DARKTRACE

SECURE AI - Data Storage and Security Schedule

Summary

1. Darktrace / SECURE AI is a SaaS product that provides visibility, controls and governance again AI related threats. Hosted on AWS to provide visibility, tracking and controls over AI activity.

Data Transfer and Storage

2. All /SECURE AI data is encrypted in transit and at rest. Data in transit is protected using Transport Layer Security (TLS) for external connections, with encrypted communication maintained between network tiers and backend services. Data at rest is protected using AES-256 encryption across all /SECURE AI data stores and supporting infrastructure, including relational databases, object storage, caching services, message queues, and backups. Encryption keys are managed using cloud-native key management services, with customer-managed keys used for selected systems and annual key rotation applied where supported.

3. Where data is stored in the cloud, Darktrace maintains Customer Data in the hosted location specified on the Order, unless otherwise directed by the Customer. /SECURE AI does not receive bulk Customer Data uploads; it ingests activity metadata and derived signals from the Customer's nominated AI and productivity services via authenticated API integrations that the Customer explicitly authorises (for example Microsoft 365 via OAuth, OpenAI via a Compliance API key, and Anthropic via a Compliance Access Key). It remains the Customer's responsibility to ensure that the permissions granted to these integrations, and any resulting cross-border transfer of information, comply with applicable international data protection laws and regulations.

Data Retention and Transfer

4. Data is retained within /SECURE AI according to its type. Data held in the /SECURE AI databases is retained for 12 weeks. Database backups are retained for 7 days, inheriting the encryption settings of the source data store. Retention categories relevant to /SECURE AI include:

   - Log and telemetry metrics;
   - Derived and aggregated signals (for example rarity, frequency and risk scores);
   - Prompt and session data extracted from integrated AI services;
   - Detection and alert records (for example Shadow AI detections, prompt detections); and
   - Model data (per-tenant behavioural models).

Data Access by Darktrace

5. Access to the /SECURE AI service by Darktrace personnel is limited to the following purposes:

    - Initial setup, configuration and validation;
    - Creation of customer reports (as part of a trial or an ongoing service agreement);
    - Security incidents; and
    - Support incidents.

6. All data access is logged and controlled. Logs of data access, whether by the Customer or by Darktrace personnel, are retained to maintain an audit trail. Darktrace personnel accessing /SECURE AI are uniquely identified and authenticated through Darktrace's Single Sign-On solution, subject to device-posture controls, with role-based access enforcing least privilege.

7. Access logs are surfaced to the Customer in-product. By default, Darktrace personnel are not granted the prompt-detailer permission and therefore cannot view prompt content.

8. Where a Customer has visibility of raw prompts, the Customer may export sessions (for example where they believe there is an issue), and such exports will include the raw prompts.