Cloud Security Features

SECURITY YOU CAN RELY ON

For greenhouses and commercial growers, data security is not optional. It's fundamental to operational stability, crop protection, and long-term success. Argus Axia is built around what growers need most: reliable control, uninterrupted performance, and trusted data security.

This document outlines the security architecture, controls, and safeguards built into the Axia cloud platform - presented in clear, practical terms for growers, but also with the technical depth IT teams need to assess risk, governance, and long-term system integrity.

Our cloud security framework reflects Argus's enduring commitment to strong, reliable data protection to help keep your operation secure today and prepared for tomorrow.

Architecture Principles

Zero Trust: Always Verify, Never Assume

Instead of automatically trusting users or devices, the system checks every request, every time.

This reduces the chances of unauthorized access or hacking.

Operational Impact: Zero Trust assumes *something could always go wrong*, so it checks every request every time to keep data and systems secure.

Device Security

Secure Device Setup: Hardening

All systems are configured following major security guidelines such as:

- **OWASP:** safe software configuration
- **NIST:** U.S. government cybersecurity standards
- **EU CRA / UK PSTI:** consumer device safety rules

This ensures devices are locked down and protected from common threats.

Operational Impact: Devices are locked down by default, with only the access needed to operate safely - nothing extra for attackers to exploit.

Identity & Access

Controlling Who Can Access What

Single Sign-On (SSO)

Users log in once using their company account, and everything works automatically.

Multi-Factor Authentication (MFA)

Even if a password is stolen, the attacker cannot log in without a second step
(ex: code from an app or security key).

Role-Based Access Control (RBAC)

People only get the exact permissions needed for their job—nothing more.

Operational Impact: Only verified users can access the system, and each person is limited to exactly what they need to do their job.

Cloud Security Features

Encryption

Making data unreadable to anyone who shouldn't see it.

Data at Rest (AES-256)
Stored data is locked with strong encryption—AES-256 is the global standard.

mTLS & API Hardening
Both sides of a connection (client and server) verify each other's identity.

Data in Processing (Confidential Computing)
When supported, data is protected even while it's being used by the system.

Operational Impact: Your information is protected when stored, when moving, and even while being processed.

Key Management

Customer-Managed Keys (CMK)
Customers can provide and control their own encryption keys.

HSM-Backed Keys
Keys can be stored inside tamper-resistant hardware for maximum security.

Operational Impact: You hold the "master key" that locks and unlocks your data.

Governance

Shared Responsibility Model
We all help secure the cloud platform.

Data Residency & Sovereignty
Data can be stored in specific regions to meet legal or compliance requirements.

Exit & Portability
Customers can export all their data and leave the platform if needed.

Operational Impact: You stay in control of your data and where it's stored.

SDLC & Security Operations

Secure Software Development (SDLC) Security is built into every stage of development:

- Code scanning
- Dependency checking
- Manual reviews
- Threat modeling

Continuous Monitoring (SSPM)
Tools like CrowdStrike and Madison continuously watch for risks.

Operational Impact: The product is built securely from the start and monitored continuously.

Certifications & Compliance

Our platform aligns with or maintains major global standards:

- **SOC 2 Type II** – Operational security and reliability
- **GDPR / CCPA** – Privacy protections for EU and U.S. customers
- **EU CRA / UK PSTI** – Device safety and cybersecurity compliance

Operational Impact: Independent organizations verify that our security meets strong global standards.

Cloud Security Features

Category	Feature	Summary
Architecture & Principles	Zero Trust	Cloud + devices use least-privilege, unique device credentials, no implicit trust, outbound-only connections.
Device Security	Device Hardening (OWASP/NIST, CRA/PSTI alignment)	Hardened firmware, secure boot, signed updates; aligns with standards but formal certification not in scope.
Identity & Access	SSO	SAML/OIDC for cloud users; offline controller UI uses local accounts.
	MFA	MFA enforced via IdP; controller UI does not implement MFA.
	RBAC	Granular cloud roles; simplified roles on controllers.
Encryption	Data at Rest (AES-256)	AES-256 cloud storage; devices store configs securely.
	Data in Transit (TLS 1.2+)	TLS-only communications; no plaintext interfaces.
	mTLS / API Hardening	Device-to-cloud mTLS; validated API schemas.
Key Management	CMK / HSM-backed Keys	Cloud KMS/HSM; secure key storage on devices.
Governance	Shared Responsibility Model	Provided as diagrams + documentation.
	Data Residency & Sovereignty	Regional hosting options; documented data flows.
	Exit & Portability	Export APIs, offboarding process, data deletion procedures.
SDLC / Security Ops	Secure SDLC & Vulnerability Mgmt.	SAST/DAST, dependency scanning, pen tests, structured patching.
	SSPM (CrowdStrike/Madison)	Integrated SaaS posture monitoring.
Certifications	SOC 2 Type II	Requires formal audit; not in initial release.
	GDPR / CCPA	Compliant design and contractual DPAs.
	EU CRA / UK PSTI	Align with principles; no formal certification.