



Why is security so important to us? Because it's important to you.

INNIO's Digital Solutions: myPlant cybersecurity policies to keep your operations secure

INNIO* Jenbacher* gives your industrial assets a digital life with myPlant* Performance - our Asset Performance Management (APM) solution. Now you can take your engine data with you wherever you go, knowing that our strong protective cybersecurity policies will help keep your operations secure throughout your Jenbacher engines' lifetime.

What is transferred to INNIO's myPlant APM solution?

Only the essential data is transferred.



- ✓ To give you the insights you need on your industrial assets' operation, we transfer operational data from control systems (such as voltages and engine state) and notification data (such as messages, warnings and alarms).
- ✓ Personal data is not transferred; however, your name and email are required to create the myPlant user account that allows access to your engine data.

Is my data protected?

Yes, your data is protected.



- ✓ All transferred data is fully encrypted and protected. It is transmitted end-to-end through the Internet-standard HTTPS protocol, which provides encryption via Transport Layer Security** (TLS).
- ✓ INNIO security experts maintain and operate the security infrastructure with strict software standards and technologies that are implemented and enforced across the entire system.
- ✓ A cloud-based Web Application Firewall (WAF) continuously protects your data against common web-based attacks.
- ✓ Access to the myPlant system is strictly controlled and managed by selected technical support personnel or administrators.

Is access to my Jenbacher engine control system protected?

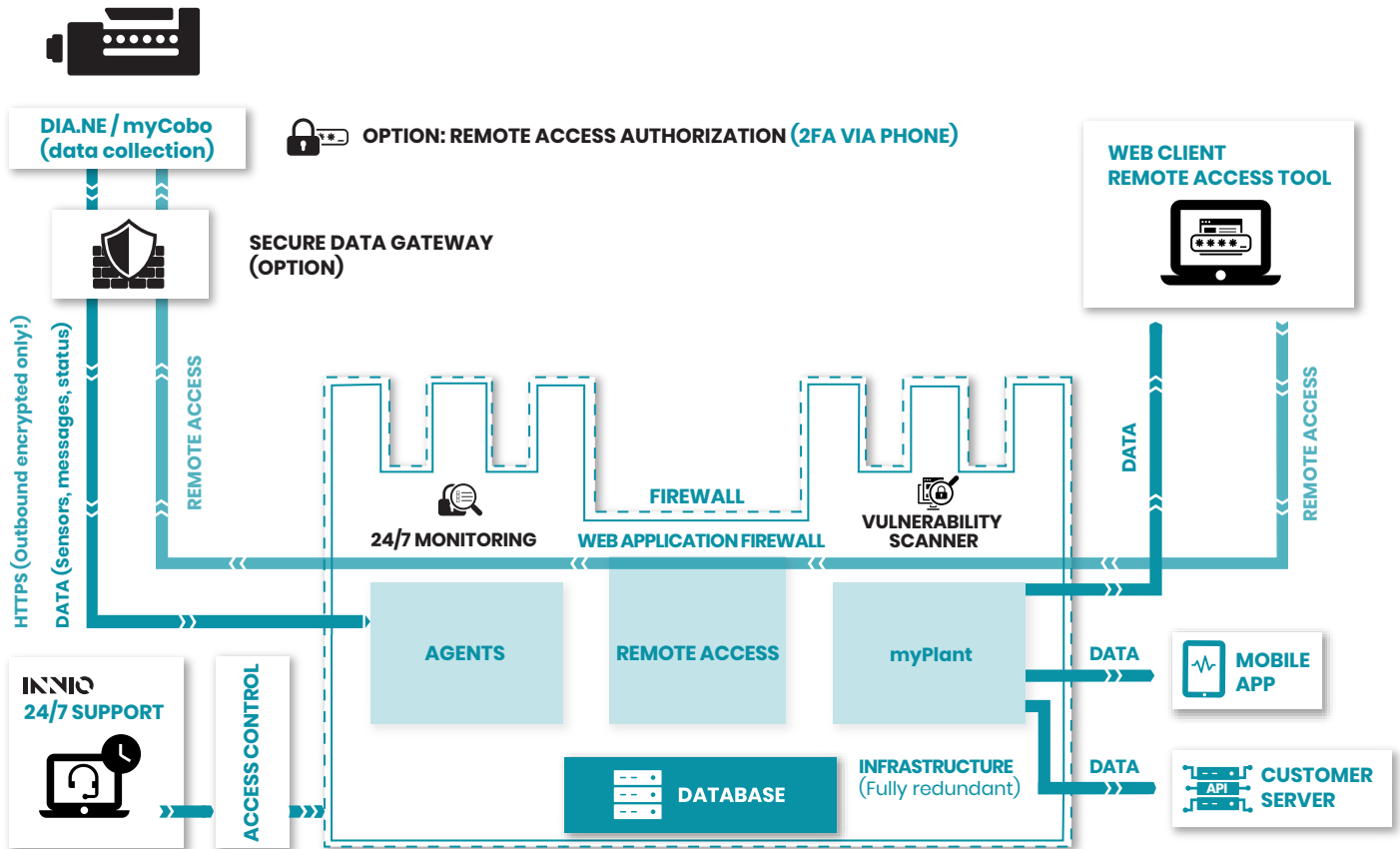
We protect access with multiple security measures.



- ✓ Additional credentials with independent restrictions are required when the DIANE* control system is accessed remotely.
- ✓ We track any remote access activity to protect your control system from unauthorized access.
- ✓ Our hosting infrastructure setup allows customers to restrict connections to a minimum and implement state-of-the-art traffic controls.
- ✓ For even more protection against unauthorized access, we offer an optional two-factor authorization process. This means that any remote access attempt must be approved by onsite personnel before a connection can be established.

Our comprehensive security model

HOW WE HAVE BUILT THE SECURITY ARCHITECTURE TO PROTECT YOUR DATA



INNIO* is a leading provider of renewable gas, natural gas, and hydrogen-based solutions and services for power generation and gas compression at or near the point of use. With our Jenbacher* and Waukesha* gas engines, INNIO helps to provide communities, industry and the public access to sustainable, reliable and economical power ranging from 200 kW to 10 MW. We also provide life-cycle support and digital solutions to the more than 53,000 delivered gas engines globally, through our service network in more than 100 countries. We deliver innovative technology driven by decarbonization, decentralization, and digitalization to help lead the way to a greener future. Headquartered in Jenbach, Austria, the business also has primary operations in Welland, Ontario, Canada, and Waukesha, Wisconsin, U.S.

Follow INNIO on Twitter and LinkedIn.

For more information, visit the myPlant website at www.myplant.io or the INNIO website at www.innio.com/en/jenbacher/myplant-performance



I JB-2 21 030-EN

*Indicates a trademark
**TLS version 1.0 / 1.1 / 1.2 with AES 128 / 256 bit
© Copyright 2021 INNIO. Information provided is subject to change without notice.