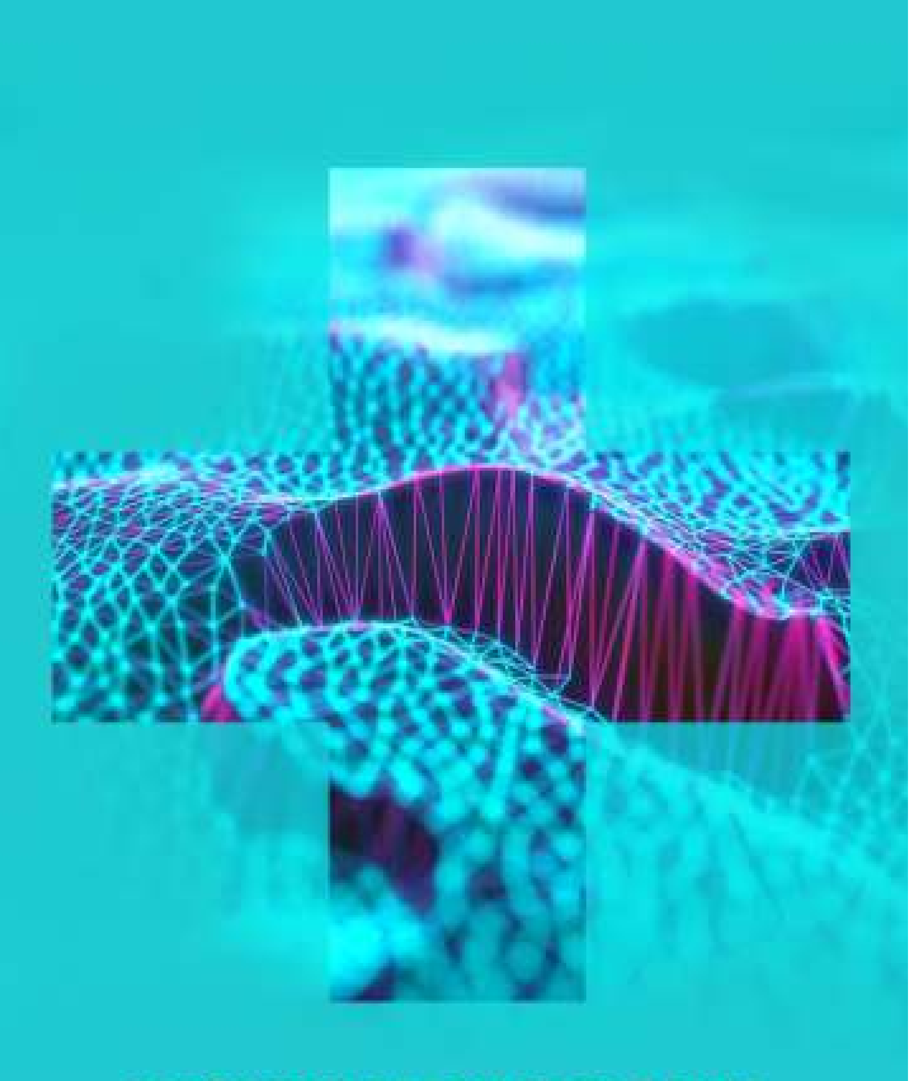
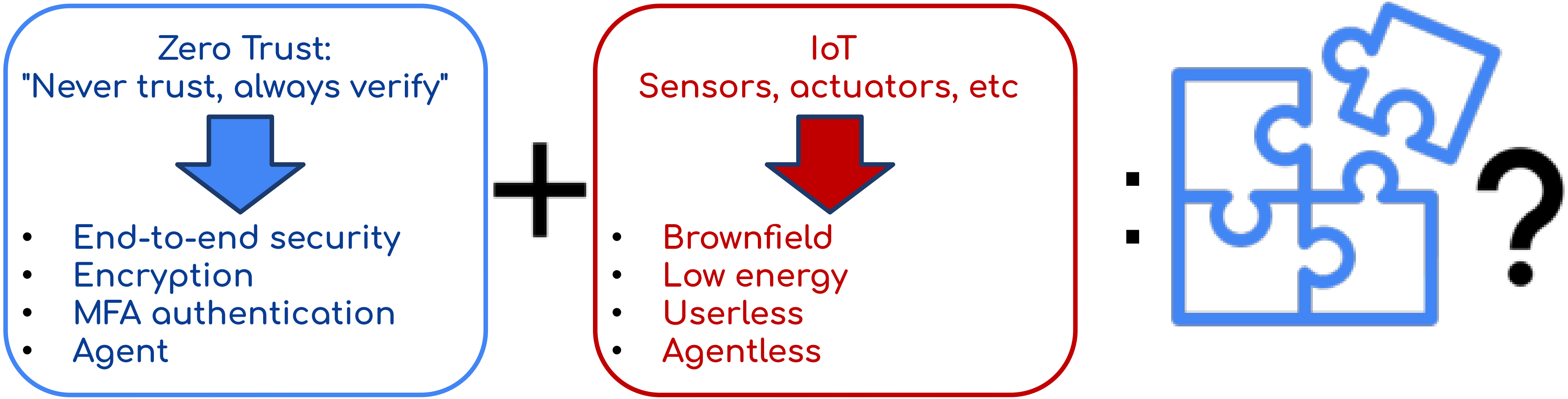


Zero Trust & IoT: An Industrial Systematic Literature Review

Dr. Laurent Bobelin
laurent.bobelin@insa-cvl.fr

Topic



Zero Trust:
"Never trust, always verify"

- End-to-end security
- Encryption
- MFA authentication
- Agent

+

IoT
Sensors, actuators, etc

- Brownfield
- Low energy
- Userless
- Agentless

: ?

Table of content

- Context
  - Zero Trust Overview
  - IoT from the ZT Point of View
  - Features, Tools and Solutions
- Study Purposes and Method
  - Questions to Be Answered
  - Systematic Literature Review Setup
- Results and Analysis
- Conclusion

Zero Trust Overview

"Never trust, always verify"

Continuous trust verification

Least priviledge by default

Continuous security inspection

Central security management

Zero Trust Guidelines

Authenticate everything

Use strong authentication (MFA)

Encrypt whenever possible

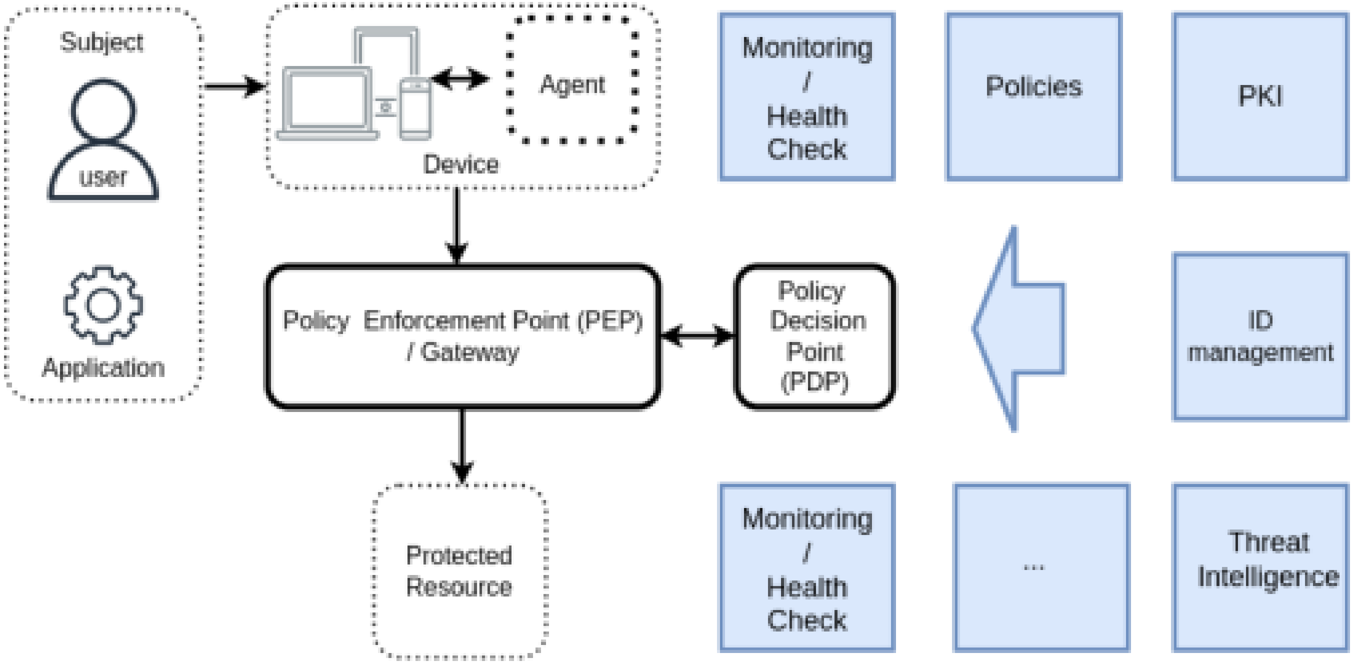
Scan, patch and rotate devices regularly

Enumerate all flows

Use Private Key Infrastructure

Use end-to-end encryption

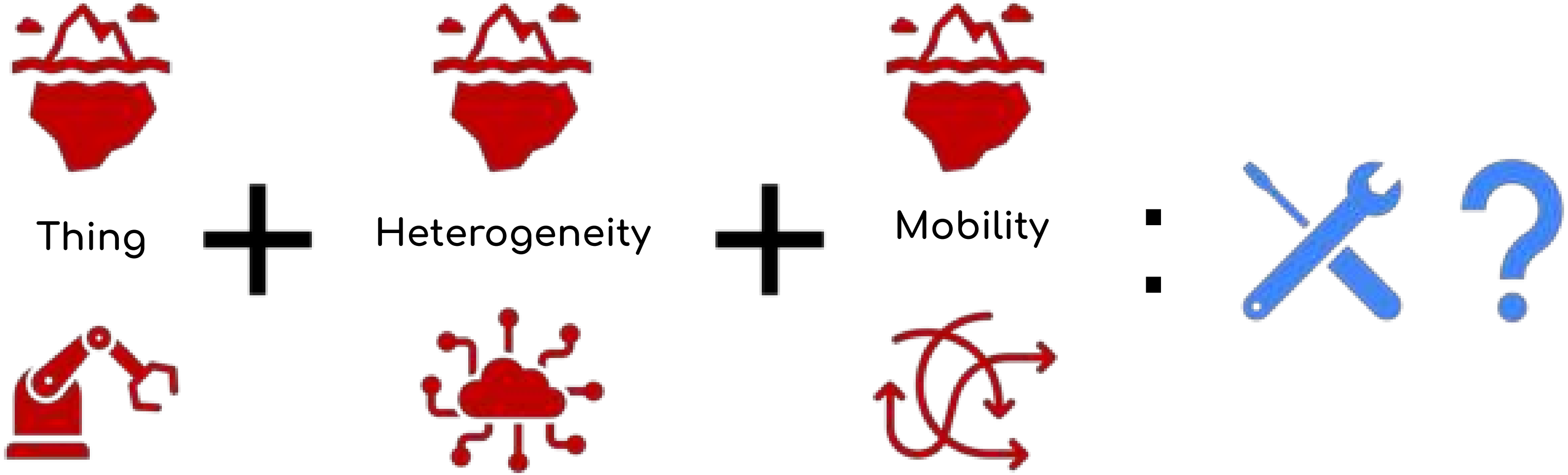
ZT NIST Architecture


Subject
user
Application
Agent
Device
Policy Enforcement Point (PEP) / Gateway
Policy Decision Point (PDP)
Protected Resource
Monitoring / Health Check
Policies
PKI
ID management
Monitoring / Health Check
...
Threat Intelligence

Things From the ZT Point of View

Userless	Low Energy	Brownfield	Short-lived
🚫	🚫	🚫	🚫
MFA	Encryption	Agent	Enrolment

IoT Infrastructure From the ZT Point of View



Thing + Heterogeneity + Mobility : ?

Features, Tools and Solutions

Agentless scanning and discovery

Digital twin

Brownfield gateway

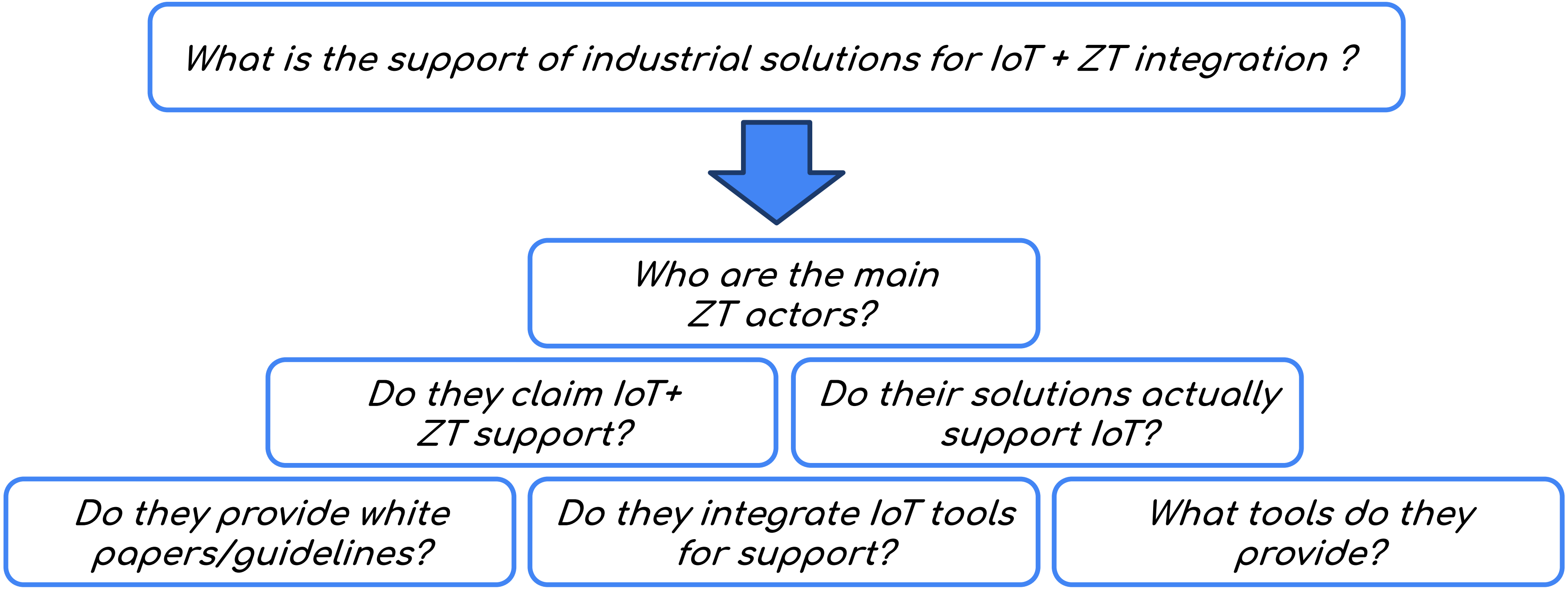
Isolation

Greenfield software

Table of content

- Context
  - Zero Trust Overview
  - IoT from the ZT Point of View
  - Specific Features, Tools and Solutions
- Study Purposes and Method
  - Questions to Be Answered
  - Systematic Literature Review Setup
- Results and Analysis
- Conclusion

Questions to be Answered



What is the support of industrial solutions for IoT + ZT integration ?

Who are the main ZT actors?

Do they claim IoT+ ZT support?

Do their solutions actually support IoT?

Do they provide white papers/guidelines?

Do they integrate IoT tools for support?

What tools do they provide?

Systematic Literature Review Setup

- Sources: **grey literature only** (white papers, website, documentation, and so on)
- Main actors: 4 criteria
  - GAFAM
  - Main cybersecurity actors in terms of revenue
  - Renowned cybersecurity actors
  - Major actors in Cloud-based hosting

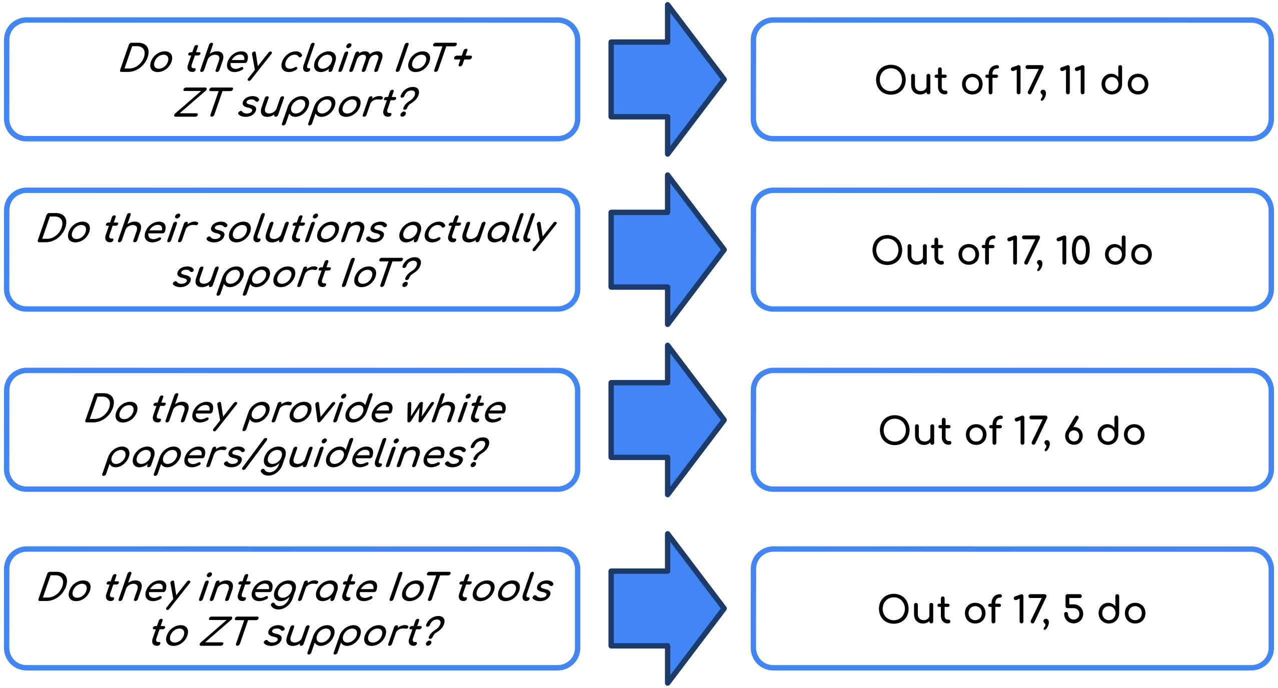
Table of content

- Context
    - Zero Trust Overview
    - IoT from the ZT Point of View
    - Features, Tools and Solutions
- Study Purposes and Method
    - Questions to Be Answered
    - Systematic Literature Review Setup
- Results and Analysis
- Conclusion

Who are the main ZT actors?

- Microsoft (Azure)
- IBM Cloud (Kyndryl)
- Oracle
- Juniper
- Synopsys
- Palo Alto Networks
- McAfee, Fortinet
- CyberArk
- Google
- Alibaba Cloud
- Tencent Cloud
- OVHCloud
- DigitalOcean
- Linode (Akamai)
- AWS

Results for those 17 actors



Do they claim IoT+ ZT support?

Out of 17, 11 do

Do their solutions actually support IoT?

Out of 17, 10 do

Do they provide white papers/guidelines?

Out of 17, 6 do

Do they integrate IoT tools to ZT support?

Out of 17, 5 do

Who provides what

	Agentless scanning and discovery	Digital twins	Greenfield software	Brownfield gateway
Azure	✓	✓	✓	✓
Palo Alto Networks	✓	✓		
AWS	✓	✓	✓	
NetFoundry	✓		✓	
Fortinet	✓	✓		

Table of content

- Context
  - Zero Trust Overview
  - IoT from the ZT Point of View
  - Features, Tools and Solutions
- Study Purposes and Method
  - Questions to Be Answered
  - Systematic Literature Review Setup
- Results and Analysis
- Conclusion

Conclusion

- There is a lot of communication about ZT and IoT, but little support
- Integration is the key, but it is most of the time up to the clients
- Some key aspects remains uncovered by companies