Backstory

SECURITY · PRIVACY · AI GOVERNANCE

Built for Trust. Engineered for the Enterprise.

A defense-in-depth program across every layer — independently audited, continuously monitored, and always under your control.

INDEPENDENTLY CERTIFIED (ANNUALLY)

- SOC 2 TYPE II
- ISO 27001
- ISO 27017
- CSA STAR LEVEL 2
- ISO 27701
- NIST CSF ALIGNED

01 — ZERO-TRUST SECURITY BY DEFAULT

Every access request verified. No standing access. No exceptions.

Identity & access

- VPN required for all production access
- SSO via Okta + MFA on every system
- Zero standing access — just-in-time only
- AWS IAM dual-layer role-based authorization
- MDM requirement for all access
- Full logging: who, what, when

Encryption

- Per-customer master keys (CMKs) via AWS KMS
- AES-256 at rest; TLS 1.2/1.3 in transit
- FIPS 140-2 compliant HSMs — no human key access
- Tenant-isolated VPC with separate storage
- Key rotation on a defined schedule

Infrastructure & cloud

- AWS-native; primary site in US-East region, DR/Backup site in US-West region
- Private VPC — segmented, firewall-protected
- Kubernetes clusters with hardened AMIs and containers
- CSPM, Container and SBOM scanning, and native AWS Security monitoring
- Daily vulnerability scanning; annual pen testing supplemented by AI-enabled continuous Red Teaming

02 — PRIVACY BY DESIGN

Privacy is built in. Not bolted on.

Compliance & classification

- GDPR, CCPA, and applicable global privacy laws
- ISO 27701 Privacy Information Management certified
- All customer data classified Confidential at ingestion
- DLP controls and device trust enforcement
- Synthetic data for all testing — never customer data

Filtering & data minimization

- Layered ingestion filters — only relevant business signals
- Global exclusions block known senders of sensitive data
- Sensitive content filtering removes financial and personal info
- CRM-based filtering excludes irrelevant communications
- Role-based filtering enforced by account ownership

AI DATA COMMITMENT

Customer data is **never** used to train AI models. All AI processing occurs in segregated, controlled environments dedicated solely to contracted services — with full oversight and auditability.

03 — RESPONSIBLE AI

Governance woven into every layer.

AI governance isn't a separate policy — it's integrated with security and privacy architecture from the ground up.

- Data used only to deliver contracted services
- AI processing in segregated, controlled environments
- Governance integrated with security and privacy programs
- Oversight and auditability for every AI operation
- Annual risk assessments cover AI-specific threat scenarios

Operational resilience

- Multi-region failover — US-East primary, US-West DR
- Daily backups with 15-day automated recovery tests
- Formal IR playbooks: ransomware, insider threats, unauthorized access
- Real-time alerting for anomalous behavior patterns

04 — YOUR DATA. YOUR RULES.

Customer-controlled from day one.

Granular privacy settings at domain, email, and CRM-object levels. Full admin and end-user self-service with no dependency on Backstory to manage your data posture.

- Customer-controlled settings at domain, email, and CRM-object levels
- Admin and end-user control — full self-service
- SAML federation with customer identity providers
- No persistent employee access — just-in-time only
- Full audit trail: every access event logged with who, when, and why

5 certifications | **Zero** standing access

Customer data is **never** used to train AI models. All processing occurs in segregated environments dedicated solely to contracted services — with full oversight and auditability.

HOW YOUR DATA FLOWS