Cycode Security Considerations

How Cycode Ensures Your SaaS Security

Cycode is built with security-by-design principles to ensure customer data is protected at every stage of the software supply chain. Our architecture minimizes data exposure, enforces strict access controls, and gives customers full ownership of their sensitive assets.

Ephemeral Infrastructure for Initial Scans

When Cycode performs an initial baseline scan, all analysis runs on ephemeral compute infrastructure. These environments are created only for the duration of the scan and are destroyed after completion.

Cycode retains only non-sensitive metadata required for visibility and traceability, such as:

- Repository name and owner
- Code snippet identifiers
- Commit hash

No persistent scan infrastructure is maintained.

Minimal Data Retention

Cycode does not store or retain complete source code. Only the limited metadata required for findings, correlation, and auditability is retained. This significantly reduces data exposure and risk.

Bring Your Own Storage (BYOS)

Customers may choose to store all scan-related snippets and metadata in their own AWS S3 buckets, governed entirely by their internal security, compliance, and retention policies.

This ensures:

- Full customer ownership of data at rest
- Alignment with internal regulatory and audit requirements

Bring Your Own Encryption Key (BYOK)

Cycode supports customer-managed encryption using AWS Key Management Service (KMS). All secrets are encrypted using your own encryption keys.

Customers maintain complete control:

- Keys can be rotated at any time
- Deleting a key or S3 bucket immediately revokes Cycode's access to the encrypted data.
- Cycode also provides the ability to obfuscate all secrets or tokens; validity checking will not be available if this is enabled.

Cycode Broker (On-Prem / Private Assets)

For scanning private or on-prem assets (e.g., GitHub Enterprise Server, private SCMs, private container registries), Cycode provides a lightweight broker deployed within the customer's network.

The broker:

- Initiates outbound HTTPS (443) connections only
- Polls the Cycode SaaS platform for scan tasks
- Executes tasks locally (e.g., clone repository, collect artifacts)
- Sends only the required scan results and metadata back to Cycode

This ensures internal assets remain isolated and inaccessible from external networks.

Defense in Depth

Cycode employs a comprehensive defense-in-depth security model, including:

- Strong authentication and role-based access controls
- Network segmentation and isolation
- Continuous monitoring and auditing
- Secure secrets management and least-privilege access

All systems are designed and operated in accordance with industry best practices for SaaS security.