PRESCIENT SECURITY

CASA Overview

CASA can feel confusing the first time you run into it. In short: if your application connects to Google user data through certain sensitive or restricted scopes, CASA is the security review framework that helps prove your app handles that access responsibly.

CASA stands for Cloud Application Security Assessment. It is an application security assessment framework created by the App Defense Alliance and built on the OWASP Application Security Verification Standard (ASVS). CASA creates a consistent way to evaluate if a cloud-connected application protects user data. For software teams, it provides a practical path to validate key application security controls through a tiered assessment model.

What CASA is really about

CASA exists because cloud applications often sit in the middle of trusted data flows. They connect to platforms, APIs, storage layers, and end users all at once. That convenience is powerful, but it also creates risk. Just because a cloud platform is well built, it does not automatically make every connected application secure.

CASA focuses on the application layers, e.g. how an app authenticates users, handles sessions, protects data, enforces authorization, manages secrets, validates input, and limits security weaknesses that could expose sensitive information. In short CASA is designed to answer the question if an application can be trusted to access and handle user data securely. That is why CASA matters for apps that request access to data from ecosystems like Google Workspace. It helps move trust from marketing claims to independent validation.

The core functions explained



It protects user data

CASA is meant to reduce common weaknesses that could lead to unauthorized access, data leakage, or misuse.



It builds trust

A successful CASA assessment shows customers and platform providers that security controls were reviewed against a recognized standard.



It supports app approval and continued access

For some integrations and scopes, CASA is not optional, but moreover is part of the path to maintaining access in the platform ecosystem.



It creates a common language

Because CASA is based on OWASP ASVS, teams are working from a known security benchmark.

It's good to think about CASA as a structured way to prove your application security posture is real and not just a formality.

How the assurance model works

CASA uses a risk-based approach. The requirements are consistent, but the assessment method changes based on the assurance level required by the ecosystem owner (Google).

Assurance level	What it means	What teams should expect
AL0	Developer-tested self assessment	Developer-led validation intended to help establish baseline readiness.
AL1	Developer tested, Lab-verified assessment	An authorized lab validates the application against CASA expectations using the required assessment method for this level.
AL2	Most rigorous lab tested, lab verified assessment	A deeper, independent review with broader hands-on validation for higher-risk application scenarios.

The exact assurance level is determined by the framework owner (Google) based on factors such as data sensitivity, scope access, user exposure, and risk tolerance. What matters for application teams is that all applicable CASA requirements must still be satisfied.

What gets looked at

CASA is centered on application security requirements derived from OWASP ASVS. While the exact scope depends on the app and tier, common focus areas typically include:

1. Authentication and session security
2. Authorization and access control
3. Secure data handling
4. Input handling and common web/API weaknesses
5. Secrets, cryptography, and configuration security
6. Architecture and deployment considerations

In practice, that means CASA often touches the web app, APIs, mobile components, connected storage, and the places where user data enters, moves through, or leaves the system.

What a successful engagement usually looks like

A strong CASA engagement usually starts well before formal testing. The most successful teams take their time and don't treat it as a last minute task.

- **Submit your application for validation by Google and receive the required assurance level and assessment path.**
- **Prepare the application and onboarding evidence.** This may include architecture context, data flow understanding, source access where needed, environment access, and prior scan outputs.
- **Run or review required testing activities.** Depending on the engagement, this can involve lab validation, scanning, manual review, or a fuller independent assessment.
- **Remediate identified issues.** Findings are addressed so the application meets applicable requirements.
- **Finalize validation output.** Once requirements are satisfied, the assessment can be closed out and reported through the required process.

The **preparation guide attached** to this page is a useful companion resource for teams getting ready for a CASA or MASA engagement. It is best used as a practical checklist before formal assessment work begins.

A simple rule of thumb, if your team can clearly explain your app, data flows, and security controls before the lab has to ask, you're on a successful path.

Where Prescient Security fits

Prescient Security helps teams approach CASA as a practical security validation exercise, not a compliance event. The value lies in helping customers understand where their real risk sits, and how to get through the process with less friction. The end goal is to help our client demonstrate that their application can securely handle the data access it requests.

Additional support here