Codreum AWSPro

Security & Data Handling Overview

Public overview for security review and procurement | Full detail: AWSPro User Guide, Chapters 13-14

Document version	v1.0
Effective period	June 2026
Product baseline	AWSPro provider v1.0.x
Website	www.codreum.com

Audience: security reviewers, procurement, platform engineering, network engineering, cloud operations, and SRE teams.

1. Executive Security Summary

AWSPro runs entirely inside the customer AWS account. Customer network telemetry remains in that account, and the only data sent to Codreum is license-entitlement metadata used to validate access. Codreum does not receive DNS queries, VPC Flow records, log content, dashboard data, or metric values.

Security position at a glance

Area	Position
Telemetry location	CloudWatch Logs and CloudWatch Metrics in the customer AWS account.
Outbound data to Codreum	License-entitlement metadata only for Premium license validation.
AI processing	Optional; invoked from the customer account using Amazon Bedrock access in that account.
Config Builder	Client-side browser tool; imported configuration is parsed locally and not uploaded.
Removal	terraform destroy removes AWSPro-created resources; customer log groups and telemetry remain untouched.

2. Where AWSPro Runs

AWSPro is a Terraform provider that creates monitoring resources in the customer AWS account. These resources include CloudWatch dashboards and alarms, an SNS alert topic, IAM roles, and, where used, Lambda functions for the VPC Flow normalizer, AI custom widgets, and license status.

AWSPro reads telemetry that the customer already collects from CloudWatch Logs and CloudWatch Metrics in the same account. It does not capture network traffic, install agents, or copy telemetry to Codreum or to an external SaaS platform.

3. License Validation and Outbound Data

Premium deployments run a small license-status Lambda in the customer AWS account. The Lambda calls Codreum's license endpoint, https://api.codreum.com/api/license/validate, every 4 hours. Basic Lite deployments make no license-validation calls. The validation request carries entitlement metadata only.

Data sent to Codreum compared with data that is never sent

Sent to Codreum	Not sent - ever
Your AWS account ID	DNS queries or query-log content
License ID and license type, such as awspro or basic	VPC Flow records
Licensed VPC IDs and hosted-zone IDs	Metric values or dashboard data
Nothing else	Logs of any kind

4. AI Insights and Amazon Bedrock

- In-account. Bedrock is invoked by an AWSPro Lambda under an IAM role in the customer AWS account, using the customer's Bedrock access. Codreum does not run the model and never receives prompts or responses.
- In-region by default. The Bedrock region defaults to the deployment region. Data does not cross a region boundary unless the customer overrides the region setting.
- Data minimization. Raw logs are excluded from prompts by default. Analysis uses summarized metric and alarm context. Guided mode makes no model calls.

5. Encryption and Secrets

- The license ID is marked sensitive in Terraform and does not print in plan or apply output.
- SNS encryption is supported through a customer-managed KMS key using sns_kms_master_key_id.
- No long-lived Codreum credentials are stored in the customer AWS account. AWS credentials are used at apply time, and in-account IAM roles are used at run time.

6. Least Privilege and AWS Account Boundaries

Boundary	Description
Can	Read the telemetry sources the customer points it at and create AWSPro monitoring resources in the customer account. AWSPro Lambda functions run under tightly scoped IAM roles created for their purpose.
Cannot	Modify VPCs, security groups, route tables, or workloads; capture packet data; or send customer telemetry outside the customer AWS account.

7. Config Builder Data Handling

The browser-based Config Builder has no backend, database, or API. Imported configurations, including VPC IDs, AWS account numbers, and license IDs, are parsed locally and never uploaded. Saved drafts remain only in the user browser storage.

8. Operational Removal and Customer Control

AWSPro-created resources can be removed through the customer Terraform workflow. Running terraform destroy removes resources created by AWSPro. Customer log groups, telemetry, and underlying AWS network resources are not deleted by AWSPro.

9. Security Review Summary

Bottom line for security review

Telemetry stays in the customer AWS account. License validation sends entitlement metadata only every 4 hours from an inspectable in-account Lambda. AI features are optional, in-account, and in-region by default, with raw logs excluded from prompts. Terraform removal does not delete customer log groups or telemetry sources.

10. Questions and Reference Documentation

Questions: www.codreum.com/contact.html

Full documentation: www.codreum.com/docs.html