SYYCLOPS

Syyclops, Inc

AI Architecture & Enterprise Overview

2026

Table of Contents

1. Executive Summary

Syyclops is a digital twin software platform designed for enterprise building operations and maintenance. The platform integrates and organizes customer-provided building information (including documents and operational system data) to support facility teams in locating information, generating analyses, and drafting operational outputs.

Syyclops is designed as an enterprise solution for use by a customer's personnel and other **Authorized Users** (as defined below). Syyclops processes building data to generate outputs intended to **support** operational workflows and decision-making; Syyclops is not a substitute for professional judgment, safety procedures, or required engineering review.

No Model Training on Building Data. Syyclops does not use building data to train, fine-tune, or otherwise improve any third-party or proprietary foundation model. Building data is processed solely to provide services to the customer.

Third-Party Model Provider. Syyclops uses Anthropic's Claude API to perform certain AI processing. All statements regarding the security posture and certifications of third-party providers reflect the providers' published documentation and contractual commitments, as applicable. Syyclops additionally implements its own administrative, technical, and organizational safeguards as described below.

2. Platform Overview

2.1 What is Syyclops?

Syyclops is purpose-built for enterprise building operations teams that need to aggregate data from multiple systems, normalize and correlate that data, and generate operationally useful outputs such as reports, planning drafts, and troubleshooting guidance.

2.2 Primary Users

Primary users include building managers, facility managers, energy managers, building technicians, maintenance professionals, and customer-approved subcontractors or service providers.

2.3 Definitions

- **Building Data**: All information provided by or on behalf of the customer to Syyclops, including uploaded files, system integrations, work order records, telemetry, metadata, prompts, and any customer-provided context.
- **Outputs**: All responses, reports, drafts, recommendations, summaries, or other content generated through the platform from Building Data.
- **Authorized Users**: Individuals expressly authorized by the customer (including employees and approved contractors) to access and use the platform under the customer's account and applicable agreements.

2.4 Data Sources & Integration

Syyclops may connect to or ingest information from customer-authorized sources, including:

- **Work Order/CMMS Systems**: service history, asset records, completion notes
- **Documents & Manuals**: O&M manuals, specifications, warranty documents
- **BIM Models**: spatial/asset context and model attributes
- **Spreadsheets**: inventories, schedules, budget worksheets
- **Building Automation Systems (BAS)**: sensor data, setpoints, alarms, trends (as provided)

2.5 Data Processing Pipeline

After ingestion, Building Data may undergo the following processing activities:

1. **Data Cleaning**: normalization, de-duplication, and quality checks
2. **Correlation**: linking data across systems (e.g., asset-to-location, asset-to-work-order)
3. **Schema/Ontology Application**: applying standardized and/or platform-defined structures to improve consistency and searchability
4. **AI Processing**: using Claude-powered workflows to generate Outputs

Human Review. Certain data preparation steps may be performed or validated by trained personnel under role-based access controls and audit logging.

2.6 AI-Powered Capabilities (Illustrative)

Syyclops may generate Outputs such as:

- **Capital Planning Drafts**: lifecycle/condition-based planning drafts based on available records
- **Maintenance Troubleshooting Guidance**: suggested diagnostics and resolution steps
- **Operational Reporting**: performance summaries and asset/system observations
- **RFP Draft Documents**: draft scopes and procurement-support documents for customer review

Important: Outputs are informational and draft in nature, depend on data quality and completeness, and require customer review and approval prior to use.

3. Syyclops System Architecture

3.1 Architecture Overview

Syyclops uses a layered architecture designed to separate ingestion, processing, AI operations, and output generation. This structure is intended to support data isolation, auditability, and least-privilege access.

3.2 Data Flows

Syyclops uses a layered architecture that separates data ingestion, processing, AI operations, and output generation. Below is a detailed breakdown of the data flow and protocols used at each stage.

Layer 1: Data Sources	Layer 2: Gateway	Layer 3: Syyclops Cloud	Layer 4: AI Processing
Building Automation System (BAS) Work Order / CMMS Documents & Manuals BIM Models Spreadsheets	**On-Premise Gateway Device** Protocol: BACnet/IP (read-only) Function: Trend data collection Outbound Only: TLS 1.2+	**Data Pipeline** Data cleaning & normalization Cross-system correlation Ontology mapping Storage: AES-256 at rest	**Anthropic Claude API** U.S. hosted infrastructure Protocol: HTTPS/TLS 1.2+ No model training on data Zero Data Retention available

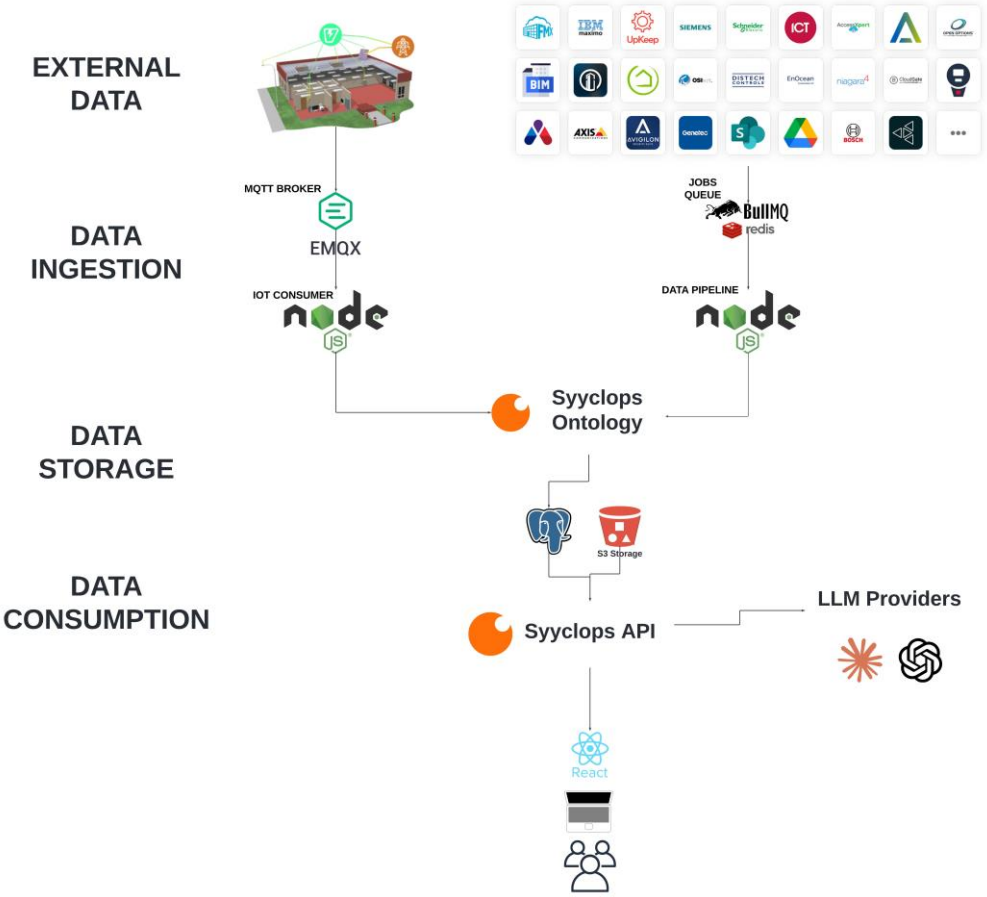
Protocol Summary

Connection	Protocol	Direction
BAS → Gateway	BACnet/IP (Read-Only)	Internal Network
Gateway → Syyclops Cloud	MQTT	Outbound Only
CMMS / Software APIs	REST API / HTTPS / TLS 1.2+	Cloud-to-Cloud
Syyclops → Anthropic API	HTTPS / TLS 1.2+	Outbound Only
Users → Syyclops Web App	HTTPS / TLS 1.2+	User Browser

3.3 Data Pipelines Explained

The Syyclops Data Pipeline is the core processing layer that cleans, organizes, and correlates data from all integrated building systems. Its primary functions include:

- Data Cleaning & Normalization: Standardizes naming conventions, removes duplicates, and performs quality checks on incoming data from disparate systems.
- Cross-System Correlation: Links related entities across systems. For example, correlating "AHU-1" in the work order system to the same unit in the BMS and associated O&M documentation.
- Ontology Mapping: Applies a standardized building ontology (common language) to all data, enabling consistent queries and analyses regardless of the source system's native naming conventions.
- Dataset Generation: Creates unified datasets that can be queried by the AI layer to generate operational insights and outputs.



3.3 AI Model Infrastructure

- **Model Provider:** Anthropic (Claude API)

- **Models Used:** Claude Sonnet 4.5 and Claude Haiku 4.5 (task-dependent), or successor models with comparable or stronger controls
- **Deployment:** Anthropic-managed API infrastructure hosted in U.S. cloud regions (per provider documentation/contract)
- **Delivery Model:** SaaS

3.4 Provider Guardrails

Syyclops relies on the provider's documented safeguards (e.g., rules, testing, and monitoring intended to reduce harmful misuse), and implements additional platform-level controls and operational guardrails.

4. Enterprise Security & Compliance

4.1 Data Privacy Commitment

Syyclops processes Building Data solely to provide the service to the customer. Syyclops does not use Data to train foundation models. Building Data and Outputs remain the customer's information, subject to the parties' contract terms.

When data is sent to the Claude API for processing:

- Provider commitments may include non-training use of API data, and contractual controls regarding handling of prompts/outputs (as applicable to the customer's guidelines).
- **Zero Data Retention (ZDR)** may be available by addendum or configuration for sensitive workloads, subject to the provider's and customer's contractual election and technical eligibility.

4.2 Security Controls

Syyclops is designed to support enterprise security expectations, including:

- **Encryption**: encryption in transit (TLS) and encryption at rest where applicable
- **Access Control**: role-based access control, least privilege, and administrative controls
- **Authentication**: Built on OAUTH and MFA
- **Audit Logging**: logging for administrative actions and relevant usage events
- **Segregation**: logical separation of customer environments (implementation dependent)

4.3 Third-Party Certifications and Assurances

Where Syyclops leverages third-party providers, Syyclops may reference the provider's published certifications (e.g., SOC 2 Type II, ISO 27001) **to the extent applicable to the provider's services** and subject to the provider's scope statements and contractual documentation.

4.4 IT & Security Systems Integration

Syyclops is designed to integrate with common enterprise security tooling, including:

- **SSO**: OAUTH/MFA
- **Network Connectivity**: private connectivity options (e.g., PrivateLink/VPC endpoints), where supported
- **SIEM**: audit log export to customer SIEM, where configured
- **Compliance/Usage Reporting**: programmatic access to usage and audit data (where available)

4.5 Incident Response and Responsibility Allocation

Syyclops maintains security logging and operational monitoring appropriate to a SaaS deployment. Incident response responsibilities and notification timelines are governed by the

customer agreement and any applicable data processing/security addenda. Third-party providers maintain their own incident response programs for their services.

4.6 PHI/PII Exclusion and Permitted Data Use

Syyclops is not designed, marketed, or intended to process PHI or regulated personal data unless the parties expressly authorize it in a written addendum (e.g., a HIPAA BAA or equivalent). Absent such written authorization, Customer shall not provide PHI or other regulated sensitive data and represents that all data provided is limited to de-identified/non-sensitive building operations information, and Syyclops may apply minimization controls to prevent or restrict ingestion of prohibited data. Syyclops is not a clinical tool and may not be used for clinical decision-making or patient communications; any PHI/PII use would require a separately scoped deployment, documented controls, and executed addenda.

5. Summary

Syyclops provides an enterprise-oriented, embedded AI platform for building operations and maintenance with a focus on data privacy and security.

Key points:

1. **Enterprise Embedded AI:** built for building operations workflows and Authorized Users
2. **No Model Training on Building Data:** Building Data is not used for model training or improvement
3. **Security Controls:** encryption, access controls, logging, and enterprise integration support
4. **U.S. Deployment (Provider):** third-party LLM processing is performed via U.S.-hosted infrastructure per provider terms
5. **Customer Review Required:** Outputs are drafts/informational; customer remains responsible for verification and operational decisions

FAQs

Will vendor require on-site access to systems?

Answer: Yes, for Building Automation System (BAS) integration, we install a gateway device on-site. This device connects to the BAS using read-only BACnet/IP and creates trend data. The gateway communicates outbound only to the Syyclops cloud over TLS 1.2+. No inbound connections are required to your network.

Will vendor require remote access to the county systems?

Answer: Syyclops requires API access to cloud-based software systems such as your work order/CMMS system. This is standard cloud-to-cloud integration using authenticated REST APIs.

Syyclops does **not** require remote access (RDP, SSH, VPN) into your hardware systems, servers, or internal network infrastructure.

How will maintenance of the product occur?

Syyclops is a fully managed SaaS platform. Maintenance includes:

- Regular Updates: We push updates and improvements on a continuous basis with no action required from your IT team.

- Customer Feedback: We take customer feedback seriously and incorporate it into our development roadmap.

- Issue Resolution: We resolve reported issues as quickly as possible and push fixes promptly.

- Zero Downtime Deployments: New versions are deployed without service interruption.

Encryption Specs?

TLS Version: TLS 1.2 or higher is required for all connections. Legacy TLS versions (1.0, 1.1) are **not supported**.

Certificate Management: SSL/TLS certificates are managed via Let's Encrypt with automated renewal.

Load Balancer/Proxy: All traffic is terminated at HAProxy configured to enforce TLS 1.2+ with strong cipher suites.

Network Isolation: All services run within private networks; public endpoints are limited to the application layer.

Encryption at Rest

Standard: AES-256 encryption is used for data at rest.

Database & Storage: All persistent storage (databases, file storage, backups) is encrypted using AES-256.

Encryption Type	Specification
Data in Transit	TLS 1.2+ (legacy versions not supported)
Data at Rest	AES-256
Certificate Provider	Let's Encrypt (automated renewal)
Load Balancer	HAProxy with TLS 1.2+ enforcement