SECURITY SUMMIT

Security Summit

Verona 28 ottobre 2026

Clusit

ASTREA

Sessione

Accesso remoto OT: quando la sicurezza incontra la realtà della fabbrica

Alessio Pennasilico | CS Clusit
Marco Bera | CTO &OT cybersecurity DIREL s.r.l.

Alessio Pennasilico aka -=mayhem=-



CISO

Member of the Board of Directors of the Association of IT Professionals

Member of the Scientific Committee

Senior Partner, Information & Cyber Security Advisor @Security Evangelist & Ethical Hacker

Vice President of the Committee for the Safeguarding of Impartiality

Member of the Scheme Committee

Scientific Director of the publication

Senior Advisor of the Cyber Security & Data Protection Observatory of the Politecnico di Milano

Core faculty

Marco Bera

CTO & OT Cybersecurity Specialist DIREL SRL



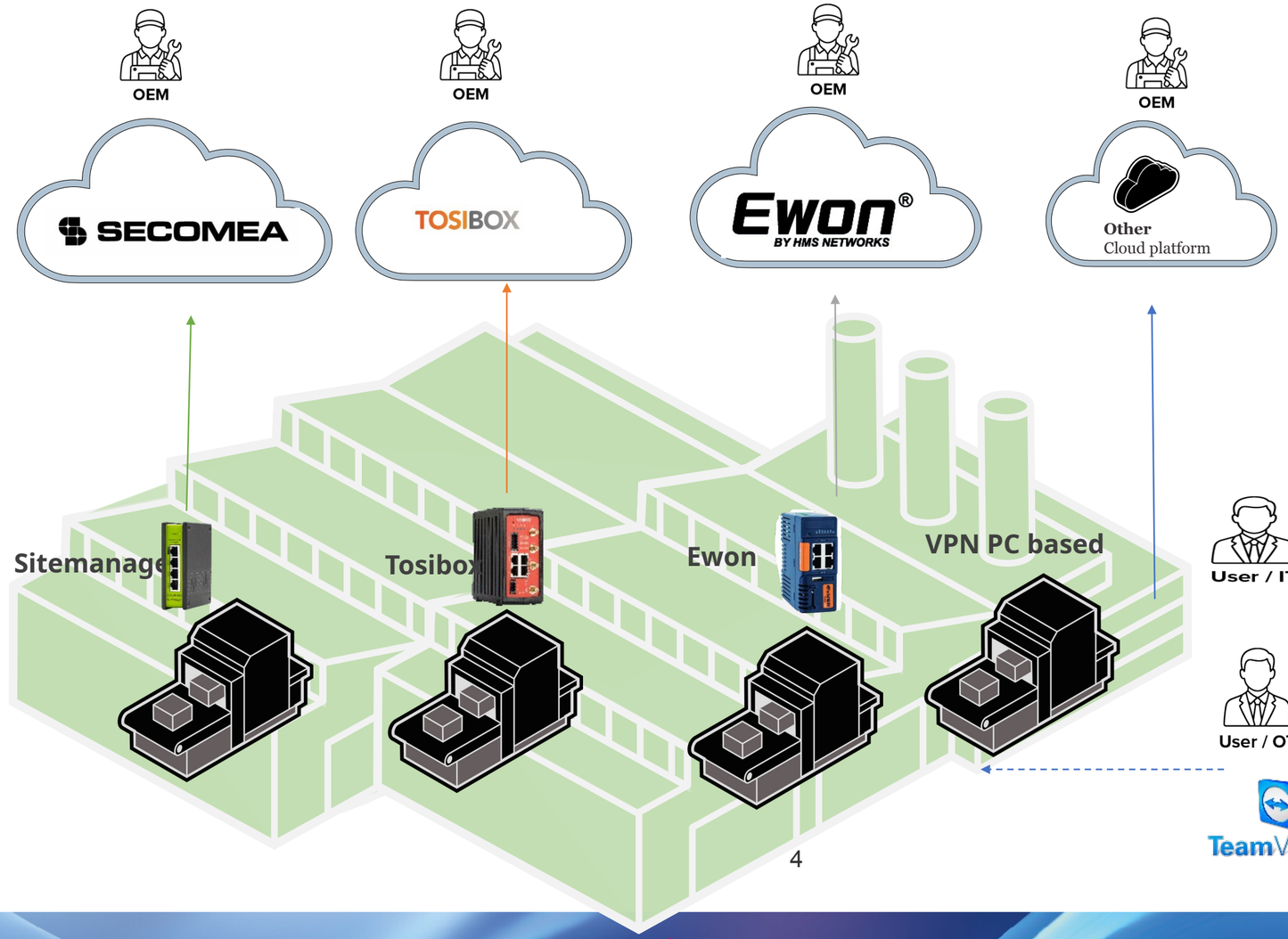
Professionista con oltre 20 anni di esperienza nell'Industrial Networking e nelle tecnologie per l'automazione industriale, ha sviluppato competenze specialistiche nella cybersecurity OT, nella convergenza IT/OT e nella progettazione di infrastrutture di comunicazione industriali sicure.

Nel ruolo di CTO di DIREL Srl affianca costruttori di macchine, system integrator ed end user nella progettazione e nell'adozione di soluzioni di Industrial Networking, Secure Remote Access e OT Cybersecurity.

Segue le tecnologie **Secomea dal 2008**, contribuendo alla loro introduzione e diffusione nel mercato industriale italiano, e vanta una consolidata esperienza nelle infrastrutture di rete industriali **Belden/Hirschmann**. Il suo approccio pone particolare attenzione all'integrazione tra requisiti di sicurezza, esigenze operative e caratteristiche degli ambienti industriali esistenti.

La realtà: uno stabilimento non parte da zero

Accessi remoti eterogenei, portali diversi, responsabilità distribuite



VPN site to site
IT VPN
..

Bypasses RA rules

Le domande dell’end user

NIS2
CYBERSECURITY

CRA
CYBER RESILIENCE

PRESSIONE NORMATIVA

COME RIPRENDO IL CONTROLLO?

- **Chi può accedere alle mie macchine?**
- **Come verifico e approvo gli accessi?**
- **Come gestisco portali e tecnologie differenti?**
- **Posso standardizzare senza sostituire tutto?**
- **Come aumento la sicurezza senza complicare l’operatività?**
- **Chi gestisce tutto questo: IT, OT o entrambi?**



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.»

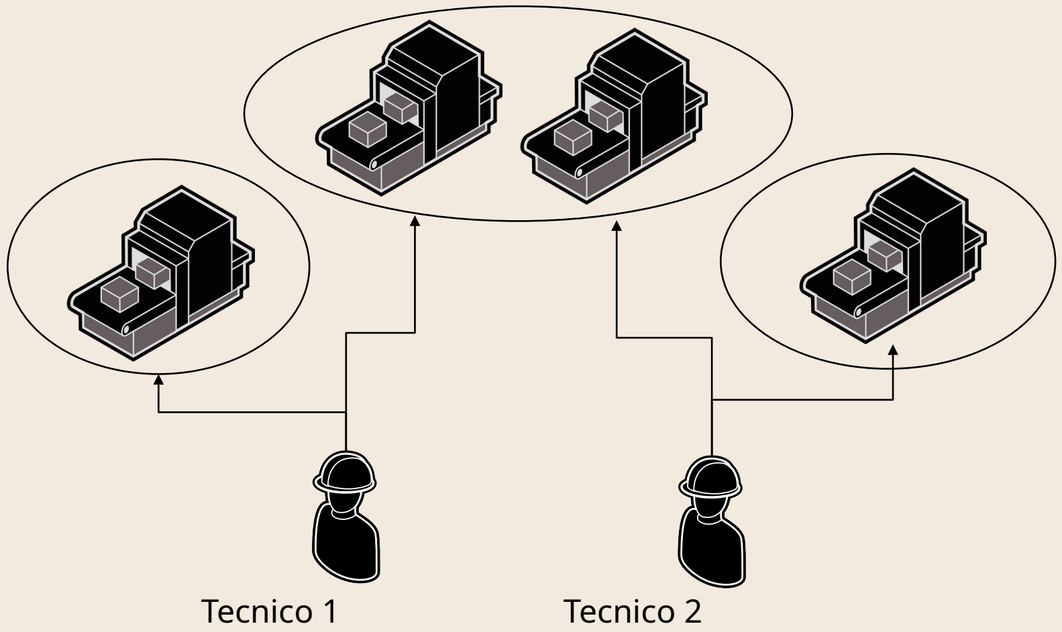
«Devo garantire la **comunicazione tra macchine**.
Devo garantire la comunicazione **da/verso MES / historian**.
senza interrompere la produzione.»

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

L’accesso remoto OT ha due prospettive diverse

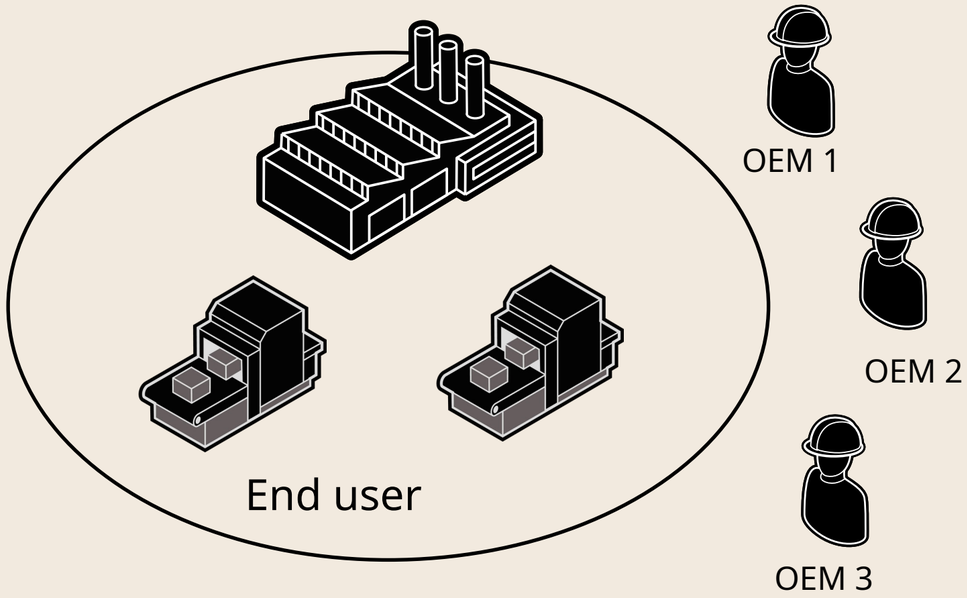
BÜHLER YASKAWA EMERSON MITSUBISHI

Deve accedere alle macchine per garantire assistenza e manutenzione.



P&G MOWI NOVARTIS Walgreens BIMBO

Deve decidere chi accede, a cosa, quando e a quali condizioni.



Quattro pilastri, un solo risultato

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



EFFECTIVE SECURITY

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?

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

IT / CYBERSECURITY
Entra ID / SSO / MFA

Identity governance

Policy e audit

OT / AUTOMATION
Conosce macchine e fornitori

Decide chi accede a quale PLC/HMI

Gestisce l'operatività

AUTENTICAZIONE

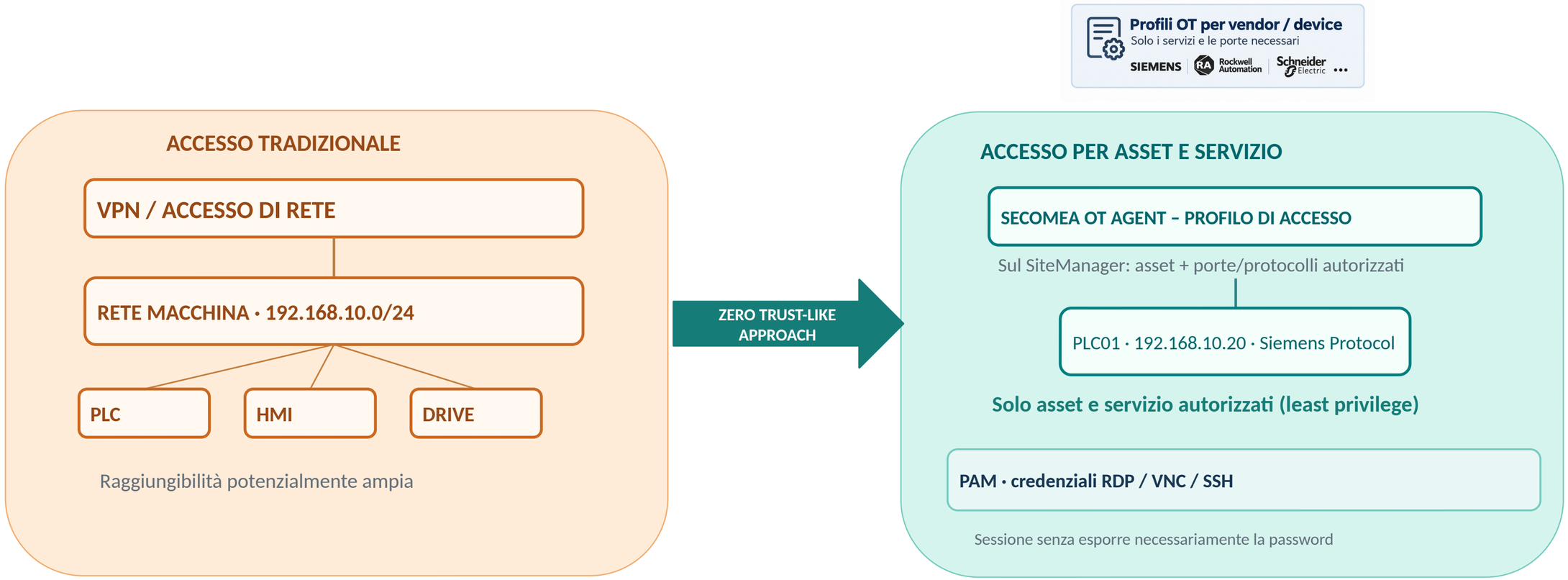
COLLABORATION

AUTORIZZAZIONE

OEM / FORNITORE
Opera nel perimetro delegato



Least Privilege OT: accesso all'asset, non alla rete



Non basta raggiungere la rete: autorizzare l'accesso necessario al singolo asset.

Dal tecnico all'asset OT: il percorso di accesso

1 · Nessuna esposizione inbound da Internet, solo outbound HTTPS

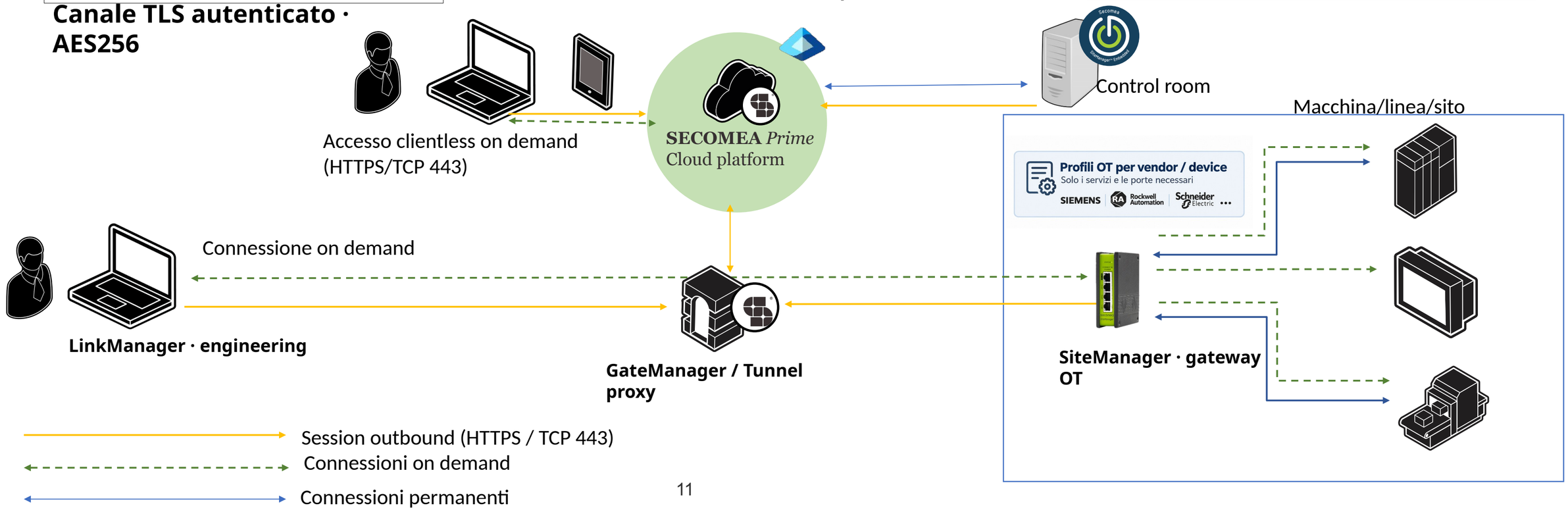
Canale TLS autenticato · AES256

2 · Accesso granulare agli asset con gli agent

Gestione delle identità, audit

3 · Compatibilità con l'operatività OT

Engineering tool nativi e accesso clientless



Dove applicare il controllo? Macchina, linea o sito ?

Hardware dedicato o software embedded? il posizionamento determina i controlli applicabili.

PER MACCHINA

Gateway dedicato alla singola macchina

Porto segmentazione e controllo al bordo macchina

Posso gestire macchine con indirizzamenti IP identici

Posso controllare le comunicazioni tramite firewall/NAT

Posizione strategica al bordo macchina

Modularità e controllo vicino agli asset.



PER LINEA/ZONA

Un punto unico di accesso per più macchine sulla stessa linea/zona/vlan

Ottimizzo il numero di gateway e mi adatto alla topologia esistente.(VLAN per fornitore)

Possibilità di gestire le comunicazioni tra macchine all'interno della linea/zona

Firewall/NAT per comunicazioni con altre zone

Valutare percorsi, segmentazione e policy.



PER STABILIMENTO/SITO

Punto di accesso per più linee o reparti o sito produttivo su VM centralizzata

Utilizzo l'infrastruttura di rete esistente e i controlli presenti

Maggiore complessità di gestione per applicare le policy su diversi dispositivi

Firewall / IPS applicabili ai flussi che li attraversano.

Topologie alternative, non livelli di maturità: la scelta dipende dalla rete e dai requisiti operativi.

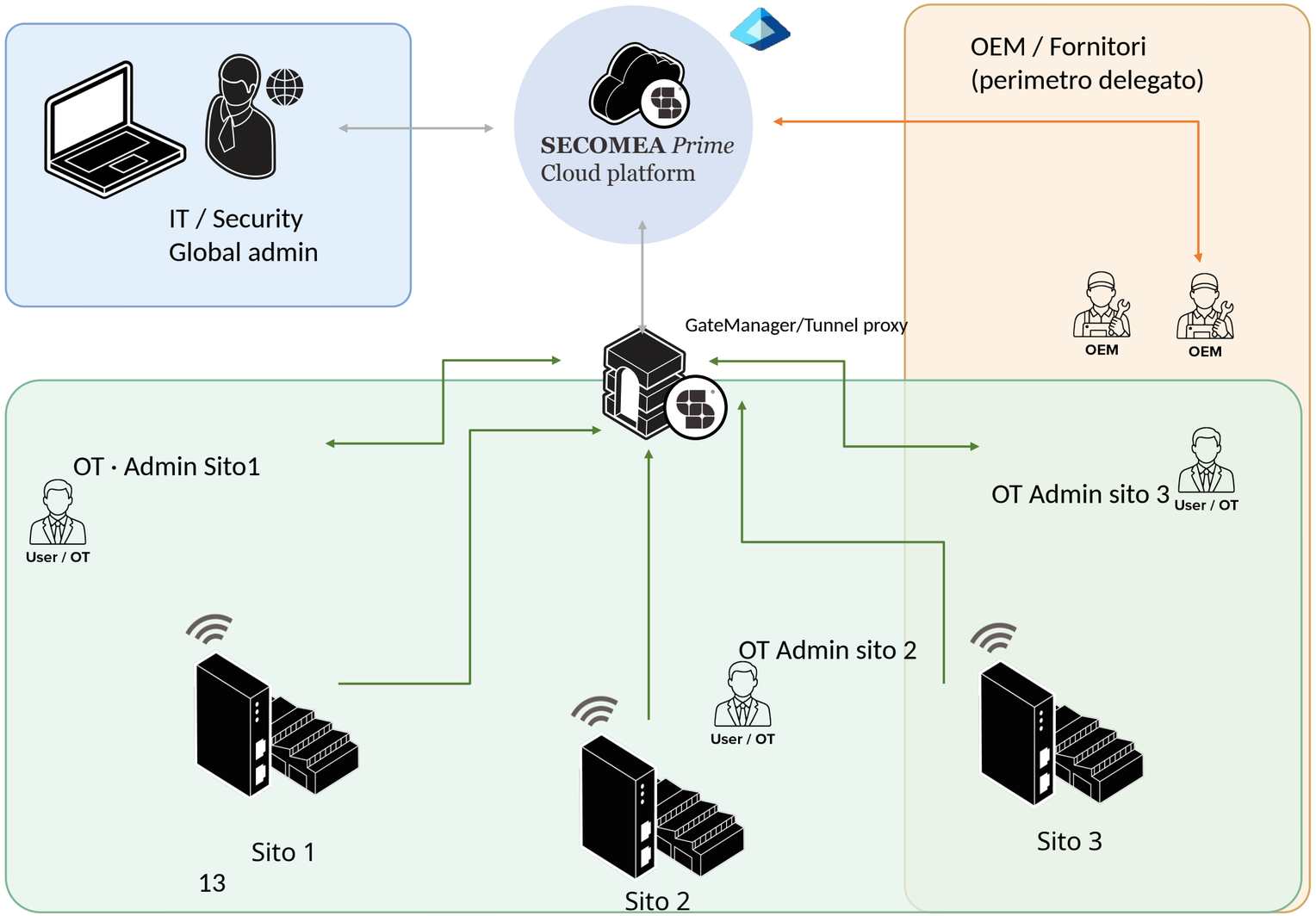
Come delegare gli accessi senza perdere il controllo?

IT / Security
Amministrazione, identità e global policy.
Integrazione per SIEM/SOC, Audit o service tools

OT / Responsabili di sito
Può essere globale o locale per sito
Assegna Permessi sugli asset
Gestione local policy
Approvazioni delle connessioni quando previsto.

OEM / Fornitori
Operatività entro il perimetro delegato
Se consentito può gestire i propri tecnici

Audit e controllo restano centralizzati.



Uno stesso workflow per tutti gli accessi?

Tre modalità di autorizzazione, secondo ruolo, rischio ed esigenze operative

01 ACCESSO PERMANENTE

RICHIESTA DI ASSISTENZA

User / OT

PERMESSI AGLI ASSET
Preassegnati o concessi al bisogno

AUTENTICAZIONE

Tecnico Interno

ACCESSO ALL'ASSET

Nessuna approvazione per sessione

02 ACCESSO SCHEDULATO

RICHIESTA DI ASSISTENZA

User / OT

PERMESSI AGLI ASSET
Preassegnati o concessi al bisogno

User / OT

DEFINIZIONE FINESTRA DI ACCESSO

AUTENTICAZIONE

OEM

ACCESSO ALL'ASSET

Accesso consentito solo nella finestra definita

03 ACCESSO CON APPROVAZIONE

RICHIESTA DI ASSISTENZA

User / OT

PERMESSI AGLI ASSET
Preassegnati o concessi al bisogno

OEM

RICHIESTA DI COLLEGAMENTO

User / OT

APPROVAZIONE DELLA SESSIONE

AUTENTICAZIONE

OEM

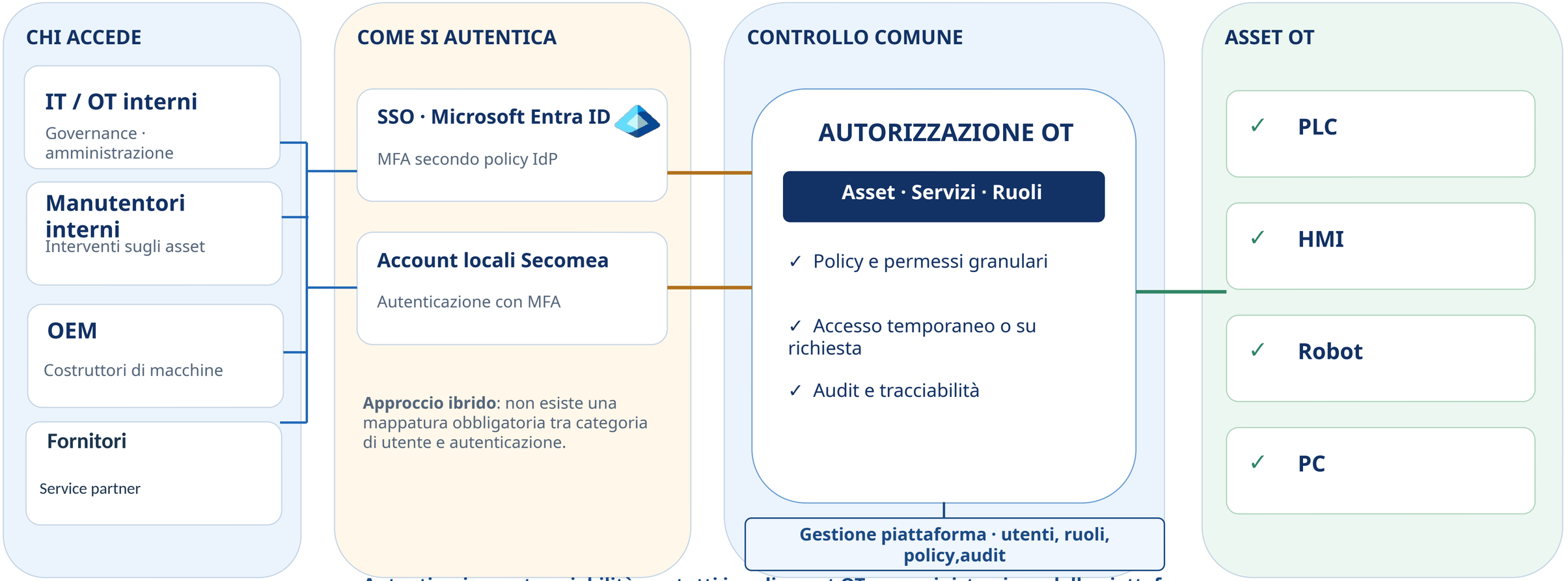
ACCESSO ALL'ASSET

Richiesta e approvazione prima dell'accesso

AUDIT COMUNE AI TRE WORKFLOW · Tracciabilità degli accessi · Registrazione sessioni dove supportata e abilitata

Chi accede, come si autentica e cosa può fare?

Identità e autenticazione flessibili, controlli e audit comuni per gli asset e la piattaforma



Autenticazione e tracciabilità per tutti i ruoli: asset OT e amministrazione della piattaforma

Accesso clientfull o clientless?

Engineering nativo con indirizzi degli asset · oppure accesso clientless da browser

01 InBrowser · Accesso clientless

Browser compatibile · Windows, Linux, Mac OS e device mobile



RDP · VNC · SSH · HTTP(S)



ACCESSO A

- **PC**
- **HMI**
- **Engineering statation**

- **Session Recording**
- **Session Join**
- **Secure File Transfer**
- **Credential Management**

02 LinkManager · Engineering nativo

Client Windows · Engineering tool nativi



IA Portal · Tool PLC · Protocolli OT ·device seriali/USB

ACCESSO A

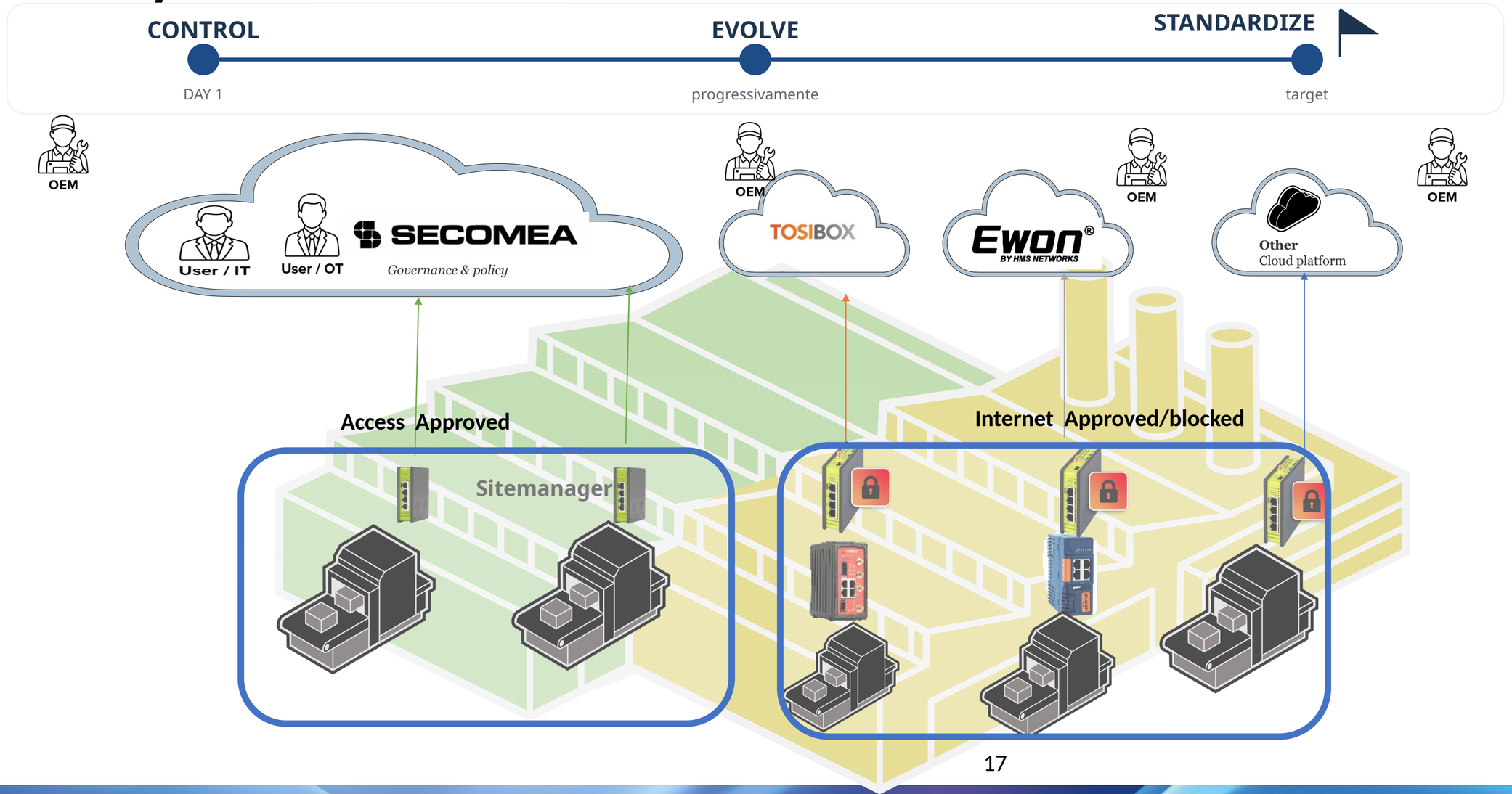
- **PLC**
- **HMI**
- **I/O · Drive Robot · Altri asset**

Stessi tool e indirizzi ip degli asset, il tecnico non deve modificare la configurazione network sul suo PC

Stessi controlli sugli asset. Cambia la modalità di connessione, non la policy.

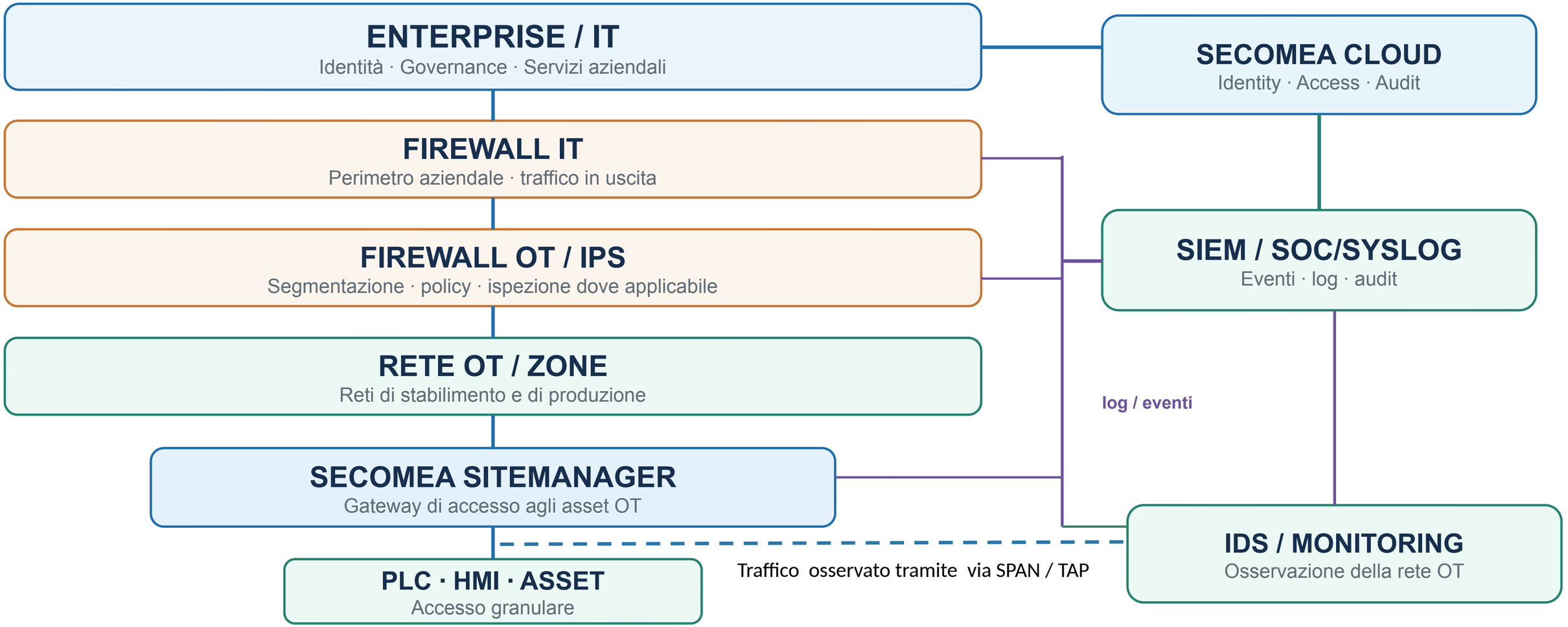
Clusit
SECURITY SUMMIT
ASTREA

Day 1: mettere sotto controllo il brownfield



Dove collochiamo il Gateway nella difesa OT?

Ipotesi: SiteManager a bordo macchina · controlli e percorsi variabili secondo la topologia



Dove termina il tunnel e chi controlla il traffico?

Dove termina il tunnel determina quali controlli possono agire sul traffico verso gli asset.

A · SITEMANAGER A BORDO MACCHINA

Secomea Cloud · tunnel cifrato

↓

SiteManager · terminazione tunnel

↓

Boundary macchina · DEV / LAN

↓

IDS (SPAN) / IPS inline opzionale

↓

PLC / HMI / Drive · L0–2

B · SITEMANAGER CENTRALIZZATO

Secomea Cloud · tunnel cifrato

↓

SiteManager · terminazione tunnel

↓

Infrastruttura OT dello stabilimento
Routing inter-VLAN · ACL · FW / IPS

↓

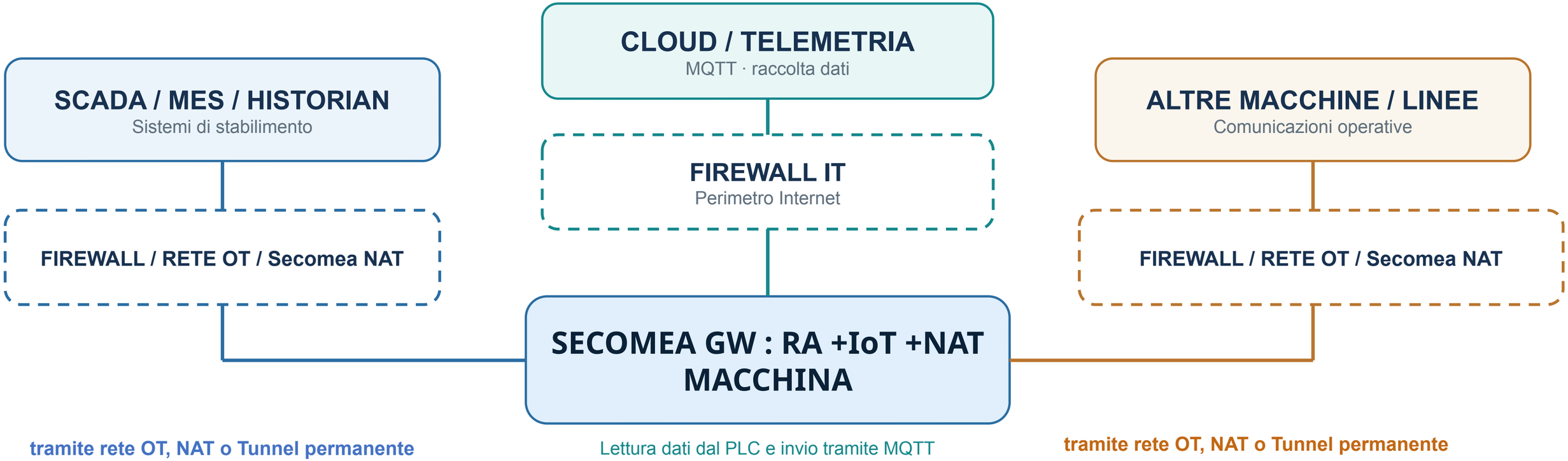
Conduit e policy verso le zone macchina

↓

VLAN linea A | VLAN linea B | VLAN linea C

Purdue come riferimento indicativo · Il traffico lato DEV è ispezionabile se attraversa il controllo e non è cifrato a livello applicativo.

Come gestiamo le altre comunicazioni operative?



FUNZIONI POSSIBILI DEL GATEWAY
SRA granulare · ACL / firewall · NAT · MQTT / Datacollection

CONTROLLI DELL'ARCHITETTURA OT
Segmentazione · firewall tra zone · IDS/IPS · SIEM/SOC

Tratteggio = elemento di percorso dipendente dalla topologia; i requisiti di sicurezza rimangono.

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 sicurezza dell’accesso remoto OT parte dall’identità, ma deve arrivare fino all’asset.
Integrandosi nell’architettura di sicurezza e adattandosi alla realtà operativa della fabbrica.

✉ marco.bera@direl.it · in linkedin.com/in/marco-bera

Q&A

Contatti:

Venite a trovarci al nostro Stand!