xylem
Let's Solve Water

HydroSphere

HydroSphere™ Cloud Platform Cybersecurity

Why is cybersecurity important to Xylem?

Product cybersecurity has become a market imperative to gain the trust of our customers. Xylem recognizes this imperative and seeks to grow the faith and trust our customers have in our products and services. Our customers are clearly expressing their concerns regarding the safety of an ever increasingly cross-connected and cloud-based solution set. In partnership with client IT departments, the Xylem cybersecurity team can help to push the boundaries of analytical and performance management capability while adhering to the most rigorous safety standards.

What is Xylem doing to protect my privacy?

Xylem follows an internal Privacy Policy that is built around the elements of the European Union ("EU") General Data Privacy Regulation ("GDPR") among others. Similar to GDPR, Xylem's Privacy Policy is intended to help our customers understand what data we collect, how we use it, what safeguards are in place to protect their data, and rights as permitted by applicable law (for details see "Where can I go for more information?").

What is Xylem doing to secure my data?

Xylem prioritizes the availability, integrity, and confidentiality of all of the capabilities we provide to our customers. Securing these products and services is governed by the Xylem Product Cybersecurity Program.

What is the Xylem Product Cybersecurity Program?

As part of our mission to bring innovation and industry best services to the global water industry, Xylem has developed an industry-aligned product security program anchored in a "3 Lines of Defense" model.

YSI, a Xylem brand
7100 Business Park Drive, Suite B
Houston, TX 77041

+1.727.565.2201
info@ysi.com
YSI.com

YSI.com/HydroSphere

First Line of Defense

Each business unit within Xylem has a Product Security Team dedicated to supporting the associated product lines. The core mission of these teams is to build security into the products, respond to vulnerabilities and incidents, and partner with clients to provide high levels of assurance. These teams are scaled to reflect the size of each individual product portfolio.

Second Line of Defense

The Global Product Security Team monitors the risk across the Xylem product portfolio, serves as an escalation point for issues, and represents the unified voice of Xylem on the subject of product security. The Global team provides several services, led by experts within the corporate team and largely fulfilled by commercial security partners which create scale for the individual business units.

Key among these services is the protection provided by our Product Security Incident Response Team (PSIRT), which keep a constant eye on vulnerabilities in the industrial space and our supply chain, and stand ready to support customers with any cybersecurity incident involving our products. Other key shared service capabilities are built around security testing and regulatory tracking, ensuring that technology platforms are developed with software security included and awareness of new regulations to ensure alignment with industry expectations. Providing these services allows the Product Security Teams to focus on what they do best – being product experts and consultative partners with engineering.

Third Line of Defense

Finally, Xylem's Internal Audit Staff regularly audits the business units to ensure the effectiveness of the program overall. The quality and effectiveness of the program is of key importance to both Xylem's Board of Directors and the internal Cyber Risk Committee which receives monthly metrics highlighting the company's ongoing efforts to improve security for all products (whether currently under development or deployed in the field).

HydroSphere™ Cloud Platform

The HydroSphere™ Cloud Platform leverages the Xylem Cloud Platform, which is Xylem's "smart infrastructure" that enables processing, transformation, and analytics of sensor data. Combined with the Xylem Cloud Platform, the HydroSphere™ Cloud Platform aligns to Xylem's Product Security Program as outlined earlier. Altogether, the program helps to enable each platform so our customers are able to glean valuable insights and quickly make data-driven decisions in a secure way.

Where is the HydroSphere™ Cloud Platform deployed?

The HydroSphere™ Cloud Platform and the Xylem Cloud Platform are deployed on Amazon Web Services (AWS) running in highly available data centers in North America. This includes all data such as backups. Locations are continuously evaluated and aligned to the needs of our customers along with applicable compliance requirements.

Is AWS a public / private / hybrid cloud?

AWS is a public cloud.

Do you have access to the datacentres? If so what physical controls are in place?

Cloud Security (environment)

Xylem believes in using world-class cloud computing partners to drive scale and increase security protections. Together with our partner Amazon Web Services (AWS), we operate in a shared accountability model that enables all participants to focus on their strengths.

As part of the shared responsibility, AWS handles security "of" the cloud, which includes the physical security of their data centers (for details see "Where can I go for more information?"). Xylem handles security "in" the cloud. Specifically, Xylem leverages the supported methods and resources provided by AWS to ensure secure setup of our applications and define appropriate access to data.

Related aspects include:

- Protection against network-layer Distributed Denial of Service (DDoS) attacks.
- Web Application Firewall (WAF) to safeguard against application-layer threats.
- Private networks that keep select data flows isolated from the public internet.
- Remote management of services via Virtual Private Network (VPN).
- Multi-factor authentication for cloud administration and role-based access.
- Industry-standard encryption of data in transit and at rest (e.g. TLS, VPN, AES).
- Security logging and monitoring 24/7.
- Multiple highly available (HA) service instances deployed across multiple zones.
- Targeted uptime of 99.9%.

Product Security (platform)

From planning through launch, building security into the HydroSphere™ Cloud Platform is a key responsibility and priority for everyone involved. As a result, the Systems Development Lifecycle (SDLC) includes activities as intended to support secure and reliable product development.

Related aspects include:

- Security framework based on best practices (e.g. Xylem policy, OWASP).
- Risk profiling, threat modeling, and architecture reviews to identify security risks.
- Requirements that help address identified risks and design with security in mind.
- Security awareness to support development effort (e.g. secure code techniques).
- Automated and manual security testing to equip team members with feedback.
- Review and approval of releases by the Product Security team.

What independent security review has been performed?

Xylem also works with world-class product security testing firms to verify our work in securing our network and our products. The HydroSphere™ Cloud Platform was assessed by an independent firm whose feedback was incorporated by the development team to further enhance the security of the system. Xylem has received formal documentation attesting to the product assessment performed and which can be provided upon request.

Where can I go for more information?

For more information on our approach to Product Cybersecurity or to contact our security team, please visit xylem.com/security. For more information on AWS security practices, please visit https://aws.amazon.com/compliance/shared-responsibility-model/. For more information on Xylem's Privacy Policy, please visit https://www.xylem.com/en-us/support/privacy/.

YSI, a Xylem brand
7100 Business Park Drive, Suite B
Houston, TX 77041

+1.727.565.2201
info@ysi.com
YSI.com

YSI.com/HydroSphere