

COREDGE

CCP Datasheet
Cirrus Cloud Platform

Datasheet

Hyper-Scaler Grade Cloud Management Platform for Sovereign and Enterprise Cloud

Version 1.0

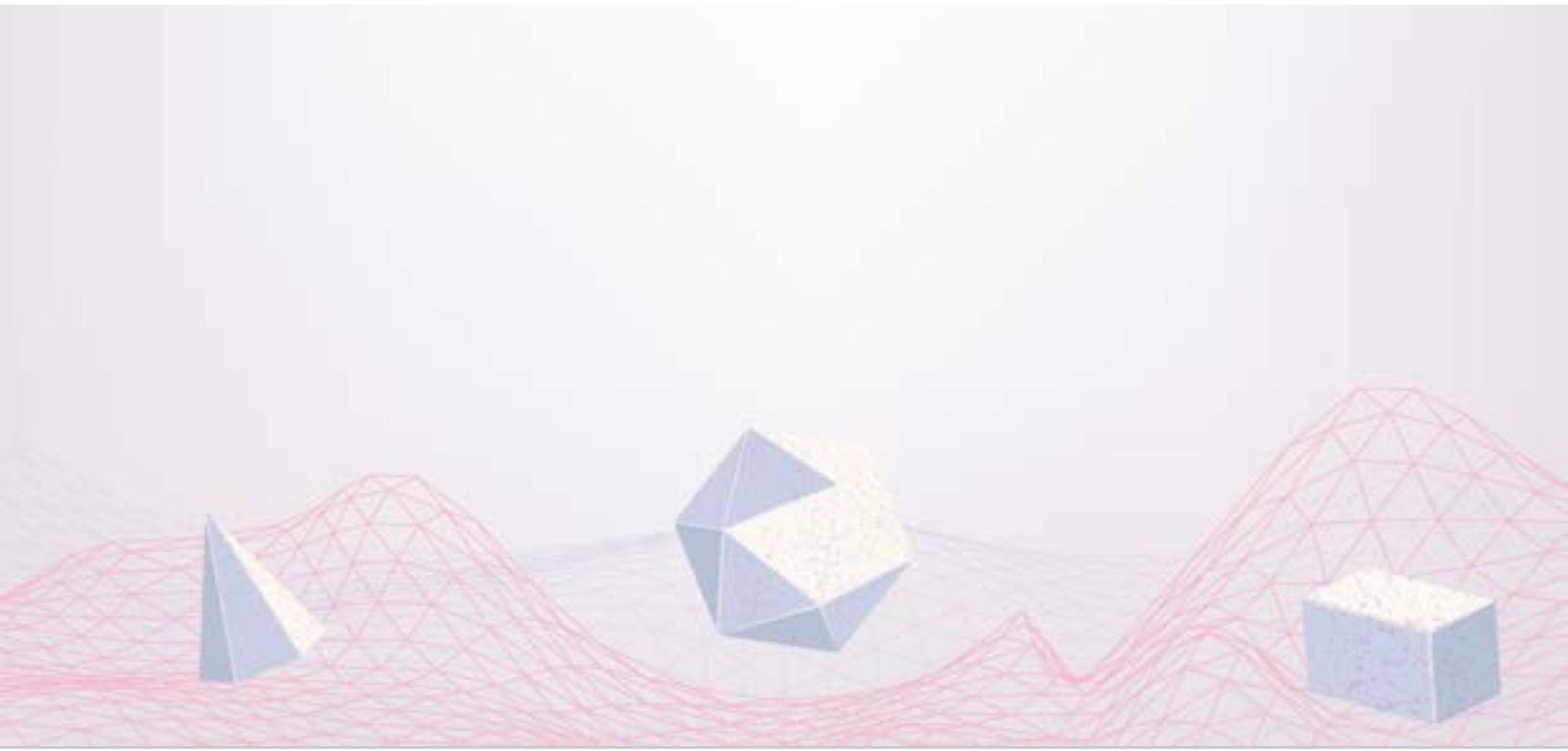
Contents

Platform Overview 3

Use Cases 4

Key Features 5

Key Benefits 6



Enterprise and sovereign cloud deployments demand self-service provisioning, strict multi-tenant isolation, high availability across availability zones, and unified governance over compute, storage, networking, and security. Traditional cloud management tools either lack the depth required for regulated environments or fail to deliver the operational simplicity that modern cloud teams expect.

Cirrus Cloud Platform (CCP)is built to address this gap — delivering hyper-scaler grade cloud management for sovereign, enterprise, and service provider environments ith full lifecycle automation, centralized governance, and a self-service portal that scales to thousands of VMs and pods.

Platform Overview

CCP is an enterprise Cloud Management Platform developed by Coredge, delivering hyper-scaler grade self-service capabilities for IaaS, PaaS, and SaaS workloads. The platform is composed of three primary layers:



Access Layer — Self-Service Portal, Admin Console, REST API Gateway



Control Plane — Workflow Orchestrator, IAM Engine (Keycloak), AuthZ Engine (OpenFGA), Metering & FinOps, Monitoring (Zabbix, Prometheus)



Data Plane — OpenStack IaaS, Cloud Orbiter Kubernetes Orchestrator, NetApp Storage, Bare Metal (MaaS)

CCP organizes resources in a three-level hierarchy:

Tenant	Top-level boundary, one per customer account Isolated
Project	project or environment
Resources	Cloud services consumed within a Project

Quota is enforced at both Tenant and Project level. Combined with Cirrus Cloud Platform (IaaS Orchestrator) and Cloud Orbiter (Kubernetes Orchestrator), CCP provides a unified platform for internal operations teams and end customers — enabling self-service provisioning, centralized governance, and optimized cloud spend through a single portal.

Use Cases

1



Sovereign Cloud for Government

National and government organizations require complete data sovereignty, air-gapped deployment options, and compliance with local data residency regulations. CCP delivers a sovereign cloud platform with per-tenant Keycloak realm isolation, SAML 2.0 federation with Microsoft ADFS and Entra, AES-256 encryption at rest, and mTLS in-transit — purpose-built for critical national infrastructure.

2



Enterprise Private Cloud

Large enterprises in regulated industries — finance, healthcare, and energy — need a private cloud with the self-service convenience of a public cloud, without sacrificing control. CCP provides on-demand VM, container, bare metal, storage, and networking provisioning with full RBAC governance, audit trails, and policy-based quota enforcement, all deployed on enterprise-owned infrastructure.

3



Managed Cloud Services for Telecom & Service Providers

Telecom operators and managed service providers need a multi-tenant platform to offer cloud services to multiple customers from shared infrastructure. CCP's multi-tenant IAM, metering, showback, and quota management enable providers to deliver IaaS and PaaS as a service — with per-tenant billing, notional invoicing, and full spend visibility — at national scale.

Key Features



Self-Service Provisioning Portal

A unified self-service portal for end users and administrators to provision and manage the full service portfolio — VMs, containers, bare metal, storage, networking, databases, and security services — with no manual intervention from the operations team. Admin Console handles platform-level governance, quota management, and tenant lifecycle.



Multi-Tenant IAM & RBAC

Keycloak based identity management with per-tenant realm isolation, SAML federation, and pre-defined RBAC roles across Tenant and Project levels. OpenFGA handles fine-grained authorization at every API boundary. Supports Microsoft ADFS, Microsoft Entra, and any SAML compatible enterprise identity provider.



High Availability Architecture

Self-service and admin console for end users, tenants, and cloud administrators. Provision VMs, storage, networking, containers, databases; manage projects and users. Manage tenants, quotas, catalogs, providers, and infrastructure health.



Metering, FinOps & Quota Management

Built-in metering engine tracks resource consumption at the Tenant and Project level in real time. Showback reporting, notional invoicing, and policy-based quota enforcement give finance and operations teams complete visibility into cloud spend.



Zero Trust Security

Defense-in-depth security model with mTLS encryption in transit. Per-tenant Keycloak realm isolation, SAML 2.0 federation, and integration with enterprise identity providers (Microsoft ADFS, Entra, Zscaler VPN) ensure that no action is trusted by default.

Key Benefits



Automated Lifecycle Management

From tenant onboarding to resource provisioning — fully automated. Self-service portal eliminates manual ticketing and operations team involvement. Provision > operate > monitor > bill without human intervention in the data path.



Hyper-Scaler Grade Scale

Scales to thousands of VMs and pods on a single platform. Add worker nodes on demand as workloads grow. Horizontally scalable architecture with no rearchitecting required to expand capacity.



Sovereign & Compliance-Ready

Purpose-built for environments where data sovereignty, regulatory compliance, and audit trails are non-negotiable. Per-tenant isolation at the identity, network, and data layer. Full audit logging across all API actions for compliance reporting.



Unified Control Plane

A single management plane across all regions and availability zones. No separate consoles for compute, storage, network, or security — all managed through one portal with consistent RBAC and audit trail. Reduces operational complexity and training overhead for cloud operations teams.



Optimized Cloud Spend

Policy-based quota enforcement at Tenant and Project level prevents runaway spend. Showback and notional invoicing give finance teams visibility into cost allocation without requiring a separate FinOps tool. Usage data feeds directly into the Portal for automated customer billing.



Enterprise-Grade Security by Default

mTLS in-transit and AES-256 at-rest are applied platform-wide — not optional add-ons. Zero-trust authorization via OpenFGA ensures least-privilege access at every API boundary. Per-tenant identity realm isolation prevents cross-tenant data leakage even on shared infrastructure.

Get in touch with us

https://coredge.io

info@coredge.io