q200 Guardian

- Integral part of an edge-to-cloud IoT solution architecture protected by Microsoft Azure Sphere
- Establishes connectivity in hard-to-reach places; supports global 2G/3G/4G bands with flexible ports at the network edge
- Enables secure collection and processing of large quantities of usage and marketing information enabling better operational and business decisions
- Seamlessly operates with qiio services to remotely monitor and control your assets, saving you millions

World's first IoT solution optimized for cellular operation on Microsoft's Azure Sphere®

Protects IoT devices from cyber threats and ensures that data transferred to and from the cloud via mobile networks is confidential, tamper-proof and authenticated.

The most secure cellular IoT solution on the market

The vast majority of IoT solutions control critical processes in industrial applications such as production, manufacturing and energy supply. The security of IT infrastructures and data for these systems is of critical importance.

The q200 Guardian is the world's first solution specifically optimized for secure, bi-directional cellular connectivity supporting IoT solutions running on Microsoft's Azure Sphere.

Built-in Microsoft security technology

Protect your IoT devices and equipment with defense in depth. The q200 Guardian embeds Azure Sphere-certified chips to provide secure connectivity based on a dependable hardware root of trust.

Azure Sphere brokers trust for device-to-cloud communications, detects threats, and renews device security. The OS adds layers of protection and ongoing security updates to create a trustworthy platform to manage your IoT devices.

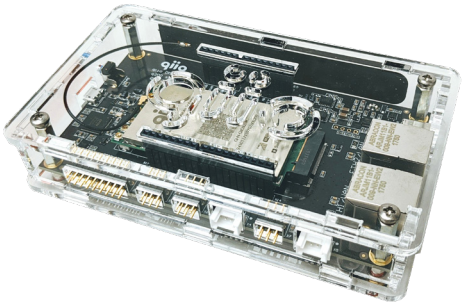
Essential part of a secure edge-to-cloud solution

In addition to the q200 Guardian, qiio offers complementary cloud services that seamlessly integrate into industrial and commercial IoT solutions.

This enables customers to securely connect, monitor and control their IoT assets via their own online dashboard. Due to the modularity of the qiio architecture, a customized solution can be developed in as little as eight weeks.

Benefits and features

- **Securely connects, monitors and controls** your IoT edge devices via an online dashboard
- **Embedded Azure Sphere** certified processor integrates built-in Microsoft security technology based on seven pillars of IoT security
- **Supports large deployments** working seamlessly with qiio cloud services for Azure
- **Zero-touch provisioning** – works Out-of-the-Box
- **Global coverage** includes roaming agreements with over 500 cellular service providers in 190 countries
- **Fast time-to-market** due to the modularity of qiio products; tailored solutions can be typcially realized within eight weeks
- **Comprehensive operational overview** of processes and activities, including usage and marketing data collection
- **Real-time monitoring** of processes and machines results in faster, low-cost and preventative maintenance.
- **Saves costs** – eliminates unnecessary travel, reduces security threats, optimizes supply chain logistics, and eases adherence to industry regulatory requirements
- **Streamlines supply chain** management resulting in cheaper and faster logistics and manufacturing processes
- **Comprehensive connectivity:** Supports 2G, 3G, 4G cellular plus Wi-Fi, Ethernet, I²C, SPI, UART, PWM and ADC interfaces
- **Robust** enclosure 136 × 91 × 30 mm (159 × 91 × 30 mm with mounting bracket)



Evaluation & Design

qiio's PoC in a Box is the quickest way to start your IoT project. The Plug & Play development board includes all the features of the q200 Guardian including global coverage and SDK for connectivity management. Use qiio's demo cloud platform or connect directly to your own.

Technical data

q200 Guardian	
Processor	▪ High-security Azure Sphere* MT3620
Azure Sphere platform security features	
Hardware-based root of trust	▪ Prevents device forgery or spoofing
Small trusted computing base	▪ Reduces attack surface area of security-critical hardware and software components
Defense in depth	▪ Multiple layers of security - each layer of software verifies that the layer above it is secured
Compartmentalization	▪ Prevents a security breach in one component from propagating to other components
Certificate-based authentication	▪ Signed certificates validated by cryptographic key
Renewable security	▪ Device software is automatically updated to correct known vulnerabilities or security breaches
Failure reporting	▪ Automatic reporting of operational data and failures to a cloud-based analysis system anticipates emerging security threats
Interface to IoT asset	
Wired interfaces	▪ I²C ▪ SPI ▪ UART (available via USB-C connector)
Interface to Azure Cloud	
Cellular interfaces**	▪ LTE-FDD, LTE-TDD, DC-HSDPA, HSPA+, HSUPA, UMTS, EDGE, GPRS
Bands	▪ LTE-FDD : B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28 ▪ LTE-TDD : B38/B39/B40/B41 ▪ WCDMA : B1/B2/B4/B5/B6/B8/B19 ▪ GSM : 850/900/1800/1900MHz
WLAN interface	▪ Wi-Fi: 2.4 and 5 GHz
Wired interface	▪ Ethernet 1 x RJ45 10/100 Mbit/secs
Certifications	▪ PTCRB/FCC/AT&T certified (FCC ID: GC520240Q200), others in progress
Roaming	
Integrated eSIM	▪ Roaming agreements with 500 service providers ▪ Plug & Play – works in 190 countries ▪ Fully programmable (on development version) ▪ External SIM slot available
GNSS positioning**	▪ GPS ▪ GLONASS ▪ BeiDou ▪ Galileo ▪ QZSS
Analog interfaces	▪ 3 PWMs/GPIOs ▪ 6 12-bit ADCs/GPIOs
LED indicators	▪ One green LED to indicate power state ▪ One multi-color LED to indicate modem state ▪ 3 green LEDS reserved for customer application
Operating conditions	
Recommended power supply	▪ 5 V/3 A
Current consumption at 5 V	▪ 0.5 A (Typ), 0.7 A (Max)
Operating temperature	▪ –40 °C to +85 °C

* Azure Sphere is a registered trademark of Microsoft Corporation
** Embedded antennas included

qiio AG · Am Wasser 24 · 8049 Zurich · Switzerland · Phone +41 44 552 02 66 · info@qiio.com · www.qiio.com