xylem

Staying cybersecure in a digital world

Security in Xylem cloud

As more system operators adopt increasingly connected and integrated solutions, there is a growing need to ensure cybersecurity protections. At Xylem, we seek to maintain your trust in our solutions, empowering clients to solve the world's greatest water challenges with innovative products, services and solutions.

Xylem is a technology company with a commitment to the continuous improvement of innovation and cybersecurity. Along with a risk-based design and implementation approach, our engineering, development, and cybersecurity teams remain diligently focused on the identification and management of cybersecurity risk.

We take a whole system view of risk, evaluating every stage of the water process.

Our approach prioritizes:

Secure products: We ensure products are secure by design, minimizing vulnerabilities and building in security features through development, testing, and deployment. Secure software development processes guided by industry standard frameworks.

Swift response: We develop response plans and provide industry-leading forensics and response for your operations when facing cyber incidents.

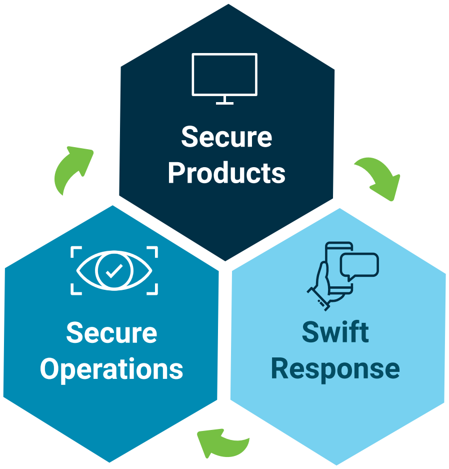
Secure operations: We prioritize continued operational resilience by conducting ongoing assessments, upgrades, and monitoring.

Cybercrime Risk is Increasing

The cost of cybercrime is projected to increase to $10.5 trillion by 2025[1], and costs $4.9 million USD on average globally to remediate each incident.[2]

[1] Cybersecurity Ventures, 2022 Official Cybercrime Report

[2] Cost of a Data Breach (2024) https://www.ibm.com/reports/data-breach



Cloud Application Security

Confidentiality, integrity, and availability of our customer data is vital to businesss operations and safety. Cloud-based deployment is designed and built using best-in-class cloud security practices guided by industry standard frameworks such as NIST CSF and ISO 27001.

Security is a key part of Xylem 's business strategy. By using secure cloud platforms, secure DevOps practices, and Security Development Lifecycle (SDL), Our cloud offerings align with our high security standards.

Physical Security - Best-In-Class, Certified Data Centers

At Xylem, our cloud offerings are hosted in Microsoft Azure and Amazon Web Services (AWS). Each company provides a robust global cloud platform that incorporates strong security practices.

Both Microsoft Azure and AWS have many security features ranging from physical security through network security, to data privacy and security controls. Cloud providers maintain compliance with numerous standards including ISO 27001 and SOC 2.

Data Security

Data protection and application security Data at rest is encrypted using industry standard techniques. For example:

- Data is encrypted in Azure Blobs, AWS S3 Buckets, Files or Databases.
- All data flow communications to and from Xylem cloud services are encrypted using SSL/TLS over HTTP (i.e., HTTPS) using TLS 1.2 or later.
- Our team constantly monitors the ever-changing trends in cybersecurity - including cryptography - to ensure that we offer the best available protections to our customers and their sensitive data.
- Regular backups are taken to restore systems to their normal state in case of accidental loss.

Secure DevOps

DevOps is key to the delivery of safe, secure, and reliable software. This team is responsible for operational control of our cloud environments. They proactively monitor our environments to identify abnormal behavior and to detect and isolate suspicious activity.

Robust security monitoring tools and practices are integrated into our cloud environments. These tools are used to ensure that security updates are applied in a timely manner and that secure configuration is maintained as new versions and features are released.

Strong Baseline secure configuration is enforced to ensure all cloud offerings have the same robust security standards. We established this configuration using standard framework such as CIS (Center for Internet Security). It enforces rules such as requiring multi-factor authentication (MFA) for infrastructure access, minimizing the number of externally exposed ports, and implementing Web Application Firewalls (WAF) along with next-generation anti-malware and threat protection..

SDL

The Security Development Lifecycle (SDL) process applies to all of our product offerings and ensures that our applications deployed on cloud are secure by design.

Secure by design guides application development with security at the core from design through to testing, implementation and operations. SDL is guided by industry best practices for designing, developing, and releasing secure software to customers. It is reviewed regularly to incorporate the latest security best practices.

Vulnerability scans and penetration tests are carried out on a yearly basis. Product applications are assessed in accordance with the latest Open Web Application Security Project (OWASP) testing guidelines, and underlying product infrastructure is assessed per NIST 800-115 guidelines.

For more information about Xylem's product security practices, please visit **www.xylem.com/security** or contact us at **product.security@xylem.com.**