SmartRite security at a glance

Frequently asked questions for SmartRite customers

WHY WE ARE SHARING THIS

On the night of 11 October 2026, attackers remotely accessed refrigeration controllers in supermarkets across France and switched them into defrost mode, spoiling stock. SmartRite was not among the products named by investigators. The attacks prompted Everidge to complete a security review of SmartRite. Here is what you need to know.

01

Monitoring only

None of SmartRite's remote functions controls or interferes with the cooling process. The door heater cannot be operated remotely.

02

Safe limits built in

Alarm thresholds are read-only in the portal. The device itself rejects any value outside limits built into its firmware.

03

Protected and encrypted

Communication with the SmartRite platform is encrypted, and only a restricted group of SmartRite administrators can manage the platform or update firmware.

QUESTIONS CUSTOMERS MAY ASK

Could someone use SmartRite to change how my equipment cools?	No. None of SmartRite's remote functions controls or interferes with the cooling process.
Can someone change my alarm settings?	Not from the portal, where thresholds are read-only. Only SmartRite platform administrators and users given explicit permission for a device can change them, and the device ignores any value outside its built-in limits.
Can a change hit all my sites at once?	Not from the portal. Settings and commands apply to one device at a time.
What happens if a security issue is found?	We acknowledge security reports within 24 hours and aim to fix critical issues within 5 business days.
Has SmartRite been security tested?	An internal code audit and platform review were completed in 2026. An independent penetration test is planned for 2027.