Bedrock CMMC

Security Practices Guide

How We Protect Your Data

Public Document

Foxx Cyber LLC
foxxcyber.com
Version 1.0 | March 2026

Executive Summary

Bedrock CMMC is a cloud-hosted compliance management platform built by Foxx Cyber LLC to help defense contractors and organizations navigate the Cybersecurity Maturity Model Certification (CMMC) process. We built it because we needed it ourselves — and we believe the tools that protect sensitive data should be held to the same standard as the data they protect.

This document explains the security measures we've implemented to safeguard your data on our platform. Whether you're evaluating Bedrock CMMC for your organization or you're already a customer, this guide provides transparency into how we operate, what we protect, and why you can trust us with your most sensitive compliance data.

Key Takeaways

- **CMMC Level 2 compliant** — 110 security practices implemented across 14 control domains, aligned to NIST SP 800-171 Rev. 2.
- **FedRAMP Moderate infrastructure** — hosted on AWS with FedRAMP Moderate inherited controls.
- **Encryption everywhere** — TLS 1.2/1.3 in transit, AES-256 (KMS) at rest. No exceptions.
- **Zero-trust architecture** — no implicit trust between components; every service authenticates via IAM roles.
- **Serverless & immutable** — no servers to patch, no SSH access, read-only containers, infrastructure-as-code.
- **Continuous monitoring** — GuardDuty threat detection, CloudTrail audit logging, Security Hub compliance scoring, 365-day log retention.

Your Data on Bedrock CMMC

When you use Bedrock CMMC, you upload compliance documentation, security artifacts, evidence of control implementation, and organizational details. This data may include system security plans, policies, procedures, risk assessments, and audit evidence — the kind of material that describes your organization's security posture in detail.

We recognize the sensitivity of this information. An attacker with access to your compliance documentation would have a roadmap to your security gaps. That's why we don't treat customer data casually.

How We Classify Your Data

All customer data on Bedrock CMMC is treated as CUI regardless of its formal designation. This means:

- Access is restricted to authenticated, authorized users with a legitimate need.
- Data is encrypted in transit and at rest using FIPS-validated cryptographic modules.
- All access is logged and auditable.
- Data isolation is enforced at the application and database layer — your data is never comingled with another organization's data.

Data Isolation

Every database query is scoped by your organization's unique identifier. There is no shared data pool. Your compliance artifacts, evidence files, and assessment data are logically isolated from every other customer on the platform. Evidence files are stored in dedicated S3 storage with server-side encryption and versioning — accidental deletion or overwrite is recoverable.

Platform Architecture

Bedrock CMMC runs on Amazon Web Services (AWS) in the us-east-1 region. AWS holds a FedRAMP Moderate authorization, which means the underlying physical infrastructure, hypervisors, and network fabric are already assessed and authorized to handle CUI-level data.

On top of that foundation, we've built a purpose-designed architecture with defense-in-depth at every layer.

Network Security

The platform operates within a Virtual Private Cloud (VPC) with a three-tier subnet architecture:

- **Public tier** — contains only the Application Load Balancer (ALB), the sole entry point from the internet. No application servers or databases are internet-accessible.
- **Application tier** — runs containerized services on AWS Fargate. These containers have no direct internet access.
- **Data tier** — hosts the Aurora PostgreSQL database. This tier has no internet access whatsoever.

Security groups enforce a deny-all-by-default posture. Traffic is allowed only on specific ports between specific tiers. Internal AWS service calls travel through VPC endpoints — private connections that never touch the public internet.

Compute Security

We run on AWS Fargate, a serverless container platform. This is a deliberate architectural choice:

- **No servers to manage or patch** — AWS manages the underlying host infrastructure.
- **Microvm isolation** — each container task runs in its own Firecracker microVM.
- **Non-root execution** — containers run as UID 1001, never root. Privilege escalation is disabled.
- **Read-only filesystem** — the container root filesystem is immutable.
- **Minimal base image** — Alpine Linux 3.21, stripped to minimum required packages.

Database Security

Customer data is stored in Aurora PostgreSQL Serverless v2:

- Encryption at rest with a customer-managed KMS key (AES-256), auto-rotated annually.
- Encryption in transit enforced — TLS is mandatory for all database connections.
- Access exclusively through RDS Proxy with IAM authentication — no database passwords stored anywhere.

- 35-day automated backup retention with point-in-time recovery.
- No public accessibility — the database exists only within private data subnets.

Encryption

Encryption is non-negotiable on Bedrock CMMC. Every byte of customer data is encrypted.

In Transit

- TLS 1.2 minimum, TLS 1.3 preferred, for all external connections.
- HTTP is never accepted — all requests are redirected to HTTPS.
- Internal service-to-service communication is encrypted via ECS Service Connect.
- Database connections are encrypted with mandatory TLS.
- AWS API calls travel through encrypted VPC endpoints (PrivateLink).

At Rest

- Aurora PostgreSQL: AES-256 encryption via KMS customer-managed key.
- S3 evidence storage: Server-side encryption with KMS (SSE-KMS), versioning enabled.
- S3 audit logs: SSE-KMS encryption with Object Lock (WORM) — logs cannot be modified or deleted.
- Secrets Manager: All credentials and API keys encrypted with KMS.
- CloudWatch Logs: Encrypted with KMS, retained for 365 days.

Access Control

Access to Bedrock CMMC is governed by the principle of least privilege at every level.

Human Access

- All administrative access through AWS IAM Identity Center (SSO) with mandatory MFA.
- No long-lived access keys. Session tokens expire and require re-authentication.
- Role-based access control (RBAC) ensures users only see what their role permits.
- No SSH, RDP, or direct management ports exposed on any production resource.

Multi-Factor Authentication (MFA)

Every user on Bedrock CMMC is required to use multi-factor authentication — no exceptions. This applies to all roles: customers, administrators, and external assessors.

- **MFA is mandatory at login** — users must provide a TOTP code from an authenticator app in addition to their credentials.
- **Compatible with any standard authenticator** — Google Authenticator, Microsoft Authenticator, Authy, 1Password, and any TOTP-compliant app.

- **Infrastructure access is also MFA-protected** — all AWS administrative access requires MFA.
- **No SMS-only fallback** — SMS is not supported as a sole MFA factor due to SIM-swapping vulnerabilities.

> ***Why MFA Matters:*** *Compromised passwords are the leading cause of unauthorized access. MFA ensures that even if a password is stolen, an attacker cannot access the platform without physical possession of the user's authentication device.*

Service Access

- Each container service has a dedicated IAM role with minimum permissions.
- CI/CD via OpenID Connect (OIDC) federation — no stored AWS credentials.
- Database access brokered through RDS Proxy with IAM authentication.

Application Access

- Users authenticate via HTTPS and receive time-limited JWT tokens.
- Sessions expire after 8 hours, with a 15-minute inactivity timeout.
- All API endpoints enforce authorization checks; admin functions gated by role.

Monitoring, Logging & Incident Response

Security is continuous practice. Bedrock CMMC is instrumented for comprehensive visibility.

What We Monitor

- **AWS CloudTrail** — records every API call with log file integrity validation.
- **Amazon GuardDuty** — continuously analyzes CloudTrail, VPC Flow Logs, and DNS logs for malicious activity.
- **AWS Security Hub** — aggregates compliance findings and scores posture against industry benchmarks.
- **AWS Config** — evaluates resource configurations against 50+ FedRAMP Moderate conformance rules.
- **VPC Flow Logs** — captures all network traffic metadata for forensic analysis.
- **CloudWatch Logs & Alarms** — 365-day retention, metric filters, and automated alerts.

Audit Trail Integrity

Audit logs are stored in a dedicated S3 bucket with Object Lock (Write Once, Read Many). Once written, these logs cannot be modified, overwritten, or deleted — even by administrators. This ensures a tamper-proof record for investigations and compliance evidence.

Incident Response

Foxx Cyber LLC maintains a documented Incident Response Plan that defines roles, escalation paths, containment procedures, and communication protocols. We conduct quarterly tabletop exercises and review the plan annually. If a security event affects customer data, we are committed to transparent and timely notification.

Infrastructure as Code & Change Management

The entire Bedrock CMMC production environment is defined in AWS CloudFormation templates — 10 stacks covering networking, compute, database, storage, security services, monitoring, and access management. There are no manual console configurations.

This approach provides:

- **Reproducibility** — the environment can be rebuilt identically from code at any time.
- **Auditability** — every infrastructure change is a tracked code commit with peer review.
- **Drift detection** — AWS Config alerts on any resource that deviates from its defined state.
- **Rollback capability** — failed deployments automatically revert to the previous known-good state.

Compliance Posture

CMMC Level 2

Bedrock CMMC implements all 110 CMMC Level 2 security practices across 14 control domains. These practices are documented in domain-specific policies and procedures, with technical evidence maintained for each control. Our compliance posture is continuously monitored through AWS Security Hub and AWS Config conformance packs.

NIST SP 800-171 Rev. 2

CMMC Level 2 maps directly to NIST SP 800-171 Rev. 2. Our System Security Plan (SSP) documents how each of the 110 security requirements is satisfied through implemented controls, inherited AWS capabilities, or documented plans of action.

FedRAMP Moderate Inheritance

AWS's FedRAMP Moderate authorization provides a baseline of inherited controls covering physical security, hypervisor security, network infrastructure, and service availability. Of the 110 CMMC practices, 21 are fully inherited from AWS, 79 are shared responsibility, and 10 are fully managed by Foxx Cyber LLC.

Category	Count	Description
AWS Inherited	21	Physical security, hypervisor, global infrastructure
Shared Responsibility	79	AWS provides infrastructure; Foxx Cyber configures and operates
Customer Only	10	Policies, training, personnel security, risk assessment

Why Trust Bedrock CMMC

We don't ask for your trust blindly. We earn it through transparency, rigor, and accountability.

- **We eat our own cooking.** Bedrock CMMC is built to the same CMMC Level 2 standard we help our customers achieve. Our own compliance documentation lives on the platform.
- **We treat your data as CUI.** Regardless of formal designation, every piece of customer data receives the full protection of NIST 800-171 controls.
- **We don't cut corners on architecture.** Serverless compute, private subnets, deny-all networking, KMS encryption, immutable audit logs — these aren't marketing bullet points, they're how the system actually works.
- **We document everything.** Our ATO package includes a complete SSP with all 320 assessment objectives, 14 domain policies, 14 procedure sets, a Plan of Action & Milestones, and continuous monitoring evidence.
- **We're transparent.** This document exists because we believe you deserve to know exactly how your data is protected.

Foxx Cyber LLC | foxxcyber.com | support@foxxcyber.com