MINSAIT

OT Energy Workshop

TECHPARK SÜDTIROL / ALTO ADIGE

endian

bjosora Operational Technologies

unibz

NOI Techpark Bolzano - Smart Minifactory UNIBZ

21 Novembre 2025

Agenda

OT Energy Workshop @ Smart Minifactory UNIBZ (NOI Techpark Bolzano)

- **09:30 – 10:00 - Benvenuto e registrazione partecipanti**
- **10:00 – 10:15 - NOI Techpark: innovazione industriale e soste**
  Vincent Mauroit – Director of Innovation & Tech Transfer NOI Tec
- **10:15 – 10:45 - Smart Minifactory UNIBZ: ricerca applicata e t**
  Prof. Erwin Rauch / Ass. Prof. Matteo De Marchi – Libera Univers
- **10:45 – 11:00 - INDRA/Minsait: esperienze e approccio integra**
  Energy
  Gianluca Sinibaldi / Alessandro Frizzi – INDRA/Minsait
- **11:00 – 11:45 - Endian Secure Digital Platform: architettura e**
  Filippo Collini – Endian
- **11:45 – 12:30 - Smart Authentication per l'accesso sicuro agli**
  Case dimostrativo
  Federico Bellio – Bjosora
  Filippo Collini / Stefano Sbalchiero – Endian
  Sonia Gentile – Minsait
- **12:30 – 12:50 - Domande e confronto tecnico**
- **13:00 – 14:00 - Business Lunch presso NOIsteria**

01

NOI Techpark

Innovazione industriale e sostenibilità al NOI Techpark

Vincent Mauroit – Director of Innovation & Tech Transfer NOI Techpark

MINSAIT

02

UNIBZ

Smart Minifactory: ricerca applicata e tour dimostrativo

Prof. Erwin Rauch / Ass. Prof. Matteo De Marchi – Libera Università di Bolzano

MINSAIT

Smart Mini Factory Lab Presentation

Prof. Erwin Rauch / Ass. Prof. Matteo De Marchi – Libera Università di Bolzano

Bolzano - 21 / 11 / 2025

Smart Mini Factory - Laboratory for Industry 4.0

Dual Transformation

Digital & Green @unibz

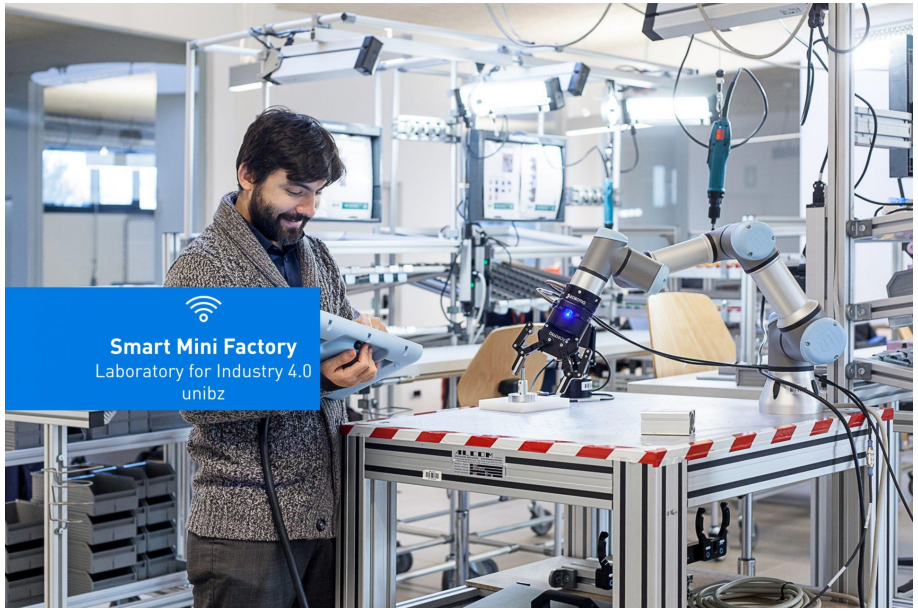
unibz
Fakultät für Ingenieurwesen
Facoltà di Ingegneria
Faculty of Engineering

Smart Mini Factory (SMF)

Bozen/Bolzano, South Tyrol, IT

Smart Manufaturing

Established in 2016
Founder Prof. Dominik Matt



Sustainable Manufacturing Lab (SML)

Brunek/Brunico, South Tyrol, IT

Sustainable Manufaturing

Established in 2023
Founder Prof. Erwin Rauch

Smart Mini Factory Lab

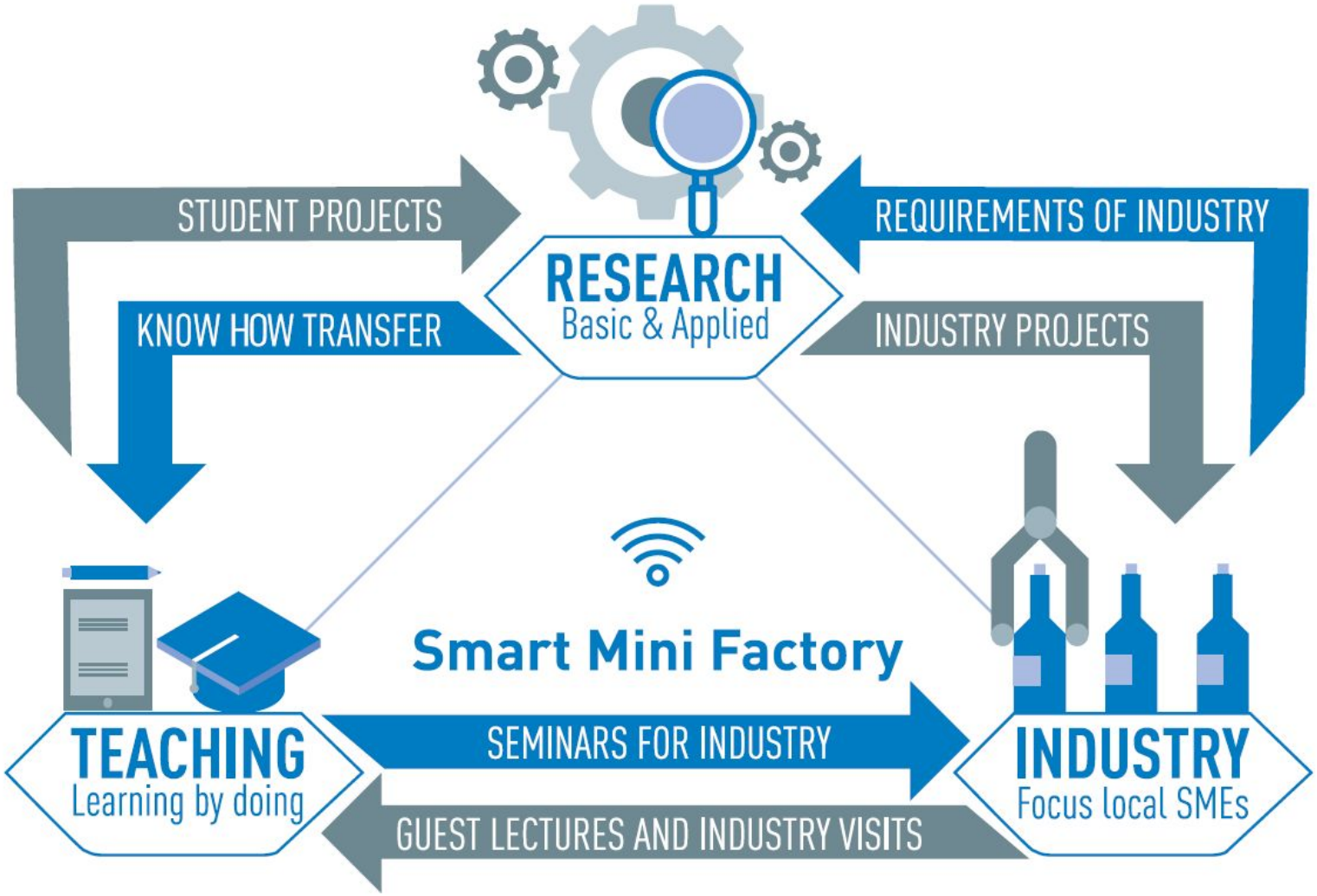
Vision

- Learning Factory for Applied Research and Teaching.
- Development and testing of new technologies and methods in manufacturing engineering in the context of Industry 4.0.
- Focus on small and medium-sized enterprises (SMEs)
- Platform for researchers, students and professionals for the technology transfer from research to industry.

Member of International Association of Learning Factories

Smart Mini Factory Lab

Mission



Collaboration with Industry

Opportunities for cooperation with companies

Contract research

Companies can obtain research services in Industry 4.0-5.0 through contract research. In this way, the laboratory provides the expertise of the people as well as laboratory equipment.

Sponsoring of PhD-positions

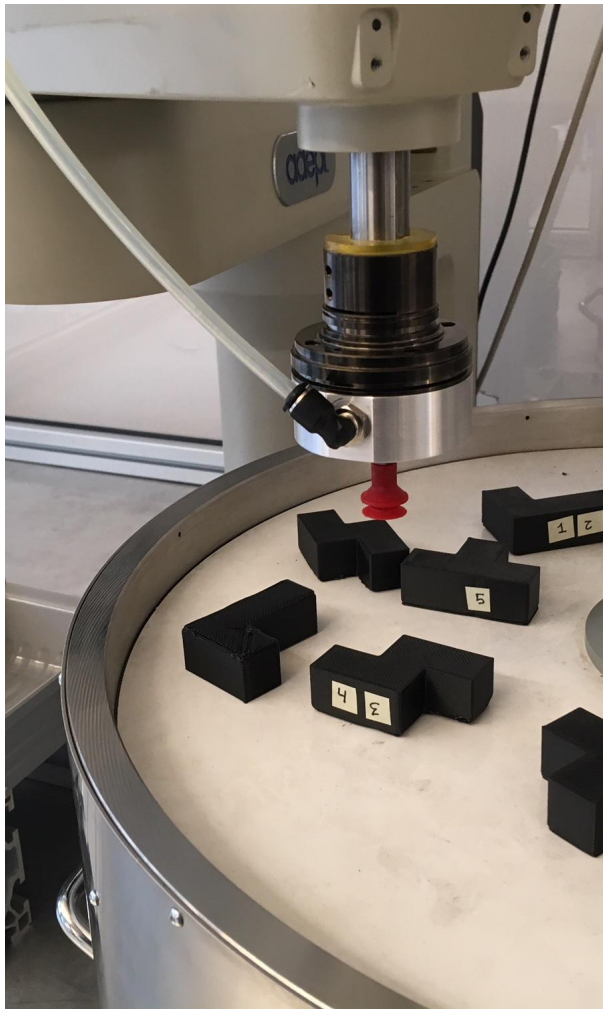
Companies can award/finance scholarships for doctoral students on specific research topics and thus contribute to the training of qualified specialists as well as to working on their own research projects.

Lifelong learning through seminars and trainings

Companies that want to train their employees on the topic of Industrie 4.0 can take advantage of the training offered by the Smart Mini Factory. Each year, the lab offers a series of seminars and summer courses on specific topics related to the application of Industrie 4.0 methods and technologies.

Collaboration with associations

Cooperation with associations in specialisation courses (e.g. Chamber of Commerce of Bolzano and lvh-apa).




unibz
Fakultät für Ingenieurwesen
Facoltà di Ingegneria
Faculty of Engineering
Smart Mini Factory - Laboratory for Industry 4.0
B1
A2
A6

PRESENTAZIONE

IN PROGRESS

03

INDRA/MINSAIT

Esperienze e approccio integrato IT/OT nel settore Energy

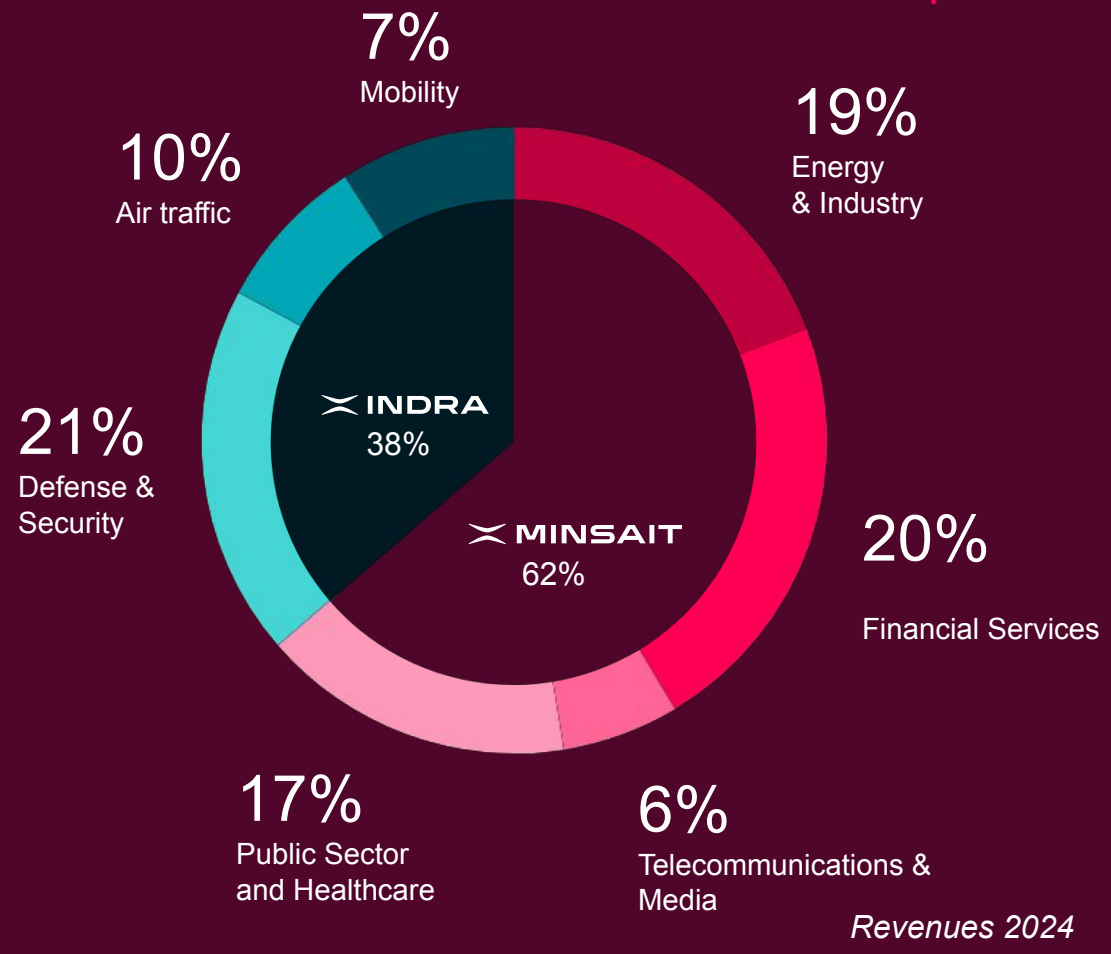
Gianluca Sinibaldi / Alessandro Frizzi

MINSAIT

Indra Group

The leading Spanish multinational in Defence & Aerospace and Advanced Digital Technologies

Technology for key business operations in multiple sectors



Revenues 2024

Main figures 2024

545M€
EBITDA
11.3% margin

4.843M€
in revenue

438M€
EBIT.
9.0% margin

+140
Countries

~60,000
Employees

427M€
In R+D+i

Indra Minsait in Italia

+3.000

Professionisti in Italia

7

Sedi su tutto il territorio nazionale (Milano, Roma, Napoli, Bologna, Bari, Potenza, Cagliari)

235M€

Revenue 2024

+2,53%

CAGR

Cosa facciamo

Acceleriamo la digitalizzazione di aziende, istituzioni e governi per generare un impatto positivo sulla società.

AI

Estraiamo valore dai dati. Adottiamo il metodo giusto. Guidiamo il futuro.

Cloud

Rivoluzioniamo il business. Costruiamo un nuovo futuro. Abbandoniamo il passato con i nostri clienti.

Phygital

Connettiamo il mondo fisico e digitale. Contribuiamo alla sostenibilità. Miglioriamo la vita delle persone.

Cybersecurity

Proteggiamo le aziende. Rileviamo le minacce. Garantiamo la conformità alle normative.

Payments

Partecipiamo a nuovi modelli di pagamento. Miglioriamo l'esperienza dell'utente. Acceleriamo il business.

Phygital – il ponte tra il mondo fisico e quello digitale

3 gli obiettivi principali

Migliorare **l'efficienza, la redditività e la flessibilità** della gestione di qualsiasi tipo di asset, prodotto o infrastruttura fisica

Trasformare **le interazioni delle persone** con il mondo fisico, unendo informazioni provenienti dal mondo reale con dati virtuali

Contribuire agli obiettivi di **sostenibilità** in tutti gli ambiti legati alla riduzione dell'impronta ecologica, all'economia circolare e all'impatto sociale.

Tecnologia geospaziale, BIM e digital twin

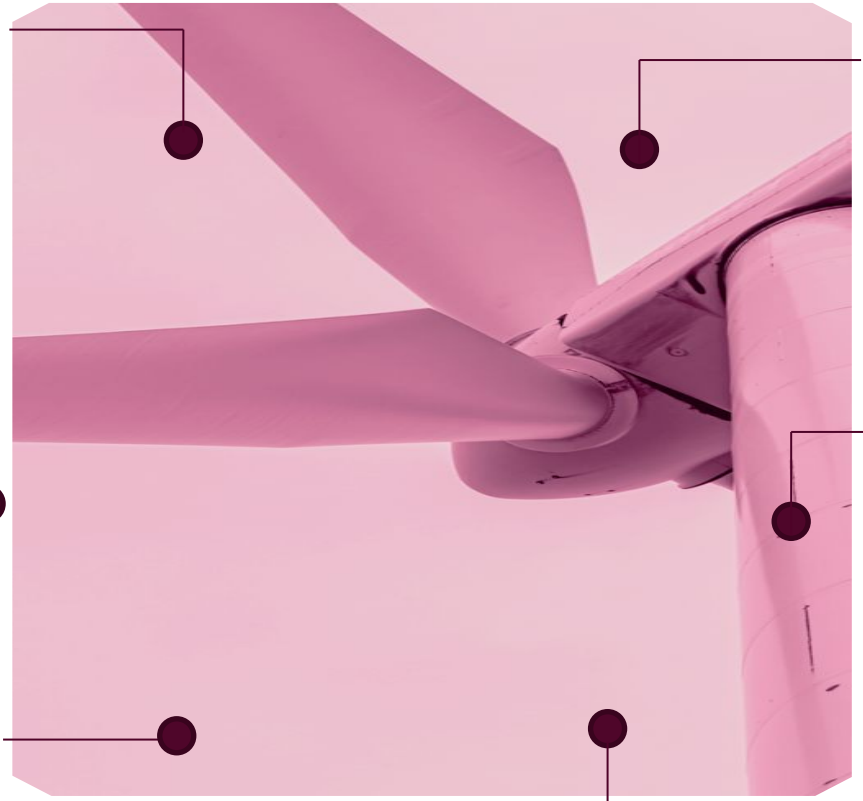
Creazione di un sistema ibrido di mondo fisico e digitale utilizzando la **tecnologia geospaziale** e il **digital twin**, che consentono di creare un modello digitale che simula il mondo fisico

Ubicazione e tracciabilità

Tecnologie per la **localizzazione e la tracciabilità** di persone, prodotti (catene logistiche) e asset in movimento (inc, Blockchain, OCR, ...)

Analytics e intelligenza artificiale

Tecnologie per la gestione dei dati e **algoritmi intelligenti** in grado di far fruttare le informazioni fornite dalla generazione massiva di dati (satelliti, fotocamere, sensori, ...)



Integrazione IoT - IT-OT

Stack di tecnologie digitali in grado di creare un sistema ibrido di funzionalità IT e OT, dando vita a un nuovo **paradigma IoT-BigData**, che permetta la connessione tra sensori e processi industriali, nell'industria e nel commercio

Automazione e intelligenza distribuita

Gestione di **sensori e attuatori** in grado di fornire informazioni che agiscono in tempo reale, integrando funzionalità di **di Edge computing, robotizzazione e comunicazione (5G, NBIoT, ...)**

Piattaforme phygital e esperienza utente

Sviluppo di **soluzioni basate su piattaforme** (architettura microservizi, ..), prodotti proprietari, di acceleratori (Onesait) e di interfacce utenti phygital, incl. tecnologie immersive (AR, VR, ...)

Prodotti e soluzioni

Sensori

Digital Assets

61850 | MODBUS | SNMP | MQTT | Analog & Digital I/O | LoraWan | LTE/5G

I nostri **Edge Devices** modulari e brevettati sono sviluppati per la supervisione e la registrazione dei dati della rete elettrica, sono in grado di controllare i parametri dal campo (in digitale e analogico) e di trasmetterli alla stazione centrale di supervisione.

[Compliant with E4S for a Standard and Open Source Solution]

Edge Layer

Software

Hardware

Onesait Edge	vPQ	vPCube	vDCU	vProtection
eWLC	Module of Power Quality	Module of virtual PCube	Module of virtual Data Concentrator Unit	Module of virtual Protection
Edge+ / Port Expander	PQ	PCube (P3)		Protection

SW Router: Ethernet | Fibra | LTE/5G

IoT Platform

Onesait Thing | Protocol Adapter | Data Hub | Broker | App Store | Connection Hub | Onesait Engine | Device Managment | Workload Managment | Digital Twins

Sistemi Core & Enterprise

Open Data

1	Vento	7	Punti caldi	13	Allagamento
2	Depositi salini	8	Dissolved gas analysis (DGA)	14	Smottamento
3	Stabilità Infrastrutture	9	Manomissioni e/o Danneggiamenti	15	Monitoraggio Linee Aeree
4	Manicotti di ghiaccio	10	Monitoraggio GAS SF6	16	Monitoraggio Cavi Interrati
5	Incendio-Fumo	11	Temperatura conduttori		
6	Vegetazione	12	Scariche Parziali		

Added Value

- Early Intervention
- Early Prevention
- Predictive Maintenance
- O&M Optimization
- TCO reduction
- Reliability Improvement
- Lifecicle Improvement
- Convergenza IT/OT

Success stories

areti

Virtualizzazione RTU

Introduzione di Edge device in cabina secondaria per la virtualizzazione delle funzioni di RTU MT/BT, Virtual Router, Data Concentrator e nuovi use case.

unareti

Infrastruttura intelligente

Introduzione di dispositivi Edge per la digitalizzazione delle reti intelligenti: acqua, energia elettrica, gas, veicoli elettrici e RSU

snam

onesait edge

Piattaforma device management

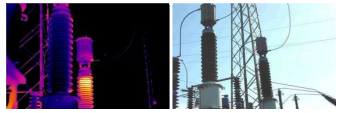
Installazione e integrazione della piattaforma Onesait Edge per offrire servizi di device management a un parco di dispositivi eterogeneo.

gridspertise

Piattaforma Smart Grid (QEd)

Realizzazione piattaforma IIoT del prodotto QEd (Quantum Edge device) per protezione, telecontrollo, automazione e supervisione della rete MT/BT.

enel Green Power



Sensorizzazione e monitoraggio impianti AT

L'obiettivo dell'intervento è la realizzazione di un'infrastruttura tecnologica in grado di acquisire dati in tempo reale da sensori di campo per consentire il rilevamento automatico di anomalie sugli asset.

enel Green Power

Convergenza IT/OT

Infrastruttura scalabile, che permette la razionalizzazione e la riduzione dei sistemi presenti in impianto, in grado di accogliere centralmente le applicazioni OT già esistenti, permettendo una gestione unificata dei sistemi.

Terna Driving Energy

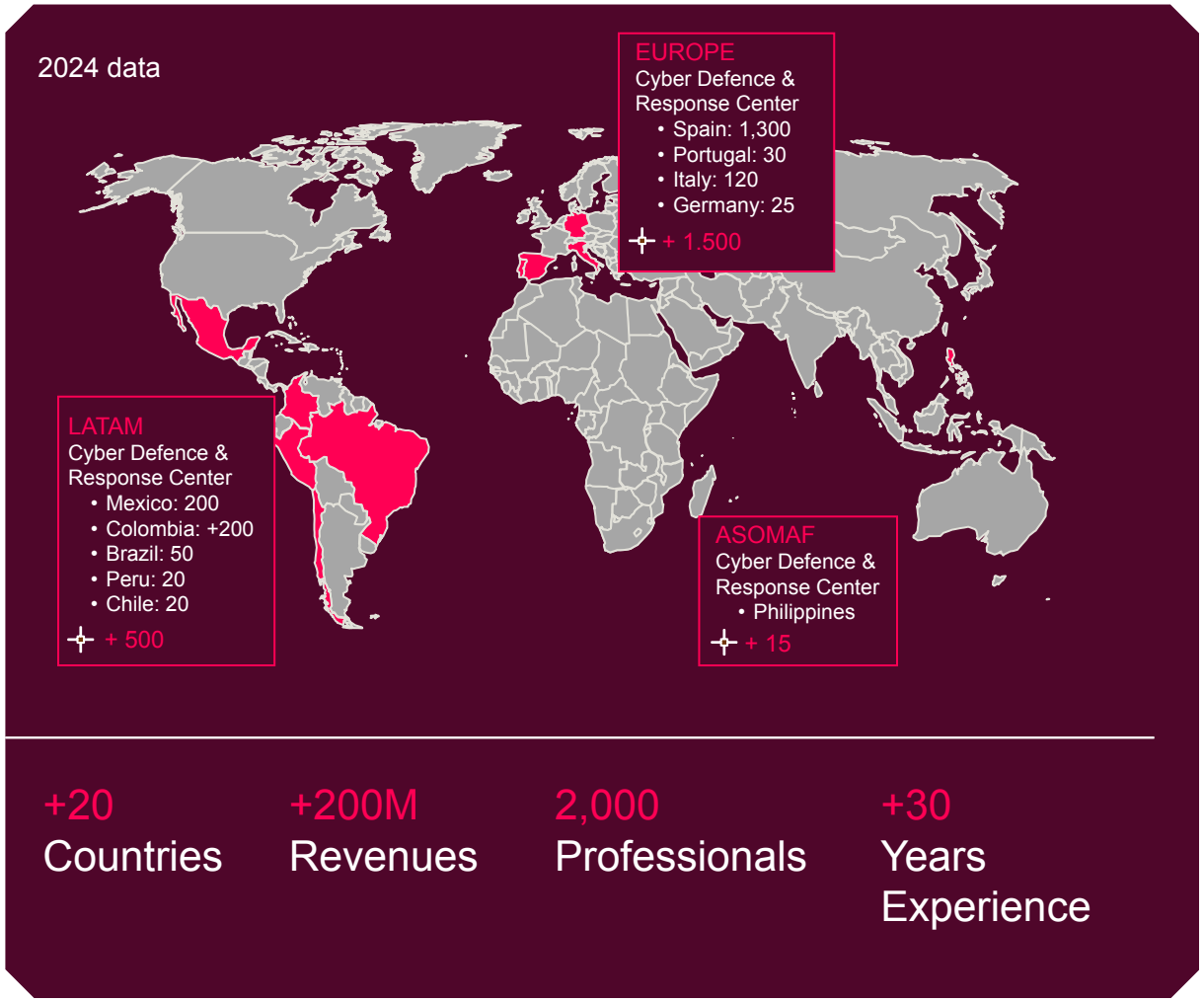
Digitalizzazione Asset

Digitalizzazione degli asset infrastrutturali, con particolare focus sui sistemi e tecnologie che governano l'infrastruttura. Sviluppo di nuovi casi d'uso IIoT, auto consistenti e sostenibili:

- Piattaforma IOT
- Soluzioni EDGE
- Algoritmi predittivi

Minsait Cyber. Indra Group Cybersecurity company

We protect digital assets and enable secure business operations, taking your company's protection further



E2E Cybersecurity

Business lines covering the entire cybersecurity lifecycle

60% Cybersecurity

40% Identity

Global Vision

+30% of **international revenues**

3 Cybersecurity Managed Detect & Respond Hubs with global coverage and coordinated service management (ESP, MEX, COL)

+500,000 endpoints/devices and **500,000 alerts** managed per day

Technology Focus

Ecosystem of strategic alliances with leading sector manufacturers. **+450 Certifications**

Advanced **propertiary & Third-Party Solutions** and **Innovative Services**

Talent Commitment

We train and incorporate +**500 professionals in cybersecurity** each year “Cyber-Capacities Talent Camp”

Agreements with +**50 Universities and Tech schools**

+400 cybersecurity annual certifications

Cybersecurity & Operational Technology BU

dal GDPR alla NIS2

RISERVATO, INTEGRO, DISPONIBILE

DOLOSO o ACCIDENTALE

CHIUNQUE abusivamente si introduce…

…il sistema DEVE essere protetto da misure di sicurezza tecniche e organizzative

***Notifica: «entro 72 ore** dal momento in cui ne è venuto a conoscenza»* il titolare. Qualora la notifica non avvenga nelle 72 ore, il titolare dovrà precisare anche i motivi del ritardo.

NOTIFICA DEGLI INCIDENTI
(marca temporale, hash)

identificare, autenticare e tracciare
chi accede ai dati.

CRITTOGRAFIA e CONFIGURAZIONE

Testare, verificare e validare regolarmente l'efficacia delle misure tecniche e organizzative....

Il GDPR ha rappresentato il primo quadro normativo europeo a introdurre principi obbligatori di sicurezza informatica, che NIS2 successivamente amplia e rafforza

Cybersecurity Solutions Portfolio




SecOps (Sec Technology delivery: Endpoint, Remote..)

IMPLEMENTATION, OPERATION, AND MANAGEMENT

NETWORK & CONNECTIVITY
- SD-WAN/SASE/SSE/ZTNA
- NGFW E VPN INDUSTRIALI

NETWORK & SEGMENTATION
- OT / IOT VISIBILITY
- IDS/IPS , ANOMALY DETEC

INDUSTRIAL FIREWALL
- IOMT SECURITY (SANITARIO)
- ACCESS & IDENTITY

ENDPOINT & PLATFORM
- XDR / EDR / APPLICATION
- OT ENDPOINT PROTECTION

Governance Risk & Compliance

ADVISORY

GRC
- STRATEGIC PLAN
- DIGITAL LAW
- CONTROL MANAGEMENT
- COMPLIANCE

SUPPLY CHAIN
- THIRD-PARTY RISK MANAGEMENT

VIRTUAL SERVICES
- VCISO

IT/OT Security Assurance

TECHNICAL AUDIT

PREVENT
- RED TEAM IT/OT
- SECURITY AUDITS (IT/OT/IOT)
- PENTESTING
- CONTINUOUS VALIDATION (BREACH & ATTACKSIMULATION)

PROTECT
- TRAINING AND AWARENESS

Managed Security Services

SMART MDR IT - OT

PREVENT
- THREAT INTELLIGENCE
- ATTACK SURFACE
- EARLY WARNING
- AUDIT AND RED TEAM
- VULNERABILITY MANAGEMENT

DETECT
- SECURITY MONITORING
- AUTOMATED AND MANUAL
- THREAT HUNTING
- DECEPTION

RESPOND
- CRISIS MANAGEMENT
- DIGITAL FORENSIC & INCIDENT
- RESPONSE
- COMPROMISE ASSESSMENT

Professional Services

- ✔ Consulting & Assessment
- ✔ Analysis & Design
- ✔ Project Management
- ✔ Implementation
- ✔ Support post go-live

Security Operation & Training

- ✔ Application Management
- ✔ Corrective Maintenance
- ✔ Evolutionary Maintenance
- ✔ Training (IT, Security Teams, End-user)

Professional Services, Security Operation & Training

CLAROTY · endian · GROUP-IB · NOZOMI NETWORKS · tenable · txOne networks · TREND MICRO · Cyber Guru · FORTINET · OPSWAT. · paloalto NETWORKS · semperis · CHECK POINT · MANDIANT · IBM

Identity Solutions Portfolio




Identity & Access Governance

- Identity Lifecycle processes (Joiner, Mover, Liver)
- Access Request process
- Access Review process;
- Provisioning and deprovisioning process
- Risk identification (e.g. SoD conflicts)
- Audit & Reporting

Access Management & MFA

- Authentication (MFA) & Access Control
- Single Sign On (SSO)
- Application Federation
- Password Management
- Passwordless & MFA
- Risk Based Authentication
- Social Identity
- Customer Identity Management (CIAM)

Privileged Access Management

- Discovery and Classification of Privileged Accounts
- Implement just-in-time access to reduce the time windows of exposure
- Centralize and automate password rotation and storage
- Record all privileged sessions for accountability
- Enable real-time alerts and session monitoring.

ITDR & ISPM

- **ITDR** focuses on Real-time threat detection and protection
- **ITDR** applies machine learning to analyze user behavior and anomaly detection
- **ISPM** enhances identity infrastructure by proactively identifying weaknesses and applying security best practices.

Professional Services

- ✔ Consulting & Assessment
- ✔ Analysis & Design
- ✔ Project Management
- ✔ Implementation
- ✔ Support post go-live

Security Operation & Training

- ✔ Application Management (AMS)
- ✔ Corrective Maintenance (MAC)
- ✔ Evolutionary Maintenance (MEV)
- ✔ Training (IT and Security Teams, End-user awareness program)

Professional Services, Security Operation & Training

SailPoint · SAVIYNT · ForgeRock · ONE IDENTITY · okta · semperis · RSA SECURITY · IBM · CYBERARK · SILVERFORT · PingIdentity. · IAMONES MAKE IDENTITY FLY · OpenIAM · Microsoft · THALES · Sharelock · Delinea · opentext

04

ENDIAN

Secure Digital Platform: Architettura e Funzionalità

Filippo Collini - Endian

endian

MINSAIT

Endian

- **Vendor di Cybersecurity Italiano**

  Fondata nel 2003, Endian rimane interamente di proprietà dei suoi fondatori originari. Pur avendo le sue radici in Alto Adige, l'azienda ha consolidato la propria posizione nel mercato tedesco, rivolgendosi a un ampio spettro di clienti industriali. Tutte le soluzioni software sono interamente progettate, sviluppate e gestite internamente, garantendo il pieno controllo su qualità, sicurezza e innovazione.

- **Oltre vent'anni di esperienza nel campo della sicurezza informatica**

  Con oltre 20 anni di esperienza nella sicurezza IT e oltre un decennio nella sicurezza OT (Operational Technology), Endian unisce un profondo know-how tecnico a una solida esperienza pratica nel settore.

- **Cultura Open Source**

  Basandosi sui principi dell'Open Source, Endian promuove un ambiente trasparente e collaborativo che stimola l'innovazione e rafforza il coinvolgimento della comunità.

- **Focus sulle esigenze IT e OT industriali**

  Le soluzioni di sicurezza Endian sono progettate specificamente per gli ambienti industriali e affrontano le sfide uniche che devono affrontare sia le infrastrutture IT tradizionali che le configurazioni tecnologiche operative.

- **Cybersecurity accessibile e intuitiva**

  Nota per offrire funzionalità avanzate in un pacchetto intuitivo, Endian garantisce che una solida sicurezza informatica rimanga accessibile e gestibile per team eterogenei, dai professionisti IT agli operatori OT.

Impatto normativo

GDPR

Il GDPR garantisce la protezione e la riservatezza dei dati personali delle persone fisiche all'interno dell'UE, regolamentando il trattamento dei dati da parte delle organizzazioni.

NIS2

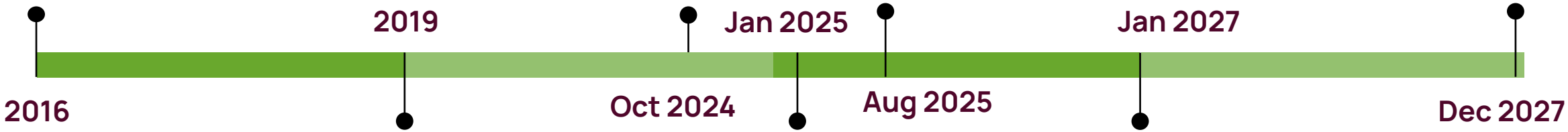
NIS2 rafforza la sicurezza informatica dell'UE nei settori critici, richiedendo misure di sicurezza più rigorose e la segnalazione degli incidenti.

RED DA

La Direttiva sulle apparecchiature radio (RED) 2025 disciplina sicurezza, compatibilità e uso dello spettro delle apparecchiature radio nell'Unione Europea.

Cyber Resilience Act

Il Cyber Resilience Act mira a migliorare gli standard di sicurezza informatica e la preparazione in tutti i settori delle infrastrutture critiche nell'UE



IEC 62443

La norma IEC 62443 fornisce standard e certificazioni di sicurezza informatica per l'automazione industriale, garantendo la sicurezza dei sistemi di controllo a livello globale.

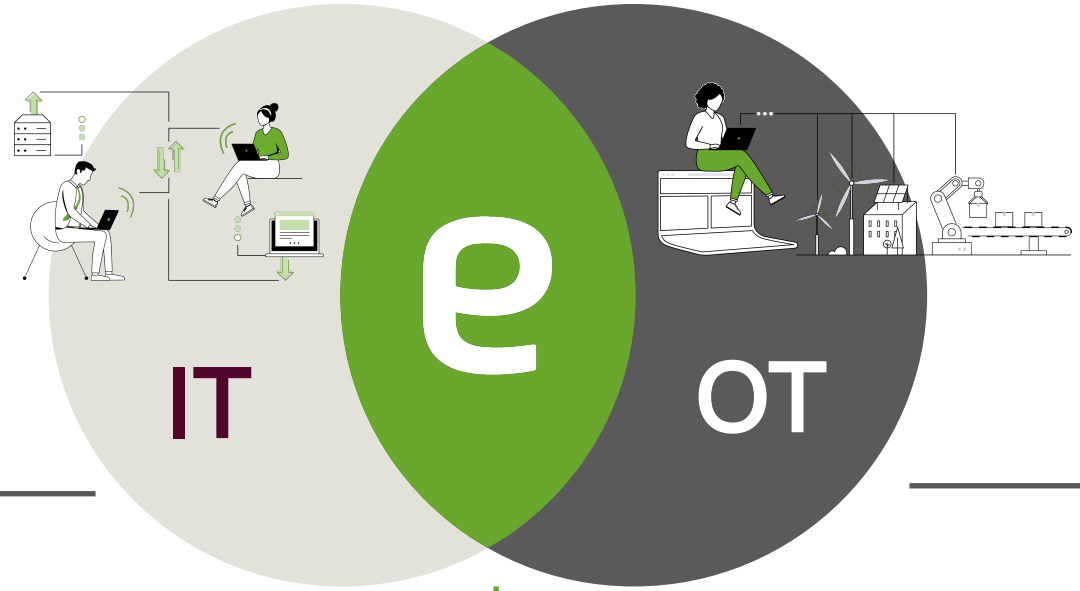
DORA

DORA rafforza la resilienza delle istituzioni finanziarie dell'UE contro le interruzioni delle TIC, garantendo una solida sicurezza informatica e un'adeguata rendicontazione.

Machinery Directive

La Direttiva Macchine 2027 garantisce la sicurezza e la conformità delle macchine all'interno del mercato dell'Unione Europea, compresa la sicurezza informatica.

Convergenza IT & OT



- Principi Zero Trust
- Osservabilità della rete distribuita
- Tool di terze parti

- Combina IT & OT
- Proteggi Asset OT/IoT
- Esperienze utente personalizzate

- Accesso Remoto Sicuro
- Maintenance Predittiva & Monitoring
- Compliance con IEC 62443, NIS2, …

Secure Digital Platform

Definizione

La Secure Digital Platform è una soluzione di sicurezza e connettività di nuova generazione che combina protezione avanzata, gestione semplificata e strumenti di analisi in tempo reale.

Sviluppata per soddisfare le esigenze sia delle reti aziendali che degli ambienti industriali, garantisce la massima affidabilità, flessibilità e scalabilità.

Grazie a tecnologie all'avanguardia e a un'interfaccia intuitiva, Endian riduce il rischio di attacchi informatici, semplifica la gestione di reti complesse e migliora la produttività dei clienti.

Componenti

1 - Management Tools

- Gestire l'intero ciclo di vita della soluzione
- Gestire i componenti della piattaforma digitale sicura

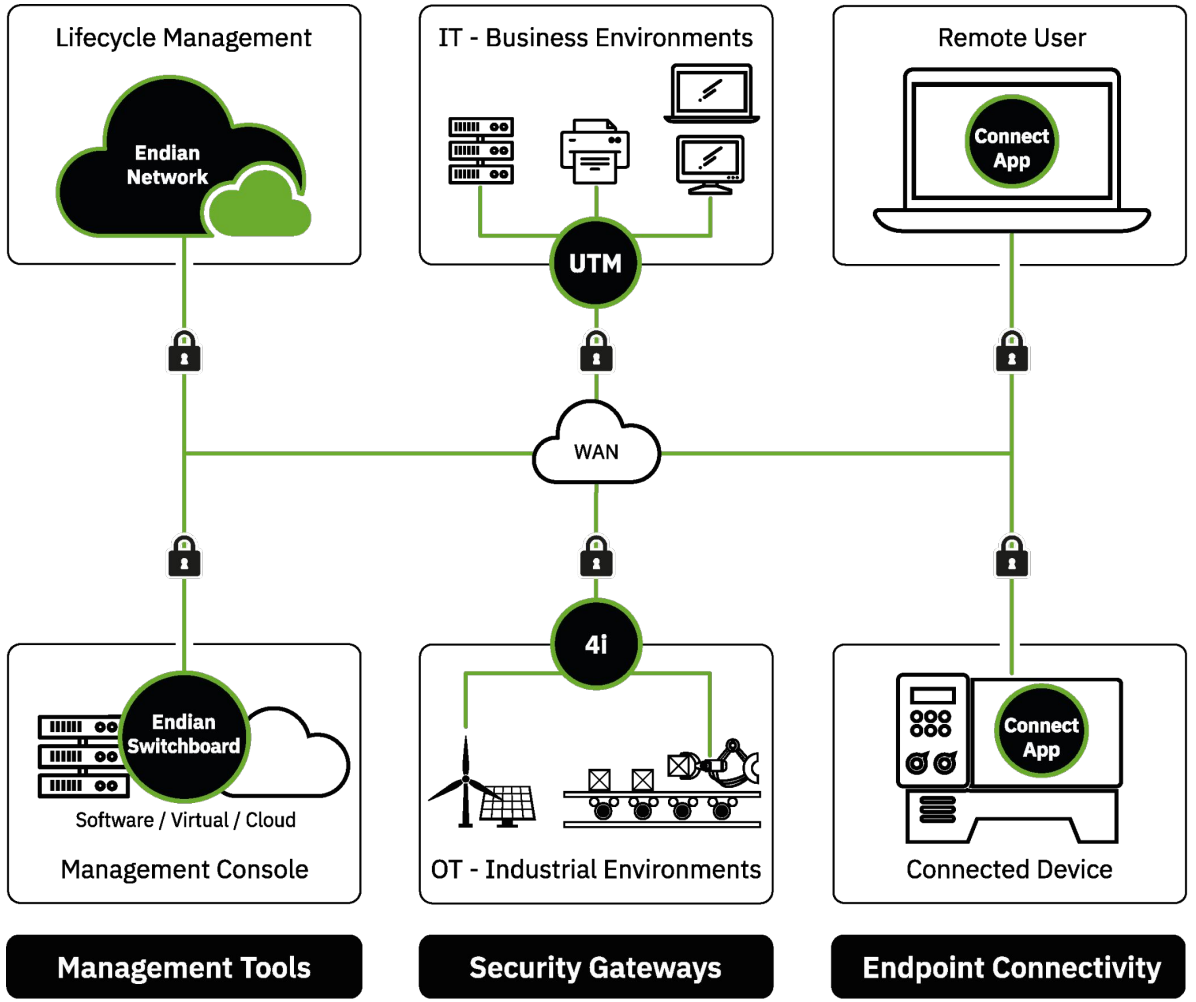
2 - Security Gateways

- L'infrastruttura sottostante
- Sicurezza rafforzata con EndianOS

3 - Endpoint Connectivity

- Accedere in remoto agli endpoint
- Fornire funzionalità sicure

Secure Digital Platform



Secure Digital Platform

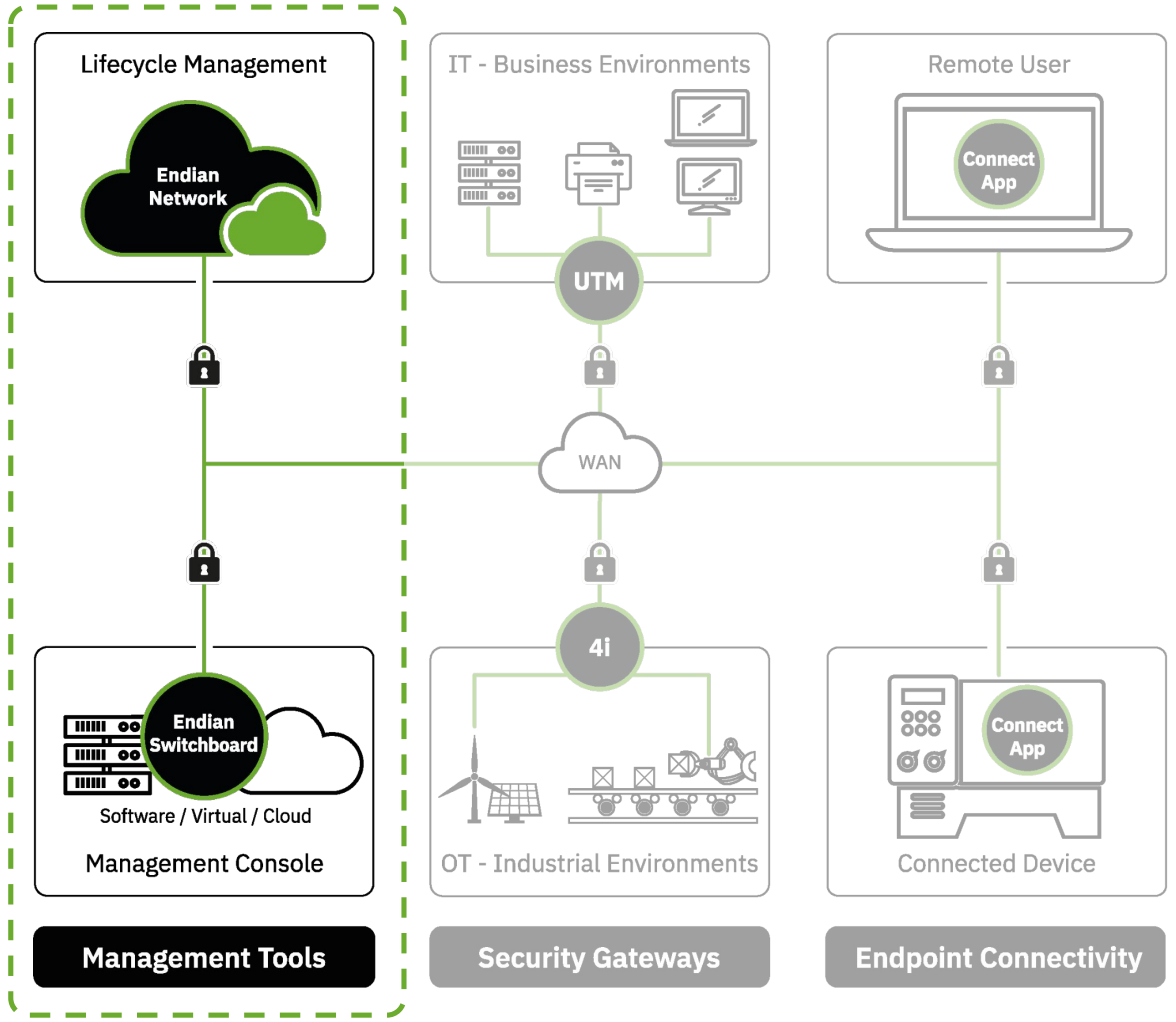
Management tools

Endian Switchboard

- Gestione centralizzata di gateway e dispositivi
- Gestione delle autorizzazioni e dell'infrastruttura
- Monitoraggio delle reti distribuite

Endian Network

- Gestione dell'organizzazione e degli abbonamenti
- Gestione del ciclo di vita dei prodotti
- Metriche e business intelligence



Secure Digital Platform

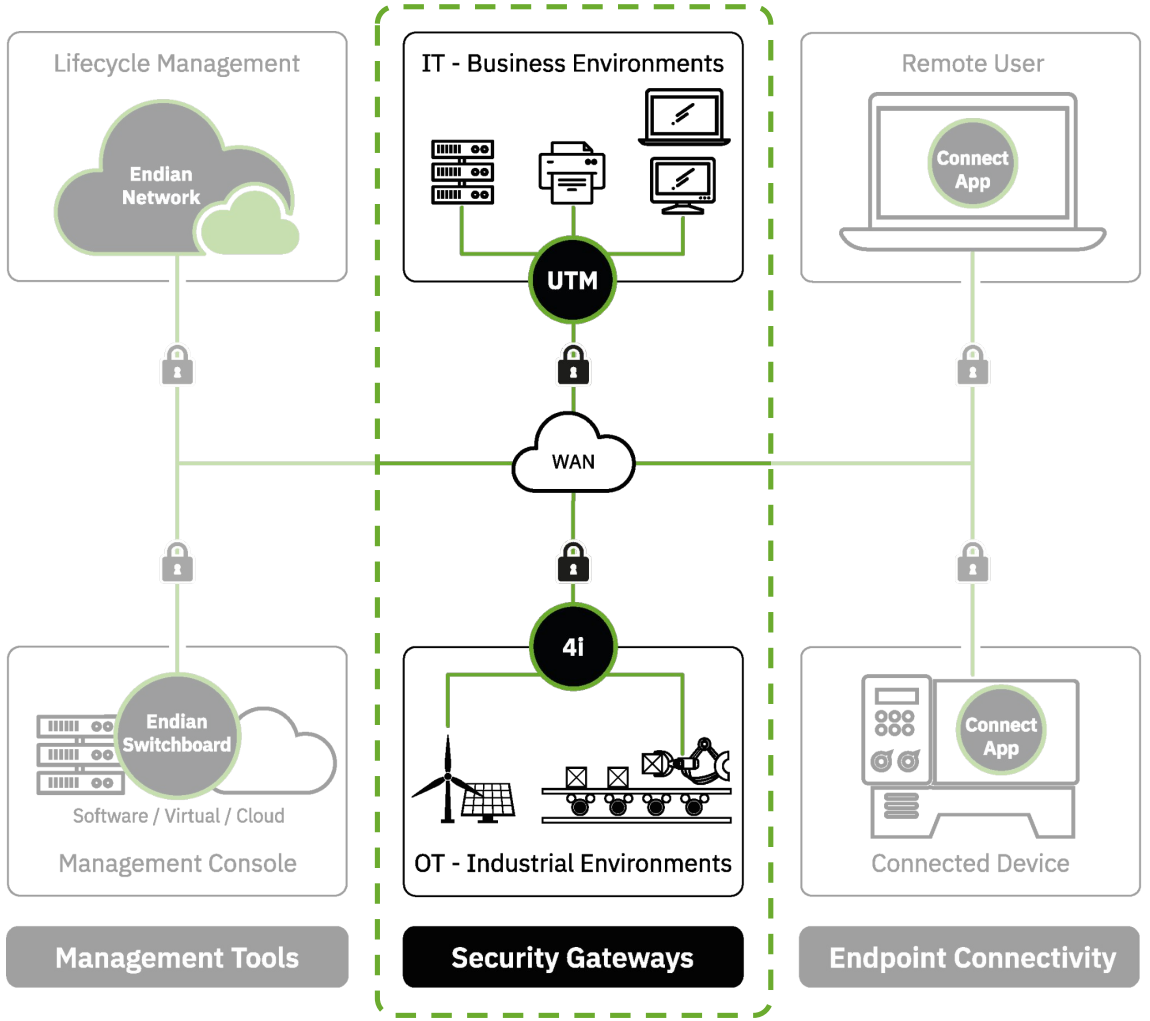
Security gateways

Endian UTM per l'IT

- Applica politiche di sicurezza di rete con EndianOS
- Ottimizza la connettività e le prestazioni della rete
- Rileva e filtra le minacce avanzate

Endian 4i per l'OT

- Proteggi e monitora le reti OT con EndianOS
- Connettività e supporto dei protocolli IoT/OT
- Connettività affidabile in ambienti industriali

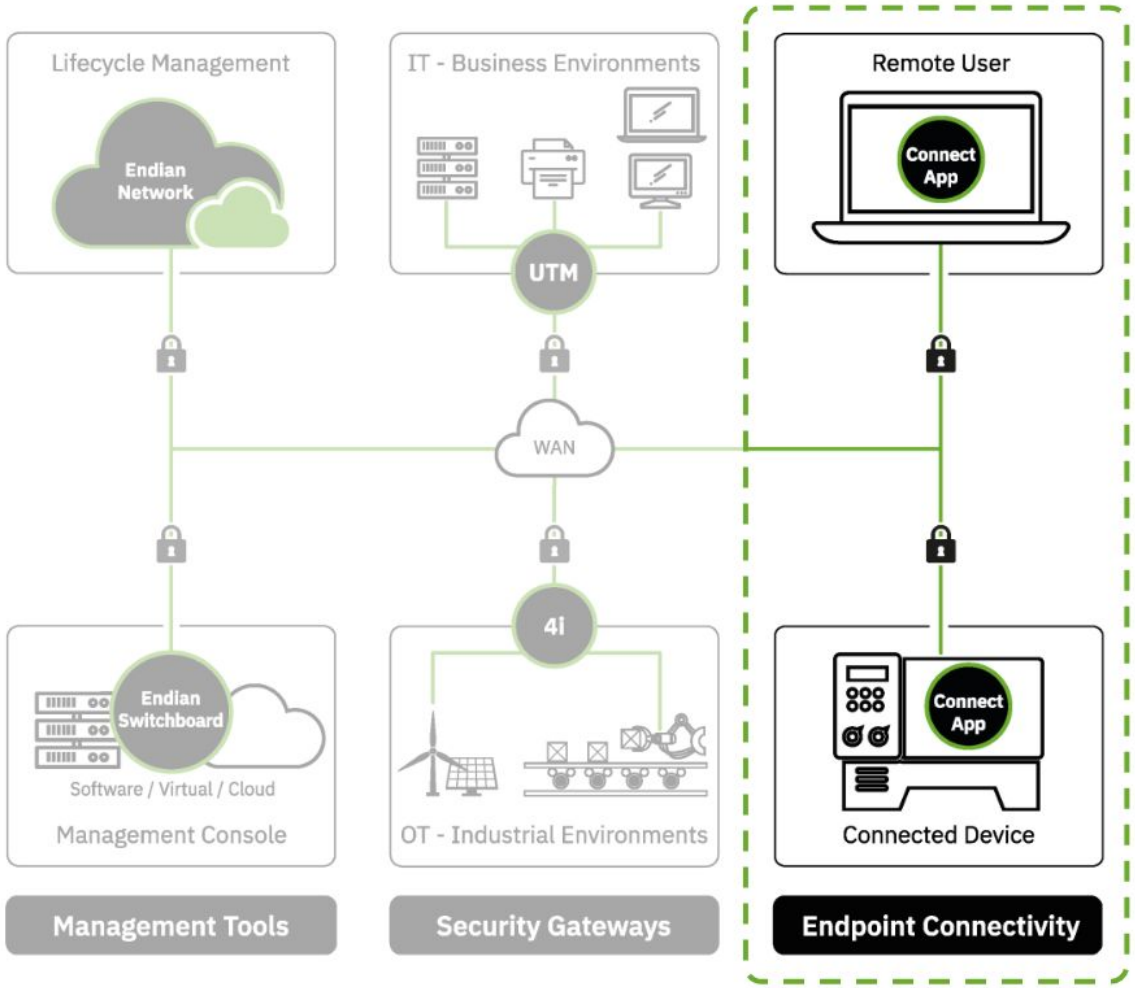


Secure Digital Platform

Endpoint connectivity

Endian ConnectApp

- Client facile da usare per Switchboard
- Rendi gli endpoint accessibili da remoto
- Fornisci le funzionalità sicure di un client VPN

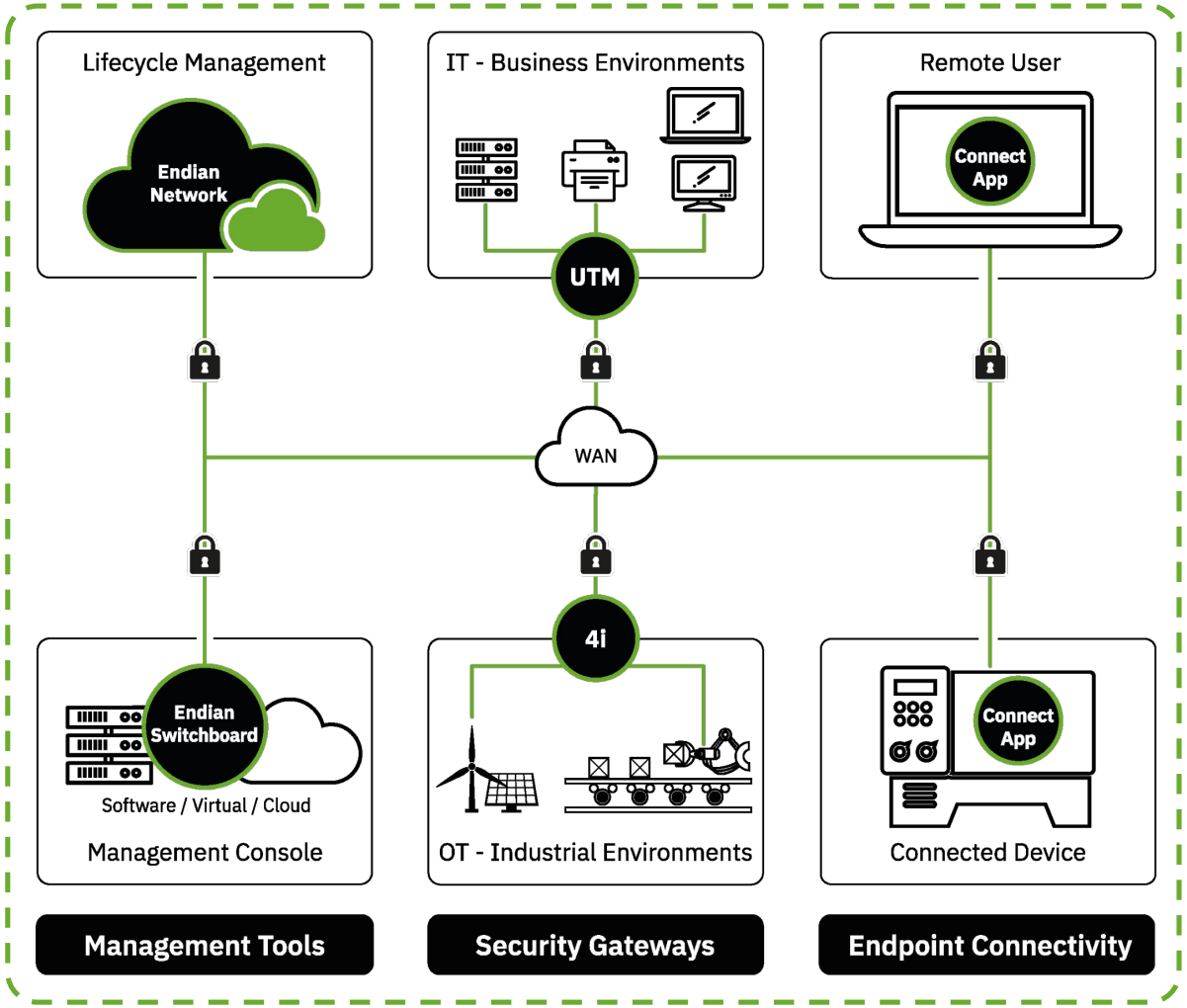


Secure Digital Platform

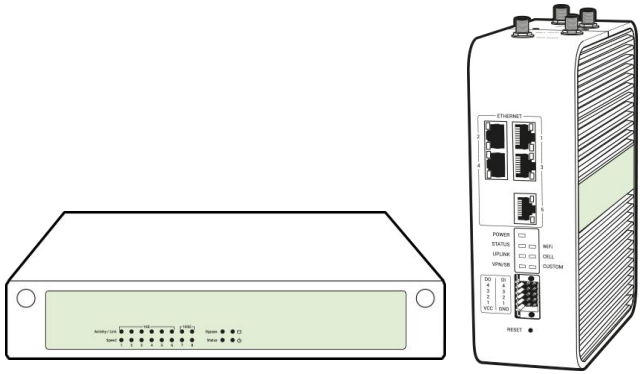
Applicazioni dei nostri Partner

Costruito sulla nostra piattaforma

- Integra qualsiasi applicazione tramite OpenAPI
- Edge computing basato su Docker
- Integrazione con provider di identità esterni



Ambienti supportati

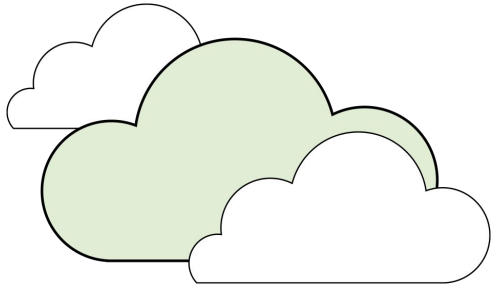


Hardware

- IT: Montabile su rack
- OT: DIN Rail

Virtual

- VMware
- Hyper-V
- KVM
- XEN
- VirtualBox



Cloud

- AWS
- Azure
- Docker

Highlights

Endian consente alle aziende di migliorare la sicurezza, semplificare le operazioni e proteggere le risorse critiche. Le nostre soluzioni consentono Zero Trust, accesso remoto sicuro, prevenzione delle minacce e gestione efficiente dei dispositivi, il tutto in un'unica piattaforma unificata.

Zero Trust

- Microsegmentazione
- IAM & MFA
- Gestione CA & Certificates

Accesso Remoto Sicuro

- Semplificare accesso a risorse
- Approvazione e registrazione delle sessioni
- Concetto di privilegio minimo

Monitoraggio reti e rischi

- Individuazione delle risorse distribuite
- Valutazione dei rischi
- Rilevamento delle anomalie

Prevenire gli attacchi

- Firewall con DPI & Routing
- Intrusion Detection/Prevention
- Alta Affidabilità

Esegui applicazioni Edge

- Abilita app di terze parti
- Gestisci facilmente l'Edge Computing
- Docker eseguibile su EndianOS

Gestione dispositivi

- Automatizza la gestione del ciclo di vita
- Centralizza gli aggiornamenti
- Fornisci configurazioni e certificati

Clienti target

Machine and equipment Manufacturers (OEM)

CATERPILLAR®
werfen
JENSEN®
MICROTEC
LIEBHERR
...

Small and Medium-sized Businesses (IT)

eurotherm® radiant comfort systems
UNIVERSITÀ DEGLI STUDI DI UDINE hic sunt futura
DEL GARDA VILLAGE
unibz Freie Universität Bozen Libera Università di Bolzano Università Liedia de Bulsan
EMERGENCY
...

Manufacturing companies (Smart Factory)

Röchling
SFS
Smart Mini Factory Laboratory for Industry 4.0 unibz
...

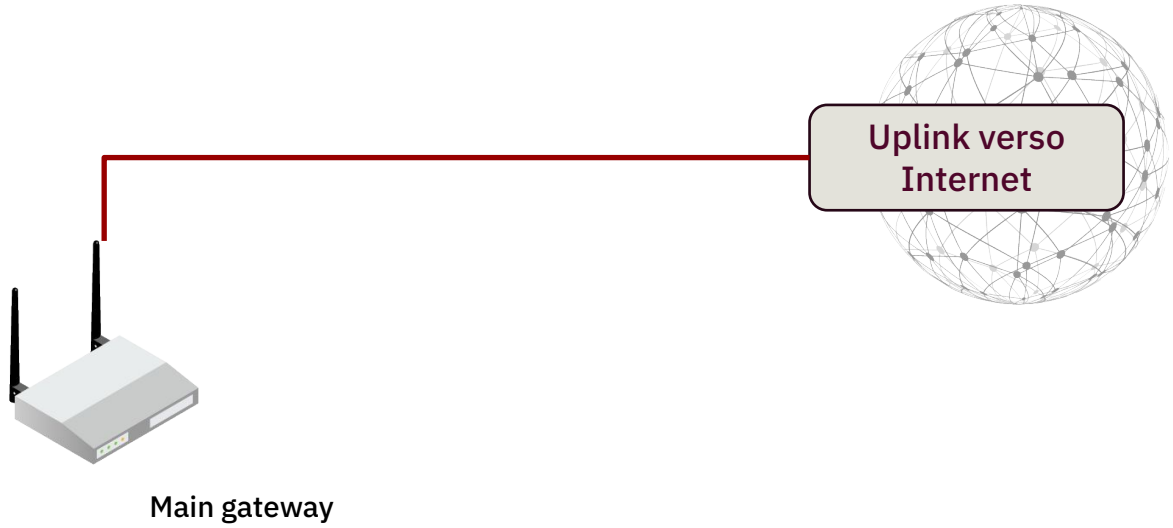
Critical Infrastructure

orange™ Business Services
GRUPPO HERA
BTS
iqony
SPIE OSMO
...

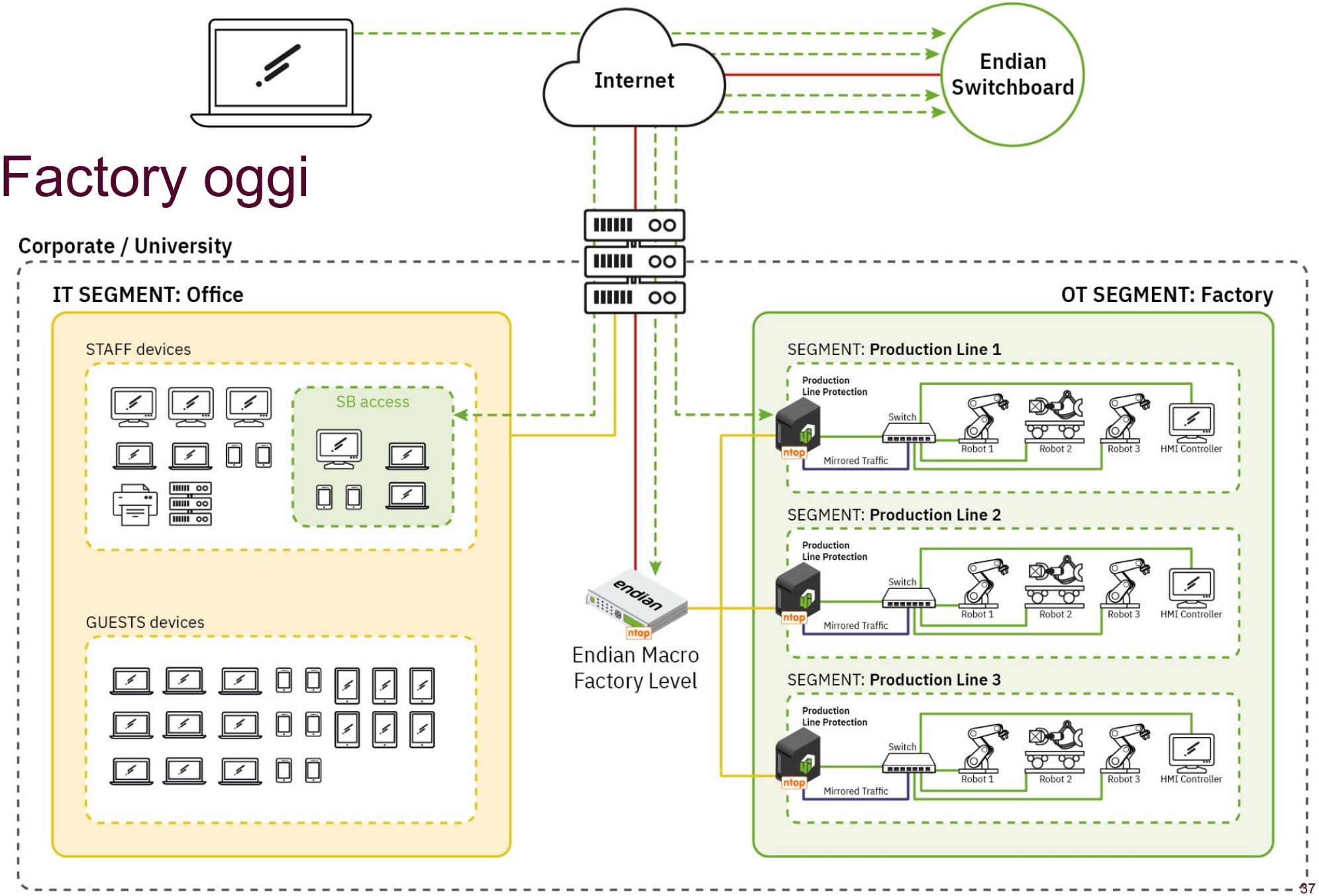
Smart Mini Factory UNIBZ

Punti di attenzione iniziali:

- Una grande rete IT/OT senza restrizioni
- Alto rischio di attacchi interni (intenzionali o non intenzionali)
- Alto pericolo di sicurezza per gli operatori se le macchine vengono compromesse



Smart Mini Factory oggi



05

Use Case Dimostrativo

Smart Authentication per l’accesso sicuro agli impianti

Federico Bellio - Bjosora

Filippo Collini - Endian

Sonia Gentile - Minsait

bjosora Operational Technologies

endian

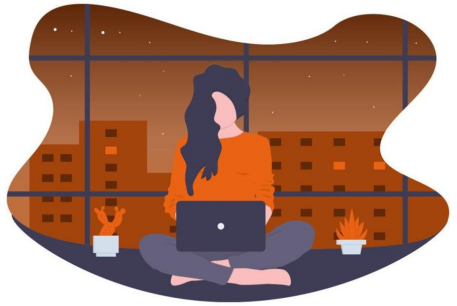
MINSAIT

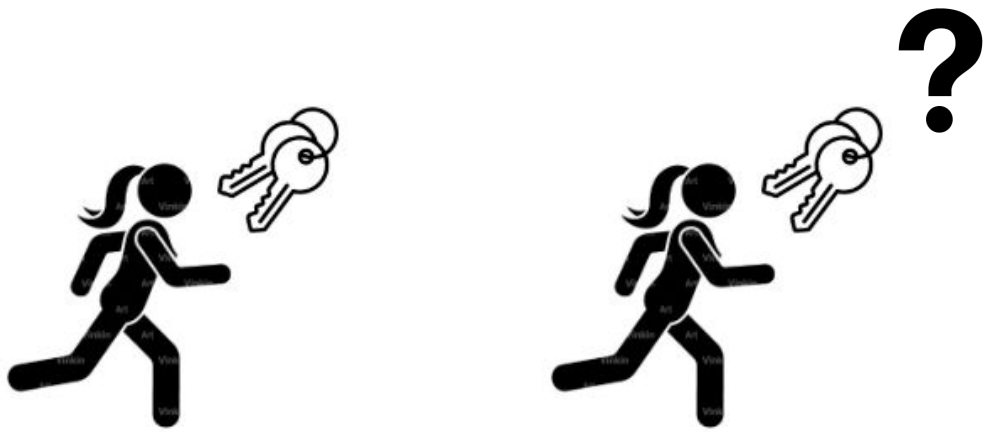
Smart Authentication per l'accesso sicuro agli impianti

case study: difficoltà di autenticazione fisica e logica

Un manutentore si scontra con l'organizzazione dei propri mezzi di autenticazione.

Un esempio. Un manutentore di un reparto operativo idroelettrico ha un portachiavi con centinaia di chiavi che aprono la porta di siti pericolosi (accesso in tensione o su ambienti confinati) e la password per accedere a decine di postazioni di controllo locale.





Smart Authentication per l'accesso sicuro agli impianti

case study: difficoltà di autenticazione fisica e logica

Policy di controllo accessi su siti presidiati e non presidiati

- Ogni accesso ad un sito va registrato (identità, società di appartenenza, ora d'ingresso ora d'uscita) e il registro va conservato
- Le chiavi di accesso vanno opportunamente gestite

Policy di cybersecurity su sistemi IACS (Industrial Automation Control System)

- Ogni accesso ad un sistema va registrato (identità, società di appartenenza, ora d'ingresso ora d'uscita) e il registro va conservato
- Le credenziali d'accesso vanno opportunamente gestite

Introduzione alla DEMO per l’accesso sicuro agli impianti

Scenario reale

- Accessi fisici gestiti tramite chiavi tradizionali su impianti distribuiti
- Password condivise o annotate localmente sulle postazioni OT
- Audit trail difficile da garantire in modo centralizzato
- Mancanza di correlazione tra accesso fisico e login ai PC OT
- Impianti con sistemi eterogenei, anche legacy e non presidiati

Cosa vedremo con la DEMO

Tre scenari concreti che coprono l’intero ciclo di accesso ai sistemi OT:

- **UC-01 – Accesso remoto** - tramite Endian Switchboard e Identity Provider esterno.
- **UC-02A – Accesso locale impianto** - combinando apertura fisica NFC (iLOQ) e autenticazione forte (Okta).
- **UC-02B – Accesso locale legacy** - con password vault e dispositivo USB sicuro su PC senza dominio/ rete.

Obiettivo della demo: mostrare un flusso di accesso OT più semplice, tracciato e conforme, senza modificare le operazioni dei tecnici né aggiornare forzatamente i sistemi esistenti.

UC-01 – Accesso remoto al PC dell’impianto - Assunzioni

Scenario autenticazione con Endian Switchboard

Endian Switchboard è una piattaforma di accesso remoto sicuro che centralizza l'autenticazione e l'autorizzazione per l'accesso a risorse OT/IT distribuite.

Consente di gestire in modo controllato e tracciato l'accesso di contractor, partner e personale remoto, integrando Identity Provider esterni (Entra ID) e garantendo visibilità completa tramite session recording.

Scenario dimostrato	Tecnologie utilizzate
Accesso controllato via browser a un PC OT, senza client VPN,con session recording integrato.	Endian Switchboard, Entra ID

Piattaforma di integrazione	Prerequisiti configurazione	Policy di accesso	Autenticazione MFA e passwordless
Una piattaforma cloud/on-premise che collega contractor e personale remoto a qualsiasi risorsa OT/IT tramite browser. Centralizza l'accesso remoto e semplifica la gestione delle sessioni.	Il PC target deve essere raggiungibile dalla rete Endian. Vengono supportati sistemi operativi da WinXP a Win11. Protocollo utilizzato: RDP	Gli amministratori possono definire regole di accesso granulari per utenti e gruppi. È possibile applicare policy Zero Trust e least-privilege basate su identità e contesto.	Integrazione con Identity Provider esterni (Entra ID). Installazione Microsoft Authenticator su smartphone. MFA obbligatorio

UC-01 – Accesso remoto al PC dell’impianto - Descrizione

OBIETTIVO

Abilitare un accesso remoto controllato, monitorato e tracciato al PC dell’impianto tramite Endian Switchboard e Identity Provider esterno.

FLUSSO DEMO

- Accesso da browser a Endian Switchboard.
- Autenticazione tramite IdP (Entra ID) + MFA.
- Verifica policy → least-privilege.
- L’utente seleziona il PC dell’impianto.
- Sessione **RDP via browser** (senza VPN client).
- Registrazione e monitoraggio sessione.

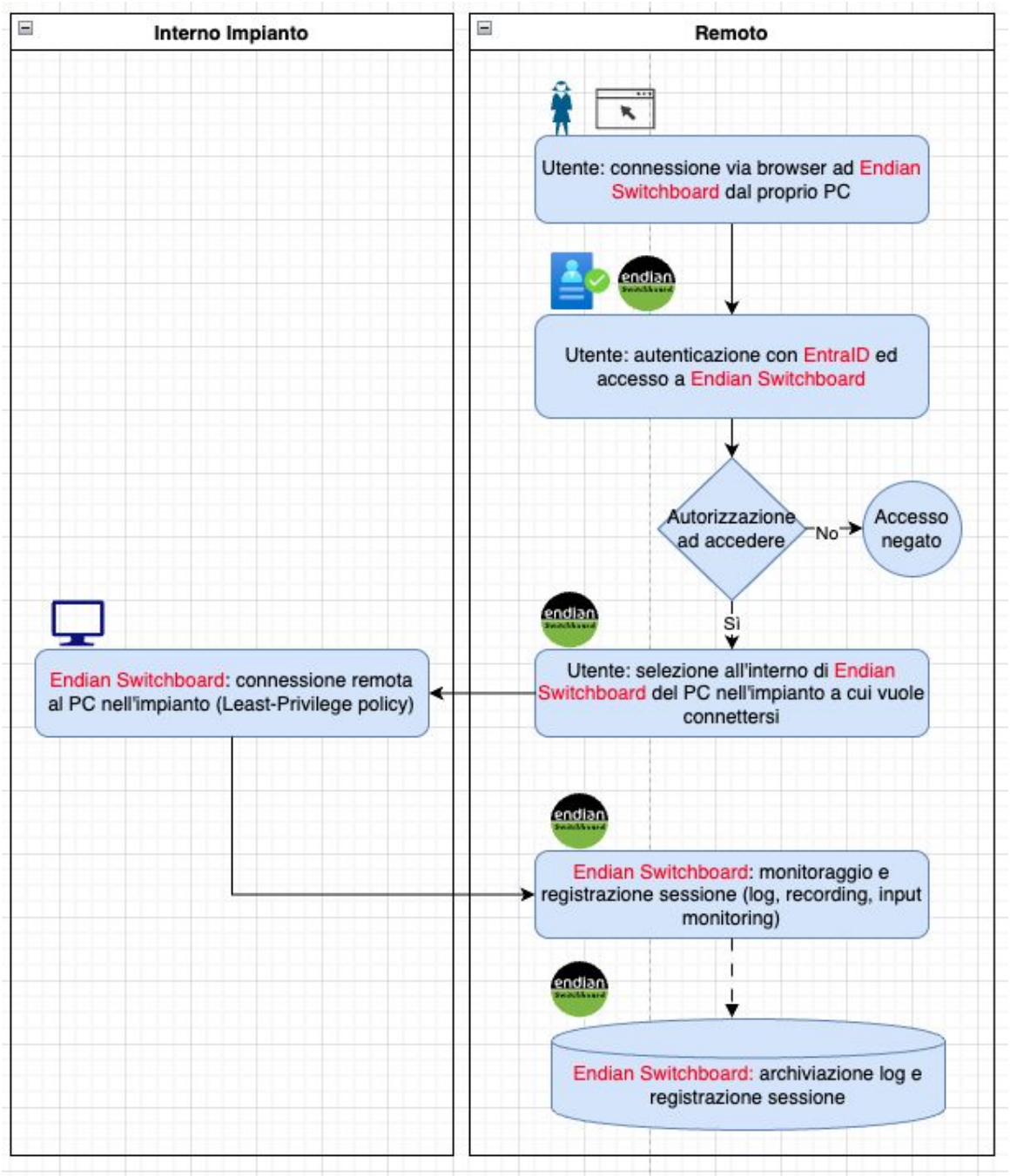
NOTE DI PERIMETRO DEMO

- Account PC shared/static (scopo dimostrativo).
- Nessun trasferimento end-to-end dell’asserzione IdP verso il PC.
- Estensioni POC: SSO completo, contextual access.

UC-01 – Accesso da remoto

Process Flow

SCENARIO	- *Manutentore/Contractor accede da remoto al PC impianto per manutenzione*
COME FUNZIONA	- *Browser → Endian Switchboard* - *Login con EntraID + MFA* - *Policy check (autorizzazione)* - *Sessione RDP via browser* - *Recording completo per audit*
VALORE	- *Zero VPN client* - *Architettura Zero Trust* - *Visibilità della sessione* - *Compliance ready*



UC-02A + UC-02B – Soluzione Ampercom / iLOQ

Al fine della DEMO, per i due use case verrà adottata la soluzione di serratura digitale e gestione degli accessi **Ampercom / iLOQ** per le sue peculiari caratteristiche:

Caratteristiche principali

- Azionamento meccatronico via NFC
- Nessuna fonte di alimentazione nel cilindro della serratura (l'energia trasferita via NFC è sufficiente)
- Accesso granulare RBAC secondo raggruppamenti per area di responsabilità o area geografica di competenza o slot temporale, tutto sulla base di certificati digitali
- Ogni operazione è loggata

UC-02A – Accesso locale PC in dominio - Assunzioni

Okta è una piattaforma cloud di Identity & Access Management che centralizza l'autenticazione e l'autorizzazione di utenti e dispositivi.
Consente di gestire in modo sicuro l'accesso di dipendenti, partner e clienti, integrando funzionalità come Single Sign-On, Multi-Factor Authentication e gestione del ciclo di vita delle identità.

Scenario dimostrato	Tecnologie utilizzate
Apertura fisica dell'impianto tramite NFC + login al PC con autenticazione forte passwordless.	iLOQ, Okta Device Access

Piattaforma di integrazione	Prerequisiti configurazione	Policy di accesso	Autenticazione MFA e passwordless
Un servizio cloud che collega qualsiasi persona a qualsiasi applicazione su qualsiasi dispositivo. Protegge l'identità digitale e semplifica l'accesso alle risorse aziendali.	Il PC deve essere in un dominio Active Directory Windows 10/11 o macOS con supporto Platform SSO	Gli amministratori possono definire regole di MFA per utenti e gruppi È possibile integrare con criteri di accesso condizionale	Installazione Okta Verify MFA obbligatorio Possibilità di configurare passwordless login o reset self-service della password

UC-02A – Accesso locale PC in dominio - Soluzioni di Mercato

Il mercato offre diverse soluzioni MFA per l'accesso al PC – tra cui Thales, Okta, Microsoft Entra ID e Namirial – ciascuna con un proprio approccio: Thales privilegia token hardware/software e smart card; Okta integra modelli cloud e passwordless; Entra ID abilita Windows Hello e criteri di accesso condizionale; Namirial combina smart card e OTP legati alla firma digitale.

Soluzione	MFA supportati	Integrazione PC	Punti di Forza	Punti di Attenzione
Microsoft Entra ID	Windows Hello (biometria/PIN), Authenticator, FIDO2, SMS/OTP	Integrazione nativa Windows 10/11	Accesso condizionale avanzato, forte integrazione Microsoft	Licenze P1/P2; dipendenza dall'ecosistema Microsoft
Namirial	Smart card CNS, token USB, OTP/app, firma digitale remota	Driver smart card/token, OTP	Identità certificate, validità legale, ideale per PA	Poco orientato al login PC aziendale; focus su firma digitale
Okta	Okta Verify (Push/TOTP), FIDO2, passwordless	Windows/macOS con Desktop MFA	Architettura cloud matura, policy granulari, UX fluida	Dipendenza dal cloud, limitazioni offline
Thales	OTP hardware/software, smart card, PKI, token USB	Windows (anche pre-Win10) tramite PKI/token	Ampia gamma metodi, sicurezza elevata, opzioni cloud/on-prem	Richiede PKI interna; gestione più complessa

Al fine della DEMO, per i due use case verranno adottate le soluzioni: **Microsoft Entra ID** e **Okta**

UC-02A – Accesso locale PC in dominio - Descrizione

OBIETTIVO

Garantire un accesso coerente, sicuro e tracciato al PC dell'impianto, combinando accesso fisico (iLOQ) e autenticazione forte (Okta), senza password visibile all'utente.

FLUSSO DEMO

- Accesso fisico tramite smartphone NFC (iLOQ).
- Generazione log di audit da parte di iLOQ.
- Sul PC locale l'utente inserisce **solo lo username**.
- Okta invia una **push notification** su Okta Verify.
- L'utente approva → il PC si sblocca (least-privilege).

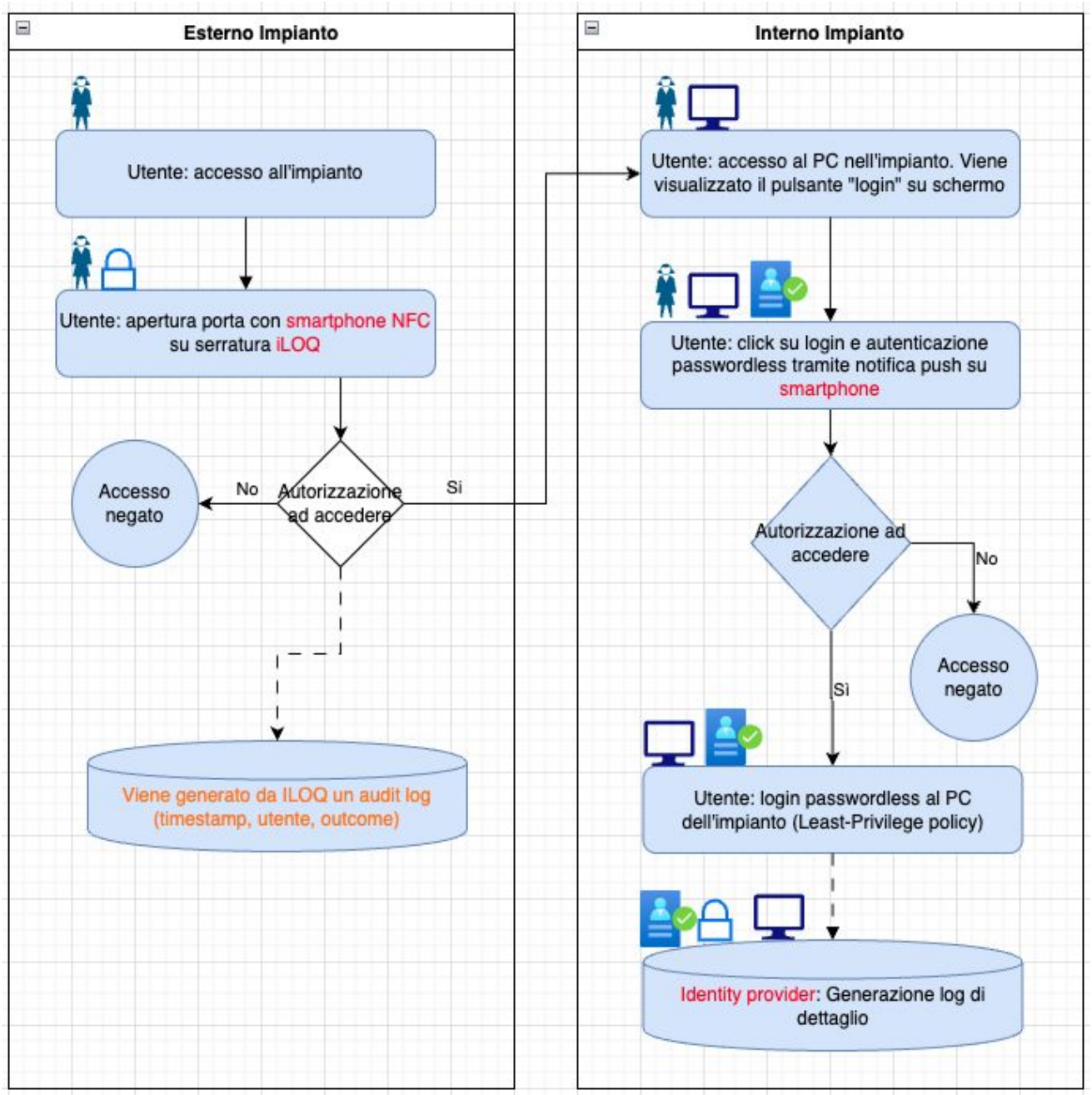
NOTE DI PERIMETRO DEMO

- Passwordless **lato utente**, non passwordless nativo Windows/FIDO2.
- Nessuna correlazione automatica tra accesso fisico e login PC.
- Estensioni valutabili in POC: integrazione API iLOQ, controllo contestuale, offline mode.

UC-02A – Accesso PC

Process Flow-Accesso Fisico Impianto

UTENTE	- *Arriva* - *Sblocca iLOQ* - *Inserisce user* - *Conferma*
DISPOSITIVO	- *Smartphone NFC* - *Riceve push Okta* - *Approvazione MFA* - *Conferma autenticazione*
SISTEMA LOCALE	- *PC locale* - *Schermata login* - *Richiesta autenticazione* - *Sblocco sessione*
BACKEND	- *iLOQ audit log autenticazione* - *Okta autenticazione* - *MFA + policy least-priv.*



UC-02B – Accesso locale al PC non in dominio - Assunzioni

Nella situazione industriale attuale pannelli operatori (PO) o altri dispositivi HMI con cui gli operatori interagiscono con il sistema di automazione e controllo dell'impianto (IACS) sono normalmente "isolati", su ognuno di essi sono definiti gli utenti di accesso.

La soluzione chi vi andiamo a presentare sostituisce il dominio della soluzione precedente con una "password vault" (cassaforte delle password) sempre a disposizione del manutentore con un piccolo dispositivo che automatizza l'inserimento di user/password sui PO.

Scenario dimostrato	Tecnologie utilizzate
Accesso a PC/PO/SCADA non integrabili con IdP: credenziali sicure dal vault + inserimento automatico via USB (emulatore di tastira).	KeePass (vault locale), micro-controller USB

UC-02B - Accesso PC non in dominio - Soluzioni di Mercato

Per sistemi legacy non in dominio e SCADA isolati, le **soluzioni enterprise tradizionali non sono applicabili.** Servono password manager con capacità di automazione locale e funzionamento standalone, abbinati al nostro dispositivo USB per l'inserimento automatico delle credenziali. Queste soluzioni funzionano su PC completamente isolati, senza dominio né rete, ideali per SCADA air-gapped.

SOLUZIONE	Architettura	Integrazione Legacy	Punti di Forza	Punti di Attenzione
Bitwarden Business	Self-hosted/Cloud, REST API	CLI tools, API per automazione	Open source, self-hosting possibile, API robuste	Richiede connettività per sync
KeePass + AutoType	File locale/condiviso	AutoType nativo, plugin automazione	Zero dipendenze rete, totalmente offline	Gestione team manuale, no audit centralizzato
LastPass Enterprise	Cloud con cache offline	Browser extension, app standalone	Gestione team matura, funziona offline dopo sync	Dipendenza cloud per admin; controversie sicurezza passate
Passbolt	On-premise/Cloud, open source	API REST, scripting supportato	Progettato per team, controllo totale	Richiede infrastruttura server
RoboForm Business	Locale con sync opzionale	Form filling, automazione macro	Funziona offline, supporto legacy ottimo	Interfaccia datata, audit limitato

Al fine della DEMO, per UC-02B utilizzeremo **KeePass locale** (per semplicità offline) **+ dispositivo USB proprietario** per keystroke injection automatica, simulando poi l'evoluzione verso Passbolt per gestione team.

UC-02B - Accesso locale al PC non in dominio - Descrizione

OBIETTIVO

Consentire l'accesso a sistemi legacy privi di integrazione con Identity Provider moderni (es. Windows XP, pannelli operatore), eliminando la digitazione locale da parte dell'utente e mantenendo un livello di sicurezza superiore allo scenario attuale.

FLUSSO DEMO

- Accesso fisico tramite smartphone NFC → iLOQ genera audit log.
- Il PC legacy mostra un **QR code** statico o generato a sessione.
- L'utente inquadra il QR tramite l'app dedicata sullo smartphone.
- L'app verifica l'autorizzazione per quella specifica postazione.
- In caso positivo, l'app invia il comando a un **micro-controller USB** collegato al PC.
- Il dispositivo USB **emula una tastiera** e inserisce automaticamente le credenziali.
- L'utente accede al sistema legacy senza digitare nulla.

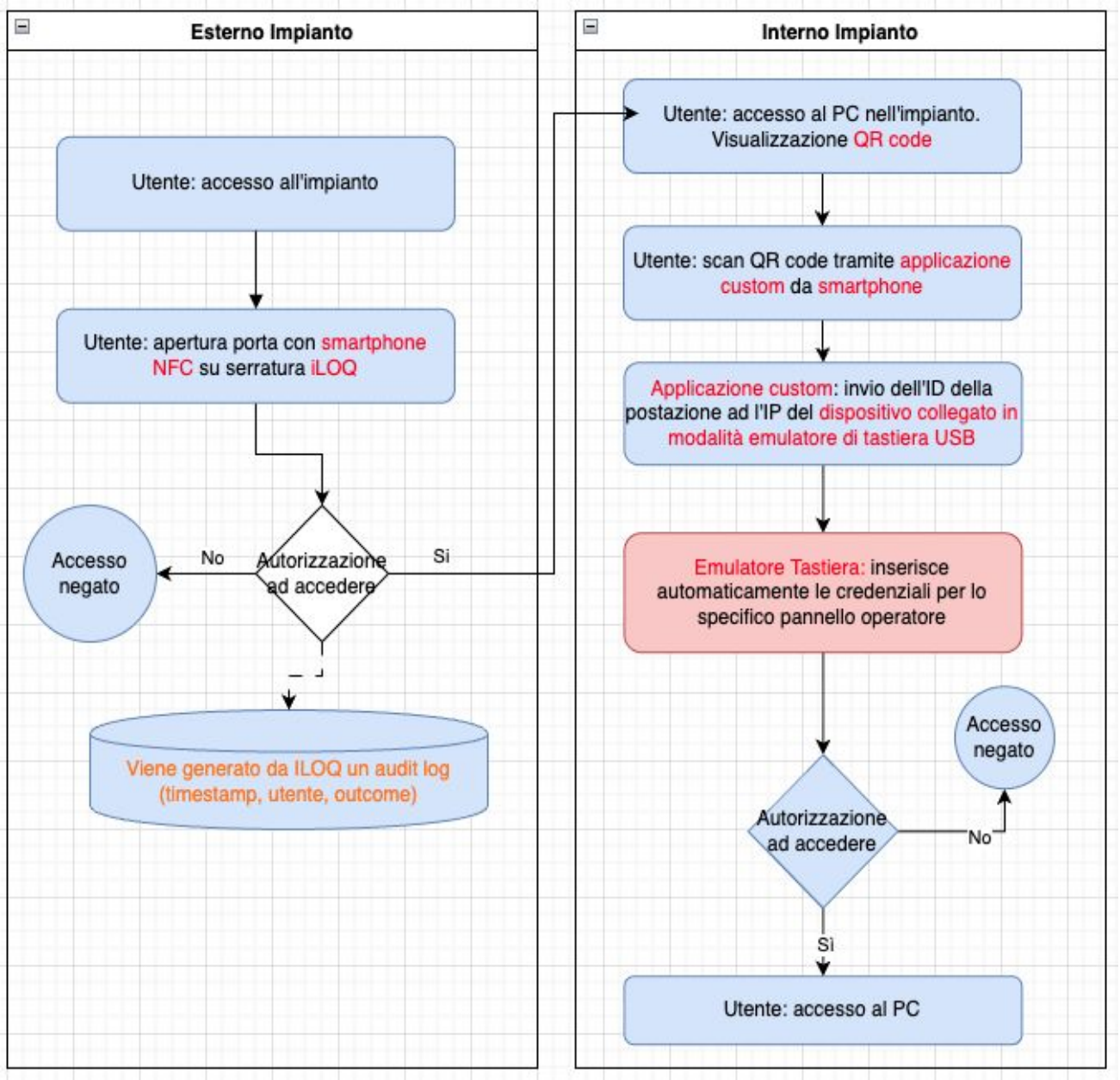
NOTE DI PERIMETRO DEMO

- Nessun supporto nativo a IdP o MFA sul PC legacy.
- Le credenziali sono custodite nel vault della piattaforma e non vengono mai esposte all'utente.
- Il PC legacy non deve essere raggiungibile in rete: la comunicazione avviene tra smartphone ↔ dispositivo USB.
- Possibili estensioni in POC: rotazione automatica delle credenziali, accesso time-bound, correlazione log fisico+logico.

UC-02B - Accesso PC legacy

Process Flow-Accesso Fisico Impianto (sistemi obsoleti)

UTENTE	- *Arriva* - *Sblocca iLOQ* - *Scansiona QR* - *Attende login*
SMARTPHONE	- *NFC → apertura iLOQ* - *Scansione QR* - *App → autorizzazione* - *Invio comando a USB*
SISTEMA LOCALE	- *Mostra QR code* - *Attesa input tastiera* - *Ricezione input USB* - *Login automatico*
BACKEND / USB DEVICE	- *iLOQ audit log* - *Verifica autorizzazione* - *Ricezione comando* - *Emulazione tastiera (credenz.)*



Valore della soluzione legacy su impianti non in dominio

1. Gestione sicura delle credenziali su PC/PO/SCADA non in dominio

- Password **complesse e uniche** gestite in un vault sicuro, non più annotate localmente
- Nessuna esposizione delle credenziali all'operatore: inserimento automatico via USB
- Riduzione drastica del rischio di compromissione e uso improprio

2. Continuità operativa per i manutentori

- Accesso rapido tramite smartphone, senza digitazioni manuali
- Flusso di lavoro uniforme per sistemi nuovi e legacy
- Nessun impatto sulle attività in campo (il tecnico mantiene il proprio modo di lavorare)

3. Tracciabilità e audit anche su sistemi isolati

- Correlazione tra accesso fisico (iLOQ) e accesso logico al PC legacy
- Registrazione automatica delle operazioni, anche senza rete o dominio
- Supporto alla compliance NIS2 / IEC 62443 anche su impianti non modernizzabili

4. Base solida per una futura integrazione IAM

- Possibilità di centralizzare il vault e gestire rotazioni programmate delle password
- Evoluzione naturale verso IdP moderni (es.: Okta, Entra ID, …) quando i sistemi verranno aggiornati
- Riuso della stessa UX e degli stessi processi introdotti oggi, senza re-training

SESSIONE Q&A

MINSAIT

Tech for impact