SupplyCare Hosting – cyber protection overview

Security measures that secure your data

Facilitate your cybersecurity compliance with a trusted partner:

Endress+Hauser ensures reliable operation of process plants in facilities worldwide.

Cyber security in industrial plants and the Industrial Internet of Things is becoming increasingly important.

To verify the protection measures of our products, we have tested our systems against some of the most well-known security standards in the IT and OT fields and obtained the corresponding certification.

Security starts in product development

To best protect our customers' production facilities, Endress+Hauser considers security from the very beginning. We establish a foundation for secure operation in our offerings during the product design phase. Security is also an important consideration during development and testing.

To ensure consistently high quality and secure products, we at Endress+Hauser Group are proud that our Secure Development Lifecycle Processes are tested and certified according to IEC 62443-4-1 by TÜV Rheinland.

More details on SupplyCare

Contact
Please contact your local Endress+Hauser location
www.addresses.endress.com

Endress+Hauser
People for Process Automation

Functions and features

We incorporated various security related measures and key functions/features in our software to maintain highly secure products and solutions:

Secure Implementation Our developers continually enhance their secure coding skills through regular training, guidance from security coaches and use of a secure coding platform. We adhere to the latest security advisories during development, including but not limited to file upload/ download functionalities and password rules. Additionally, we implement meticulous error handling and logging to prevent exposure of sensitive data. We use widely accepted and rigorously tested libraries for cryptography in our implementation to minimize errors and vulnerabilities.

Security Testing Our software, developed in line with the latest secure coding standards, undergoes daily automated scans using cutting-edge security scanners that adhere to OWASP and SEI Cert standards. Our process includes dedicated tests for security requirements identified by common practices and threat modeling, ensuring the utmost quality and security of our products.

Customer data Our customers are the sole owners of their data and can export it for re-use in other systems. Your data is continuously backed up to support quick recovery in case of problems. Endress+Hauser has a comprehensive disaster recovery plan in place to avoid loss of data. After termination of the customer relationship, Endress+Hauser deletes all customer data. This applies to both Endress+Hauser and our sub-suppliers including our cloud hosting partners which do not have access to customer data.

User information All customer data including user-related data is treated with care in accordance with latest GDPR guidelines. We only utilize user data, which is absolutely necessary to fulfill the provided services and adhere to the principle of data economy.

Passwords and Authentication - OAuth To ensure personal information stays confidential, all applications follow strict password policies. To facilitate secure logins, we use state of the art cloud-based authentication service to securely store passwords. In our Endress+Hauser user management system we use a tokenized process to identify users safely and reliably prior to software usage. User passwords are transmitted only for token generation. This prevents scamming attempts and guarantees a safe authorization.

Server location All data is stored in redundant secure servers in different locations in Europe to ensure continuity of customer business. These servers are operated under the protection of European law and jurisdiction, so our customers can be sure that their data is subject to one of the highest data security standards worldwide.

Data interfaces State-of-the-art security mechanisms protect the integrity of data communicated between SupplyCare Hosting, the interfaces and data sources. On the Endress+Hauser webserver and Hosting API interfaces, communication is done via HTTPS. All access to data inside SupplyCare Hosting, as well as the execution of actions, requires authorization.

Processes The possibility of a security breach exists, even in the most secure environment. We have accordingly established internal processes to enable us to react as quickly as possible should such a breach occur. This includes informing all affected parties so they can react to and minimize their risk as soon as possible. Therefore Endress+Hauser established an entity wide specialized Product Security Incident Response Team.

Governance All activities and measures are taken to protect SupplyCare and the data within SupplyCare as part of a bigger system, where all processes are governed by detailed policies, standards, processes and instructions. This holistic approach ensures that all parts of the information value chain are clearly identified and protected.

www.addresses.endress.com

PU01587S/00/EN/01.24

Endress+Hauser

People for Process Automation