

S-Core Ecliptor Security Practices Overview

Published by S-Core Analytics, Inc. · Contact: s-coreecliptorsupport@s-coreanalytics.com

Document ID	SEC-EC-2026-01	Version	2.0
Classification	Public	Effective date	11 August 2026
Owner	S-Core Analytics, Inc., Engineering	Next scheduled review	11 February 2027

What this document is, and is not. This is a first-party description of the security controls S-Core Ecliptor has implemented and internally verified as of the effective date above, published for transparency to customers and prospects. It is **not** a SOC 2 report, and S-Core Ecliptor has **not** completed an independent third-party penetration test as of this date. See Section 6 for our current certification status and roadmap. Nothing in this document should be relied upon as equivalent to an independent audit opinion.

1. Executive summary

S-Core Ecliptor is an AI-first e-commerce intelligence platform for Amazon sellers, providing revenue, profitability, refund, and market-analysis insights built on the Amazon Selling Partner API (SP-API). Ecliptor is in early access and is not yet onboarding live customer Amazon Seller accounts through this site. We are publishing this overview now, before general availability, so that any seller evaluating Ecliptor can see exactly what will protect their data once they connect an account, and where we still have work in progress.

2. Scope and methodology

This overview covers the production application, its data stores, and the cloud infrastructure it runs on. Controls described below were verified through the following methods:

- Manual line-by-line review of the authentication middleware, authorization checks on every API route, and tenant-isolation logic.
- Automated dependency vulnerability scanning (npm audit) across both the API and the web client.
- Direct review of the Amazon SP-API integration for outbound request handling, including the allowlist that constrains which hosts the server is permitted to call.

- Review of CORS configuration, rate-limiting configuration, and password-handling (hashing) code.
- Search across the codebase for string-concatenated or templated SQL to confirm query parameterization is used consistently.

3. Identity and access management

- Passwords are never stored in plain text; they are hashed with an industry-standard, computationally expensive hashing algorithm (bcrypt) before storage.
- Sign-in issues a signed JSON Web Token. Every request to your data is independently verified against that token server-side.
- Sign-in attempts are rate-limited to slow down credential-guessing attempts.
- Every database query that reads or writes your business data is scoped to your authenticated account.

4. Your Amazon connection and data protection

- When you connect an Amazon Seller account, Ecliptor calls Amazon's Selling Partner API (SP-API) through an allowlist that restricts outbound requests to Amazon's own API hosts: protection against a class of attack (server-side request forgery) where a server is tricked into calling an internal or unintended address.
- Amazon refresh tokens and client secrets are held as server-side application secrets and are never sent to or exposed in your browser.
- All traffic to and from Ecliptor is encrypted in transit via TLS.

5. Application and infrastructure security

- Database queries are parameterized throughout the codebase, the standard defense against SQL injection; we reviewed every query in the application for this specifically.
- Cross-origin requests are restricted to an explicit allowlist of approved origins rather than a permissive wildcard.
- API requests are rate-limited to reduce the impact of abuse or credential-stuffing attempts.
- Application dependencies are scanned for known vulnerabilities.
- The running application reads its database credentials and Amazon API keys from the hosting provider's environment configuration at runtime, not from a file bundled into the application or sent to your browser.

6. Third-party and sub-processor management

Ecliptor currently relies on the following sub-processors:

- Microsoft Azure: application hosting and database (current; migration to Google Cloud is in progress) (United States).
- Amazon Selling Partner API: used exclusively to retrieve the connected Customer's own Amazon seller data on their behalf (United States).

7. What we are still building

We would rather tell you what is incomplete than imply otherwise. Before we consider Ecliptor ready to onboard live customer accounts, we are actively working on:

- A dedicated, fully self-service sign-in experience for the application dashboard itself, replacing the current early-access request flow on this site.
- Completing our infrastructure migration to Google Cloud, bringing the same least-privilege service accounts and centralized secret management already in place across our other products.
- Adding a Content-Security-Policy header to the application's HTTP responses, currently in progress as part of the broader hardening pass ahead of general availability.
- Removing all remaining development-only configuration paths from anything that could run in a live environment.

8. Data retention and customer rights

- Because Ecliptor is not yet onboarding live customer accounts, no customer Amazon Seller data is currently retained in production.
- Once general availability begins, this section will be updated with concrete data retention periods and self-service deletion controls, consistent with the practices already shipped across our other products.

6. Independent assurance and certification status

- S-Core Ecliptor is **not** currently SOC 2 certified.
- S-Core Ecliptor has **not** completed an independent third-party penetration test as of the effective date of this document.
- Both are goals we are working toward ahead of general availability. This document will be updated, and the version above incremented, the moment either status changes to reflect a completed, independently verified engagement.

7. Responsible disclosure

If you believe you have found a security vulnerability, please report it to s-coreecliptorsupport@s-coreanalytics.com rather than filing a public report. We investigate every report and will acknowledge

receipt promptly. Please include enough detail (steps to reproduce, affected endpoint) for us to verify and address the issue quickly.

S-Core Analytics, Inc. · Ecliptor is in early access and is not yet onboarding live customer Amazon Seller accounts through this site.
This document does not constitute a warranty or independent audit opinion.