dash0

TRUST & SECURITY

Security & Compliance Overview

How Dash0 protects customer telemetry across platform, data handling, compliance, security controls, AI features, and retention.

DOCUMENT	CLASSIFICATION	MORE AT
REVISION 08 / 2026	PUBLIC	TRUST.DASH0.COM

CONTENTS

01 Platform and hosting

02 Data we process

03 Customer-side data control

04 Compliance and assurance

05 Security controls

06 AI features

07 Data retention and deletion

08 Subprocessors and security documentation

01 Platform and hosting

Dash0 runs on AWS and Google Cloud. Each customer organization is homed to a single deployment region. Customer telemetry is stored and processed within that region, and AI inference follows the cloud and regional placement of the corresponding Dash0 deployment.

> For EU-hosted organizations, data residency — including customer telemetry storage, processing, and AI inference — remains in the EU.

Application workloads run in private subnets without direct inbound access from the internet. Public access is limited to designated load-balancer endpoints. Administrative access to production systems requires VPN access with SSO and MFA.

02 Data we process

Dash0 acts as a data processor. Customers determine what telemetry they send to the platform.

CATEGORY	WHAT IT IS
Telemetry	Logs, traces, metrics, and related context sent through the customer's OpenTelemetry infrastructure.
Account data	Name, business email, and IP address used for authentication, security, and access control.

Dash0 does not require customers to send personal or sensitive data as part of their telemetry. Telemetry may nevertheless contain such data depending on what the customer collects and sends. IP addresses are anonymized by default.

03 Customer-side data control

Customers can remove sensitive content **before it reaches Dash0** using their own OpenTelemetry Collector. OTTL and the redaction, attributes, transform, and filter processors support masking, hashing, filtering, and fail-closed allowlisting of data such as PII, secrets, JWTs, and payment information.

> Pre-ingest filtering is the highest-leverage customer-side data control. It must be configured before ingestion and does not apply retroactively.

For coding-agent telemetry, Dash0 additionally supports irreversible redaction at ingestion. Sensitive conversation content, tool inputs, results, and errors can be removed before storage while retaining non-sensitive operational fields required for analytics.

04 Compliance and assurance

FRAMEWORK	STATUS
SOC 2 Type II	Current. Report available under NDA.
GDPR	Dash0 acts as a processor under a DPA incorporating the EU Standard Contractual Clauses. Dash0 maintains a Transfer Impact Assessment for applicable international data transfers, which can be shared upon request.
HIPAA	Business Associate Agreement available. Dash0 does not intend customers to send PHI. The BAA provides contractual protection where PHI is inadvertently processed; customers are responsible for filtering PHI before ingestion.
ISO 27001	Certification to be completed by Q1 2027.
PCI DSS	Certification to be completed by Q1 2027.

05 Security controls

Access
RBAC, SAML SSO, MFA, scoped API tokens, least privilege, and quarterly access reviews.

Encryption
TLS 1.2 or higher for data in transit. AES-256 with managed keys for data at rest.

Tenancy
Customer organizations are logically isolated. Tenant identity is derived from the authenticated credential and is never accepted from request content. Organization identity is a leading key in the telemetry storage layout, and unscoped access fails closed.

Software assurance
Peer-reviewed SDLC with automated security scanning and manual approval before production deployment. Continuous dependency and infrastructure scanning and an annual independent penetration test.

Monitoring
Security monitoring uses CloudTrail, CloudWatch, and GuardDuty, with Falco providing Kubernetes runtime protection.

Incident response
Dash0 maintains a formal Incident Management Policy and dedicated incident-response function. Customers are notified within 72 hours of a confirmed security incident where notification is required. Dash0 maintains a published Vulnerability Disclosure Policy.

06 AI features

Agent0 and Dash0's other AI features use unmodified Anthropic Claude foundation models through Amazon Bedrock or Google Cloud Vertex AI, according to the cloud and region of the customer's Dash0 deployment.

> **Customer data is not used for model training.** Dash0 does not train or fine-tune models on customer data. Model access is brokered by Dash0 and operates under provider zero-retention terms. Where inference infrastructure uses transient prompt caching, cached content is ephemeral, is not used for model training, and expires on a rolling five-minute basis.

Agent0 runs model-directed code in an ephemeral, per-conversation sandbox isolated from the trusted Dash0 control plane. The sandbox contains no long-lived credentials and supports customer-selectable network isolation.

Agent0 is read-only against customer telemetry. Write capabilities exist only through integrations the customer has explicitly installed and scoped, and remain subject to the permissions of those integrations.

Dash0 does not rely on model instructions as a security boundary. Authorization, credential isolation, tool permissions, tenant isolation, and network restrictions are independently enforced outside the model.

07 Data retention and deletion

DATA	STANDARD RETENTION
Logs and traces	30 days
Metrics	13 months
Agent0 conversation history	13 months

Dash0 supports retention-based automatic deletion and deletion on request, together with applicable data-subject rights under the DPA.

08 Subprocessors and security documentation

Dash0 maintains a list of subprocessors and provides contractual data-processing terms through its DPA at dash0.com/policies/dpa.

SOC 2 documentation and additional security and compliance materials are available at trust.dash0.com.