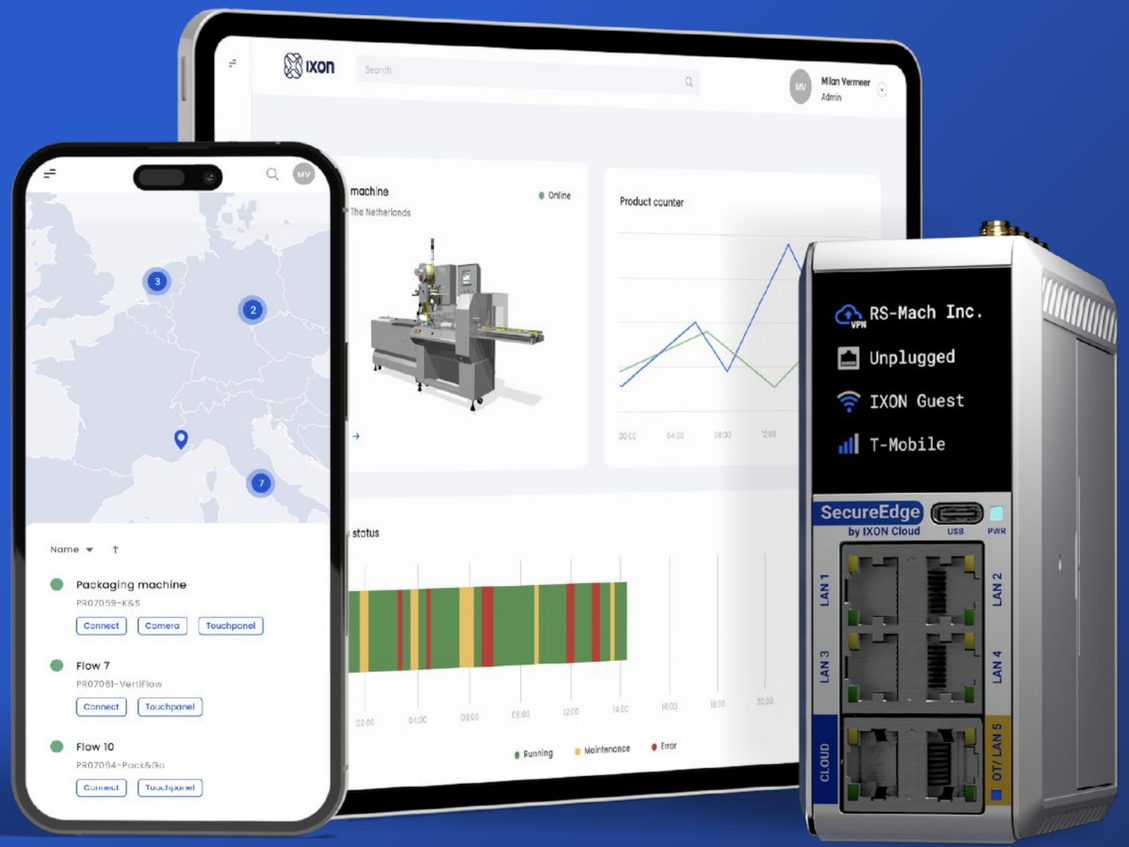
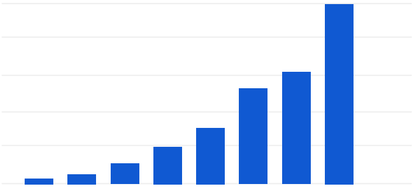
Cybersecurity: sfida o opportunità per l'OEM? Analisi di 5 casi d'uso



Cosa fa IXON

50 Paesi

30% Crescita annua



130+

collaboratori

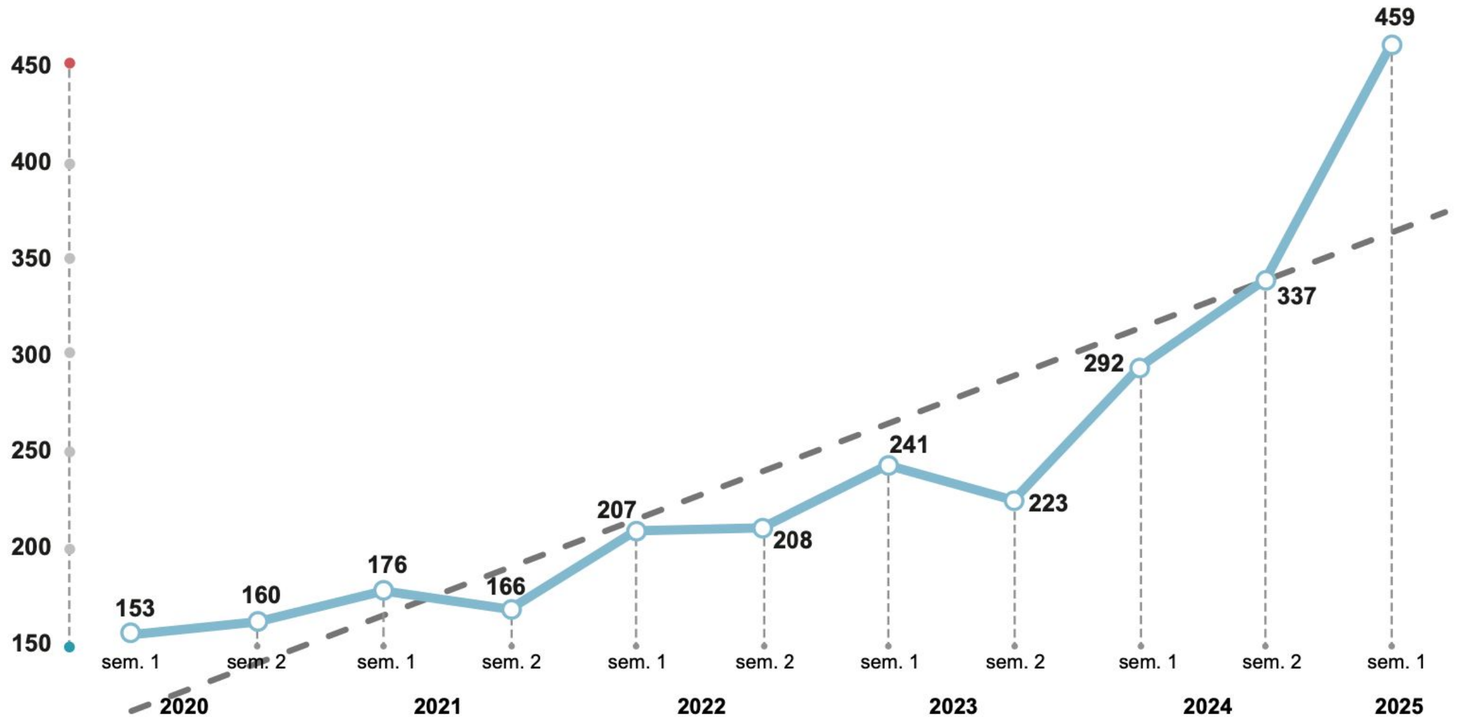
10 Uffici commerciali

Argomenti

- Scenario e contesto normativo
- Impatto operativo: la sfida della manutenzione sicura
- Analisi di 5 casi d’uso: sicurezza, conformità normativa ed efficienza operativa
- Conclusioni

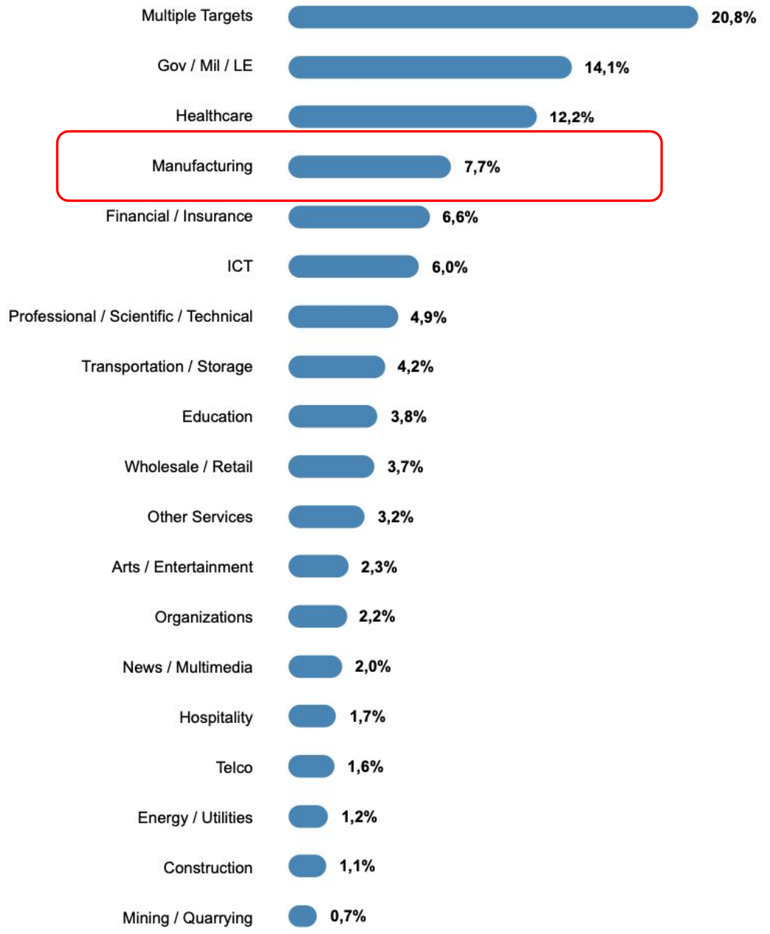
Scenario: l'aumento degli attacchi

Medie mensili/mondo



Periodo 2020 - I sem. 2025

Distribuzione delle vittime/mondo



NIS2 e Regolamento Macchine 2023/1230: impatto per i costruttori

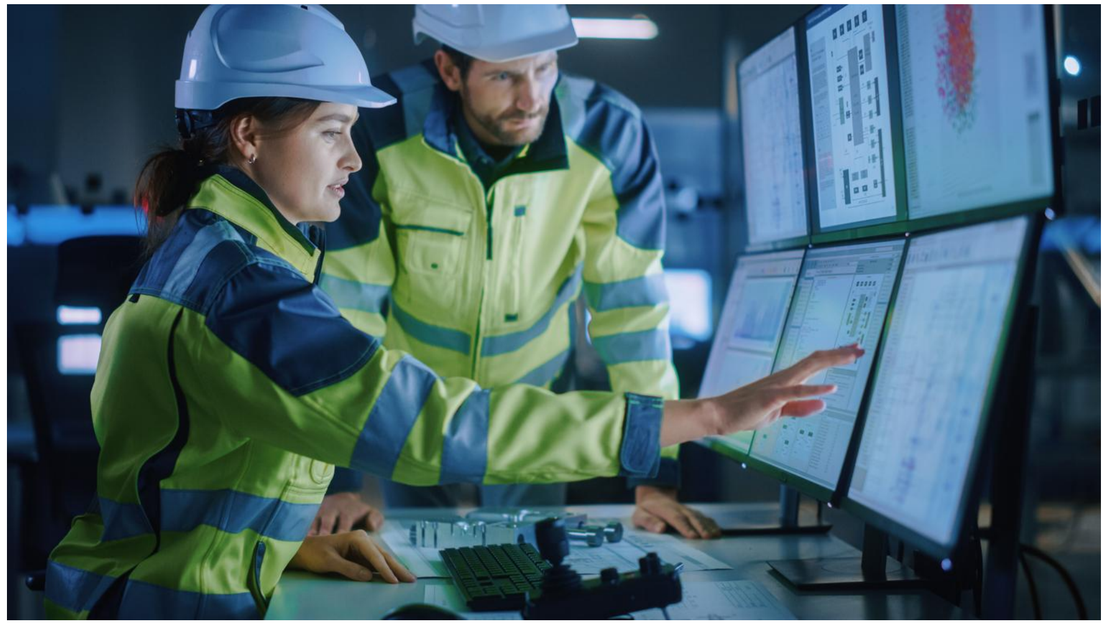
- Garantire l’integrità del software di controllo durante il ciclo di vita
- Valutazione supply chain
- Accesso remoto sotto controllo

→ Nuove responsabilità per i costruttori di macchine

Impatto operativo: la sfida della manutenzione sicura

- Costi e risorse
- Complessità tecnica
- Safety e Security

→ Vantaggi competitivi



Analisi di 5 casi d’uso: sicurezza, conformità normativa ed efficienza operativa

1. Gestione sicura degli utenti e dei ruoli

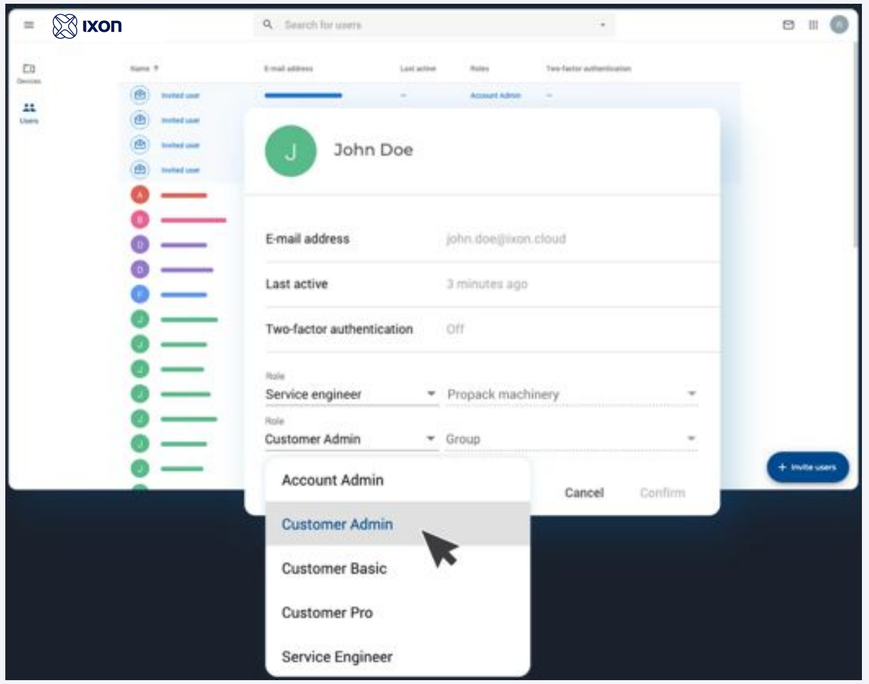
La base della cybersecurity industriale: definire chi può accedere a cosa.

Implementare una gestione centralizzata di utenti e permessi consente di limitare l’accesso solo al personale autorizzato, ridurre il rischio di errori e soddisfare i requisiti di tracciabilità richiesti dalle normative.

- **Normative di riferimento:**
  - IEC 62443-3-3, SR 1.1 / SR 1.2 / SR 1.3: gestione delle identità e controllo degli accessi.
  - NIS2, Art. 21(2)(i): obbligo di implementare controlli di accesso.
  - Reg. Macchine 2023/1230, Allegato III, punto 1.1.9: prevenzione dell’alterazione non autorizzata del software.

1. Gestione sicura degli utenti e dei ruoli

- **Rischio mitigato:** accessi non autorizzati, errori umani.
- **Beneficio operativo:** accesso controllato e tracciabile, conformità garantita.



Esempio

Assistenza remota con credenziali condivise.
Mancanza gestione versioning e collaborazione sul software.
***Soluzione:** gestione multiutente con audit e log degli accessi.*
Divisione ruoli tra utenti e amministratori.

2. Automazione dei flussi di accesso e approvazione

Velocità e sicurezza possono coesistere.

Automatizzare la gestione delle richieste di accesso (notifiche, approvazioni, scadenze) consente di rispettare i protocolli di sicurezza senza rallentare gli interventi urgenti, riducendo la dipendenza da processi manuali.

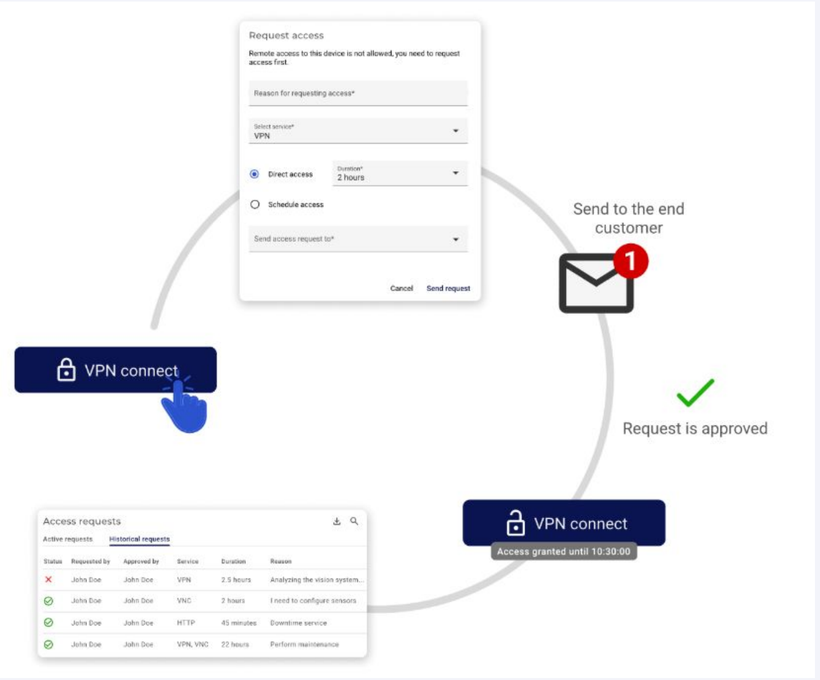
- **Normative di riferimento**
  - IEC 62443-3-3 SR 1.13: accesso tramite reti non attendibili.
  - NIS2, Art. 21(2)(i): obbligo di implementare controlli di accesso.
  - Reg. Macchine 2023/1230, Allegato III, punto 1.1.9: prevenzione dell’alterazione non autorizzata del software.

2. Automazione dei flussi di accesso e approvazione

- **Rischio mitigato:** errori nei processi manuali di accesso.
- **Beneficio operativo:** accessi rapidi, sicuri e documentati.

Esempio

VPN gestita da IT cliente finale.
Soluzioni rapide ma pericolose.
***Soluzione:** gestione strutturata delle autorizzazioni agli interventi remoti.*



3. Aggiornamenti software e firmware sicuri da remoto

Un punto critico spesso trascurato.

Distribuire aggiornamenti e patch in modo sicuro è essenziale per mantenere le macchine protette da vulnerabilità note, evitando procedure manuali o non verificate che possono introdurre nuovi rischi.

- **Normative di riferimento**
  - IEC 62443-4-2, CR 3.4: integrità del software e delle informazioni.
  - NIS2, Art. 21(2)(e): gestione delle vulnerabilità e aggiornamenti di sicurezza.
  - Reg. Macchine 2023/1230, Allegato III, punto 1.1.9: prevenzione dell’alterazione non autorizzata del software.

3. Aggiornamenti software e firmware sicuri da remoto

- **Rischio mitigato:** installazione di versioni compromesse.
- **Beneficio operativo:** patch e update gestiti in modo affidabile.

Esempi

- *Soluzione connettività e accesso remoto integrate nel sistema di automazione.*
- *Macchina esposta sulla rete OT.*

Soluzione: *hardware dedicato alla connessione OT-macchina e accesso remoto.*

4. Monitoraggio continuo delle connessioni

Osservare per prevenire.

Un sistema che registra e analizza in tempo reale le connessioni e i comportamenti anomali permette di individuare tentativi di accesso sospetti e reagire tempestivamente prima che si trasformino in incidenti.

- **Normative di riferimento**
  - IEC 62443-3-3, SR 6.1 / SR 6.2 / SR 6.3: rilevamento di intrusioni e monitoraggio continuo.
  - NIS2, Art. 21(2)(b): capacità di rilevamento e gestione degli incidenti.
  - Reg. Macchine 2023/1230, Allegato III, punto 1.7.4.2: raccolta e analisi dei dati per la sicurezza della macchina.

4. Monitoraggio continuo delle connessioni

- **Rischio mitigato:** attacchi non rilevati in tempo.
- **Beneficio operativo:** individuazione tempestiva di anomalie.

Esempio

Intercettare traffico di rete anomalo.

Soluzione: *utilizzo sistemi SIEM (da parte del cliente finale). Fornire soluzioni compatibili Syslog (da parte del costruttore).*

5. Integrazione della cybersecurity nei contratti di service

La sicurezza come parte dell’offerta di manutenzione.

Includere requisiti e procedure di sicurezza nei contratti di assistenza (SLA, policy di accesso, gestione dati) aiuta a garantire che la conformità normativa sia condivisa tra costruttore e cliente, riducendo i rischi legali e operativi.

- **Normative di riferimento:**
  - IEC 62443-2-4: requisiti di cybersecurity per i fornitori di servizi industriali.
  - NIS2, Art. 21(d): responsabilità condivisa e gestione della supply chain.
  - Reg. Macchine 2023/1230, Art. 10 e Allegato III: responsabilità del fabbricante e documentazione tecnica sulla sicurezza.

5. Integrazione della cybersecurity nei contratti di service

- **Rischio mitigato:** ambiguità su ruoli e responsabilità.
- **Beneficio operativo:** responsabilità chiare e riduzione del rischio legale.

Esempio

Assenza di accordi su chi garantisce la sicurezza del sistema.

Soluzione: *contratti di servizio che includano i doveri per ciascuna parte. Riferimento alle rispettive normative.*

Tabella riassuntiva

Casi trattati

Caso d’uso	Rischio mitigato	Normativa	Beneficio operativo
Gestione sicura degli utenti e dei ruoli	Accessi non autorizzati, errori umani	IEC 62443-3-3 - SR 1.1/1.2 /1.3 NIS2, Art. 21(2)(i) Reg. 2023/1230, All. III, 1.1.9	Accesso controllato e tracciabile, conformità garantita
Automazione dei flussi di accesso e approvazione	Errori nei processi manuali di accesso	IEC 62443-3-3 SR 1.13 NIS2, Art. 21(2)(i) Reg. 2023/1230, All. III, 1.1.9	Accessi rapidi, sicuri e documentati
Aggiornamenti software e firmware sicuri da remoto	Installazione di versioni compromesse	IEC 62443-4-2, CR 3.4 NIS2, Art. 21(2)(e) Reg. 2023/1230, All. III, 1.1.9	Patch e update gestiti in modo affidabile
Monitoraggio continuo delle connessioni	Attacchi non rilevati in tempo	IEC 62443-3-3, SR 6.1/6.2 /6.3 NIS2, Art. 21(2)(b) Reg. 2023/1230, All. III, 1.7.4.2	Individuazione tempestiva di anomalie
Integrazione della cybersecurity nei contratti di service	Ambiguità su ruoli e responsabilità	IEC 62443-2-4 NIS2, Art. 21 (d) Reg. 2023/1230, Art. 10 e All. III	Responsabilità chiare e riduzione del rischio legale

Conclusione: verso la manutenzione “secure by design”

- La sicurezza integrata può semplificare, non complicare.
- Strumenti e soluzioni per rendere la cybersecurity parte naturale del processo.
- La sicurezza non è solo un requisito: è un acceleratore di efficienza e fiducia tra costruttori, integratori ed end user.

Security & Legal desk

Stan van Duijnhoven **Bauke Spoor**

Restiamo in contatto

Paolo Quaglino Solution Engineer
E-mail: paolo.quaglino@ixon.cloud

IXON

Grazie per l'attenzione