

DenseAI Armour

The AI-usage surface your last assessment never looked at. Your people are already using AI assistants, and the vendor keys they hand those assistants tend to sit in plaintext on the same machines you just had assessed. DenseAI Armour is the DenseDefense suite's answer to that surface. In active development -- this is an overview of what it is for, not an API reference.

● Early Adopter -- in active development

● Read-only by design -- it changes nothing on your systems

● Not assessed != passed -- the honest-reach doctrine

● API reference published at general availability

What this document is

STATUS

DenseAI Armour is an **Early-Adopter** capability, in active development. There is no shipping public REST API yet, so an API reference would be premature. This page is a product overview: what it is for and where it fits.

SCOPE OF CLAIMS

This overview describes *purpose and intent*. It does not assert current capability -- nothing here should be read as a claim that the product finds, scans, or reports on your environment today.

WHAT COMES NEXT

Full API documentation will be published at general availability. Until then, [contact us for early access](#) to help shape the surface before it ships.

CONTENTS

- 1 What DenseAI Armour is
- 2 What it is for

- 3 The honest-reach doctrine
- 4 Where it fits in the suite
- 5 Status & what comes next

1 | What DenseAI Armour is

DenseAI Armour is the DenseDefense suite's AI-usage assessment capability. Compliance assessments were designed for a world of servers, shares, and endpoints. They were not designed for the assistants your people now type into every day -- and the credentials those assistants are handed to do their work. DenseAI Armour exists to bring that surface into the same honest, evidence-first posture the rest of the suite already holds.

It is being built as a **read-only** capability: its purpose is to look and report, never to change anything on the systems it looks at. That is a deliberate design choice, not a limitation to be lifted later.

Tip -- This is an overview of a product in active development. It describes what DenseAI Armour is *for*. It is not an API reference, and nothing here is a claim that the product performs any of these functions on your environment today.

2 | What it is for

Your people are already using AI assistants, and the vendor keys they hand those assistants tend to sit in plaintext on the same machines you just had assessed. DenseAI Armour is aimed squarely at that gap: the AI-usage surface that a traditional CMMC or 800-171 assessment simply never looked at.

The surface it is being built to bring into view includes:

SURFACE	WHY IT MATTERS
Local model endpoints	An AI model running on a workstation is a service on your network like any other -- and one your last assessment did not enumerate.
Agent configurations	The assistants and agents your people wire up define what an AI can reach and act on. Their configuration is part of your real attack surface.
Credentials at rest	The vendor keys handed to those assistants often live in plaintext beside the work they touch -- exactly the exposure the rest of the suite is built to surface.
The AI vendor organization	The account and organization behind the assistant carry their own settings and posture, outside the boundary an on-host scan alone can see.

Note -- Positioning only. Each row above states an *intended* area of coverage for a product in active development, not a shipped feature list. Coverage, names, and behavior may change before general availability.

3 | The honest-reach doctrine

DenseAI Armour is being built to hold the same line the whole DenseDefense suite holds: **a clean result you cannot trust is worse than no result at all**. Where the product cannot reach a part of the surface, the design intent is to mark that part *not assessed* rather than quietly report it as passed.

This matters most for AI usage, because AI reachability is a vantage: what one collection point can see is not the whole picture, and a network view can call a host clean while missing what only a host-local view would show. The doctrine is to be explicit about the edge of what was reached, so an assessor is never handed a false all-clear.

Tip -- "Not assessed, not passed" is the same principle that governs the rest of the suite's evidence: report what was reached, name what was not, and never let a gap in reach read as a clean bill of health.

4 | Where it fits in the suite

DenseAI Armour is one product in the DenseDefense suite, alongside the compliance engine that scans and remediates your Windows and Linux fleet against CMMC Level 2 / NIST 800-171, the offensive console that proves exposures are real, and the evidence-and-custody layer beneath them. DenseAI Armour extends that same posture to a surface the others were never built to cover: how AI is actually used across your environment.

The intent is that AI-usage findings live in the same honest, evidence-first frame as everything else the suite reports -- so a shop that has assessed its fleet can also account for the AI its people brought in, rather than leaving that surface uninventoried and unspoken-for.

Tip -- DenseAI Armour reads; by design it changes nothing on your systems. It is meant to add visibility to your posture, not to act on your hosts.

5 | Status & what comes next

DenseAI Armour is an **Early-Adopter** capability, in active development. There is no shipping public REST API today, which is why this is an overview and not an API reference -- publishing an interface reference for a surface still being shaped would be a promise the product is not yet ready to keep.

- **Available now:** the early-access program. [Contact us for early access](#) to see the product take shape and to help steer what it covers first.
- **At general availability: full API documentation will be published** -- every route, its inputs, and its outputs -- in the same detailed reference form as the rest of the suite's products.

Note -- Everything in this overview describes purpose and direction for a product in active development. Treat any capability named here as *not available today* for planning purposes, and confirm current status against the build you are offered.

DenseAI Armour (Early Adopter) -- an AI-usage assessment capability in active development inside the DenseDefense suite. This overview describes the product's purpose and its place in the suite; it is not a specification, a commitment to a delivery date, or a claim of shipped behavior. Full API documentation will be published at general availability.

DenseDefense | densedefense.com. [Contact us for early access](#) to be part of the preview.