trust

point

PITCH DECK.

secure, compliant and streamlined digital identity management in OT environments

›

JANUARY 2026

INTRO

Open-source platform for automated, secure identity management in industrial networks.

INDUSTRIAL DIGITALIZATION

Industry is shifting to **connected, intelligent, and automated** environments.

MANDATORY SECURITY

Cybersecurity and compliance (e.g., CRA, NIS2) will be mandatory.

TRUSTPOINTS APPROACH

Trustpoint enables **manufacturers and operators** to integrate digital identities easily and securely.

Let's secure automation

PROBLEM

Security & Compliance in Industrial OT: **Still Manual, Costly, Risk-Prone**

CERTIFICATE CHAOS

Manual certificate provisioning is **error-prone** and doesn't scale.

SECURITY SKILL GAP

Engineering teams lack **time, resources, and expertise** to manage secure PKI.

VENDOR LOCK-IN

Existing solutions are often **proprietary**, **costly**, or **not designed for OT**.
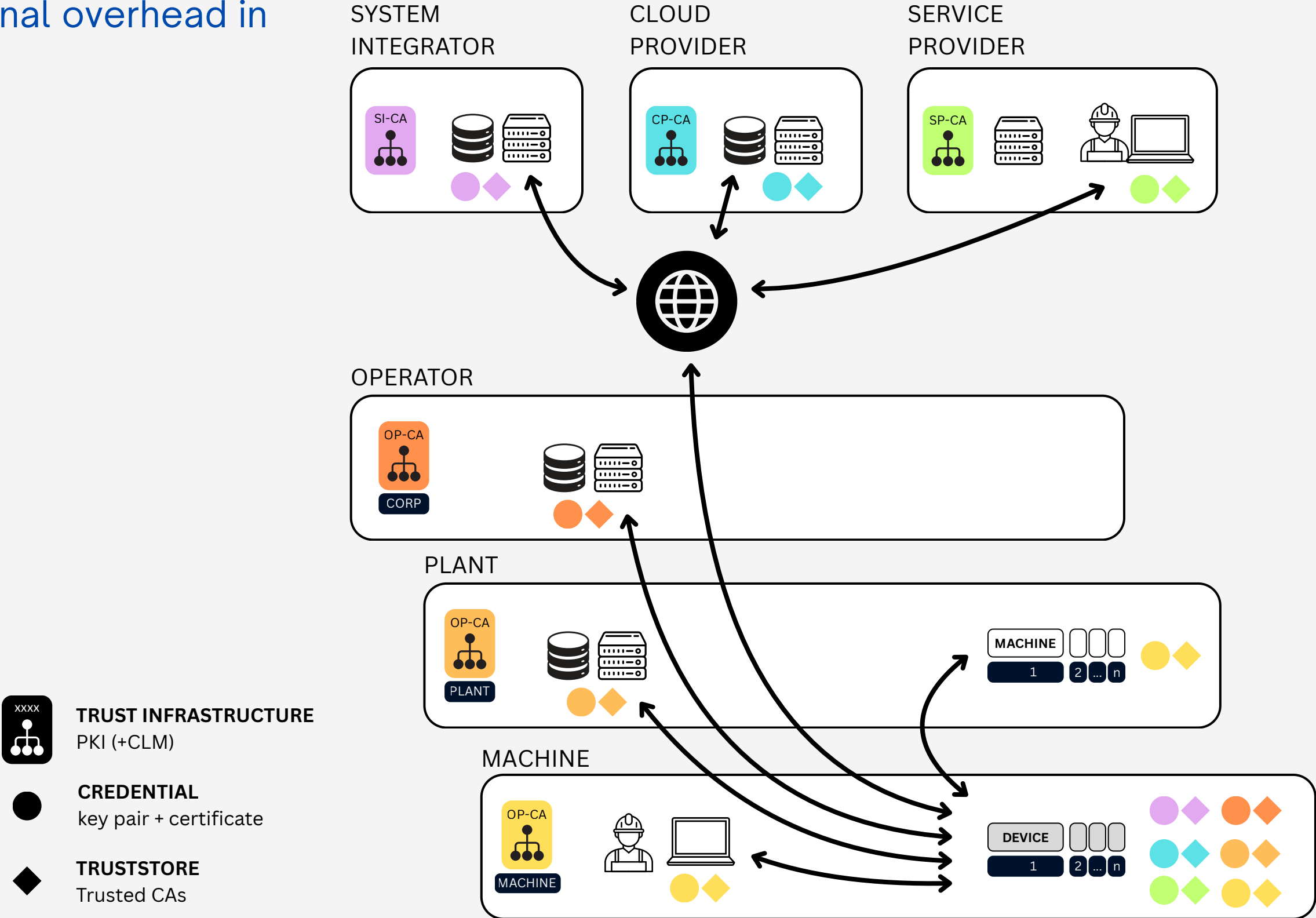
Let's secure automation

* More information about certificates can be found in the appendix.

FRAGMENTATION

trust point

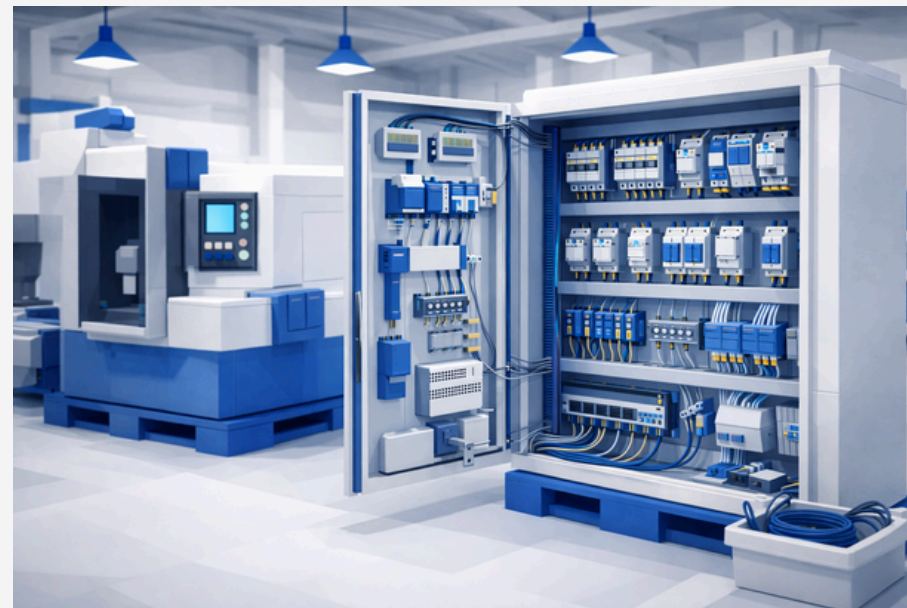Disconnected **certificate silos** increase complexity, risk, and operational overhead in OT environments.

SYSTEM INTEGRATOR
SI-CA

CLOUD PROVIDER
CP-CA

SERVICE PROVIDER
SP-CA

OPERATOR
OP-CA
CORP

PLANT
OP-CA
PLANT

MACHINE
OP-CA
MACHINE

MACHINE
1 2 ... n

DEVICE
1 2 ... n

TRUST INFRASTRUCTURE
PKI (+CLM)

CREDENTIAL
key pair + certificate
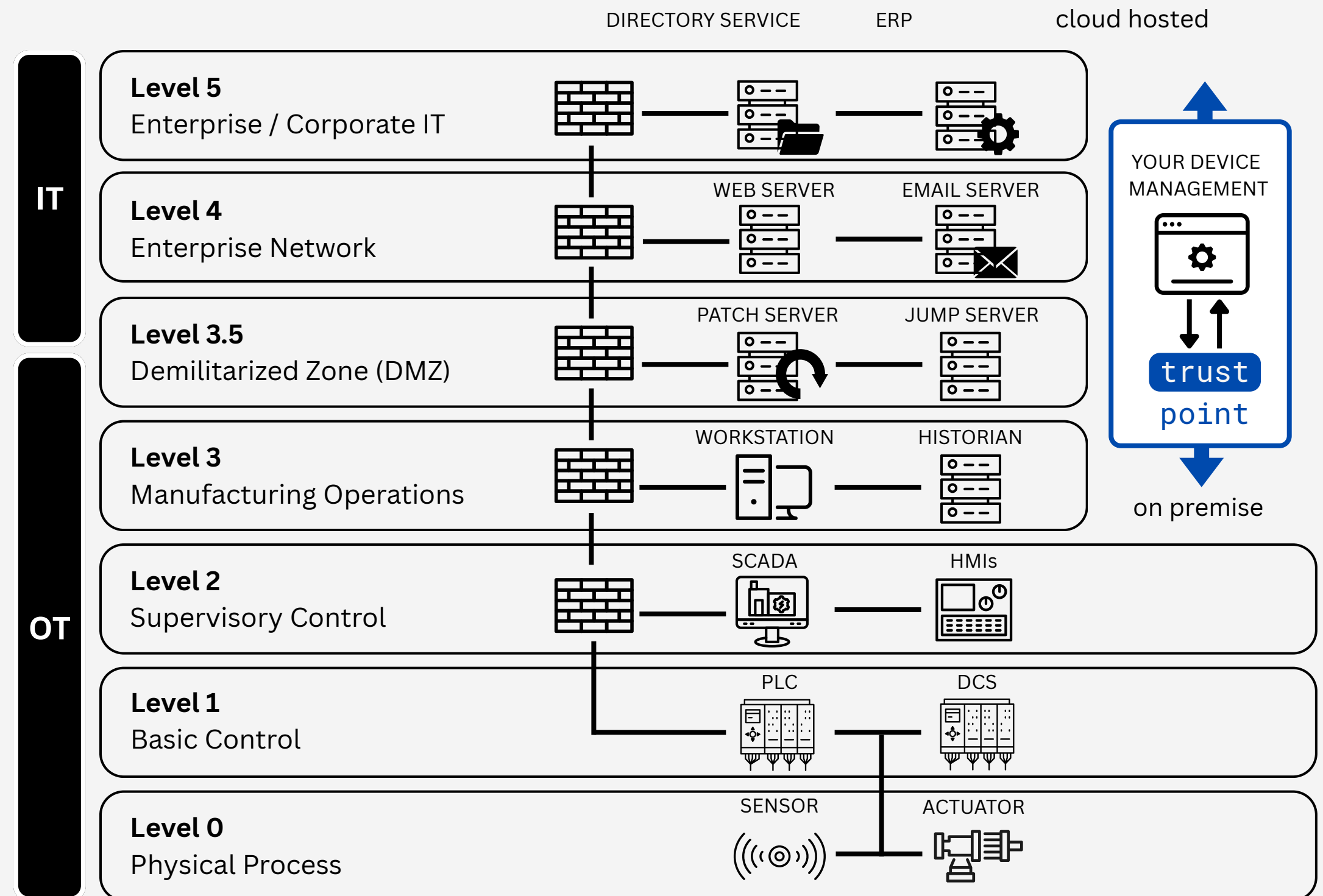
TRUSTSTORE
Trusted CAs

Let's secure automation

DEVICE MANUFACTURER

trust point

Trustpoint can be integrated (headless) into devices, machines, or management platforms to provide built-in certificate and identity management.
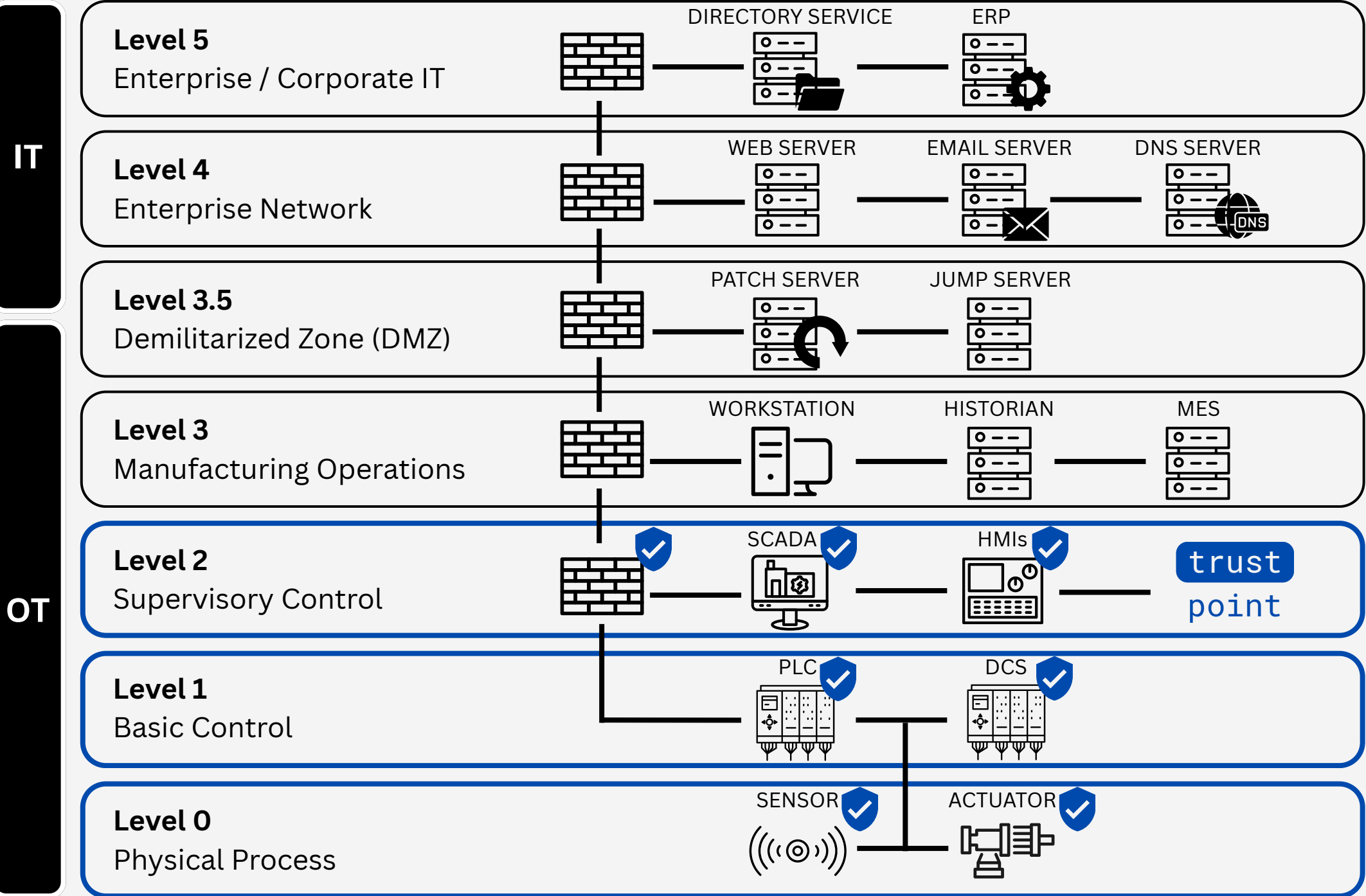
Let's secure automation

	DIRECTORY SERVICE	ERP	cloud hosted

IT

Level 5 — Enterprise / Corporate IT

Level 4 — Enterprise Network — WEB SERVER — EMAIL SERVER

Level 3.5 — Demilitarized Zone (DMZ) — PATCH SERVER — JUMP SERVER

OT

Level 3 — Manufacturing Operations — WORKSTATION — HISTORIAN

Level 2 — Supervisory Control — SCADA — HMIs

Level 1 — Basic Control — PLC — DCS

Level 0 — Physical Process — SENSOR — ACTUATOR

YOUR DEVICE MANAGEMENT

trust point

on premise

SYSTEM INTEGRATORS

trust point

Trustpoint enables system integrators to centrally manage device identities and certificates even in restricted or offline industrial environments.
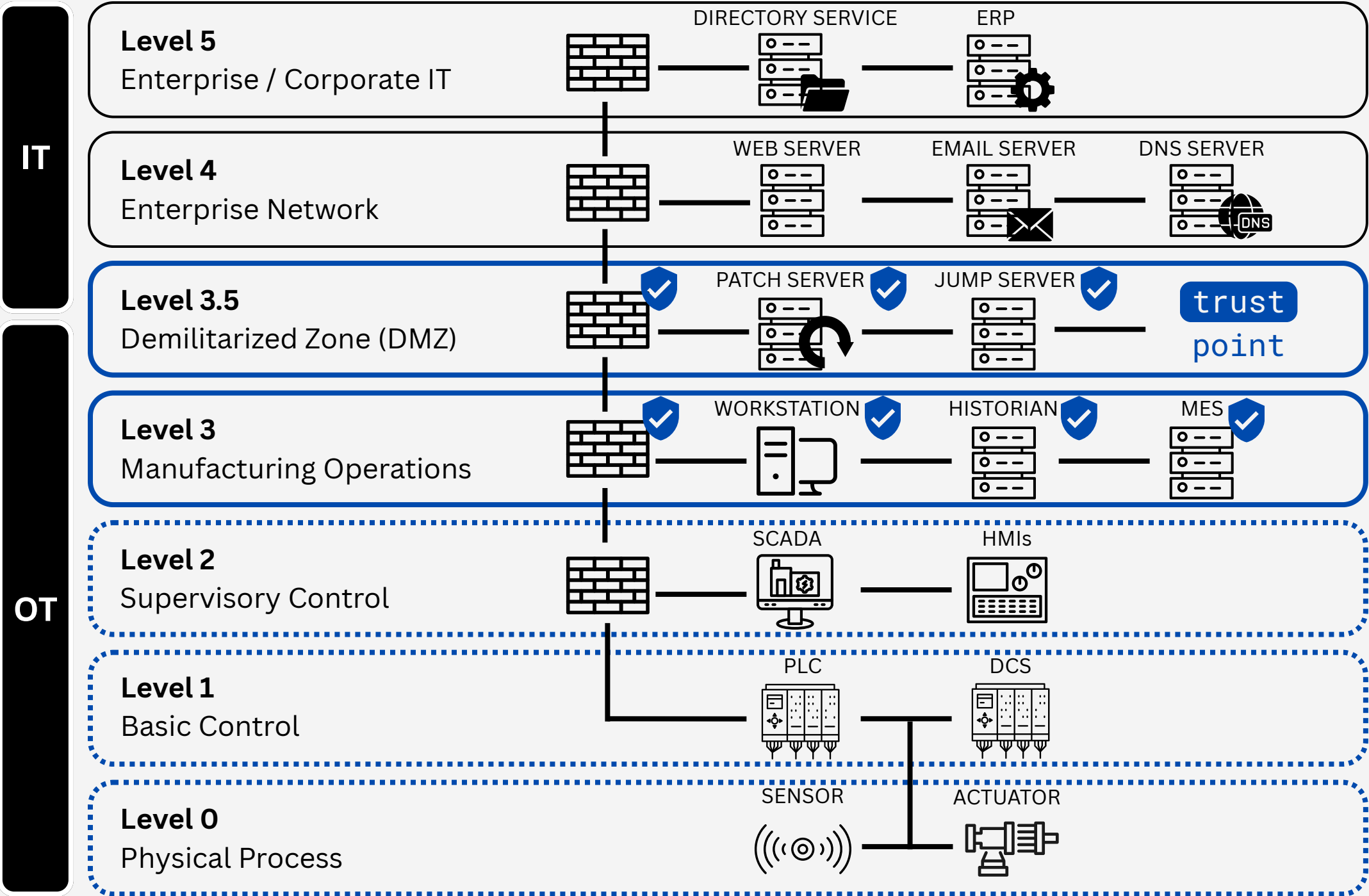
Let's secure automation

OPERATORS

trust point

Trustpoint helps operators securely manage machine identities throughout the entire lifecycle—from commissioning to decommissioning

Let's secure automation

IT

Level 5
Enterprise / Corporate IT

DIRECTORY SERVICE   ERP

Level 4
Enterprise Network

WEB SERVER   EMAIL SERVER   DNS SERVER

Level 3.5
Demilitarized Zone (DMZ)

PATCH SERVER   JUMP SERVER   **trust point**

Level 3
Manufacturing Operations

WORKSTATION   HISTORIAN   MES

OT

Level 2
Supervisory Control

SCADA   HMIs

Level 1
Basic Control

PLC   DCS

Level 0
Physical Process

SENSOR   ACTUATOR

SOLUTION

trust point

Trustpoint – Open, Flexible, and Automatable

LIFECYCLE AUTOMATION

Automated **certificate lifecycle management** for OT devices and systems.

FLEXIBLE ONBOARDING

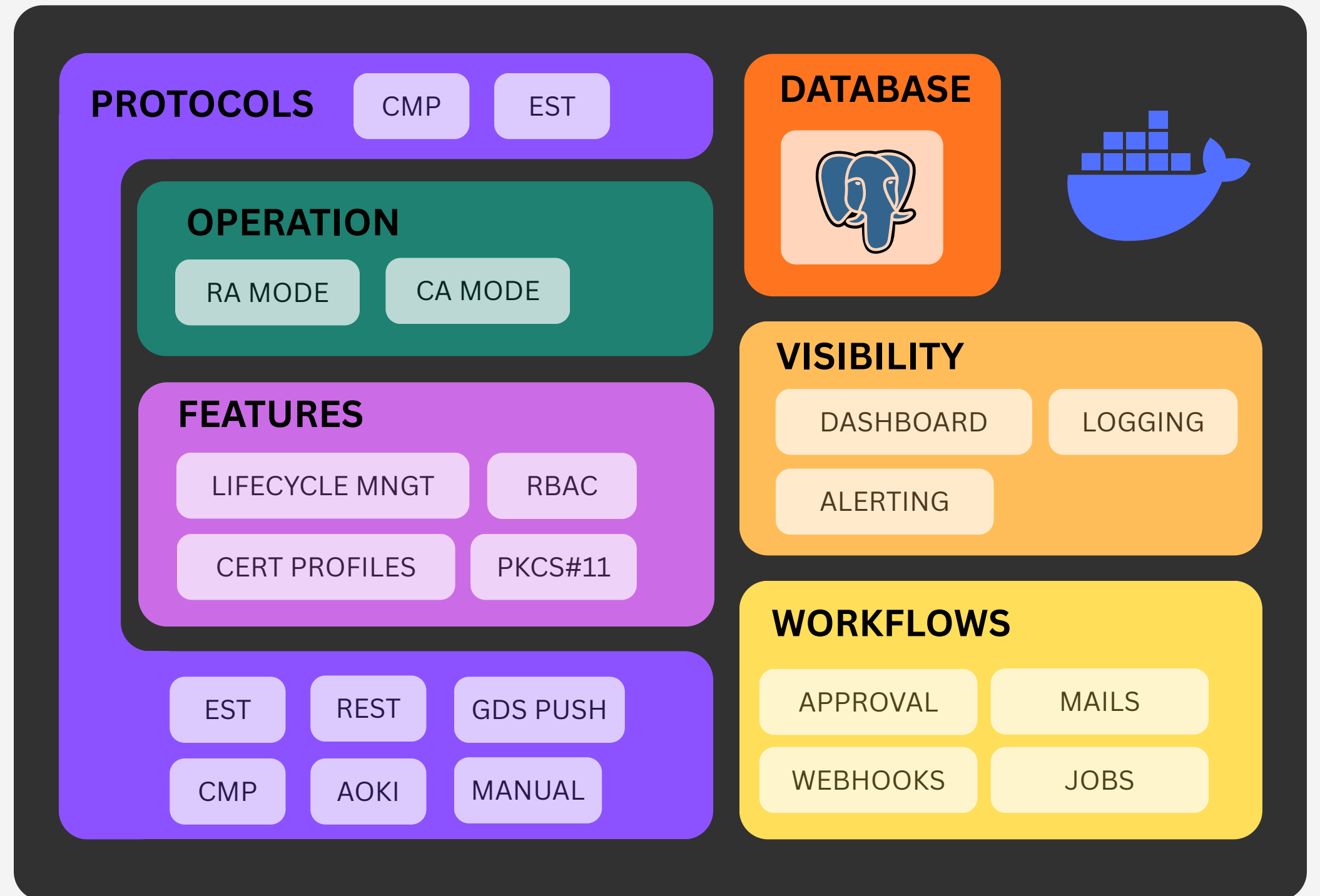Supports **manual**, **semi-automated**, and **Zero-Touch** onboarding.

OPEN CORE

OSS foundation with optional professional services and integrations.

Let's secure automation

ARCHITECTURE

trust
point

From onboarding to decommissioning — Trustpoint
automates the entire certificate lifecycle.

PROTOCOLS CMP EST

OPERATION RA MODE CA MODE

FEATURES LIFECYCLE MNGT RBAC CERT PROFILES PKCS#11

EST REST GDS PUSH CMP AOKI MANUAL

DATABASE

VISIBILITY DASHBOARD LOGGING ALERTING

WORKFLOWS APPROVAL MAILS WEBHOOKS JOBS

Let's secure automation

* Some features will be available in future versions.

REFERENCE PROJECTS

Secure Device Onboarding in Real Industrial Environments

trust
point

SECURE ONBOARDING

A Belden Hirschmann BOBCAT Switch is securely onboarded using its **Initial Device Identifier** (IDevID) for authentication.

Belden

OPC UA GDS

Certificates are issued to a Siemens S7-1500 via UaGDS, which handles **centralized certificate provisioning**, trust list management, and automated renewal

Unified Automation   SIEMENS

Let's secure automation

BUSINESS MODEL

Open Source Base – Sustainable Service & Support Model

REVENUE STREAMS

- **Professional services** (deployment, training, compliance consulting)
- **SLA**-based support and incident response
- **Custom integrations & feature** development

GO-TO-MARKET STRATEGY

- **Community-first** (GitHub, DockerHub, events)
- Partner & integrator channels
- OEM-ready modules
- Industrial marketplace visibility

Let's secure automation

* As of today, Trustpoint is not yet an operating company (due to funding guidelines; expected 09/26). Nevertheless, we look forward to discussing use cases and PoCs with you.
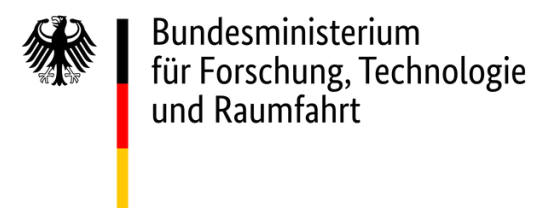
THANK YOU.

Let's secure automation

CONTACT US:

Florian Handke

Director Industrial Security

Campus Schwarzwald

📞 +49 151 55360339

✉️ florian.handke@campus-schwarzwald.de

🌐 www.industrial-security.io

APPENDIX

LOGISTICS

trust point

Trustpoint different ways to manage certificates on end devices. From zero-touch to manual ways.

| Method	Auth Methods	Key Capabilities
AOKI (Zero-Touch)	IDevID	Zero-touch onboarding; automatic LDevID issuance
EST (RFC 7030)	Username+Password, IDevID, mTLS	LDevID onboarding; app cert enrollment; renewal & re-enrollment
CMP (RFC 9483)	Shared Secret, IDevID, mTLS	LDevID onboarding; app cert enrollment; automated renewal & rekey
Manual Download	—	Server-generated credentials; PKCS#12/PEM download
Remote Credential Download	OTP	Browser-based retrieval of issued credentials

Let's secure automation

OPERATION

Trustpoint supports **local (air-gapped)** certificate management and acts as a local **registration authority**, issuing certificates via a remote PKI.
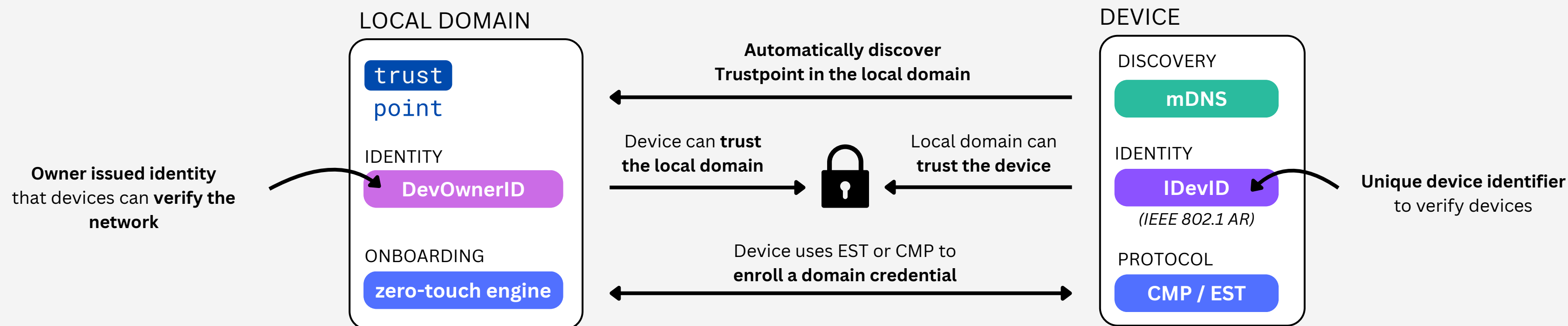
IT DOMAIN / INTEGRATOR / SERVICE PROVIDER / ...

CORPORATE
PKI

e.g. Keyfactor EJBCA

OT DOMAIN

trust
point

CA mode

RA mode

DEVICE

DEVICE

1

2
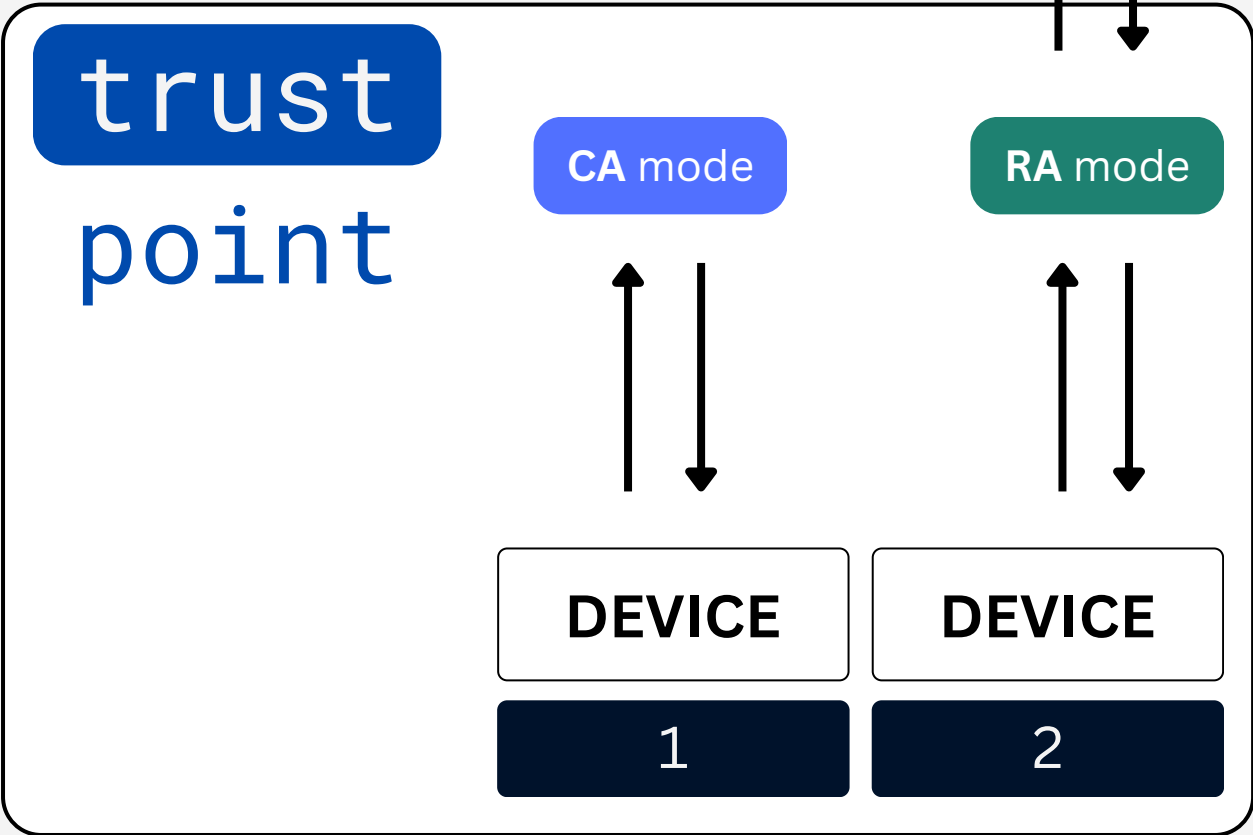
Let's secure automation

AOKI

BETA

trust point

Devices can automatically onboard into Trustpoint using the Automated Onboarding Key Infrastructure (AOKI) for **zero-touch onboarding**, leveraging their manufacturer device identity and multicast DNS for Owner Service discovery.

LOCAL DOMAIN

trust point

IDENTITY
DevOwnerID

ONBOARDING
zero-touch engine

Owner issued identity that devices can **verify the network**

Automatically discover **Trustpoint in the local domain**

Device can **trust the local domain**

Local domain can **trust the device**

Device uses EST or CMP to **enroll a domain credential**

DEVICE

DISCOVERY
mDNS

IDENTITY
IDevID
(IEEE 802.1 AR)

PROTOCOL
CMP / EST

Unique device identifier to verify devices

Let's secure automation

AOKI OPTIONS

trust
point

Devices can **automatically onboard** into Trustpoint using their manufacturer device identity utilizing multicast DNS.

PER-DOMAIN AOKI

- DevOwnerIDs are **issued per owner domain**, not per device.
- Device establishes trust by **pinning the DevOwnerID issuer chain** used during onboarding.

> **No direct device–owner cryptographic binding**, but more scalable for large and distributed environments.

PER-DEVICE AOKI

- Each device is associated with a **device-specific DevOwnerID** (by referencing the IDevID in the SAN)
- Ownership is **cryptographically tied to the individual device** from the beginning.

> **Maximum security through device-intrinsic ownership** binding, at the cost of higher operational effort

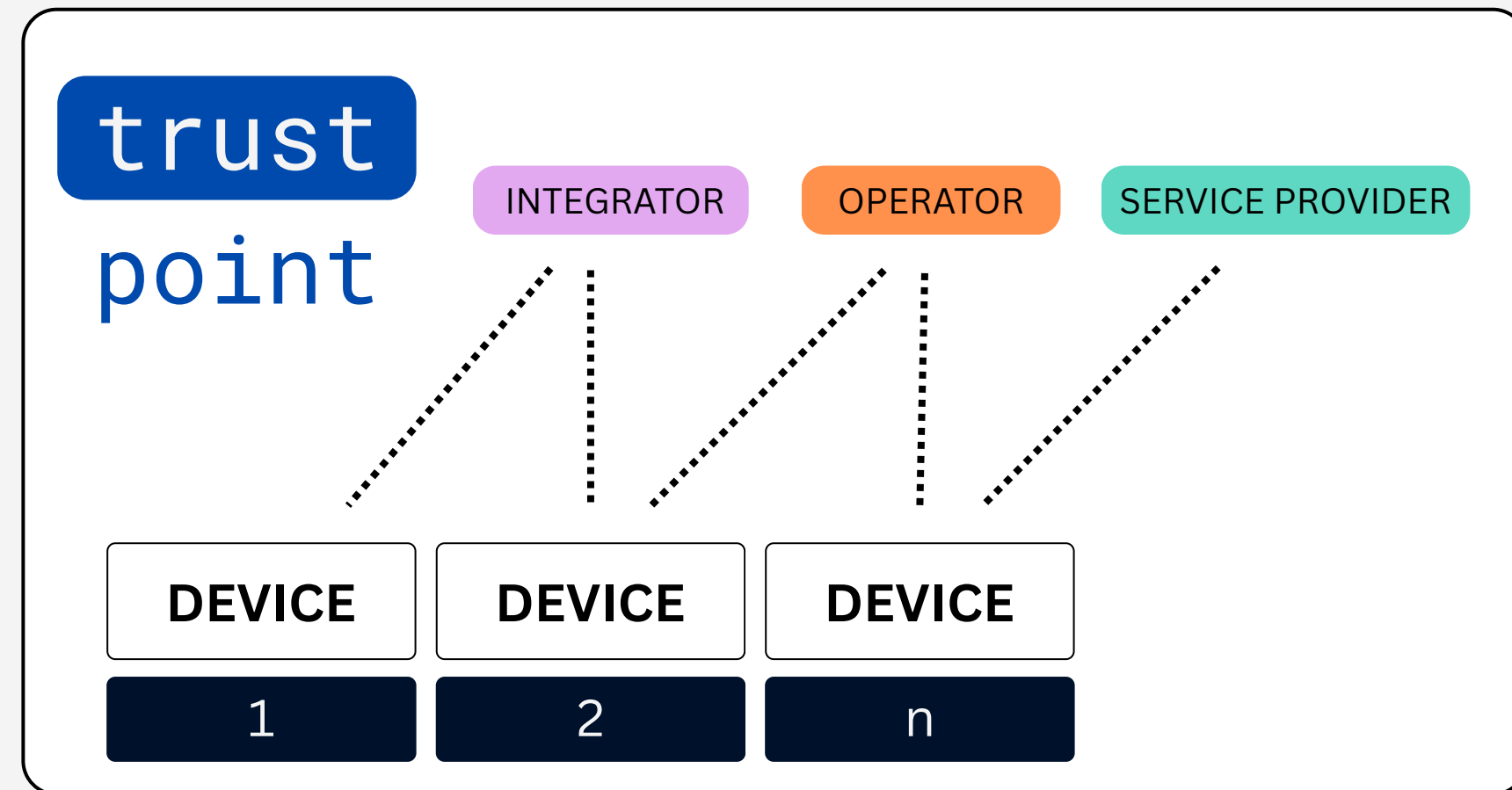**Let's secure automation**

MULTI-TENANCY

UPCOMING FEATURE

trust point

Since multiple actors need to manage certificates on the device, Trustpoint offers **multi-tenancy for different actors**, such as integrators, operators, and service providers.
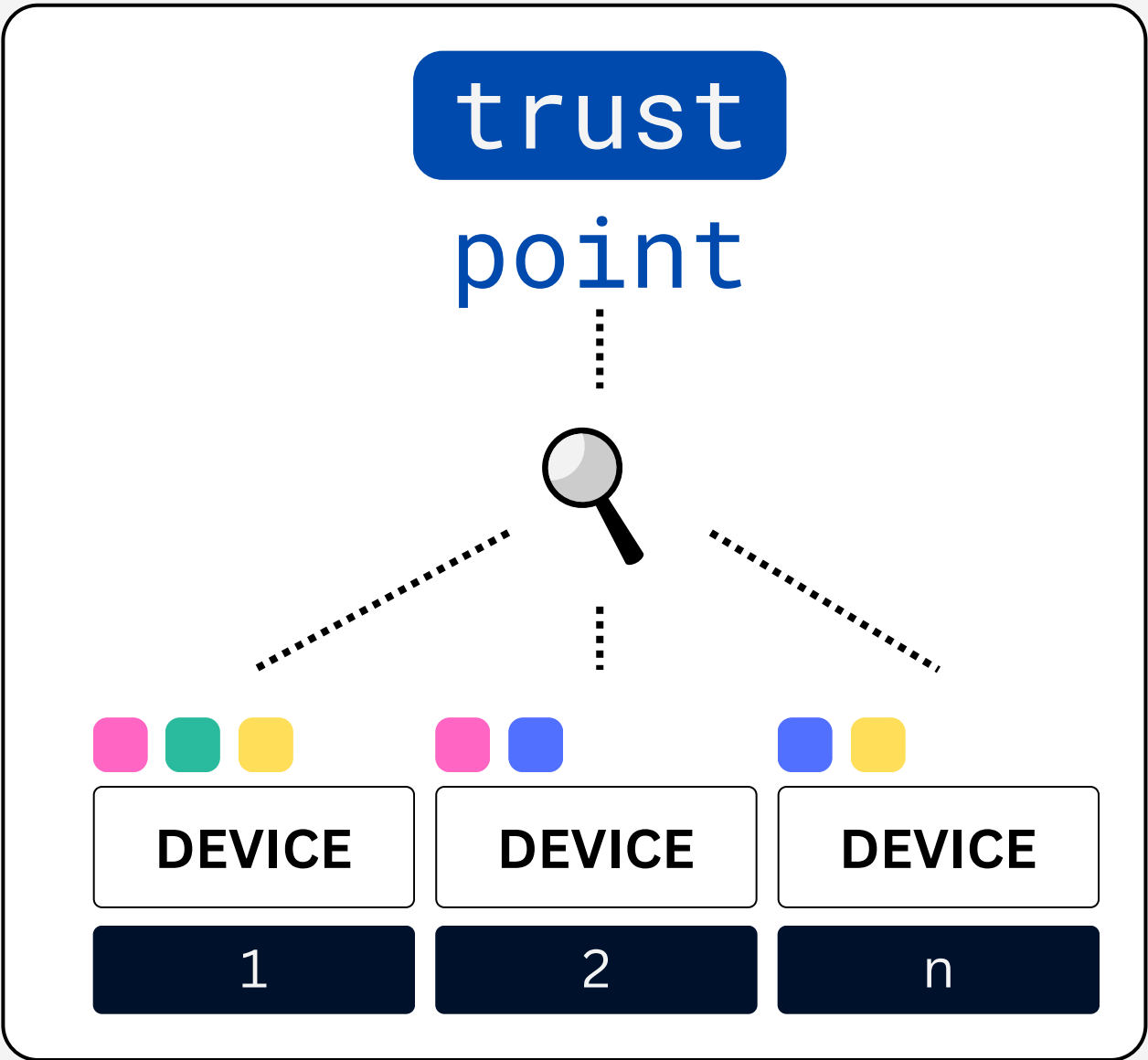
DOMAIN

Let's secure automation

CRYPTO DETECTION

trust
point

Trustpoint **detects devices** and their capabilities on certificates. Our device library offers an individualized workflow for certificate management.

DOMAIN

trust
point

DEVICE | DEVICE | DEVICE
1 | 2 | n

HTTPS WEBSERVER
OPC UA SERVER
IPsec
BACnet

Let's secure automation