Harbinger Security

Executive Summary

Client	[Redacted B2B SaaS Platform]
Assessment Type	Web Application & API Vulnerability Assessment
Assessment Period	January 2026
Assessor	Harbinger Security Consulting, LLC
Lead Consultant	Anthony D'Onofrio, PhD

Purpose of Assessment

Harbinger Security conducted an independent security assessment of the in-scope web application and associated APIs to identify security weaknesses that could materially impact confidentiality, integrity, or availability. This assessment was commissioned to support enterprise sales diligence and security review processes.

Scope Overview

The assessment evaluated the primary production web application, authenticated user workflows, and selected API endpoints. Infrastructure, denial-of-service testing, source code review, and third-party services were out of scope.

Methodology

Testing was conducted using an industry-recognized methodology aligned with the OWASP Top Web Application Security Risks. Assessment activities were tailored to application architecture and trust boundaries, including evaluation of authentication and authorization mechanisms, access control enforcement, object-level authorization logic, session handling, business logic abuse scenarios, and data exposure risks.

Overall Security Posture

The application demonstrated a generally mature security posture, with no evidence of systemic control failures. Most findings were categorized as low or informational and would pose risk primarily if chained together under novel exploitation scenarios.

Assessment Classification: **Diligence-Ready**

Anthony D'Onofrio, PhD
Principal Security Consultant
Harbinger Security Consulting, LLC

21 January 2026