



Security & Privacy Whitepaper

R-Zero occupancy intelligence and ODCV platform

How R-Zero protects your network, your building systems, your data, and the privacy of the people in your spaces.

Prepared by:	R-Zero Systems, Inc.
Audience:	Security, IT, and facilities leadership
Companion document:	R-Zero ODCV Connectivity Guide (for detailed IT / network implementation)
Document version:	v2.0 · June 2026

Introduction and security philosophy

R-Zero's ODCV system ventilates for the people actually in the building — not an assumed full house. Anonymous occupancy sensors feed an R-Zero Hub, which pushes data to the cloud. R-Zero's Gateway relays this data to your existing BMS. The result: energy savings and occupancy insights through the R-Zero Connect app, no capital retrofits required.

The system integrates with the building's existing Building Management System (BMS) via BACnet/IP. Security and privacy are not just features added at the end — they are integral to the system. R-Zero is engineered to add no inbound attack surface to your network and no operational risk to your building. Two principles run through every layer of the system:

- **Add no risk to your network:** every external connection R-Zero makes is outbound-only. The system requires zero inbound firewall rules, so it opens no new path into your environment from the internet.
- **Add no risk to your building:** R-Zero is additive to your controls. If R-Zero data stops arriving for any reason, your BMS keeps operating exactly as it does today.

This document is written for the people who evaluate that risk. It describes the system at the level you need to make an informed decision — what data is collected, how data is collected, and how your building and data are protected. Port-level detail for your network engineers lives in the companion **R-Zero ODCV Connectivity Guide**.

Security at a glance

- **No PII:** sensors detect people, not identities. No images are transmitted from or stored on the sensor; only anonymous counts are transmitted.
- **No inbound connections:** all cloud communication is outbound-only and encrypted. No inbound firewall rules are required.
- **Sensors stay off your network:** occupancy sensors talk to a local Hub over Bluetooth Low Energy (BLE); they never join your IP network.
- **Your BMS stays in control:** R-Zero informs your controls without taking them over, and your building reverts to its native sequence if R-Zero is unavailable.
- **Encrypted in transit and at rest:** data is protected with TLS in transit and AES-256 at rest.

- **Independently audited:** R-Zero maintains SOC 2 Type II compliance; a public SOC 3 report and completed HECVAT are available on request.

What R-Zero collects — and what it never collects

R-Zero collects only the minimum data required to optimize ventilation, and nothing that can identify a person.

Occupancy is anonymous at the source

R-Zero's sensors count people — that's it. For sensors that use imaging, all processing happens on-device via an on-board AI model: the sensor sees a frame, determines "that's a person," increments the count, and discards the image — no images ever leave the device. Non-imaging sensors never capture frames at all. Either way, what goes out is a tiny BLE packet with five fields: device ID, sensor status, occupancy count, battery level, and firmware version. No video, no stored imagery, no biometric data — because none is ever created.

Operational building data

To align ventilation with occupancy and to verify the resulting savings, R-Zero also reads operational data from your BMS over BACnet — for example, ventilation rates, airflow, and related setpoint and energy readings. This is equipment data, not personal data.

What R-Zero collects and does not collect

R-Zero collects	R-Zero never collects
Anonymous occupancy counts and status	Names, identities, or any personally identifiable information of occupants
Device health (battery, connectivity, firmware version)	Images, video, or audio
Operational BMS data (airflow, setpoints, energy)	Biometric, demographic, or behavioral profiles
Space and building names you assign	Occupants' personal devices — no Wi-Fi, Bluetooth, or MAC-address tracking of people

Energy consumption and tariff data from your utility (with your permission)	IP or business data from your other systems
---	---

Table 1: Data R-Zero collects versus data it never collects.

The only limited personal information R-Zero processes are the names and emails that customers use to login to Connect, as is standard for any enterprise application. R-Zero's customer agreements also include acceptable use provisions that prohibit users from entering personally identifiable information as metadata when labeling spaces or contextualizing occupancy data, providing a contractual safeguard in addition to the technical controls.

How the system connects

The R-Zero system has four parts: (1) occupancy sensors, (2) a local Hub, (3) a Gateway, and (4) the R-Zero Cloud, which authorized users access through the Connect web application. The diagram below shows how they connect and where data flows.

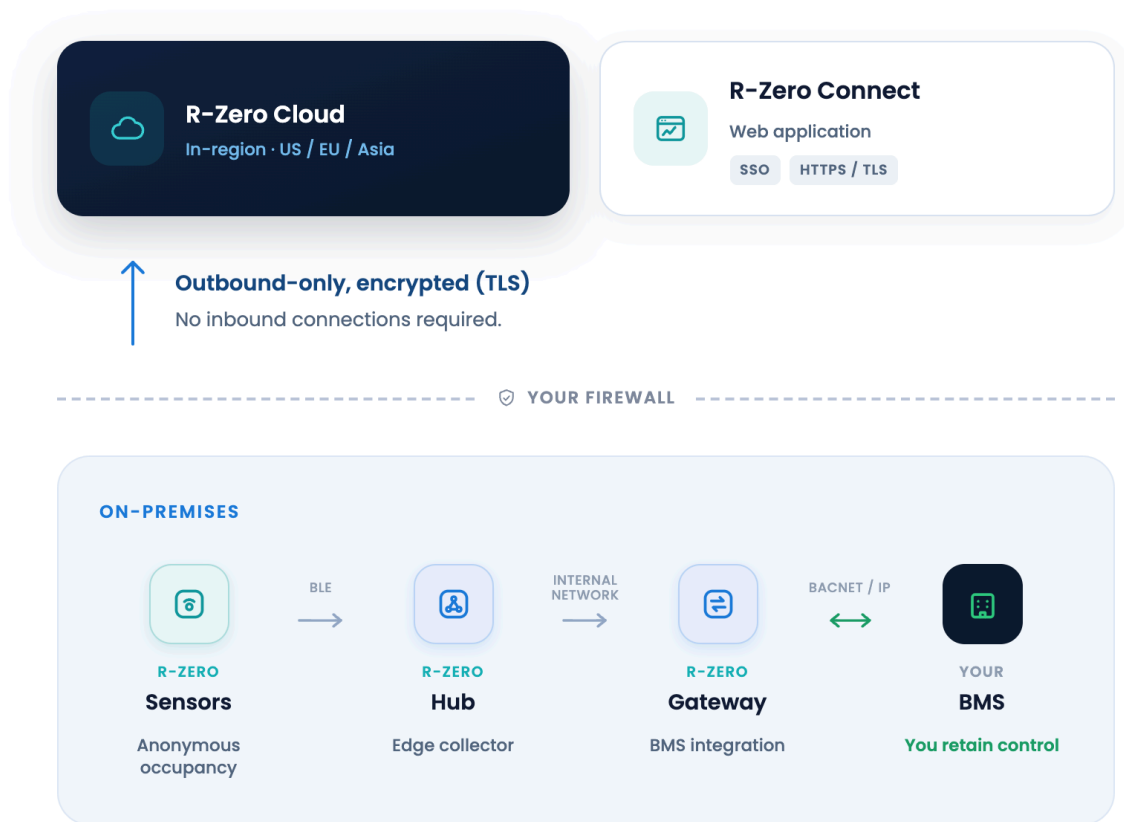


Figure 1: R-Zero ODCV system architecture and data flow.

Sensors to Hub (on-premises)

Sensors send anonymous occupancy data to a nearby Hub over BLE. Sensors have no IP stack, no Wi-Fi capability and are never internet-connected.

Hub to Gateway to BMS (on-premises)

The Hub forwards occupancy data to the Gateway, which integrates with your BMS using BACnet, the standard building-automation protocol. All of this traffic stays on your local building-automation network.

Hub and Gateway to R-Zero Cloud (outbound only)

The Hub and Gateway send building health and occupancy data to the R-Zero Cloud over encrypted connections that they initiate outbound. No inbound connections from the internet are required or accepted. Firmware updates and remote diagnostics also run over these outbound-initiated sessions — the same connection model used by standard enterprise software.

Connect (web application)

Authorized users access occupancy intelligence and reporting through the Connect web application over HTTPS.

The R-Zero Cloud runs in the region of your deployment, with in-region instances available for the US, EU, and Asia.

For your IT and network team

Exact ports, protocols, and destination hosts are documented in the R-Zero ODCV Connectivity Guide. In summary: R-Zero requires only outbound firewall rules — no inbound rules are needed.

Protecting your building systems

Connecting to building controls is where customers scrutinize any vendor most closely — and rightly so. R-Zero is designed so that integrating it carries no operational risk to your HVAC.

Fail-safe by design

If your BMS stops receiving data from R-Zero — whether from a powered-down Hub, a network interruption, or a removed device — it continues operating exactly as it does today, using its own native control sequences. R-Zero is additive: its absence

returns the building to your existing baseline, never to an unventilated or unsafe state.

Your BMS retains control authority

R-Zero operates as a software intelligence layer within your existing systems. Occupancy data is delivered into your control environment as standard BACnet points, and your building's own control logic, safety interlocks, and minimum-ventilation limits remain in force at all times. The scope of what R-Zero contributes is configured with your controls contractor during commissioning and is bounded to what you approve.

How occupancy informs ventilation

Today, R-Zero publishes anonymized occupancy counts as BACnet points for your sequences to use. As the platform evolves, R-Zero will also provide ASHRAE 62.1-aligned ventilation recommendations — recommended outdoor-air values calculated from real occupancy — delivered into the same control environment and always within the operating limits your team defines.

Data governance

Encryption

All data is encrypted in transit using TLS, including the encrypted MQTT channel used for building-data trending. Data at rest in the R-Zero Cloud is encrypted using AES-256.

Access control and tenant isolation

Access to Connect is role-based and follows least-privilege principles, with distinct permission tiers for view-only, manager, and administrator users. Customer data is logically isolated by organization in a multi-tenant architecture. R-Zero's customer agreements contractually require R-Zero to maintain and protect Customer Data in accordance with SOC 2 Type II standards, including appropriate safeguards against unauthorized access, disclosure, or alteration.

The Connect app supports all major SSO/SAML providers for you to manage your own enterprise authentication. Where API access is enabled, R-Zero issues unique authentication keys that are restricted to the customer's internal business use and may not be shared with third parties without R-Zero's written consent.

Data residency

Customer data is stored in the cloud region that matches your deployment – US, EU, or Asia. Where required by applicable privacy laws (including GDPR, CCPA, or other state and federal privacy regulations), R-Zero will enter into a Data Processing Addendum specifying the purposes and means of processing, data subject rights, security measures, and breach notification procedures.

Data ownership

You own your data. R-Zero does not sell customer data. R-Zero may use de-identified, aggregated technical and usage data (excluding any personal data in identifiable form) to improve the accuracy and performance of its platform, including its AI and machine learning models. Any data used for this purpose is aggregated and de-identified so that it cannot reasonably be used to identify any customer or individual.

Third parties and sub-processors

R-Zero relies on a small set of vetted infrastructure providers to deliver the service. Third parties do not access your data except as required to provide the service, and never without authorization.

Provider	Purpose	Data location
Amazon Web Services (AWS)	Cloud hosting and storage	In-region (US / EU / Asia)
Google Cloud Platform (GCP)	Occupancy data processing and storage	In-region (US / EU / Asia)
Cloudflare	Secure outbound connectivity / diagnostics	Global edge

Supabase	Cloud-hosted data storage	In-region AWS
Vercel	CDN	In-region AWS

Table 2: Infrastructure sub-processors.

Platform operations

- **Monitoring:** R-Zero continuously monitors device health and connectivity – battery levels, connection quality, and data integrity – with automated internal alerts when a device behaves unexpectedly.
- **Vulnerability management:** R-Zero tracks and remediates vulnerabilities on a risk-prioritized basis and undergoes regular third-party penetration testing and vulnerability scanning.
- **Firmware updates:** firmware is updated over outbound-initiated connections, with no inbound access to devices required. Updates are managed by R-Zero as part of routine maintenance.
- **Incident response:** R-Zero maintains a documented incident-response process and notifies affected customers of confirmed security incidents in line with contractual and regulatory obligations.
- **Availability and recovery:** the R-Zero Cloud uses redundant, managed cloud infrastructure with regular backups to support availability and recovery.

Certifications and compliance

- **SOC 2 Type II:** R-Zero maintains a SOC 2 Type II attestation, independently audited against the Trust Services Criteria. The full report is available under NDA.
- **SOC 3:** a SOC 3 report is available publicly and can be shared without an NDA.
- **HECVAT:** R-Zero has completed the Higher Education Community Vendor Assessment Toolkit and can provide it to support your vendor review.
- **Privacy by design:** because occupancy is anonymous at the source and no personal data is collected from occupants, R-Zero substantially reduces the privacy and compliance burden associated with workplace sensing.

Working with your security and IT teams

R-Zero welcomes security review. To support your evaluation, we can provide:

- **SOC 2 Type II report:** under NDA.
- **SOC 3 report:** public, no NDA required.
- **Completed HECVAT:** for your vendor-assessment process.
- **Data Processing Agreement:** on request.
- **ODCV Connectivity Guide:** for your network and controls teams.

Questions, or to request any of the above, contact your sales account manager. To report a security concern, contact security@rzero.com.

Appendix: R-Zero Hardware Security and Privacy

Sensor Security

R-Zero occupancy sensors are passive, battery-powered BLE devices. They have no IP stack, no Wi-Fi capability, and no writable storage accessible over the air. Sensors transmit occupancy event data to the nearest Hub via BLE in broadcast mode with no pairing. Because sensors have no network presence and accept no inbound connections, they present no IP-based attack surface. R-Zero sensor hardware carries FCC, IC, CE, UKCA, and additional regional certifications (IMDA, HKCA, RCM, TELEC) for global deployment. The BLE Specific Absorption Rate (SAR) is so low the FCC does not require testing, confirming the sensors are safe for continuous use near people.

Sensor Privacy

R-Zero sensors are designed for privacy first operation, there is no option to disable privacy. Sensors report only private, anonymous occupancy or air quality data, along with basic sensor health data (firmware version and battery status).

Sensor Model	Data Transmitted	PII Stored on device	PII transmitted to cloud
Area Counter	Count of occupants in a space (thermal camera with on-board AI; no RGB imagery)	None	None
Entry/Exit Counter	Count of occupants passing through a doorway; Temperature, humidity (RGB camera with on-board AI; images processed and discarded on-device)	None	None
Room Occupancy	Binary presence of occupants in a	None	None

Sensor	wider area; Temperature, humidity (passive infrared; no camera)		
Desk Occupancy Sensor	Binary presence of occupants in a narrow area (passive infrared; no camera)	None	None
Indoor Air Quality Sensor	Particulate Matter, CO2, TVOC, Formaldehyde, Pressure, Noise level, Light intensity, Temperature, Humidity (RESET-accredited and WELL qualified; no camera or occupancy detection)	None	None

Table 3: Sensor model details.

Hub and Gateway security

The R-Zero BACnet Gateway runs proprietary software on industrial-grade, fanless hardware designed for long-term reliability in building environments. It connects to the local network via wired Ethernet. Like the Hub, the Gateway initiates **only outbound connections** to the R-Zero Cloud, requires no inbound firewall rules, and receives firmware and vulnerability patches deployed remotely by R-Zero on a regular cadence or as coordinated with your team. The Gateway carries EN/UL/IEC 62368-1, FCC, and CE certifications.

Hubs and Gateways run a hardened embedded Linux distribution. Only services required for R-Zero operation are enabled.

- **OS and firmware patching:** RZero keeps the hubs and gateways patched and updated with the latest firmware updates. Your IT team does not need to manage these devices. Hubs and gateways periodically check for updates by initiating outbound connections to the update endpoint. No inbound access is required.
- **No user-accessible storage:** Hubs and gateways do not store persistent customer data locally. Occupancy and HVAC operation data is transmitted to the cloud in near-real-time and is not cached on the device beyond the operational buffer

- **No local user-interface or local user accounts:** Hubs and Gateways are designed for secure, automated operation by the R-Zero system. There is no local UI or local user accounts to be subjected to password-sharing risks.