Security & Compliance Overview

Revive AI - Customer Win-back Platform

Executive Summary

Revive AI is built on **AWS's SOC 2 and ISO 27001 certified infrastructure**, providing enterprise-grade security for customer data. Our architecture leverages AWS managed services to inherit compliance certifications and implement security best practices from day one.

Current Status: Functional prototype
Production Timeline: 2 weeks for full security implementation
Compliance: GDPR-ready, SOC 2 path, HIPAA-eligible

Security Architecture

Data Encryption

- **At Rest:** AES-256 encryption via AWS S3 (enabled in production)
- **In Transit:** TLS 1.3 via HTTPS (CloudFront + API Gateway)
- **Keys:** AWS-managed keys (upgradeable to customer-managed KMS)

Authentication & Access Control

- **Identity Provider:** AWS Cognito
  - Multi-factor authentication (MFA)
  - Password policies enforcement
  - SSO integration (SAML/OIDC for enterprise)
- **Data Isolation:** Per-user S3 prefixes with IAM policies
- **Principle of Least Privilege:** Resource-level IAM permissions

Audit & Monitoring

- **CloudTrail:** Full audit log of all API calls
- **CloudWatch:** Real-time monitoring and alerts
- **GuardDuty:** Automated threat detection
- **Retention:** 90-day log retention (configurable)

Network Security

- **API Gateway:** AWS WAF for DDoS protection
- **Serverless Architecture:** No exposed servers or databases
- **VPC:** Optional private networking for enterprise customers

Privacy & Compliance

GDPR Compliance

Data Processing Agreement: AWS GDPR-compliant DPA
Data Residency: EU region deployment (eu-west-1) available
Right to Access: Data export API
Right to Deletion: 72-hour deletion SLA
Privacy by Design: Minimal data collection
Consent Management: User consent tracking

Data Protection

- **PII Handling:** Encrypted storage, access logging, automatic deletion
- **Data Retention:** Active subscription period + 30 days
- **Third-party AI:** AWS Bedrock (data NOT used for training)
- **No Data Sharing:** Customer data never sold or shared

Certifications & Standards

Certification	Status	Timeline
AWS SOC 2 (inherited)	Active	Immediate
AWS ISO 27001 (inherited)	Active	Immediate
GDPR Compliance	In Progress	2-3 weeks
SOC 2 Type II (own)	Planned	6-12 months
HIPAA (optional)	Available	2-4 weeks

AI Data Privacy

AWS Bedrock Guarantees

No Training on Customer Data: AWS does not use prompts or outputs for model training
No Data Retention: Prompts and outputs are not stored by AWS
Regional Processing: Data processed within selected AWS region
HIPAA Eligible: With Business Associate Agreement (BAA)
Enterprise Ready: Built for compliance from day one

Why Bedrock vs OpenAI?

Feature	AWS Bedrock	OpenAI API
Training opt-out	Automatic	Manual request
Data residency	AWS region choice	US-only
HIPAA eligible	Yes	No
SOC 2 inherited	Yes	Partial
Enterprise DPA	Included	Separate

Architectural Decision: We chose AWS Bedrock specifically for enterprise compliance requirements.

Security Roadmap

Phase 1: MVP Security (Week 1-2)

Status: Ready to implement
Timeline: 2 weeks
Cost: <$10/month

- ☒ S3 bucket encryption (AES-256)
- ☒ HTTPS via CloudFront with SSL/TLS
- ☒ AWS Cognito authentication
- ☒ Data isolation per user
- ☒ Privacy policy deployment
- ☒ AWS DPA signed

Deliverable: Production-ready for first customers

Phase 2: Production Hardening (Month 1-2)

Status: Planned
Timeline: 4-6 weeks
Cost: $20-50/month

- ☐ CloudTrail audit logging enabled
- ☐ Data deletion API (GDPR compliance)
- ☐ AWS WAF protection
- ☐ CloudWatch alerting
- ☐ Penetration testing
- ☐ Security documentation
- ☐ Incident response plan

Deliverable: General availability release

Phase 3: Enterprise Ready (Month 3-6)

Status: Roadmap
Timeline: 6-12 months
Cost: $100-500/month + audit fees

- ☐ SOC 2 Type II audit ($15-30k)
- ☐ SSO integration (SAML/OIDC)
- ☐ VPC deployment
- ☐ Customer-managed encryption keys
- ☐ Advanced threat detection
- ☐ DDoS protection (AWS Shield)
- ☐ Annual penetration testing

Deliverable: Enterprise sales ready

Cost Analysis

Monthly Operating Costs

Component	Free Tier	Production Cost
S3 Encryption	Included	$0
CloudFront (HTTPS)	1TB free	$1-5
Cognito Auth	50k users	$0-10
CloudTrail Logs	First trail free	$5
GuardDuty	30-day trial	$10-20
Total Monthly	**~$0**	**$10-50**

One-time Costs

- Privacy policy (template): **$0-1,000**
- Security implementation: **40-60 developer hours**
- SOC 2 audit (optional): **$15-30k**

Comparison: Enterprise SaaS alternatives cost $200-2000/month. We achieve enterprise-grade security at startup prices.

Security Best Practices

What We Do

Encryption at rest and in transit
Multi-factor authentication
Principle of least privilege IAM

Regular security audits
Automated threat detection
Incident response procedures
Data backup and recovery
Security awareness training

What We Don't Do

Store payment information (use Stripe if needed)
Collect unnecessary PII
Share data with third parties
Use customer data for AI training
Allow weak passwords
Ignore security vulnerabilities

Risk Assessment

Low Risk

No Database: Serverless architecture eliminates SQL injection
Managed Services: AWS handles patching and updates
No Server Access: No SSH, no OS-level vulnerabilities
Automated Backups: S3 versioning and replication

Medium Risk (Mitigated)

IAM Misconfiguration: Audited and tested policies
API Exposure: Rate limiting and WAF protection
Cost Overruns: CloudWatch billing alerts

Minimal Attack Surface

- No exposed servers or databases
- All services behind AWS authentication
- Automated security patching via managed services
- DDoS protection via CloudFront

Audit & Compliance Verification

Available Documentation

- AWS Well-Architected Framework assessment
- Data flow diagrams
- IAM policy documentation
- Incident response procedures

- Privacy policy and Terms of Service
- AWS DPA and service agreements

Third-party Verification

- AWS Artifact (SOC 2/ISO reports)
- Penetration testing reports (upon request)
- CloudTrail audit logs
- Compliance attestations

For Enterprise Customers

Security Deep Dive Available

We provide detailed security reviews including: - Architecture diagrams and threat models - Compliance documentation - Penetration test results - Data processing agreements - Custom security controls (per requirement)

Custom Deployments

For customers with specific requirements: - **Dedicated VPC:** Isolated network environment - **Customer-managed Keys:** BYOK encryption - **Private Endpoints:** VPC PrivateLink - **Custom Regions:** Deploy in your preferred AWS region - **On-premises:** AWS Outposts for hybrid deployment

Contact

For security inquiries or enterprise compliance discussions: - Email: security@[yourdomain].com - Schedule security review call - Request SOC 2 roadmap documentation

---

Key Differentiators

Why Revive AI is Enterprise-Ready

1. **AWS Bedrock vs OpenAI**
   - No data training on customer prompts
   - HIPAA-eligible with BAA
   - Regional data processing
2. **Serverless Architecture**
   - Smaller attack surface
   - Automatic scaling and patching
   - Inherits AWS security certifications
3. **Security-First Design**
   - Compliance roadmap from day one

- Following AWS Well-Architected Framework
- Clear path to SOC 2 certification

4. **Cost-Effective Compliance**
   - Enterprise security at startup prices
   - No dedicated security team required
   - Leverage AWS managed services

References & Resources

AWS Security Documentation

- AWS Well-Architected Framework
- AWS Bedrock Security
- AWS Compliance Programs
- GDPR on AWS

Industry Standards

- SOC 2 Overview
- GDPR Official Text
- NIST Cybersecurity Framework

AWS Service Terms

- Bedrock AI Service Terms
- AWS Data Processing Addendum

Compliance Checklist

Before First Customer

☐ Enable S3 encryption
☐ Deploy CloudFront HTTPS
☐ Implement Cognito authentication
☐ Deploy privacy policy
☐ Sign AWS DPA
☐ Security testing completed

Before General Availability

☐ CloudTrail logging enabled
☐ Data deletion API deployed
☐ Penetration testing completed
☐ Incident response plan documented
☐ Terms of Service reviewed by legal

☐ Customer DPA template created

Before Enterprise Sales

☐ SOC 2 Type II initiated
☐ SSO implemented
☐ VPC deployment available
☐ Security documentation complete
☐ Reference customers available

Last Updated: 2025-10-10
Document Version: 1.0
Contact: For questions about this document, contact the security team.

This document provides an overview of Revive AI's security and compliance posture. For detailed technical specifications or enterprise security reviews, please contact our team.