

InsightCM™ Product Security Overview

**Architecture, Data Protection, and Shared Responsibility
for On-Premises Monitoring Deployments**

Contents

- Product Overview 3
- Architecture 4
- Identity and Access Management 4
- Data Security 5
- Network and Infrastructure Security 5
- Application Security 6
- Observability and Operations 6
- Deployment Model 6
- Shared Responsibility 7
- Summary 7

Product Overview

InsightCM is Cutsforth's on-premises industrial condition monitoring platform. It is not a control system, has no control capabilities, and is typically deployed on the customer's business/plant information network or on a separate monitoring network — not the controls network.

Cutsforth targets two major releases per year, each delivering new functionality, updated third-party dependencies (databases, runtimes, libraries), and security enhancements validated against the engineering source repository. For high-criticality cybersecurity issues, Cutsforth issues targeted patches outside the standard release cycle.

Cutsforth's enterprise security program is aligned with NIST SP 800-53 Revision 5 and ISO 27001, supported by a dedicated cybersecurity team, 24/7 managed detection and response (Sophos MDR), MFA across the organization (Okta), and documented security policies reviewed annually. InsightCM installs on a customer-owned Windows Server — all monitoring data stays on the customer's infrastructure, with no data sent back to Cutsforth — and supports LDAP/Active Directory integration, role-based access control, SSL/HTTPS encryption, and AES-encrypted device communications by default.

A Software Bill of Materials (SBOM) is available on request, and Cutsforth fully supports customer-directed vulnerability assessments. For a deeper technical review of architecture, encryption mechanisms, shared responsibilities, and compliance positioning, Cutsforth can provide a detailed Technical Whitepaper under NDA.

Pillar	What It Means for You
Customer-controlled deployment	Runs entirely inside your network; no inbound cloud dependency
Hardware-rooted ingest	Devices authenticate to InsightCM using vendor-specific protocols
Local persistence	Time-series and configuration data managed on industry-standard databases

Component	Role
InsightCM Service	Core .NET service that brokers, normalizes, and persists sensor data
Message Bus	RabbitMQ broker carrying real-time telemetry between collectors and consumers
Configuration Store	Document database holding asset hierarchy, device definitions, and configuration
Time-Series Store	Relational database with time-series extensions for waveform and feature data
Web Application	User-facing UI for configuration, asset browsing, and data review

Architecture

InsightCM is deployed entirely within the customer plant network. Field devices send authenticated telemetry into the message bus; the core service normalizes the data, persists it locally, and exposes it through a user web application.

Trust Boundaries

Boundary	Crossing Mechanism
Device to InsightCM	Customer on-premises network rules
User to Web UI	HTTPS with local or directory-backed authentication

Identity and Access Management

Surface	Mechanism
User login	Local accounts or directory federation (Active Directory)
Service-to-service	Internal service identities scoped to the InsightCM host
Device-to-service	Vendor-specific protocols, dependent on the hardware used
Database access	Database-native authentication
Administrative access	Role-based, separated from user-level roles

Data Security

Where Data Is Stored

Data Class	Location	Protection
Sensor waveforms	Time-series store, customer-managed	Binary files stored on customer-owned InsightCM server
Asset hierarchy and configuration	Document store, customer-managed	MongoDB server running on customer-owned InsightCM server
User credentials	Authentication backend (local or AD)	Hashing per identity provider
System configuration	Application configuration files	File-system permissions, restricted access
Audit events	Local log files created by the application	Append-only, retention-controlled

Encryption

Channel	Protection
Device to InsightCM	Vendor-specific protocols, dependent on the hardware used
User to Web UI	HTTP during initial configuration with built-in account(s); the customer then switches to HTTPS with LDAP-backed authentication

Network and Infrastructure Security

Control	Description
Deployment scope	Single host within customer network
Inbound exposure	N/A
Outbound exposure	N/A
Operating system	Hardened Windows Server baseline managed by customer
Backup	Customer-managed snapshots of databases and configuration

Application Security

Practice	Implementation
Code review	Every change requires peer review before merging
Static analysis	Automated scanning on every pull request
Dependency scanning	Continuous vulnerability monitoring of third-party packages
Build provenance	Installer artifacts produced only by trusted CI/CD workflows
Patch cadence	Regular maintenance releases with security advisories
Penetration testing	Conducted on an annual basis

Observability and Operations

Capability	Tooling
Service health	Built-in health endpoints and user dashboard
Logs	Local log files, forwardable to customer SIEM
Metrics	Exportable to customer monitoring platform
Backup and restore	Customer-defined schedule using standard database tooling

Deployment Model

Attribute	Detail
Tier	Plant / on-premises
Topology	Single tenant per installation
User	Customer
Cloud connectivity	Not required
Air-gap support	Fully supported

Shared Responsibility

Responsibility	Cutsforth	Customer
Software development and security testing	Yes	—
Installer and patch delivery	Yes	—
Operating-system hardening and patching	Guidance	Yes
Backup, disaster recovery, and capacity planning	Guidance	Yes
Network segmentation and firewall rules	Guidance	Yes
User account lifecycle and authentication policy	Guidance	Yes
Physical security of the InsightCM server	—	Yes
Physical security of plant devices	—	Yes

Summary

Dimension	Posture
Deployment	Customer-controlled, on-premises
Inbound cloud dependency	None
Authentication	Vendor-specific; local or AD-federated for users
Encryption	TLS in transit; encryption at rest is customer-controlled
Data residency	Customer-defined and customer-controlled
Air-gap support	Fully supported

To request the Technical Whitepaper under NDA or schedule a security review with your IT/OT team, contact Cutsforth at info@cutsforth.com or 800-290-6458 x1.