IT & OT SECURITY
FAQ

1. How does QiO approach IT and OT cybersecurity?

QiO uses a security-by-design approach that helps customers stay in control of systems, data and Connectivity.

QiO deployments are designed to work within a customer's existing security architecture, rather than requiring broad trust, unnecessary internet exposure or weakened network boundaries.
Data Centre and Industrial environments are treated differently. IT security protects systems and information. OT security also protects the safety, availability and predictable behaviour of physical processes. For Industrial use cases, this means additional emphasis on approved control authority, operating limits, existing interlocks, fallback behaviour and operator control.

Applies to: QiO overall

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

2. Is QiO ISO 27001 certified?

Yes. QiO Technologies Ltd's Information Security Management System is certified to ISO 27001:2022 by Citation ISO Certification.

The certificate covers the management system for Industry 4.0 software applications infused with artificial intelligence to create real-time digital twins, provide smart automated workflows for team collaboration and scale across production and supply chains.

The original approval date is 14 September 2018. The current certificate was issued on 27 November 2025 and is valid until 13 September 2028.

Applies to: QiO overall

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

3. Does QiO require cloud or internet connectivity?

No. QiO does not require a cloud connection for core operational control.

Data Centre deployments, can operate entirely on-premises with no internet connection or cloud dependency.

For Industrial deployments, operational control is designed to remain local to the site, close to the assets and PLCs being controlled. Optional external services can support functions such as central visibility, benchmarking or model development, but the plant control path does not need to rely on a public internet connection.

Applies to: Data Centre and Industrial

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

4. Can QiO's Data Centre product run in an air-gapped environment?

Yes. Our product can be deployed entirely within your own data centre, including firewalled or air-gapped environments.

Telemetry collection, decision-making and control can remain inside the customer's Data Centre boundary. No internet connection is required for normal operation.

This means organisations can deploy without making significant changes to their existing security architecture.

Applies to: Data Centre

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

5. Does operational data have to leave the customer's site?

No. Core operational data can remain within the customer's environment.
For the Data Centre product, telemetry and logs can remain on the customer's network and the local optimisation loop does not require data to leave the site.

For Industrial deployments, process data required for local monitoring and control can also remain on-site. If a customer chooses optional centralised or cloud-based functions, the permitted data flows should be explicitly defined and approved as part of the deployment architecture.

Applies to: Data Centre and Industrial

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

6. What data does QiO's Data Centre product access or inspect?

QiO optimises servers using performance and utilisation data. It does not need to inspect application content or business data to operate.

The optimisation process is concerned with how heavily the server is being used and how server settings can be adjusted without degrading performance.

Our product does not need to understand the business purpose of the workload or inspect the customer's application content. Keeping the decision process focused on operational telemetry reduces the amount and sensitivity of information needed for optimisation.

Applies to: Data Centre

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

7. How does QiO minimise attack surface and preserve network segmentation?

QiO reduces cybersecurity risk by avoiding unnecessary connectivity and limiting access to only the systems required for operation.

For Data Centres, we can operate without external connectivity, reducing the need for internet-facing services or cloud control dependencies.

In Industrial environments, control authority is kept local where possible and access can be limited to the specific assets, PLC tags and control actions agreed with the customer. When remote access is enabled, the preferred approach is device-specific access rather than broad or flat access across the OT estate.

Applies to: Data Centre and Industrial

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

8. How does QiO secure remote access and support?

Any remote access is optional and remains under customer control.

The Data Centre product does not require a remote connection for normal operation.

For Industrial support, where remote access is enabled, QiO recommends an architecture based on outbound authenticated connectivity, multi-factor authentication, access to a specific authorised device for a time-bound session and session logging. This helps reduce the risk associated with shared credentials, flat routing and long- lived firewall exceptions.

Applies to: Primarily Industrial; Data Centre does not require remote access

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

9. How does QiO apply least privilege?

QiO follows the principle of “only the access that is needed”.

People, services and automated optimisers should only have the minimum authority needed for their approved function.

In an Industrial deployment, an optimiser can be given a unique identity and limited to specific PLC tags and write paths rather than broad control-system authority. Its operating authority can also be set per asset, from read-only observation through recommendation and supervised control to autonomous operation within agreed limits.

For Data Centre deployments, QiO is designed to operate within the customer’s existing access-control and security boundaries.

Applies to: Data Centre and Industrial

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

10. How does QiO connect to PLCs and control systems without weakening OT safety?

QiO is designed to support local Industrial control using only the specific connections and control actions agreed by the customer.

A local industrial computer can read approved process information, apply optimisation within defined limits and write permitted setpoints locally.

QiO's architecture is intended to work with the plant's existing PLC controls, safe states and interlocks rather than bypassing them. The customer decides how much authority is granted and can retain human or PLC control where required.

Applies to: Industrial

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

11. What happens if external connectivity fails or an Industrial optimisation loop is interrupted?

Loss of internet or external network connectivity does not have to mean loss of local control.

In an Industrial deployment, the local optimisation loop can continue operating on-site or fall back to existing PLC control, depending on the approved configuration.

Operators can also reduce authority to recommendation or manual operation for a specific asset. In the Data Centre, the local optimisation function can continue without an internet connection because the core control loop is on-premises.

Applies to: Data Centre and Industrial

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

12. Does QiO carry out penetration testing and how is its software updated?

Security testing forms part of QiO's ongoing information security programme.

This includes activities such as vulnerability assessment, security reviews and penetration testing to help identify and address potential security issues.

QiO develops and releases software continuously, so security improvements, defect fixes and product enhancements can be incorporated on an ongoing basis. Release cadence remains separate from production deployment: customer environments, particularly OT and air-gapped environments, can apply their own validation and change-control process before an update is introduced.

Applies to: QiO overall

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

13. How does QiO fit into our existing cybersecurity and governance requirements?

QiO is designed to operate within established cybersecurity practices rather than requiring customers to weaken existing controls.

QiO focuses on principles that are widely recognised across both IT and OT environments, including least- privilege access, network segmentation, auditability, customer-controlled connectivity and resilient local operation.

QiO also follows the OWASP guidelines as part of its secure development practices, helping reduce common application-security risks across its software lifecycle.

For Industrial deployments, additional safeguards such as staged autonomy, operational guardrails, controlled write authority and fallback to existing control systems help organisations maintain oversight of critical processes.

Cont. overleaf

QiO
AUTONOMOUS OPTIMISATION

IT & OT SECURITY
FAQ

Cont.

QiO Technologies Ltd also operates an ISO 27001:2022-certified Information Security Management System, providing a structured framework for managing information security risks across the business. Where required, customers can assess QiO deployments against their own security, compliance and governance requirements as part of their normal approval process.

Applies to: QiO overall

QiO
AUTONOMOUS OPTIMISATION