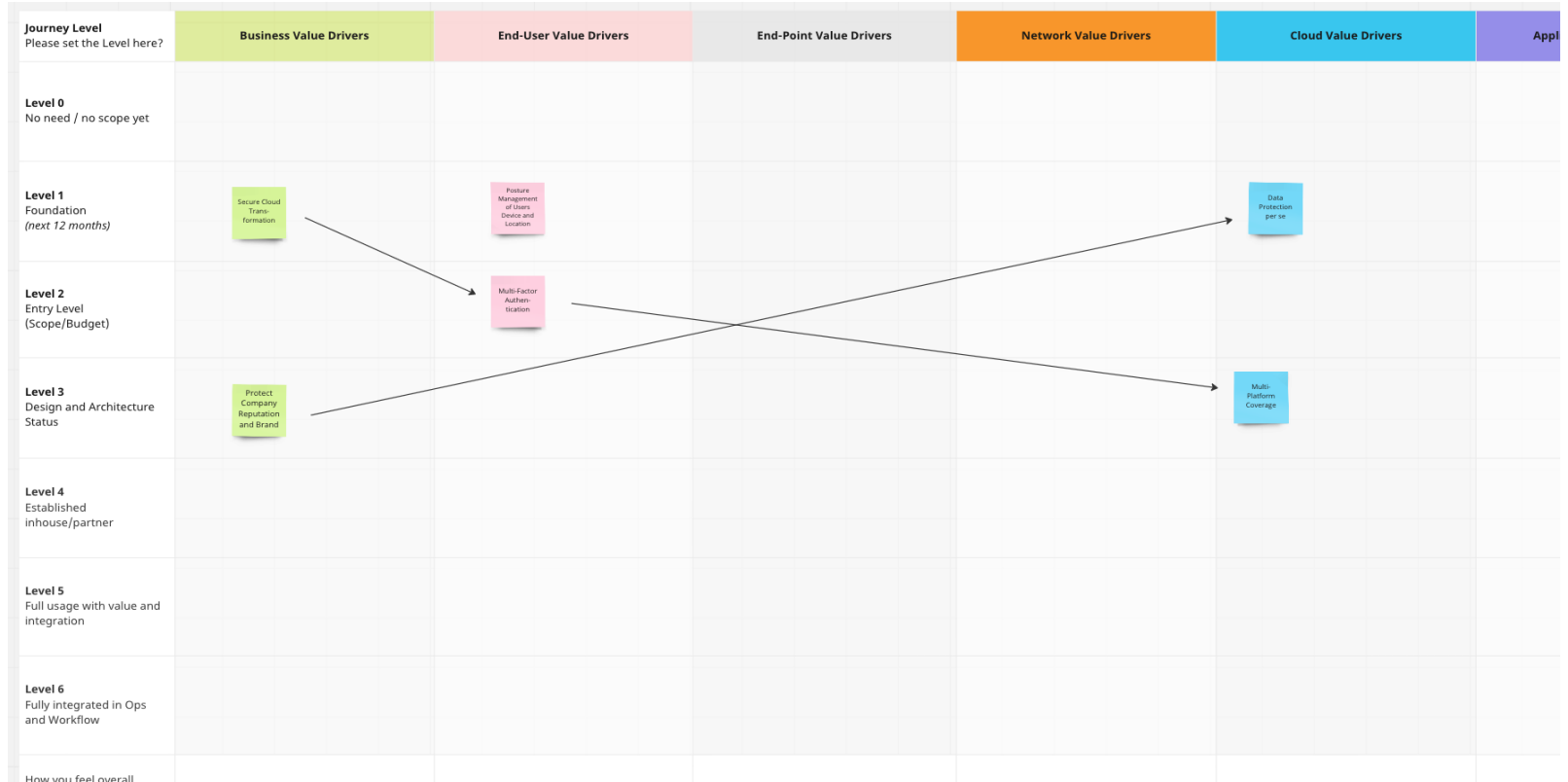
**Journey Level**  
Please set the Level here?

	Business Value Drivers	End-User Value Drivers	End-Point
<b>Level 0</b> No need / no scope yet			
<b>Level 1</b> Foundation (next 12 months)			
<b>Level 2</b> Entry Level (Scope/Budget)			
<b>Level 3</b> Design and Architecture Status			
<b>Level 4</b> Established inhouse/partner			
<b>Level 5</b> Full usage with value and integration			
<b>Level 6</b> Fully integrated in Ops and Workflow			
How you feel overall			

How you feel overall

😊 😐 😞 😡

# Self-Assessment (reflection from key stake-holder)



# Mapping the business goals

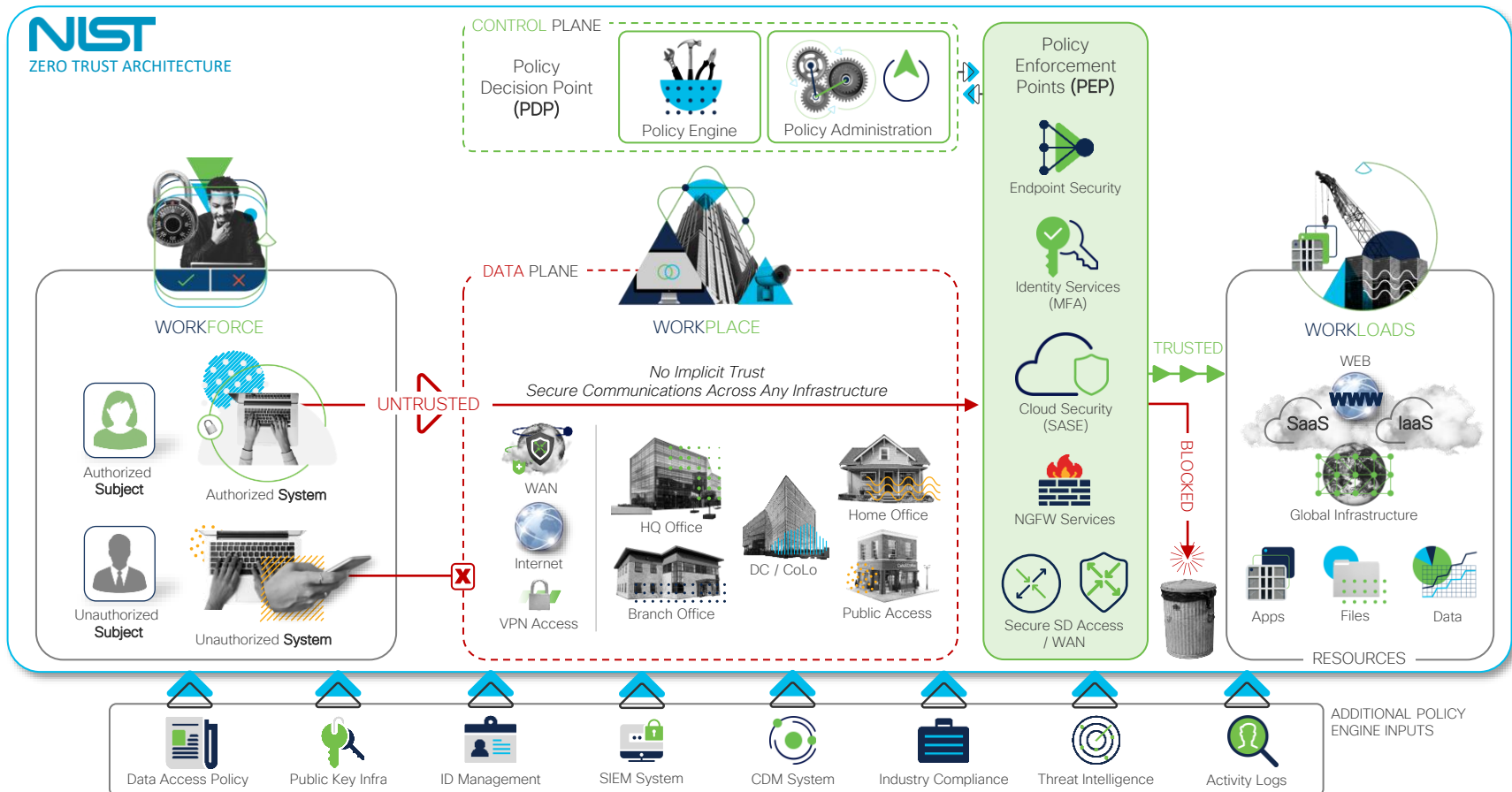
Key instrument of a successful foundation on ZT

Business goals	Zero Trust instrument
Compliance and Governance	Visibility and Authentication
Protect each business flow and process	Segmentation
Business scale / extensibility	Workload strategy on-prem/cloud
cost-efficient	Flexible components (e.g. cloud, containerization)
Flexible business adaption	Frictionless by Authentication and Segmentation of workloads
...	...

# Cisco's Zero Trust – a Framework for the future



# Cisco's Zero Trust Mapping on NIST Framework



Enrich your  
core-business in  
all IT areas



**CISCO** *Live!*



# Conclusion



# Strategy and Planning your Zero Trust journey

- (1) Start a conversation with a business solutions architect
- (2) Include your main key stakeholders of your IT & LOB
  - What's your business goal in 2-3 years from now
  - Define objectives (desired Zero Trust outcomes)
  - Maturity your IT infrastructure
  - Consider Quick-Wins incl. gap analysis
  - Create a strategic roadmap (on business and strategic architecture) – action plan
- (3) Review (2) this every 3-4 months

Use a Business Focus  
Approach for your Zero  
Trust Architecture

Enrich, Empower, Secure  
your Business Resilience  
with Cisco

Book your ZT Workshop  
now!



# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).





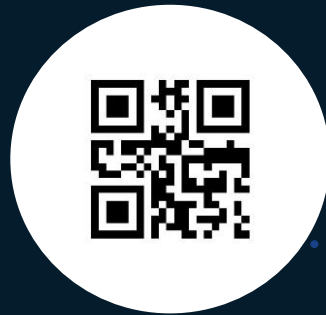
The bridge to possible

# Thank you

CISCO *Live!*

# Are you playing the Cisco Live Game?

Scan the QR code and earn your  
**Cisco Theater** points here



CISCO *Live!*

ALL IN