Escape AI Overview & Trust Guidelines

Last Updated: December 2025

Escape uses AI to enhance security operations through Automated Security Testing and Attack Surface Management (ASM). This document outlines how AI features function, how data is handled, and the security measures in place.

AI-Powered Features

Escape's AI capabilities integrate into DAST and ASM workflows, leveraging proprietary AI models and external services, such as Azure, to enhance functionality.

First-Party Proprietary AI Features

Escape's proprietary AI models deployed on AWS infrastructure enhance security workflows through the following features:

- **Business Logic Security Testing**: AI-driven testing to identify business logic security vulnerabilities in WebbApps and APIs.
- **Attack Surface Management and Asset Discovery**: Automatically identifies and maps assets (APIs and web applications) in your environment to detect potential attack surfaces.

Externally-enhanced AI Features

Escape leverages Microsoft Azure LLM Deployments to complement its proprietary AI models for enhanced security capabilities, including:

- **API Schema Generation from Source Code**: Generates data schemas from source code to facilitate Business Logic
- **Escape MCP**: An AI assistant integrated within Escape to manage applications, monitor scans, review issues, and more, based on MCP over Escape's API.
- **AI Context and Remediations**: Provides contextual guidance and recommendations for security vulnerabilities based on real-time scan data.
- **Agentic Pentesting**: Uses AI to automate and optimize testing, improving detection and remediation of vulnerabilities.
- **False Positive Filtering**: AI filters out false positives to improve the accuracy and efficiency of security scans.

Security and Privacy Policies

Escape implements multiple layers of security to protect AI features, both internally and externally.

- **First-party and Proprietary AI Models**: Data is processed and stored within Escape's designated region (AWS infrastructure).
- **External AI Services**: Data processed by Azure is retained for up to 30 days for abuse detection and moderation but is not used for model training or stored long-term. Escape ensures that external processing complies with security and privacy guarantees defined by Azure.

AI-generated outputs are intended for operational use and may be used commercially, provided they comply with Escape's platform terms.

AI features include safeguards for moderation, ensuring that inappropriate content is filtered, and abuse is prevented. Rate limits are applied to ensure system stability and performance. Escape monitors AI output using internal content validation to maintain response quality and safety. AI-generated output is deterministic.

All AI interactions are contained within your Escape environment, and Escape does not store customer data for training purposes. Data is not shared between customers to ensure tenant-isolation. Interactions are governed by role-based access controls (RBAC), ensuring that users only access data allowed by their role.

Processing is conducted in compliance with regional policies. By default, all AI processing occurs within Escape infrastructure. In cases of external processing (e.g., Azure), compliance with applicable retention policies and standards (including EU and US regulations) applies.

Escape AI Principles

- **No customer data for training**: Customer data is never used to train AI models.
- **Data privacy**: Customer data is processed securely within the scope of your Escape environment.
- **Opt-out**: Customers can request to disable External AI features at any time, with all actions logged and auditable.
- **Transparent interactions**: AI features are explainable, deterministic, and aligned with cybersecurity standards (e.g., SOC 2 Type II, GDPR).

For questions or more information about Escape's AI features, please contact your account manager.
