Perché la sicurezza è così importante per noi?

myplant

Perché è importante per voi

Soluzioni digitali di INNIO Group: Il ruolo della cybersecurity in myplant per la sicurezza delle vostre attività

INNIO fornisce una vita digitale ai vostri asset industriali con myplant. Con myplant potete portare con voi i dati dei vostri motori ovunque andiate, sapendo che le nostre efficaci politiche di cybersecurity tutelano la sicurezza delle vostre operazioni durante l'intero ciclo di vita dei motori.

Quali dati vengono inviati alla piattaforma myplant?
Vengono inviati solo i dati essenziali.

- Per fornirvi informazioni chiave necessarie all'operazione dei vostri asset industriali, trasferiamo dati operativi (come voltaggi e stato operativo del motore) e notifiche (come messaggi, avvertenze e allarmi) dai sistemi di controllo.
- Non vengono trasferiti dati personali; tuttavia per creare l'account utente myplant che vi permette di accedere ai vostri dati motore sono necessari nome ed e-mail dell'utente.

I miei dati sono protetti?
Sì, i vostri dati sono protetti.

- Tutti i dati trasferiti sono completamente criptati e protetti. Vengono trasmessi end-to-end attraverso il protocollo internet-standard HTTPS che fornisce la cifratura attraverso Transport Layer Security[1] (TLS).
- Gli esperti di sicurezza INNIO mantengono ed operano l'infrastruttura di sicurezza con rigidi standard nel software e nelle tecnologie implementate ed applicate in tutto il sistema.
- Un Web Application Firewall (WAF) cloud-based protegge costantemente i vostri dati contro i comuni attacchi web-based.
- L'accesso al sistema myplant è rigidamente controllato e gestito da un team selezionato di support tecnico ed amministrazione.

L'accesso al sistema di controllo del mio motore Jenbacher o alla mia myplant Connectivity Box (myCoBo) è protetto?
Proteggiamo l'accesso con molteplici misure di sicurezza.

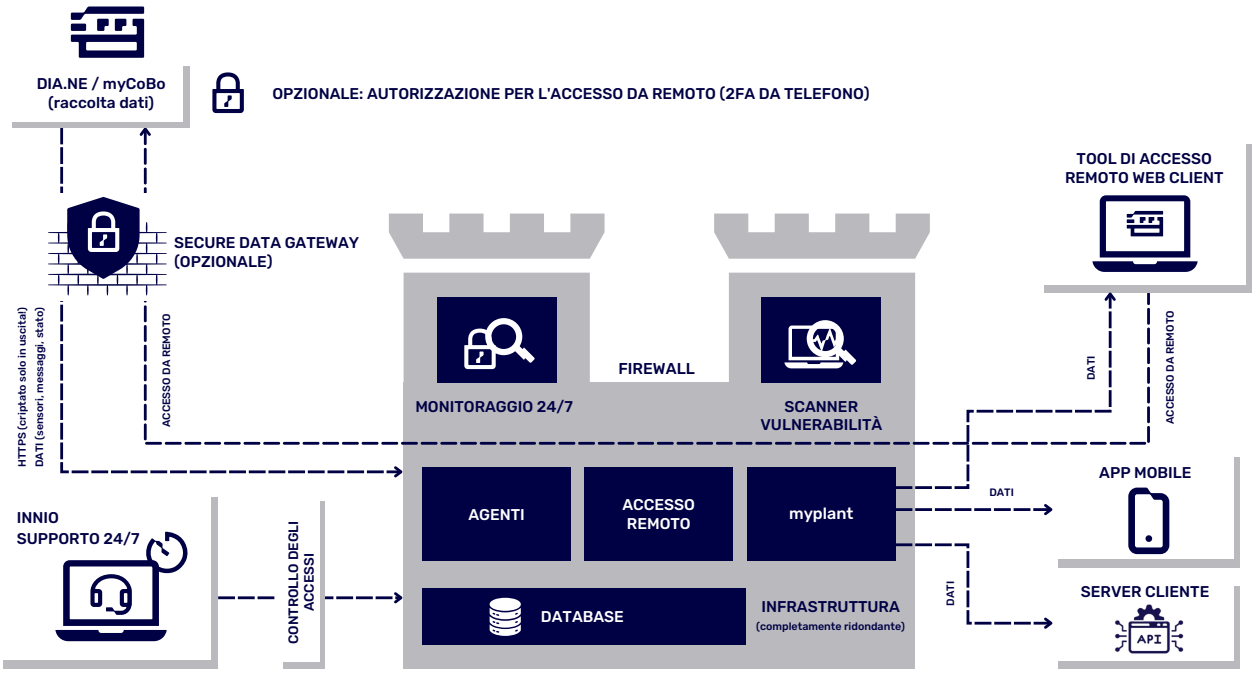
- Per fornire l'accesso da remoto al sistema di controllo DIA.NE o alla myCoBo, richiediamo credenziali aggiuntive con restrizioni specifiche ed indipendenti.
- Tracciamo tutte le attività in accesso remoto per proteggere il vostro sistema di controllo da accessi non autorizzati.
- La nostra infrastruttura permette ai clienti di limitare le connessioni al minimo necessario, e di implementare controlli del traffico d'avanguardia.
- Per un'ancora maggiore protezione contro gli accessi non autorizzati, offriamo opzionalmente un processo di autorizzazione a due fattori. Questo significa che ogni accesso da remoto dev'essere approvato da personale sul sito prima che possa essere stabilita una connessione.

La vostra energia. I vostri dati.
Nelle vostre mani.

Il nostro completo modello di sicurezza

myplant

Come abbiamo costruito l'architettura di sicurezza per proteggere i vostri dati



Scansionate il codice QR e scoprite da Nikolaus Brunner, il nostro Product Cybersecurity Leader, come in INNIO ci impegniamo per la cybersecurity – così potrete concentrare la vostra attenzione sul vostro core business.

[1] TLS versione 1.0 / 1.1 / 1.2 con AES 128 / 256 bit

Ulteriori informazioni sono disponibili sui siti di INNIO Group all'indirizzo **innio.com** e **myplant.io/it**

Seguite INNIO Group e i suoi marchi su 𝕏 e in

© Copyright 2026 INNIO. Con riserva di modifica delle informazioni.

INNIO, Jenbacher, Waukesha e myplant sono marchi o marchi registrati dell'INNIO Group, o di una delle sue controllate, nell'UE, negli USA e in altri Paesi. Per un elenco dei marchi commerciali dell'INNIO Group, visitare **innio.com/trademarks.** Tutti gli altri marchi e nomi di società appartengono ai rispettivi proprietari.

myplant is part of the INNIO Group

I MP-1 26 0005-IT