Netilion Network Insights security feature overview

End to end, from the field to the cloud

Facilitate your cybersecurity compliance with a trusted partner:
Endress+Hauser measuring instruments and components ensure the reliable operation of process plants in countless facilities worldwide.

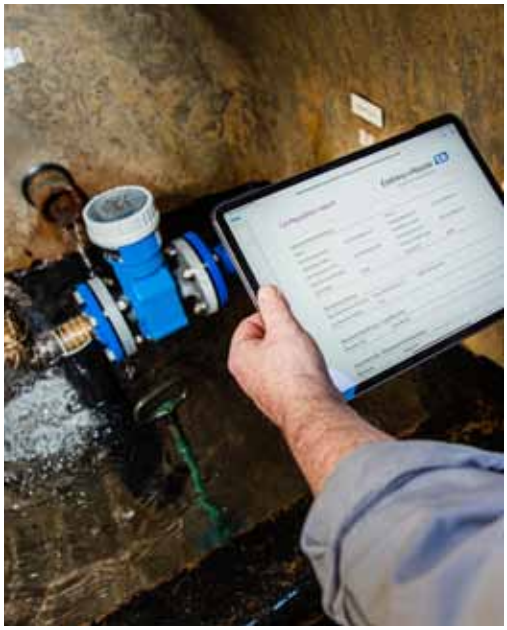
Cybersecurity in industrial plants and the Industrial Internet of Things is becoming increasingly important.

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

Security starts in product development

To best protect our customers production facilities, Endress+Hauser considers security from the start. For our offerings we establish a foundation for secure operation already during product design. Security is also a key consideration during development and testing.

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



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

More details on Netilion?

netilion.endress.com

Endress+Hauser
People for Process Automation

Functions and features

To maintain highly secure products and solutions we incorporated various security related measures and key functions/ features in our software. The following outlines a selection of these:

Password Encryption To ensure personal information stays confidential we do not store passwords. To facilitate secure logins, we rather store hashes of passwords to determine the validity of a password. Such password hashes cannot be reverse engineered to determine the original passwords.

OAuth To identify users safely and reliably prior to software usage, we use a tokenized process to identify users in our Endress+Hauser user management system. User passwords are transmitted only for token generation. This complicates scamming attempts and guarantees a safe authorization.

Encrypted communication channels only We always establish end-to-end communication to and from the cloud over a secure and encrypted https connection. We also use certificate-based authentication which relies on certificates issued by a worldwide renowned and trusted certification authority. This is how we ensure that all payload data is protected and instruments and servers are authenticated.

User information Our customers have the possibility to track all login activities in their account(s). User-related data is treated with care in accordance with GDPR guidelines. We also apply the same mechanisms used for online banking to detect possible fraud usage or failed login attempts.

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 ss possible.

Server location We use proven and reputable global cloud hosting partners and insist on server locations in Europe. These servers operated under the protection of European law and jurisdiction, one of the most stringent in the world. Our customers can be sure that their data is subject to one of the highest data security standards worldwide.

Edge device data security An edge device is a critical point in the architecture because it represents the access point from and to the user's data. By default, we only transfer data from the edge to the cloud and incoming ports are blocked on the edge device. If customers require a function that requires data transfer from the cloud to the edge device, it must be explicitly configured and enabled before deployment. The data variables used must be explicitly named and enabled. Our architecture is designed in such a way that this is only possible locally on the edge device.

Customer may allow edge device to download application updates from the cloud. To guarantee security all updates are signed and before updates are applied, they are checked against the original file to prevent manipulation.

Customer data Our customers are the sole owners of their data and can export it for re-use in another system. This applies to both Endress+Hauser and our sub-suppliers including our cloud hosting partners which do not have access to customer data. We reserve the right to use this data for the operation, maintenance, analysis and improvement of our services. For this purpose, Endress+Hauser anonymizes the data so that neither the customer nor any user can be identified. After termination of the customer relationship, Endress+Hauser deletes all customer data within 30 days.

Governance All activities and measures are taken to protect Netilion and the data within Netilion 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

Eco-friendly produced and printed on paper from sustainable forestry.

PU01475D/06/EN/01.22

Endress+Hauser

People for Process Automation