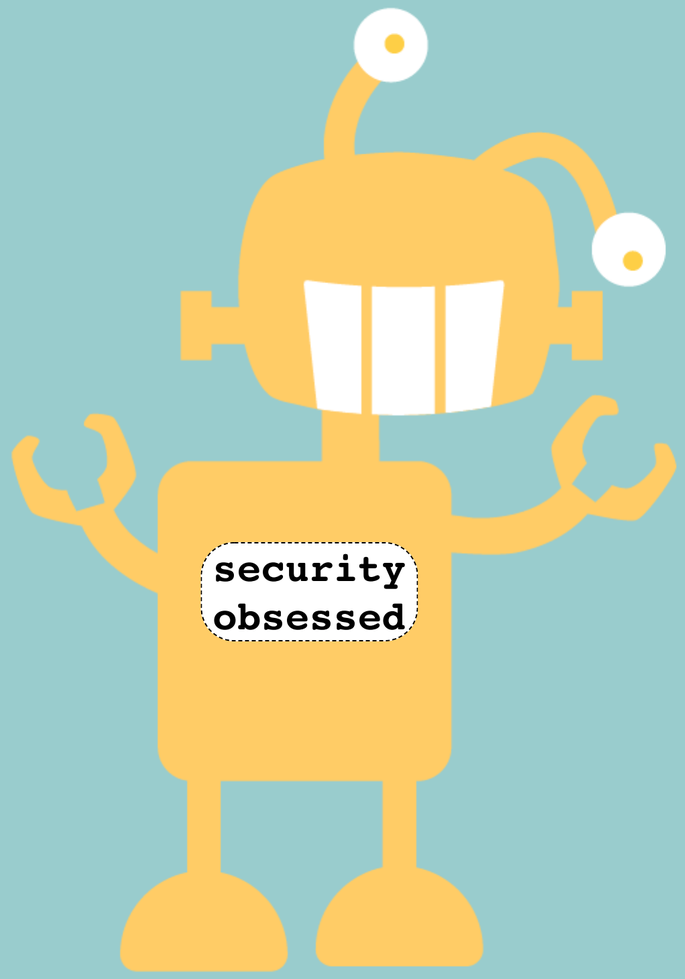
Zero Trust

Enabler for data sovereignty
and secure data communication

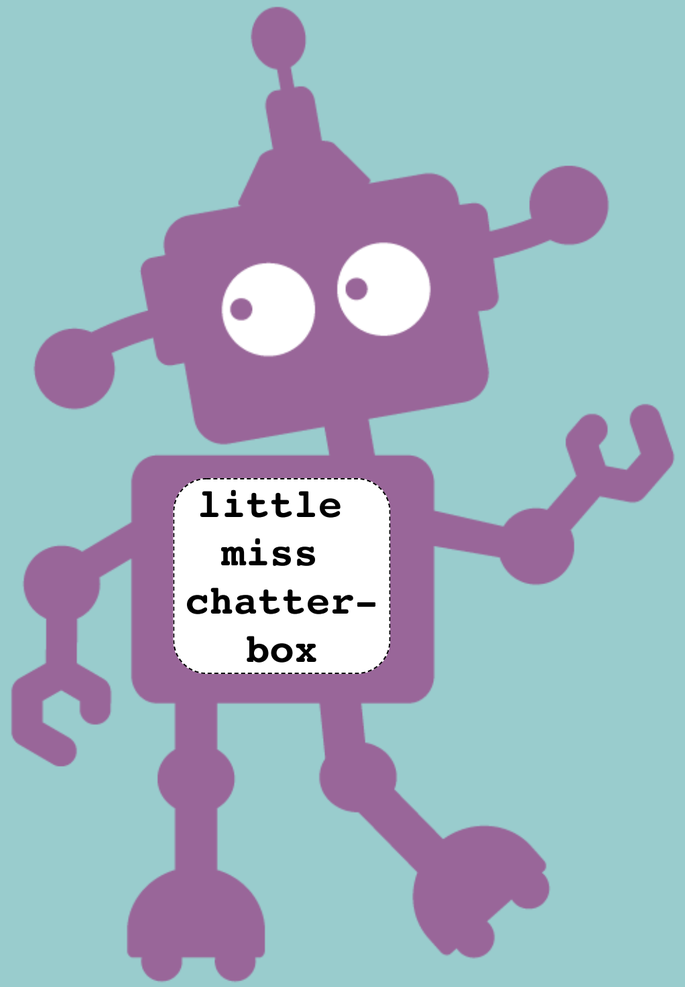
Hello from pi-lar

Short introduction to zero trust (~15 minutes)
Data Sovereignty example (~10 minutes)
Questions and discussion (~20 minutes)

Meet Marvin



and Eliza

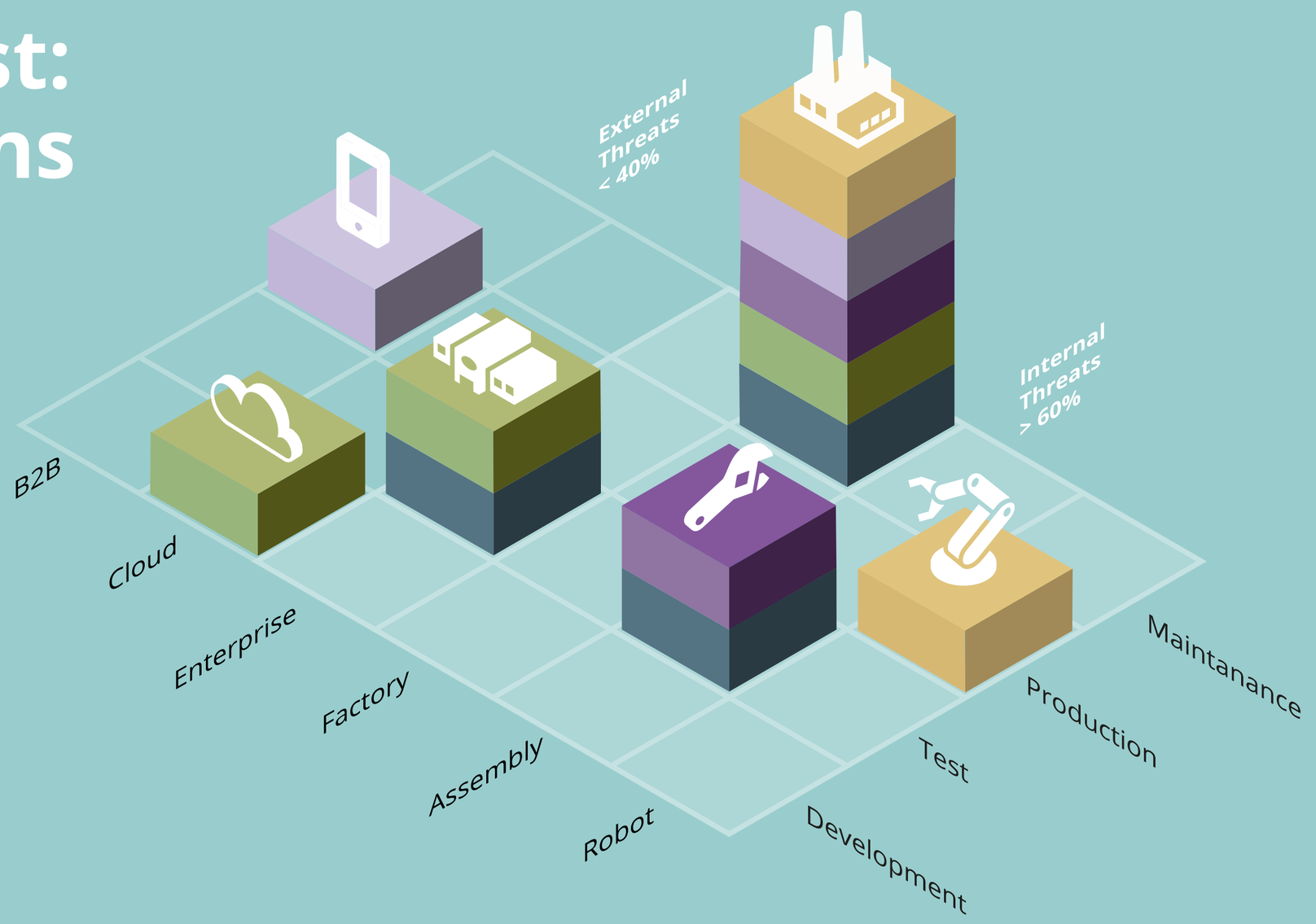


Security of the Past: Limitations

_ only protection of bilateral IP connections
_ not protecting different data objects, but apis
_ unsuited for rapid change of
data owners / new data channels

pi-lar

Security of the Past: Limitations

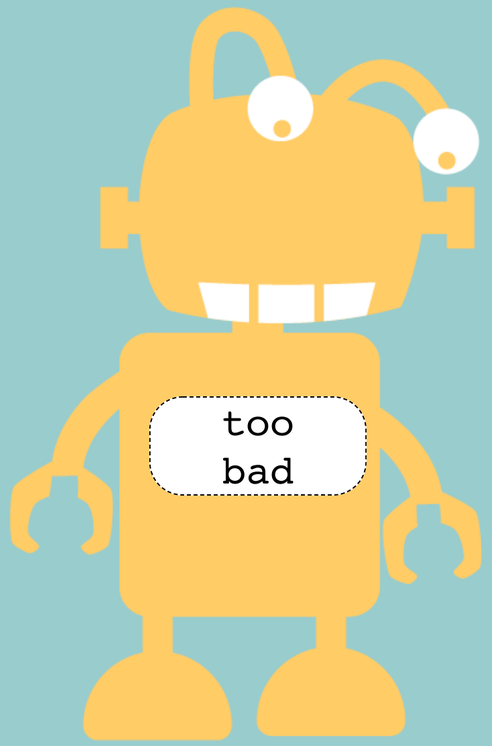


Security of the Past: Limitations

_ static design: build once, run forever

_ new requirements vs. security design

_ introduce security exceptions on change



Security of the Future: Zero Trust

_ trust perimeter has changed

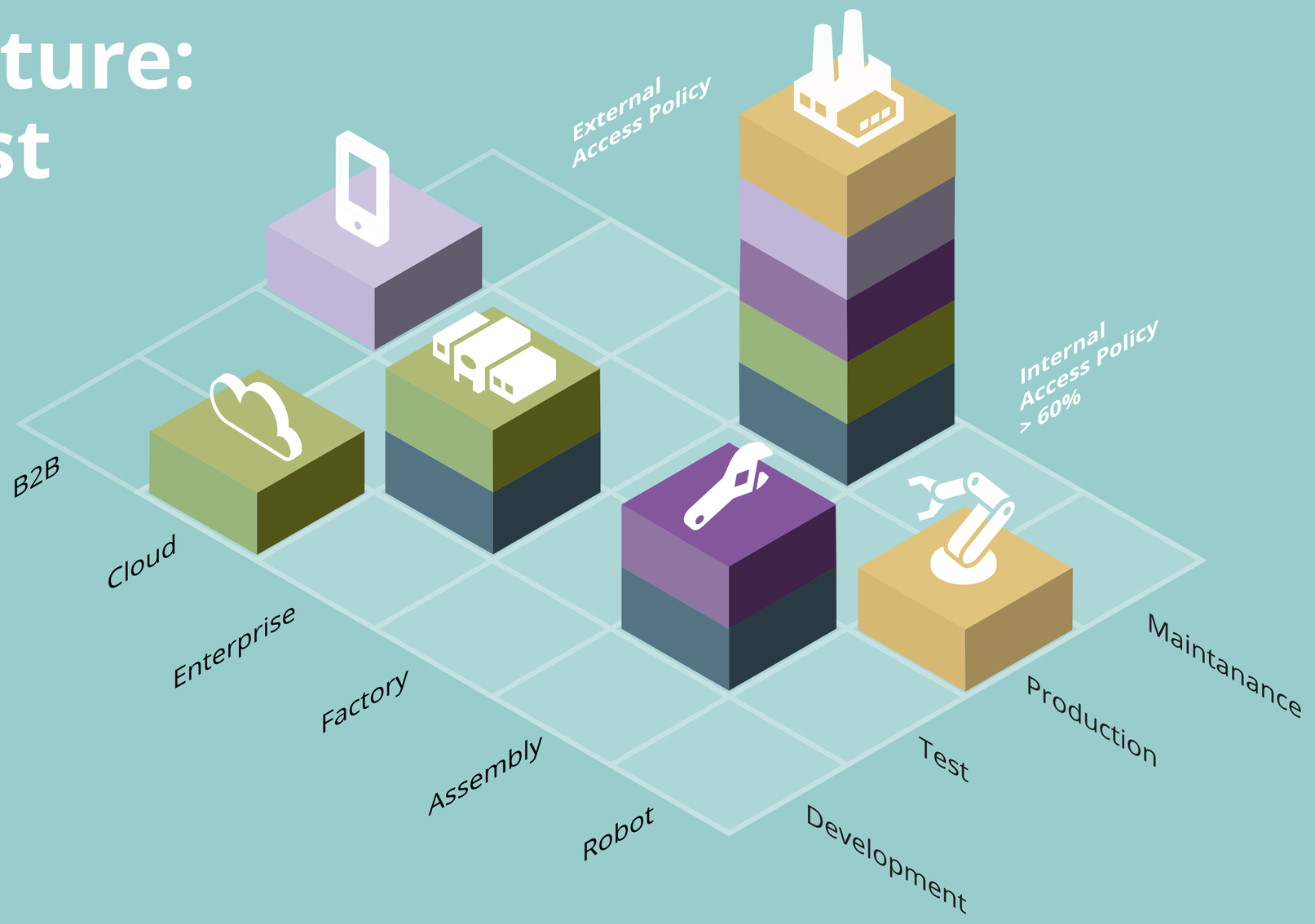
_ fragmented information (flows) need protection

_ authn/authz must be possible everywhere

_ data objects governed by
external/internal access policies (AP)

pi-lar

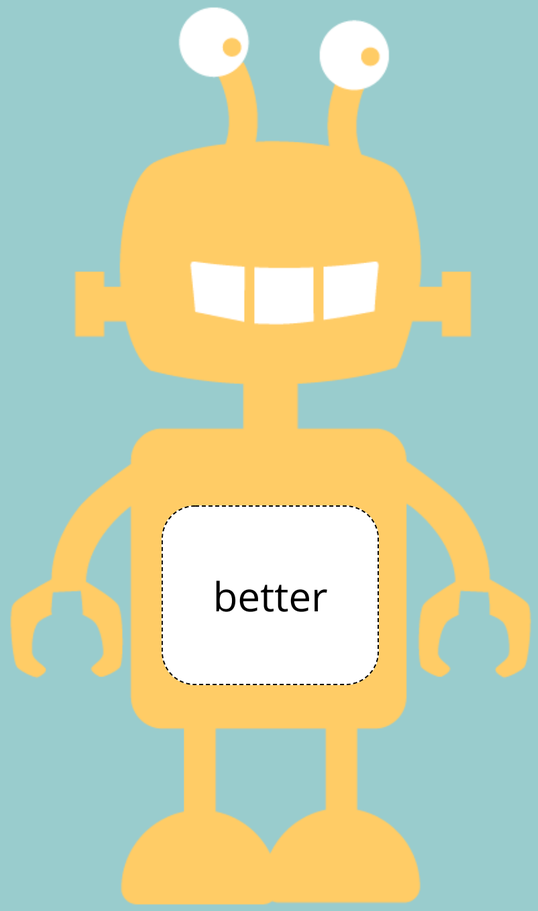
Security of the Future: Zero Trust



- Business
- Functional
- Information
- Communication
- Device

Security of the Future: Zero Trust

- defines trust levels for data objects or smaller groups
- fine grained access to objects possible
- more insights means minimizing risk
- Never trust, always verify

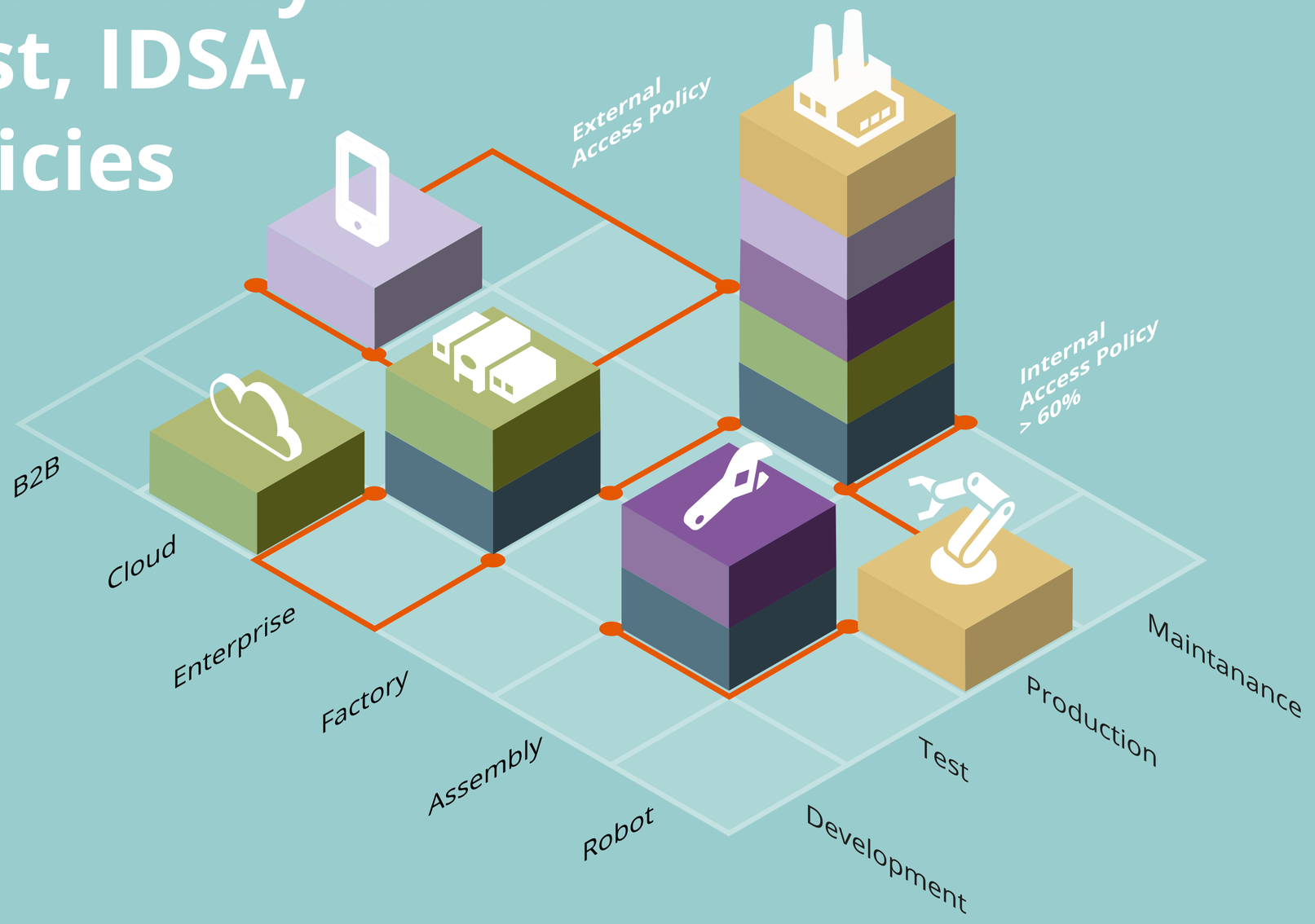


Security for Complex Ecosystems: Zero Trust & Access Policy

_ data object interactions main driver
for future IT architecture
_ devices produce and consume data
at the same time
_ respect different data owners per device
if one fails, all suffer!

pi-lar

Security of Ecosystems: Zero Trust, IDSA, AccesPolicies



- Business
- Functional
- Information
- Communication
- Device

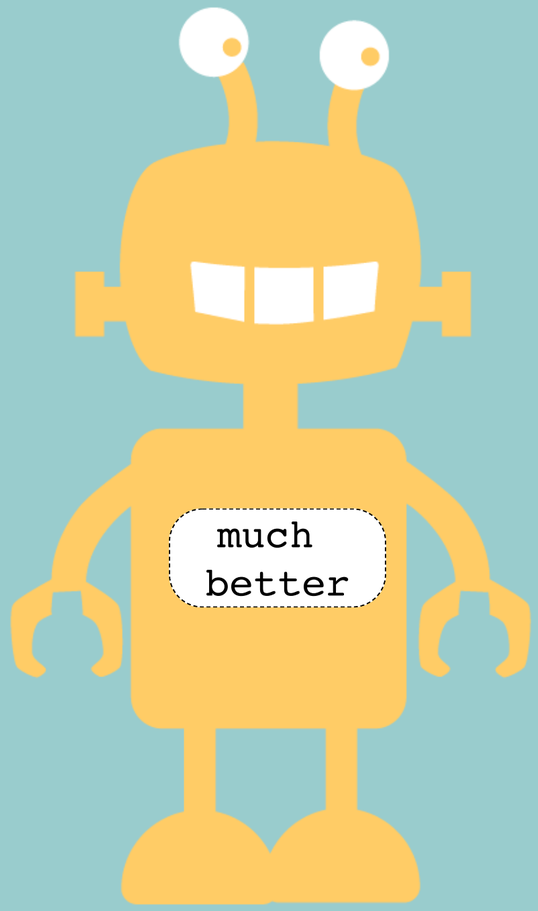
Security of Ecosystems: Zero Trust, AccesPolicies

_ business agility: enables your company to adapt and survive

_ switch to a different service provider is easy

_ change policies in days (rather than months)

_ enables data reduction and data economy



Reliability

Integrity

Multi-Tenant
Operational Context
Data Ownership
Safety First

Confidentiality

Business Model Innovation
Service / Product
CAPEX vs. OPEX
Time2Market
B2B Ecosystem

Privacy

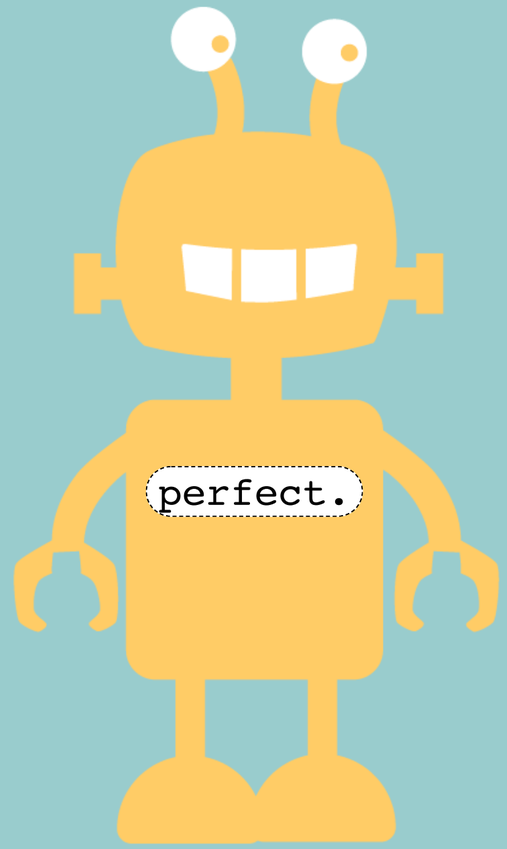
GDPR
Governance Risk Compliance
Intellectual Property
KRITIS / Legal Enforcement

Availability

Access Rights
Operation Excellence
IT Security KnowHow
Skill Gap

Ten principles of Zero Trust Architecture:

- Know your architecture including users, devices, services
- Create a single strong user identity
- Create a strong device identity
- Authenticate everywhere
- Know the health of your devices and services
- Focus your monitoring on devices and services
- Set policies according to value of the service or data
- Control access to your services and data
- Don’t trust the network, including the local network
- Choose services designed for zero trust

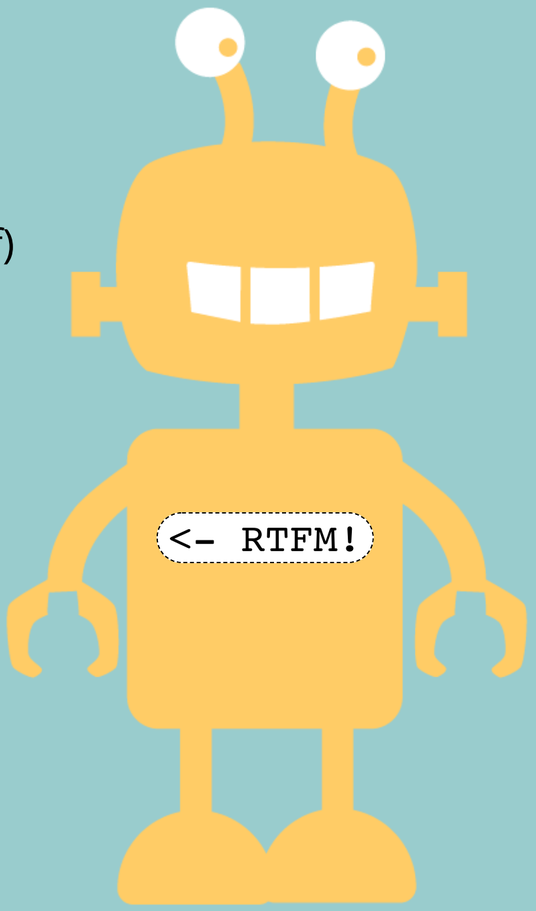


Ressources:

- NIST -
  Implementing a zero trust architecture (March 2020)
  (www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zt-arch-project-description-draft.pdf)

- O’Reilly -
  Zero Trust Fundamentals
  (www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html)

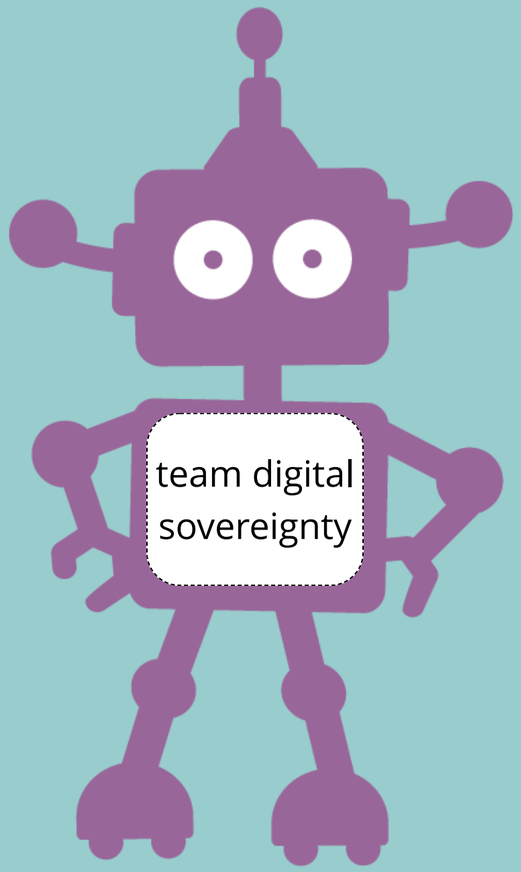
- UK NCSC
  Principles to help you design and deploy a zero trust architecture (github.com/ukncsc/zero-trust-architecture)



Data Sovereignty

_The capability of an individual or an organization to have control over their personal and business data. This entails that they should be able to know which party holds which data, under what conditions (purpose, duration, reward), where data is kept, and are able to re-use the data at other places.

Source: Data Sovereignty Now



Secure Data Exchange with IDSA

_ important **roles** of data sovereignty:

_ data owner

_ data provider

_ data creator

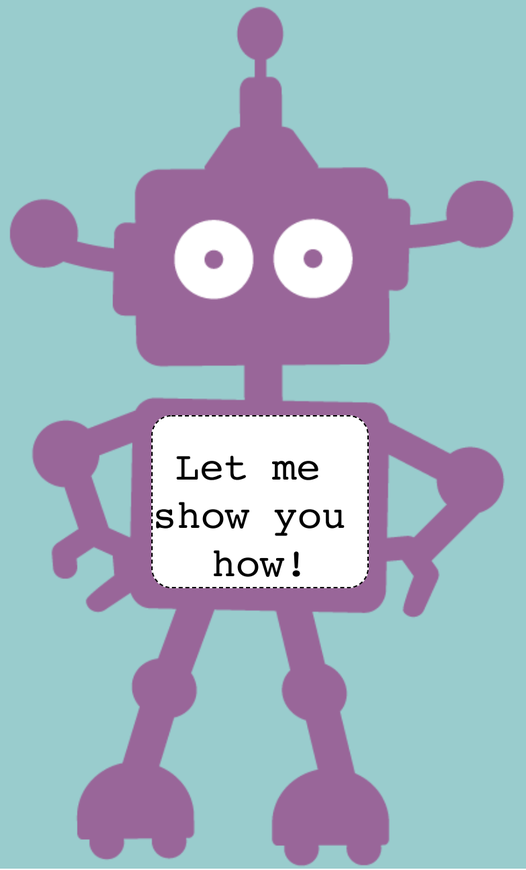
_ data consumer

_ application provider

_ vocabulary provider

_ service provider

_ service data consumer

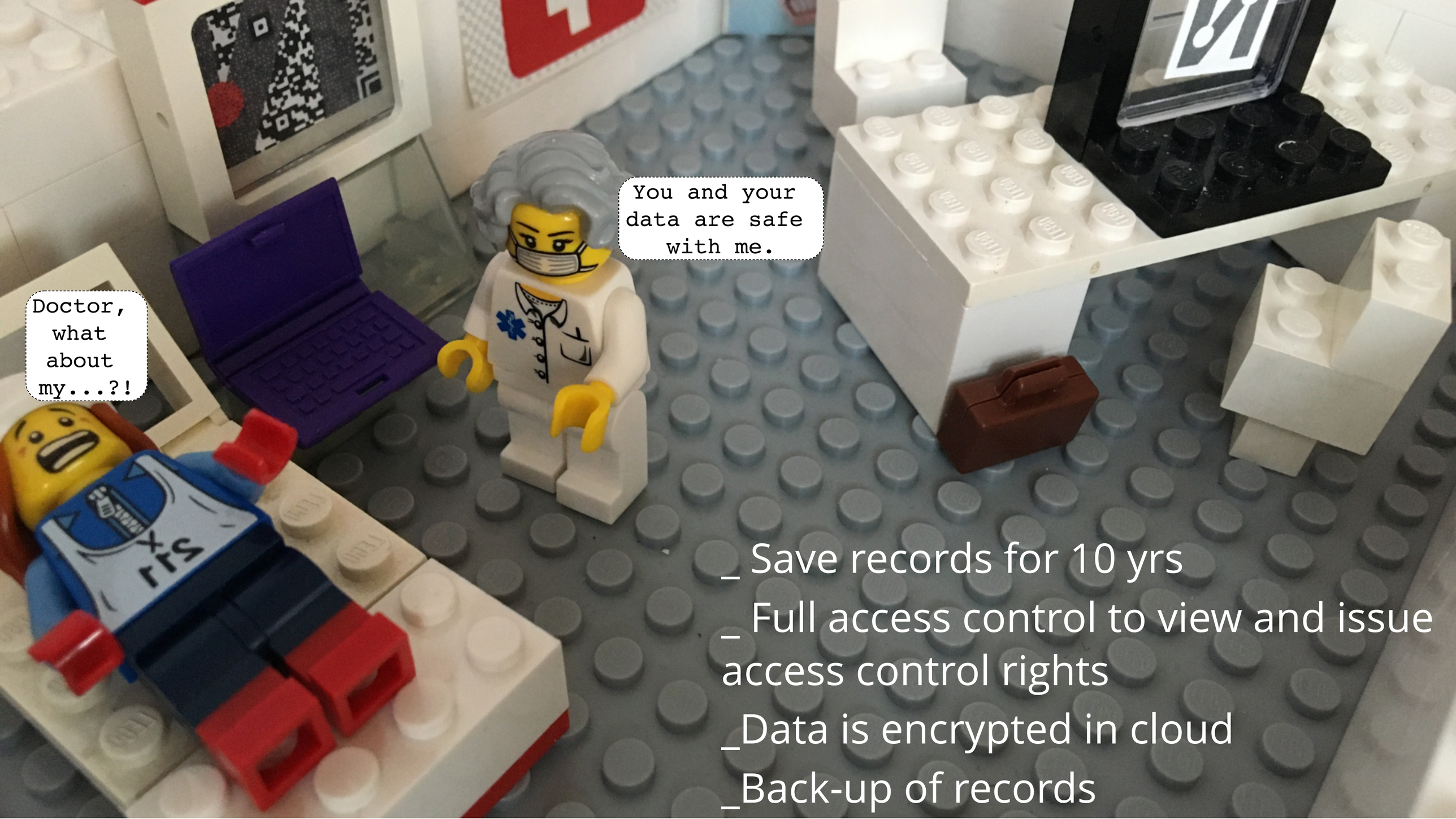


source: https://www.internationaldataspaces.org/ids-ram-3-0/

*$!%/&!#X

Dr. SiTh* has not only taken the hippocratic oath, she also believes in protecting her patients' data.

*Secure internet of Things



_ Save records for 10 yrs

_ Full access control to view and issue access control rights

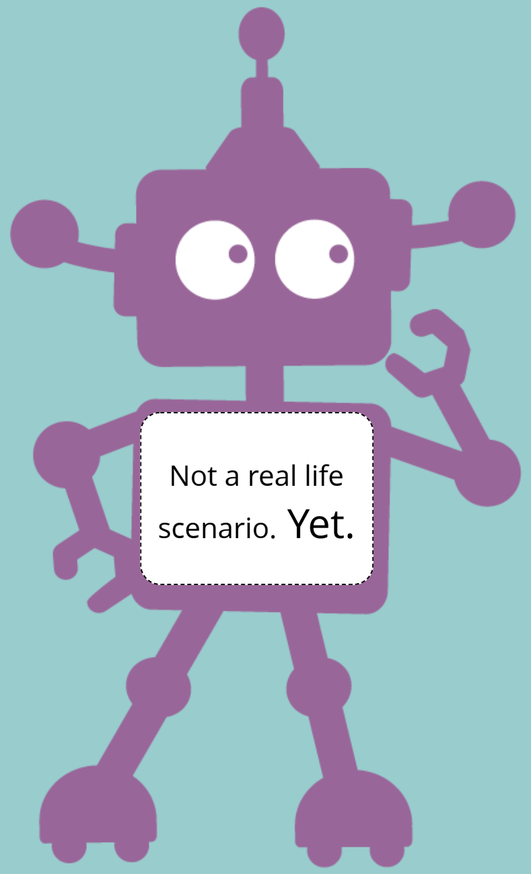
_Data is encrypted in cloud

_Back-up of records

Dr. Bone just received encrypted patient record and can add the x-rays.

Mr. Caseworker from Social Security Services is already processing the accident data to which Chris has provided access.

Data Sovereignty: a Zero-Trust Security Environment



Transparent data communication should be available to everyone!

Our Approach: neuropil.org

_ secure, sovereign and sustainable data integration

_ small, secure connector library

_ a decentralized identity space enabling privacy

_ discovery of data channels funded by NGI Zero Discovery

_ pub/sub message encryption funded by NGI Zero Discovery

pi-lar

Collaboration via neuropil.io

_ would you like to help implementing the medical use case?

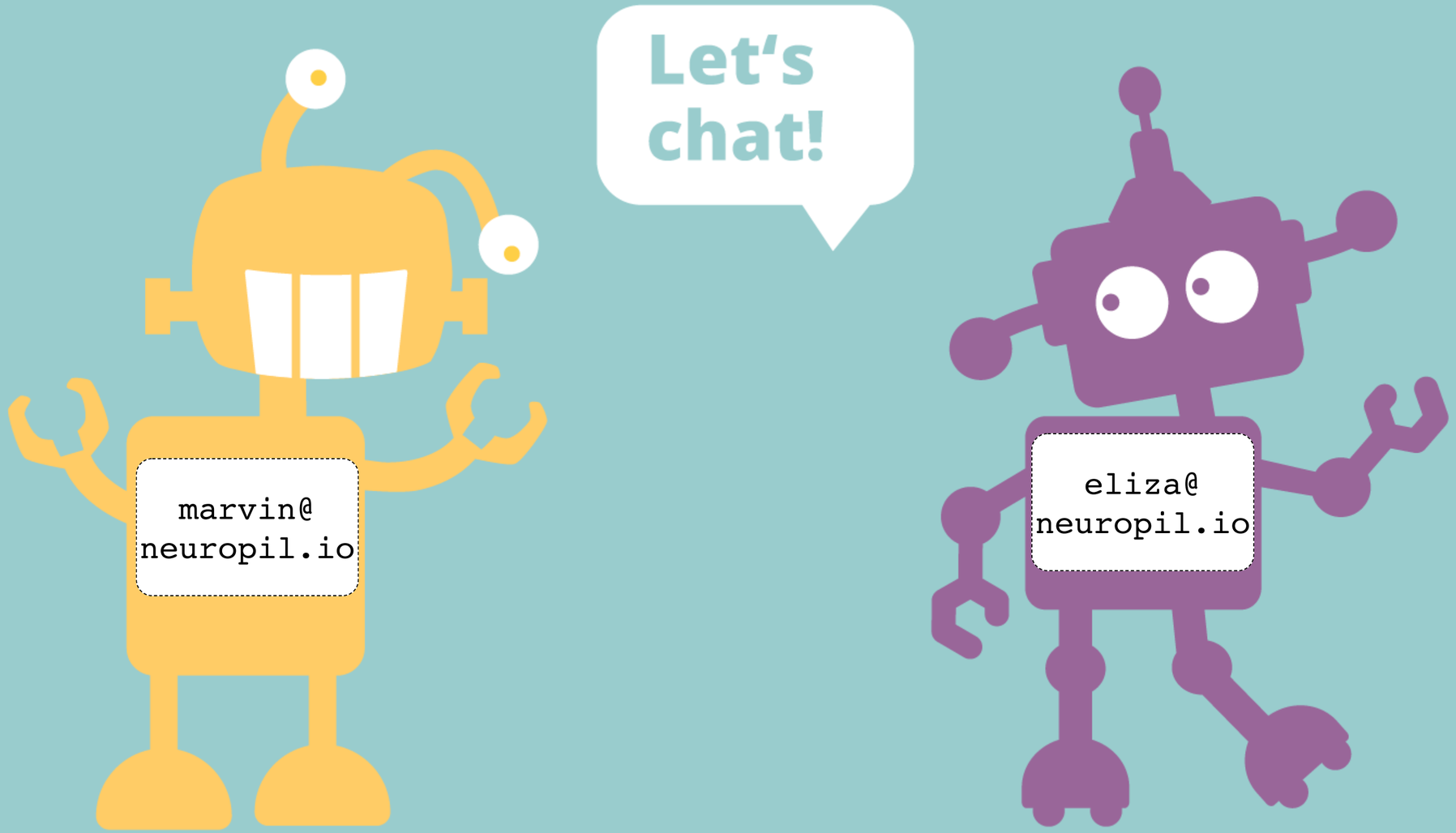
_ other ideas about joint development in the context of the NGI?

_ let's redefine IIoT security together !

_ check out our development repository:

_ https://gitlab.com/pi-lar/neuropil/

pi-lar



pi-lar GmbH
Kreuzgasse 2-4
D-50667 Köln

+49 221 16531700
info@pi-lar.net
www.pi-lar.net

pi-lar