



Security Summit OT

Milano 24 settembre 2026



Come rendere realmente sicuro l'accesso remoto OT
senza perdere di vista la realtà della fabbrica?

Marco Bera

CTO DIREL Srl | OT Cybersecurity Specialist

Security Summit OT · 24 settembre 2026

✉ marco.bera@direl.it · in [linkedin.com/in/marco-bera](https://www.linkedin.com/in/marco-bera)



La realtà: uno stabilimento non parte da zero

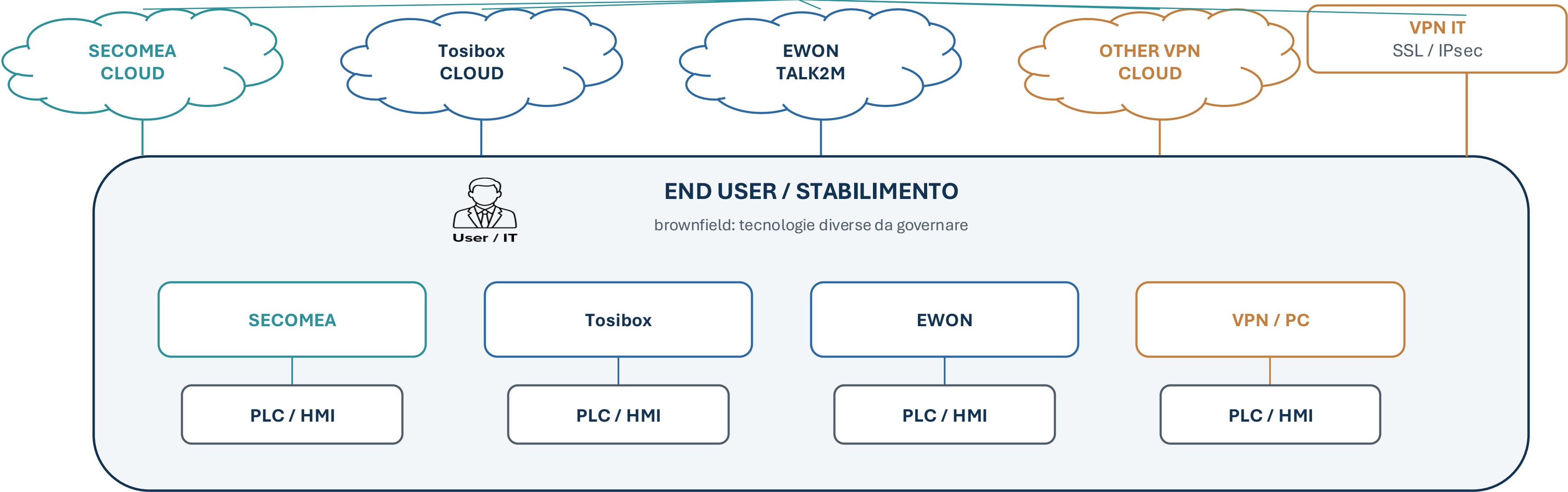
Accessi remoti eterogenei, portali diversi, responsabilità distribuite



OEM

OEM / FORNITORI / MANUTENTORI

possono utilizzare uno o più servizi / modalità di accesso remoto



Le domande dell'end user

Riprendere il controllo degli accessi non è più solo un'esigenza operativa

Chi può accedere alle mie macchine?

Come gestisco portali e tecnologie differenti?

Posso standardizzare senza sostituire tutto?

Come verifico e approvo gli accessi?

COME RIPRENDO IL CONTROLLO?

Come aumento la sicurezza senza complicare l'operatività?

Chi gestisce tutto questo: IT, OT o entrambi?



PRESSIONE NORMATIVA



La soluzione più sicura... sulla carta

Una checklist di feature non basta se il modello non funziona in fabbrica

REQUISITI IT / SECURITY

- Identity Management
- SSO / MFA
- RBAC
- Least Privilege
- PAM
- Credential Vaulting
- Approval Workflow
- Just-in-Time Access
- Session Recording
- Full Audit
- SIEM Integration
- SOC Monitoring
- Conditional Access
- Network Segmentation
- Compliance / Reporting
- Access Review
- Lifecycle Management
- ...

Tutto corretto. Ma la lista può crescere molto velocemente.

IL BISOGNO OPERATIVO

«Devo far collegare il fornitore a

QUEL PLC

con il suo tool di engineering

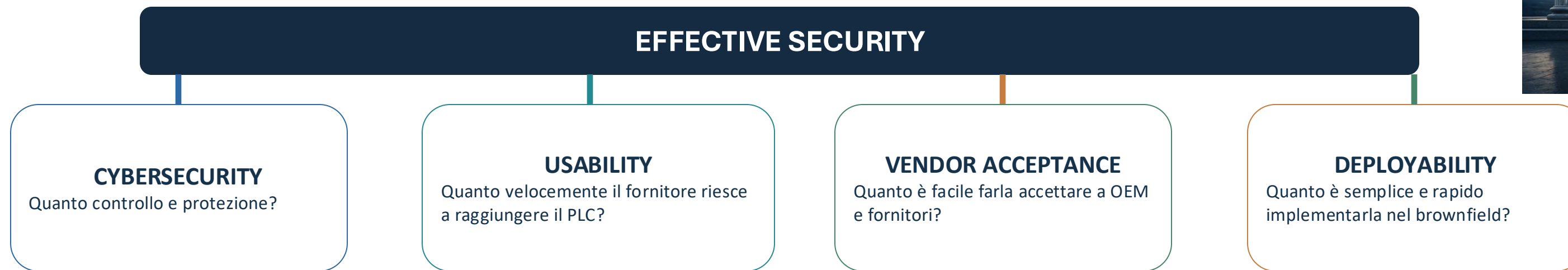
e risolvere il problema della macchina.

Possibilmente adesso.»

Quanto possiamo aumentare la sicurezza senza rendere impraticabile l'operatività?

Quattro pilastri, un solo risultato

Tutti hanno lo stesso peso: se uno manca, la sicurezza effettiva si indebolisce



Nessun pilastro è accessorio.

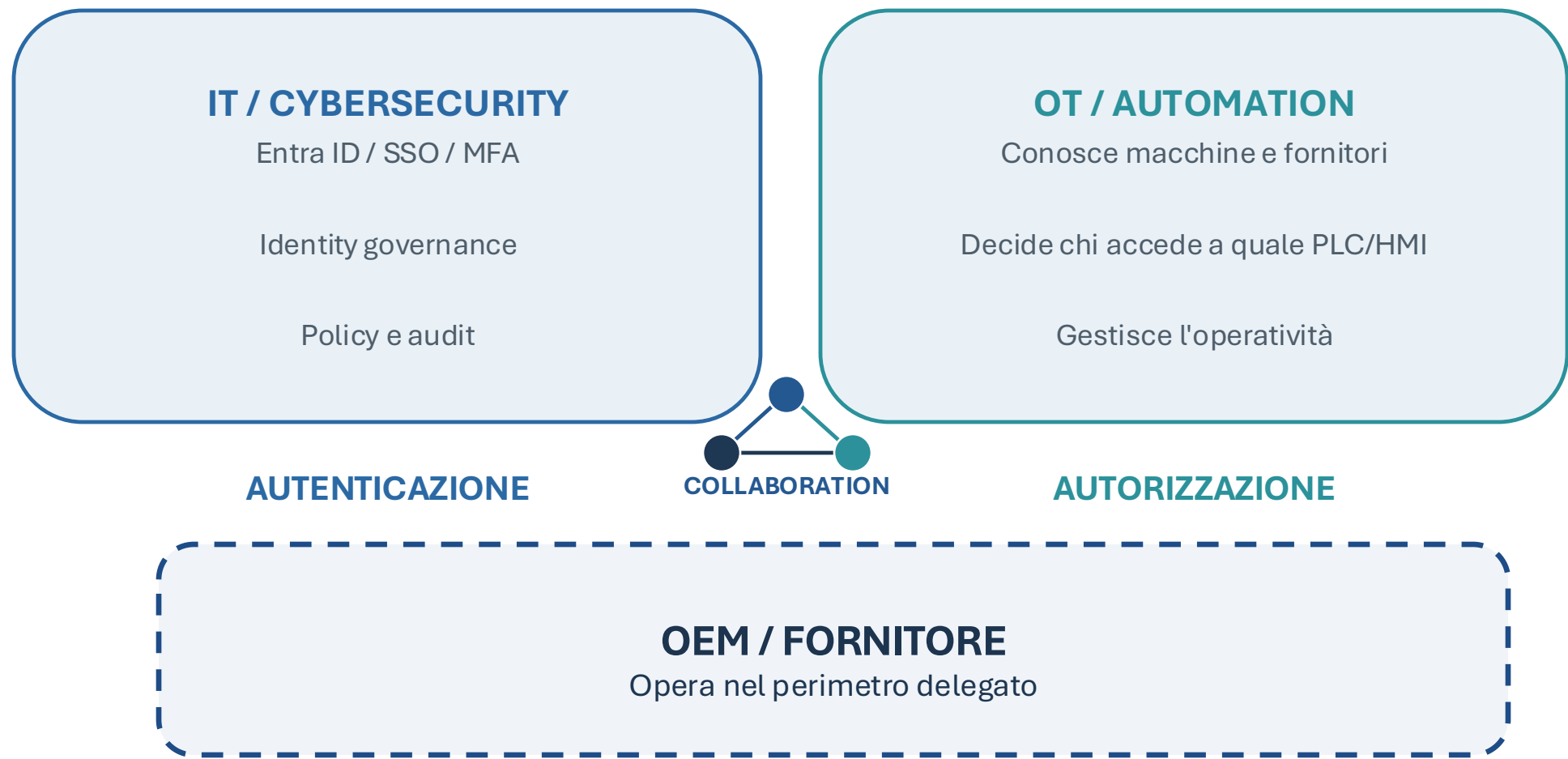


Governance centralizzata. Responsabilità distribuite.

L'IT governa l'identità; l'OT governa l'accesso agli asset

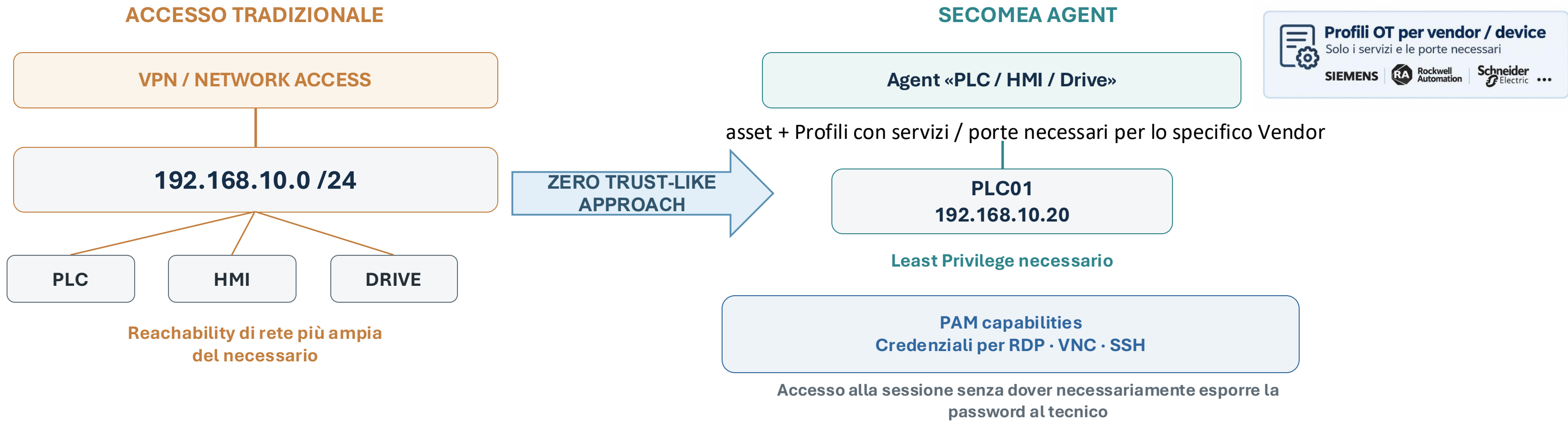
Governance centralizzata, operatività flessibile

Separare chi autentica da chi decide a quali asset si può accedere



Accesso all'asset, non alla rete: il modello Secomea Agents

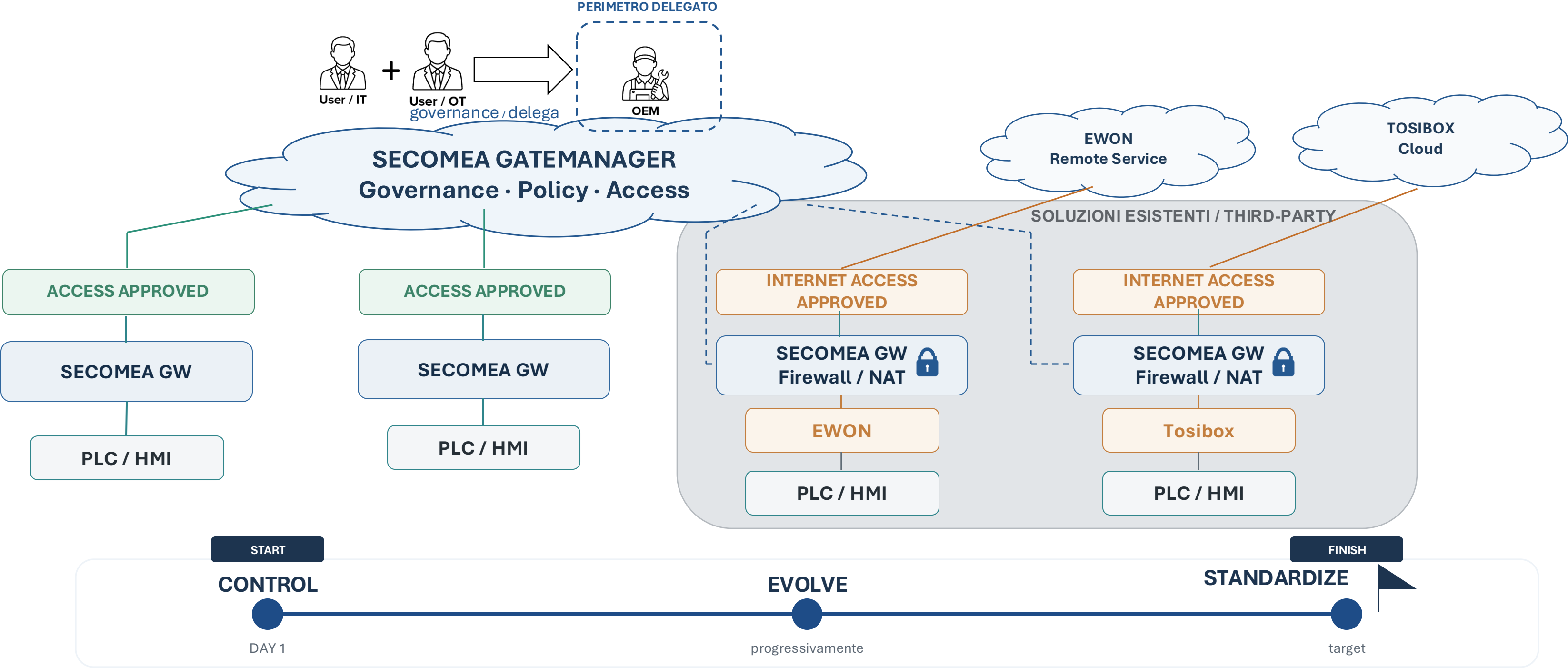
Conoscenza OT incorporata nei profili di accesso



Non concedere accesso alla rete. → Concedere l'accesso necessario allo specifico asset.

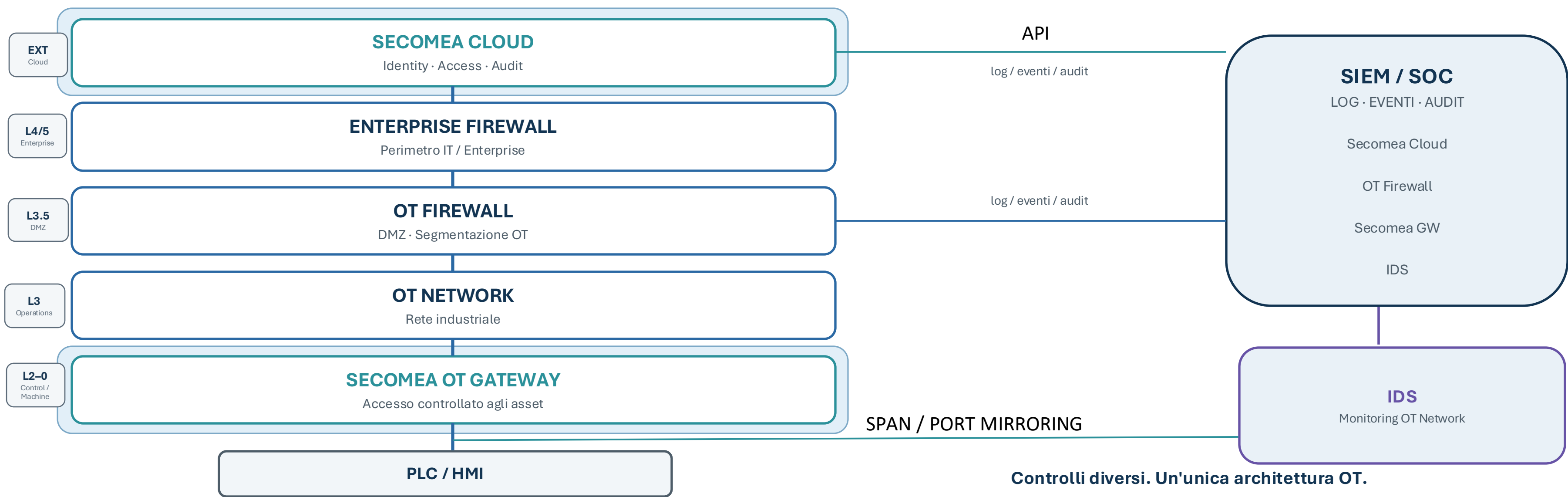
Day 1: mettere sotto controllo il brownfield

non devo sostituire tutto: dal Day 1 posso applicare livelli di controllo differenti sotto una governance comune.



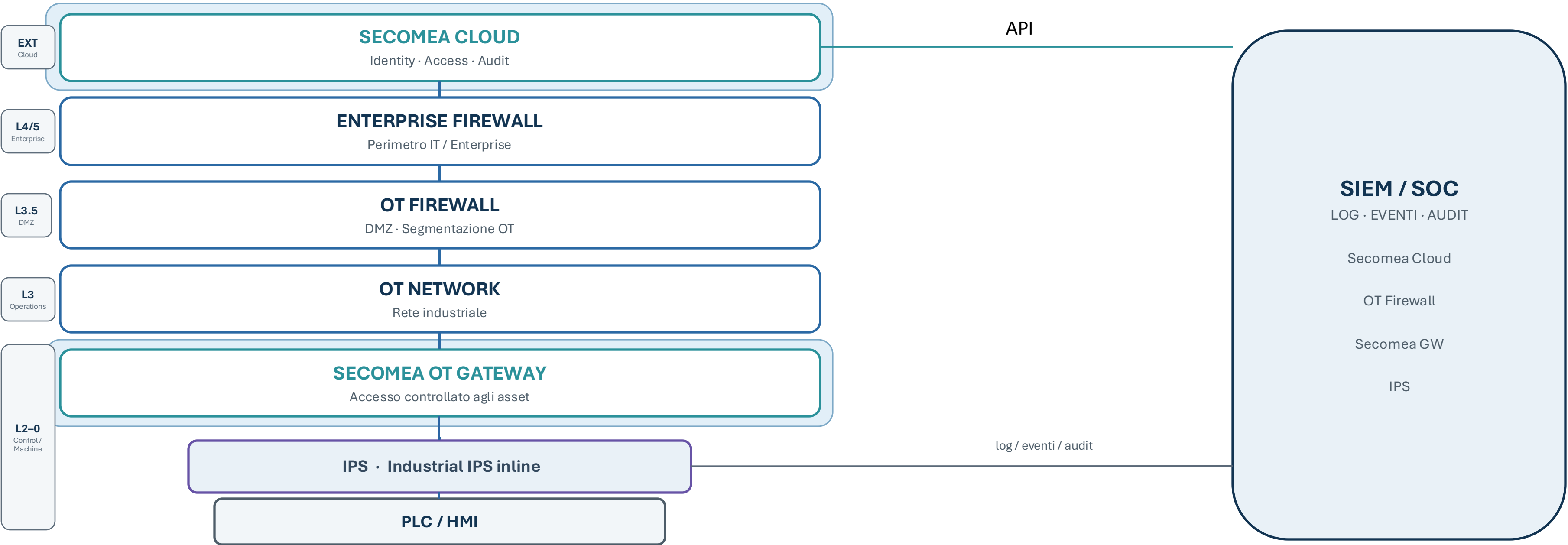
ZOOM OUT: SECURE REMOTE ACCESS NELL'ARCHITETTURA OT

Un layer tra i layer: complementare, non sostitutivo



ZOOM OUT: SECURE REMOTE ACCESS NELL'ARCHITETTURA OT

VARIANTE 9B · IPS inline sul boundary della macchina

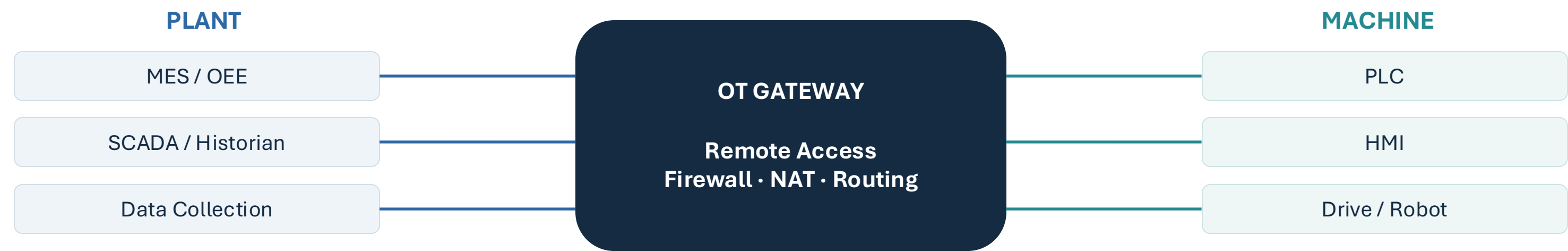


9B

Controlli diversi. Un'unica architettura OT.

Portare il controllo fino al boundary della macchina

Il boundary della macchina non riguarda solo il Remote Access



Complementare a segmentazione, IDS/IPS, monitoring ed endpoint security.

Remote Access + Firewall / NAT / Routing + comunicazioni Industria 4.0

La sicurezza deve funzionare nel mondo reale

Questa è l'architettura giusta per tutti?

NO.

NON ESISTE UNA SOLUZIONE

“ONE SIZE FITS ALL”

**Esiste l'architettura più adatta
al proprio contesto OT.**

...e al Risk Appetite dell'organizzazione.

CYBERSECURITY

Quanto controllo e protezione?

USABILITY

Quanto velocemente il fornitore riesce a raggiungere il PLC?

VENDOR ACCEPTANCE

Quanto è facile farla accettare a OEM e fornitori?

DEPLOYABILITY

Quanto è semplice e rapido implementarla nel brownfield?

La standardizzazione può richiedere mesi. Il controllo può iniziare dal Day 1.

✉ marco.bera@direl.it · in [linkedin.com/in/marco-bera](https://www.linkedin.com/in/marco-bera)

11