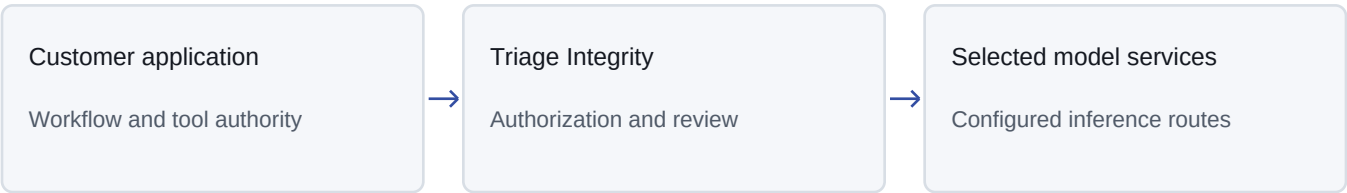


Architecture and data handling

Data handling and technical control boundaries | 29 September 2026

Integrity connects customer-defined policy with AI workflow activity and review evidence. The architecture separates the customer application, Triage's administrative services, workflow processing, model evaluation, and retained evidence.

This guide is intended for technical security reviewers. It describes the hosted service and identifies the configuration decisions that determine data access and processing. A deployment-specific review records the enabled capabilities and any additional customer requirements.



Workspace administration and scoped evidence access support the processing path.

Processing sequence

- The customer application sends an authorized request with the applicable deployment and workflow context.
- Triage validates scope and routes the request to the configured customer model and Integrity evaluation components.
- The selected integration returns the response, judgment, or supported intervention. The customer application controls tool execution.
- Authorized workspace users inspect retained outcomes and evidence associated with their projects and sessions.

Provider routing and retained content depend on the selected integration. Bring-your-own-key changes the credential used for inference; it does not remove Triage or the configured provider from the processing path.

Data inventory and processing purposes

The service processes the information needed for the configured workflow. Customers can reduce exposure by choosing representative inputs, removing unnecessary sensitive content, and using opaque identifiers.

Data category	Purpose and handling
Account and membership information	Authenticate users and govern workspace access. Includes account identifiers, membership, and role information.
Project and deployment configuration	Select policy, provider routes, integration behavior, and runtime versions. Configuration is subject to workspace authorization.
Workflow content	Instructions, conversation context, model outputs, and submitted tool activity used for the requested evaluation. Configured model services may process relevant content.
Provider credentials	Authenticate an authorized inference route. Saved credentials use authenticated encryption and are resolved within the service.
Retained evidence	Session records, review outcomes, and associated evidence used for investigation, evaluation, and authorized export. Protected content is encrypted and scoped to its owning records.
Operational metadata	Identifiers, timestamps, status, usage, and accounting information used for routing, reliability, metering, and security. Metadata has its own access and retention requirements.

Customer instructions govern use

The customer agreement and documented instructions govern processing of Customer Data. Unrelated model training and cross-customer reuse are not authorized by acceptance of Triage's standard terms. Authorized customer-specific adaptation is a separate workflow and depends on the selected deployment's capabilities.

Provider terms also apply to the selected inference route. The security review records the providers involved and their treatment of submitted content, including any provider retention configuration.

Identity and tenant boundaries

Administrative access

The portal authenticates users and resolves their current workspace authority. Backend checks enforce the organization, project, and operation being requested. Administrative state and evidence are not authorized solely by a client-supplied identifier or by whether a page is visible in the user interface.

Application credentials

Deployment credentials admit workflow traffic for the relevant project. Current project ownership and availability are checked by the service. Provider keys authenticate inference with the selected model provider. Reviewer grants authorize the separate evaluation path. These credentials have distinct purposes and are not interchangeable.

Session and evidence scope

Stored workflow data carries organization, project, deployment, and session associations. Evidence access is evaluated against the caller's permitted scope. Supported export workflows bind the data snapshot and recipient, with authorization checked as the export is read.

Runtime authority

Native processing uses bounded grants and release identities. Requests are checked against the selected runtime context and durable operation state. Deployment or model availability alone does not authorize an arbitrary tool action; the customer application must enforce the executor authorization required by its integration.

Hosted isolation model

The standard hosted service uses shared infrastructure with logical tenant isolation. Customers receive scoped workspaces and processing authority rather than a promise of dedicated physical hardware. A deployment review can establish whether additional isolation requirements are needed for the proposed workload.

Customers manage authorized participants and integration keys. Triage manages the platform authorization boundary and the operation of the agreed hosted services.

Encryption and sensitive configuration

Transport protection

Hosted endpoints use HTTPS. Production database connections use TLS with certificate verification. Runtime-to-service communication is authenticated, and authorization is checked independently of transport encryption.

Authenticated content encryption

Saved provider credentials and supported session content use AES-256-GCM. Protected session records bind ciphertext to the expected organization, project, deployment, trajectory, and record identity. The service verifies that context when opening the record.

This protection applies to the content envelope. Routing, configuration, accounting, and other operational metadata are stored separately for authorized service operation. Infrastructure encryption and application-level encryption serve different purposes; the hosted service does not currently promise customer-managed keys or a unique encryption key for each customer.

Secret storage and release packaging

Sensitive runtime configuration is delivered through managed secret storage. Container and runtime packaging separate source and public configuration from private credentials. Immutable release identities connect the reviewed source, packaged application, and deployed runtime.

Evidence redaction

Selected evidence views apply pattern-based redaction to supported fields, including recognized credential and personal-information patterns. This reduces incidental exposure when reviewing evidence. Pattern matching is not a complete classification system: customers should review material before sharing or exporting it.

Redaction is a presentation control. It does not alter content already processed by a selected provider or erase the encrypted original retained for the service. Data minimization at the source remains the most direct way to limit what enters the processing path.

Retention and controlled data use

Retention follows the data lifecycle

Supported retention settings govern the availability of retained session evidence. The service may need to process content during a live request even when the customer chooses limited retention. Expired evidence can become unavailable for viewing, grading, or export.

Layer	Review consideration
Application evidence	Confirm supported retention settings and the records available to workspace members.
Runtime state and journals	Identify retained native evidence, cleanup capabilities, and minimal identifiers required for safe operation recovery.
Model providers	Confirm the selected route, provider retention configuration, and applicable data-use terms.
Backups	Document backup retention and the treatment of removed application records in existing recovery points.
Authorized adaptation	Confirm permitted source data, preparation and evaluation steps, activation authority, and retention of resulting artifacts.

Deletion and end of service

Return, export, deletion, and any continuing retention are handled under the customer agreement, documented instructions, and applicable law. A deletion request is reviewed across the relevant stores and providers. Backup expiry and provider cleanup can follow a different schedule from removal in the application.

Adaptation requires a separate decision

Where a deployment supports customer-specific adaptation, preparation, training, evaluation, and activation are separate steps. Completing training does not automatically activate a new version. The current Base connection's supported lifecycle must be checked before planning customer-version training or rollback.

Use info@triage-sec.com to request the retention and cleanup scope for a proposed deployment or to raise a Customer Data request.

Infrastructure and service providers

Triage uses managed services for application hosting, identity, runtime computation, storage, and monitoring. The providers below describe the principal hosted architecture; the deployment inventory identifies the exact services and data flows in scope.

Service provider	Role in the hosted architecture
Amazon Web Services	Application services, managed database and storage infrastructure, secret management, logs, and backup services.
Modal	Hosted workflow gateway and native runtime computation, with runtime storage and managed configuration.
Vercel	Web application hosting and delivery.
Auth0	User authentication for the customer portal.
Configured model providers	Customer-model inference and applicable evaluation routes. Provider selection depends on enabled features and customer configuration.
Oneleet	Security program management, control monitoring, evidence workflow, and the Trust Center.

Network and access boundaries

Cloud permissions and service configuration restrict access to application infrastructure. Runtime credentials are scoped to the service role. Database access is limited to approved network paths; processing-location and private-connectivity requirements are reviewed for the proposed deployment.

Processing location and vendor review

A hosting region does not define every downstream processing location. The deployment review identifies the location and role of each relevant provider, including inference and support services. Vendor security materials, data-processing terms, and retention settings are considered as part of that review.

This architecture inventory is not a claim that each provider receives all categories of Customer Data. The actual data flow determines the applicable subprocessors and contractual disclosures.

Release assurance and technical diligence

Evidence-backed releases

Triage records source revisions and image identities, exercises installed runtime behavior, and verifies the deployed service. Application tests cover authorization, tenant boundaries, persisted operations, and supported failure behavior. Container scans and dependency checks contribute separate supply-chain evidence.

Operational acceptance

Readiness checks, synthetic workflow canaries, and release observation provide evidence that the service is available and processing requests. Production qualification additionally evaluates the intended workload and required behavior. An operational health result is not a substitute for that qualification.

Continuity

The hosted environment maintains automated database backups, encrypted snapshots, and monitored runtime backups. Recovery planning includes the application and data versions needed to interpret restored records. Recovery objectives and availability commitments are defined for the agreed customer service.

Review materials

- Deployment architecture and the categories of data sent to each relevant processor.
- Authorization and encryption design, with supporting tests and implementation evidence.
- Release identity, verification results, current operating evidence, and relevant remediation.
- Retention, cleanup, incident cooperation, and customer responsibilities.

Assessment status

The SOC 2 Security program is in readiness and evidence review with Oneleet. Independent penetration testing is scheduled. Auditor-issued SOC 2 Type II and completed penetration-test reports are not yet available; the Security Overview contains the current assurance statement.

Version 1.0 | 29 September 2026 | Public customer information
Request technical diligence: info@triage-sec.com | trust.triage-sec.com