Alder

SECURITY WHITEPAPER

Security at Alder

An overview of Alder's approach to security, privacy, and trust.

PUBLISHED BY
Viridian Technologies, LLC

CONTACT
security@getalder.com

VERSION
April 2026

CONTENTS

In this document

An overview of how Alder is designed, deployed, monitored, and operated — written so security and procurement teams can evaluate us with confidence.

SECTION 01

Introduction

Alder is built and operated by Viridian Technologies, LLC. We know that when you entrust your documents and customer data to a SaaS platform, you are also entrusting the team behind that platform to protect it, and we take that responsibility seriously.

This document explains how Alder is designed, deployed, monitored, and operated, so that your security and procurement teams can evaluate us with confidence. The controls described here are implemented today in infrastructure-as-code and continuously enforced, not aspirational. Where a specific control is still being formalized, we say so plainly.

If you have security questions that aren't answered here, please contact **security@getalder.com**.

SECTION 02

Infrastructure Overview

Hosting

Alder runs entirely on **Amazon Web Services (AWS)** in the United States, with global edge acceleration provided by Amazon CloudFront. AWS is responsible for the physical security of its data centers, the underlying network fabric, the hypervisor, and the host operating system under the AWS Shared Responsibility Model. AWS's own security program is independently audited (SOC 1 / SOC 2 / SOC 3, ISO 27001, PCI DSS Level 1, FedRAMP, and more). We are responsible for how we configure and use those services, and that's what the rest of this document describes.

Network Architecture

All of Alder's production compute and data resources run inside a dedicated **Virtual Private Cloud (VPC)** isolated from the public internet. Traffic is segmented into public and private subnets across multiple Availability Zones:

- **Public subnets** hold only load balancers and NAT gateways. No application servers, databases, caches, or secrets are ever placed on a public subnet.
- **Private subnets** hold all application workloads, data stores, and any administrative infrastructure. These have no public IP addresses and cannot be reached from the internet.

Traffic flow is controlled by **Security Groups** that reference other Security Groups (not raw IP ranges), so access is defined in terms of "the API can talk to the database," not "these IPs can." The default VPC Security Group is closed and monitored by AWS Config. All egress to the public internet flows through NAT gateways.

Compute

Alder's API and background workloads run as containerized services orchestrated by **Amazon Elastic Container Service (ECS)**. Tasks run in isolated containers with no shared filesystem or process namespace. We build our container images from minimal, modern Linux base images and rebuild them on every deploy, so OS-level packages are refreshed frequently by default.

Static application assets (the single-page application) are served from an origin-access-controlled private S3 bucket fronted by CloudFront. The S3 bucket itself is not reachable directly from the internet.

SECTION 03

Data Security

Data Location

All customer data is stored in the United States. CloudFront caches static, non-sensitive assets at edge locations worldwide, but dynamic API traffic and all persistent customer data remain within the US.

Encryption at Rest

All customer data is encrypted at rest using **AES-256** via the **AWS Key Management Service (KMS)**, using a dedicated **Customer-Managed KMS Key (CMK)** with **annual automatic key rotation** enabled. The CMK is backed by FIPS 140-2 Level 3 validated hardware security modules operated by AWS.

This applies uniformly to every data store Alder uses, including:

- Primary databases and their automated backups
- Caches and background-job queues
- Object storage for customer uploads
- Application secrets and configuration
- Centralized application and infrastructure logs
- Block storage volumes
- Container images

Audit-log stores (CloudTrail, AWS Config, VPC Flow Log cold archive, WAF logs) are encrypted with **separate, dedicated CMKs**, so the keys that protect evidence of activity on the platform are not the same as the keys that protect production data. This means a compromise of any one key cannot be used to both access customer data and tamper with the record of that access.

Encryption in Transit

Every network boundary in Alder uses TLS:

- **Browser / API client to Alder:** TLS 1.2 minimum, TLS 1.3 preferred, using modern cipher suites with forward secrecy. HTTP requests are redirected to HTTPS, and HSTS is set on every response so that compliant browsers never issue a plaintext request after the first visit.
- **CloudFront to origin:** HTTPS only; origin-access-controlled to prevent bypass of the CDN.
- **Application to database:** the database server rejects unencrypted connections at the protocol level, and the application verifies both the certificate chain and the hostname on every connection using Amazon's root CA bundle. This prevents man-in-the-middle attacks even inside the VPC.
- **Application to cache and queue layer:** TLS required end-to-end, with an authenticated connection string.
- **Application to object storage:** bucket policies deny any request not made over TLS.
- **Operators to infrastructure:** AWS Systems Manager Session Manager (TLS).

Passwords and User Authentication

User passwords are hashed and salted with **Argon2**, a modern, memory-hard password hashing function recommended by OWASP for new applications. Plaintext passwords are never stored, logged, or retrievable by anyone at Alder. If you forget your password, you must reset it via an emailed, single-use token.

Alder supports **multi-factor authentication (MFA)** natively. Users can enroll a TOTP authenticator app (Google Authenticator, 1Password, Authy, etc.), and once MFA is enabled, a valid one-time code is required for every login. MFA enrollment, verification, and disable flows are all first-class endpoints in the authentication service.

Session tokens are delivered as `HttpOnly`, `Secure`, `SameSite` cookies, which prevents JavaScript from reading them and mitigates cross-site request forgery. Sessions use short-lived access tokens (2 hours) combined with longer-lived refresh tokens; refresh tokens are individually revocable, and logout revokes both the access and refresh tokens server-side.

Multi-Tenancy

Alder is a multi-tenant SaaS application. Every authenticated request carries a signed account identifier derived from the session token, and the API layer applies that identifier as a scoping

constraint on every data access: every database query, every storage-object key, and every cache lookup. The frontend cannot issue a request that crosses account boundaries; tenant scoping is enforced server-side, on the trusted side of every API call.

Backups, Recovery, and Business Continuity

- **Database backups and recovery:** automated backups with **Point-in-Time Recovery (PITR)** allow the database to be restored to any second within the backup retention window, yielding an effective Recovery Point Objective (RPO) of approximately 5 minutes.
- **High availability:** The production database runs in a **Multi-AZ** configuration. A synchronous standby is maintained in a second Availability Zone, and AWS automatically fails over to the standby if the primary becomes unavailable.
- **S3 versioning:** Customer-data buckets have versioning enabled, so accidental deletes or overwrites are recoverable. Non-current versions transition to lower-cost storage tiers on a documented lifecycle.

Data Retention and Deletion

Customer data is retained for the life of your Alder subscription. On account termination, data is scheduled for deletion and fully purged from primary systems within 30 days. Backup copies are purged on a defined rolling retention window so that no residual copies of customer data persist beyond a bounded recovery period.

Audit-log data has stricter retention to support compliance and forensic investigation:

- **AWS CloudTrail (API activity):** 7 years, with S3 Object Lock in COMPLIANCE mode and log-file validation. Records cannot be modified or deleted, even by us, until their retention period expires.
- **VPC Flow Logs:** 30-day hot tier (CloudWatch) + 365-day cold archive (S3).
- **CloudFront access logs / WAF logs:** centralized in dedicated, KMS- encrypted audit buckets in a separate account boundary.

Secrets Management

Application secrets (database credentials, API keys for subprocessors, signing keys, etc.) are stored in **AWS Secrets Manager** or **SSM Parameter Store** (SecureString), encrypted with the Alder CMK. Secrets are injected into containers at runtime; they are never baked into images, committed to source control, or logged.

SECTION 04

Application Security

Development Practices

Alder's engineering team follows secure-development practices aligned with the **OWASP Top 10**. Our core defenses include:

- Parameterized queries via a type-safe data-access layer. We do not build SQL by string concatenation.
- Strict schema-based request validation on every API endpoint, with both inbound and outbound payloads checked against an explicit shape.
- Authentication and authorization enforced server-side on every protected route, with account-level tenant scoping applied at the data-access layer.
- HTTP security headers on every response, including Content Security Policy, HSTS, `X-Content-Type-Options`, and frame-options, applied both at the application layer and at the CDN edge.
- `HttpOnly`, `Secure`, `SameSite` cookies for session material.
- Rate limiting at the edge (AWS WAF) and inside the application.
- CORS restricted to Alder's own origins; credentialed requests only from approved origins.
- No unsafe deserialization paths; all inter-service messaging uses schema-validated JSON.
- Structured logging with explicit redaction of sensitive request headers (`Authorization`, `Cookie`, API keys, auth tokens) so that credentials cannot leak into centralized log storage.

Web Application Firewall

Every internet-facing Alder distribution (the application SPA, the API, and the marketing website) sits behind **AWS WAF** with AWS-managed rule groups enabled:

- Core Rule Set (OWASP-aligned)
- Known Bad Inputs
- SQL injection rules
- Linux / Unix rules
- Amazon IP Reputation list

- Anonymous IP list (VPN / Tor / hosting-provider ranges)
- Rate-based rule to throttle abusive clients

Every WAF Web ACL streams per-request logs to a centralized, encrypted audit bucket so that blocked and allowed activity is both observable and retained for forensic analysis.

Dependency and Image Security

- **Container image scanning:** every image pushed to our registry is scanned for known vulnerabilities on push.
- **Immutable image tags:** image tags cannot be overwritten, which prevents a class of supply-chain attacks where an attacker replaces a tag like `:latest` with malicious content.
- **GuardDuty Malware Protection:** AWS GuardDuty performs malware scans on findings involving our compute and S3 workloads.
- **Dependency updates:** we track and apply security updates to application dependencies on a regular cadence.

Change Management

- **Infrastructure as Code:** Alder's AWS infrastructure is defined in Terraform and version-controlled.
- **Deploy gates:** production releases go through an automated CI/CD pipeline with required pre-deploy checks. A failed check stops the release, which catches an entire category of regressions before they reach customers.
- **Federated deployment credentials:** the CI/CD system authenticates to AWS using short-lived, federated tokens scoped to a narrowly privileged IAM role. No static AWS credentials are stored by the CI/CD system or in source control.
- **Traceability:** every production change is recorded in AWS CloudTrail and correlated to a specific commit SHA via the deployed image tag.

SECTION 05

Access Control and Identity

Human Access

- **Scoped administrative access:** AWS administrative access is provisioned with narrowly scoped IAM policies following the principle of least privilege.
- **No SSH:** we do not run SSH on any server and do not expose port 22 anywhere. All interactive access to infrastructure, including database administration, goes through **AWS Systems Manager Session Manager**. Session Manager is TLS-encrypted, requires an authenticated IAM principal, and can be centrally logged.
- **Multi-Factor Authentication:** required for administrative console access, and enforcement is continuously monitored.
- **Password policy:** administrative password policies follow modern NIST guidance, with strong minimum length and reuse prevention.

Workload Access

Every Alder service runs under its own **IAM role**, with a policy scoped to only the exact resources and actions that service needs to operate. Wildcards are avoided, privilege escalation paths are closed off with conditional access controls, and no service can assume or act on behalf of another outside of the narrow patterns it requires.

Team Practices

All Alder personnel with access to production systems sign a confidentiality agreement before they are granted access, and production access is provisioned on the principle of least privilege. As the team grows, additional HR controls (including formal background checks prior to production access and a documented off-boarding checklist) are being rolled in as part of our SOC 2 readiness track.

SECTION 06

Monitoring, Detection, and Incident Response

Continuous Monitoring

Alder's infrastructure is watched by a layered set of AWS security services:

Service	What it watches
AWS CloudTrail	Every AWS API call, multi-region, with log-file validation and write-once long-term retention
AWS Config	Continuous configuration recording, with managed rules covering encryption, MFA, public-access blocks, and other posture checks
AWS GuardDuty	Intelligent threat detection on API activity, network traffic, and object-storage usage, with malware protection enabled
AWS Security Hub	Posture aggregation against the AWS Foundational Security Best Practices and CIS AWS Foundations benchmarks
IAM Access Analyzer	Detects any resource policy that grants access outside the Alder account boundary
VPC Flow Logs	Full network flow visibility, with hot-tier retention for recent traffic and long-term cold-tier archival
AWS WAF logging	Per-request web-attack activity retained centrally

Application-Level Alerting

Health, performance, and error-rate alarms cover every tier of the production system, and alerts route through an encrypted delivery path to on-call. Every service emits structured logs to a

centralized, searchable log store, so that both day-to-day anomalies and incident post-mortems have the data they need.

Vulnerability Management

- Container images: scan-on-push in our container registry; findings reviewed as part of the deployment flow.
- Application dependencies: tracked and updated on a regular cadence.
- Underlying compute: hosts are patched on a managed schedule, with security-relevant updates prioritized.
- Database engine: automatic minor-version upgrades enabled, so security-relevant patches land automatically during the defined maintenance window.

SECTION 07

Compliance and Certifications

SOC 2

Alder's controls are designed and operated against the **SOC 2 Trust Services Criteria**, with initial scope on the **Security** criterion. This whitepaper is organized around those criteria, and every control described here is tracked internally against a SOC 2 readiness assessment. A formal SOC 2 Type II audit engagement will follow as the company matures; customers with specific compliance requirements are welcome to discuss their timelines with us.

AWS Inherited Controls

As an AWS-hosted service, Alder inherits a significant set of controls from AWS's independently-audited compliance programs, including SOC 1 / SOC 2 / SOC 3 Type II, ISO 27001, and PCI DSS Level 1. AWS's audit reports are available through AWS Artifact.

GDPR and Data Processing

Alder processes personal data on behalf of its customers and offers a Data Processing Addendum (DPA) for customers with GDPR obligations. Contact **security@getalder.com** for a copy.

SECTION 08

Subprocessors

Alder uses a small, carefully-vetted set of subprocessors. Each vendor is reviewed before onboarding for its security posture, data-handling practices, compliance attestations, and contractual protections, and our agreements with each require equivalent protections for data processed on Alder's behalf.

The list below reflects our current subprocessors at the time of publication. As the product evolves, we may add or change subprocessors.

Subprocessor	Purpose
Amazon Web Services	Primary cloud host (compute, storage, database, CDN)
Google Cloud Platform	Secondary cloud services, including LLM inference and analytics
OpenAI	LLM inference
Anthropic	LLM inference
Stripe	Payment processing
Attio	Customer relationship management
Sentry	Application error tracking
MailerLite	Marketing email delivery
GitHub	Source code hosting
Google Workspace	Internal email and collaboration
Slack	Internal communications and operational alerts

SECTION 09

Customer Security Questions: FAQ

Question	Answer
Where is data hosted?	On AWS, in the United States, with global CDN edge caching of non-sensitive assets.
Is data encrypted at rest?	Yes. AES-256 via AWS KMS, customer-managed key.
Is data encrypted in transit?	Yes. TLS 1.2+ everywhere
Do you support MFA for end users?	Yes. TOTP-based multi-factor authentication is built into the product and can be enabled per user.
Do you support customer SSO?	SAML/OIDC SSO for customer-side authentication is on our future roadmap. Contact us for timing.
Do you have a SOC 2 report?	Not yet. Controls are designed and operated against the SOC 2 Trust Services Criteria, and a Type II audit will be pursued as the company matures.
What is your RPO / RTO?	RPO ≈ 5 minutes via point-in-time recovery. RTO targets are formalized as part of our ongoing business-continuity program.
Do you perform penetration testing?	Third-party penetration testing is part of our SOC 2 audit readiness plan.
Do you offer a HIPAA BAA?	No. Alder is a planning and collaboration tool and storing PHI is not within our product scope.
Do you offer a GDPR DPA?	Yes. Contact security@getalder.com.

SECTION 10

Conclusion

The Alder team uses Alder ourselves. Our own operational data sits on the infrastructure described in this document, so every control here protects us both.

Security is ultimately about trust. We work to earn and maintain that trust with every line of code we ship, every control we implement, and every question you ask. If there is something we haven't addressed here, or a control your security team needs to evaluate in more depth, please reach out.

security@getalder.com

Have a security question?

If there is something this document hasn't addressed, or a control your security team needs to evaluate in more depth, reach out and we'll be glad to discuss.

security@getalder.com

Alder is built and operated by Viridian Technologies, LLC.