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* Waukesha* gives your industrial assets a digital life with the myPlant* 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 Waukesha engines' lifetime

What is transferred to INNIO's myPlant APM?
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 (e.g. temperature, pressure and engine state) and notification data (e.g. alarm and shutdown).
- ✓ 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 Waukesha engine control system protected?
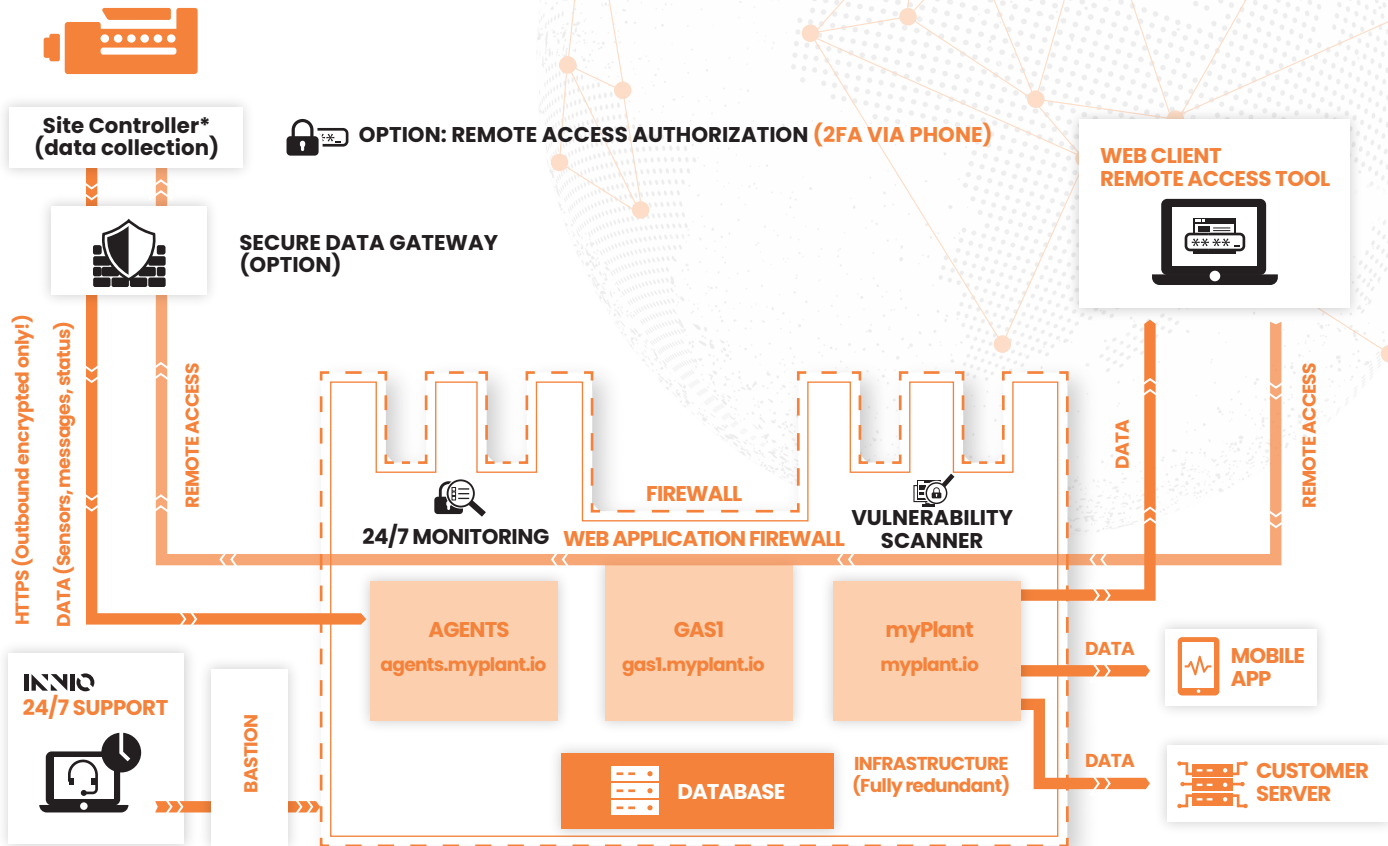We protect access with multiple security measures.

- ✓ Additional credentials with independent restrictions are required when the ESM2 control system is accessed remotely.
- ✓ We track any remote access activity to protect your control system from unauthorized access.
- ✓ We use a staic IP address and pre-configured ports, which allow you to easily white-list myPlant within your site's firewall configuration.
- ✓ 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 BUILD THE SECURITY ARCHITECTURE TO PROTECT YOUR DATA

Site Controller* (data collection)

OPTION: REMOTE ACCESS AUTHORIZATION (2FA VIA PHONE)

WEB CLIENT REMOTE ACCESS TOOL

SECURE DATA GATEWAY (OPTION)

HTTPS (Outbound encrypted only!)

DATA (Sensors, messages, status)

REMOTE ACCESS

24/7 MONITORING

FIREWALL

WEB APPLICATION FIREWALL

VULNERABILITY SCANNER

DATA

REMOTE ACCESS

INNIO 24/7 SUPPORT

BASTION

AGENTS agents.myplant.io

GAS1 gas1.myplant.io

myPlant myplant.io

DATA

MOBILE APP

DATABASE

INFRASTRUCTURE (Fully redundant)

DATA

CUSTOMER SERVER

*ESM, ESM2, CEC, Murphy, Altronic, Allen Bradley, ADEM (CAT), PLC, or SCADA system/controller

At Waukesha, we're working every day to design and build engines and programs that help power your tomorrow. INNIO is a leading solutions provider of gas engines, power equipment, a digital platform and related service for power generation and gas compression at or near the point of use. With our Jenbacher and Waukesha product brands, INNIO pushes beyond the possible and looks bodly toward tomorrow. Our diverse portfolio of reliable, economical and sustainable industrial gas engines generates 200 kW to 10 MW of power for numerous industries globally. We can provide lifecycle support to more than 52,000 delivered gas engines worlwide. And backed by our service network in more than 100 countries, INNIO connects with you locally for rapid responses to your service needs. Headquartered in Jenbach, Austria, the business also has primary operations in Welland, Ontario, Canada, and Waukesha, WIsconsin, US.

For more information visit the myPlant website at www.myplant.io; **or** www.innio.com/en/p/waukesha-myplant.