App Defense Alliance | **CASA**

Validation Report

TAC Security
CYBERSECURITY'S FUTURE

Application Name: Mailmeteor	**Certification ID:** 1008170693301
Assessment Type: Tier 3	**Issue Date**: 04/29/2023
Assessment Status: Complete	**Expiration Date**: 04/29/2024

Statement of Validation

The purpose of this report is to provide users verification that Mailmeteor has successfully completed a Cloud Application Security Assessment (CASA) Assessment, validating mailmeteor.com has satisfied CASA application security requirements for Web applications set forth by the App Defense Alliance (ADA).

In meeting these assessment requirements, mailmeteor.com is verified to meet the CASA Tier 3 requirements.

About CASA

As global ecosystems of applications, platforms, and systems evolve and connect through complex cloud-to-cloud integrations, an established and industry-recognized application securitization standard becomes evermore paramount to guarding consumer data and privacy. At risk in this evolution are non-hardened applications exchanging data with secure cloud infrastructure through trusted data sharing integrations. Thus introducing: CASA.

CASA is based on the industry-recognized Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) to provide third-party (3P) application developers with: (1) a basis for testing technical application security controls, (2) a consistent set of requirements for secure application development, and (3) homogenized coverage and assurance levels for providing security verification using industry-aligned frameworks and open security standards.

More information on CASA, including a complete list of CASA requirements can be located on the CASA developer site.

The following assessment was performed using the OWASP Application Security Verification Standard (ASVS) version 4.0. Under the CASA Framework:

Category	Status	Justification
Architecture, Design and Threat Modeling Requirements	Pass	Application uses a single vetted authentication for communication between application components, including APIs, middleware and data layers, are authenticated.
Authentication Verification Requirements	Pass	Application uses approved cryptographic algorithms and internal secrets, API Keys stored in the secured environment.
Session Management Verification Requirements	Pass	Application handles all the cookie attributes in a secure way of implementation.
Access Control Verification Requirements	Pass	Directory browsing is disabled for directory metadata which can reveal any sensitive information.
Validation, Sanitization and Encoding Verification Requirements	Pass	Application has defenses against HTTP parameter pollution attacks, all the security HTTP headers are properly implemented.
Stored Cryptography Verification Requirements	Pass	Application protects against cryptographic breaks whether it’s random number, encryption or hashing algorithms, key lengths, rounds, ciphers.
Error Handling and Logging Verification Requirements	Pass	Application protects sensitive data from being cached in server components and application caches.
Data Protection Verification Requirements	Pass	Data stored in the browser storage is securely managed by the application.
Communications Verification Requirements	Pass	Connections to and from the server use trusted TLS certificates.
Malicious Code Verification Requirements	Pass	Application source code and third party libraries do not contain back doors, such

		as hard-coded or additional undocumented accounts or keys.
Business Logic Verification Requirements	Pass	Application has anti-automation controls to protect against denial of service attacks.
File and Resources Verification Requirements	Pass	Files obtained from untrusted sources are stored outside the web root, with limited permissions.
API and Web Service Verification Requirements	Pass	Application APIs do not expose sensitive information such as API Key, session tokens, etc.
Configuration Verification Requirements	Pass	Application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.

Security Support Period

There is a public security end of life policy at https://mailmeteor.com/privacy-policy