OPENAI ARCHITECTURE PRIMER

The OpenAI Daybreak Cyber Stack

Products, access, evidence,
and operating authority

A visual guide to the OpenAI cyber program and the enterprise controls that surround its use.

FIRST-PARTY DOCUMENTATION / INDEPENDENT LUMINITY SYNTHESIS



Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

OpenAI Select Partner

Daybreak Combines Access, Products, and Operating Controls

OpenAI defines the program and product surfaces. The organization still supplies target authority, review, and change control.

AT A GLANCE

3	7	2	1
access states	entry points	authority gates	retained record
Standard, Blue, Red	managed and programmable	target and downstream action	evidence and disposition

TWO DISTINCTIONS PROTECT THE REVIEW

Access Tier Versus Product Surface

Blue and Red describe trusted access. Defense Factory, plugin, review, CLI, SDK, and API describe where work happens.

Product Capability Versus Authority

A product can analyze or propose. The customer still establishes target permission and authorizes consequential action.

BOUNDARY

Documented Boundary

Daybreak access does not establish entitlement for a specific workspace, permission to test a target, or authority to merge, deploy, or close work.

IN THIS PRIMER

Key Points

01 Read the Stack

Separate access, products, runtime controls, and enterprise systems.

02 Choose the Surface

Match the target, trigger, runtime, evidence store, and review method.

03 Govern the Outcome

Retain the evidence, record the decision, and bind the next step to authority.

OpenAI supplies the program and product capabilities. Luminity composes the client operating model.

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://openai.com/daybreak/ · verified Nov 13, 2026

OpenAI Select Partner

Daybreak Stack Architecture

Governed work moves from approved access through a selected surface and controlled runtime into evidence and an authorized enterprise decision.

01 WHAT ENTERS THE STACK?

Approved target	ENTERPRISE
Access tier and model	PROGRAM
Selected product surface	PRODUCT
Runtime identity and connection	RUNTIME
Downstream authority	NOT SUPPLIED

Approved context → Governed execution

02 HOW GOVERNED WORK MOVES THROUGH THE STACK

Access · Standard, Blue, Red

Surface · managed or programmable

Enterprise · named authority



OPENAI PROGRAM
Access and product capability

CONTROL STATE
Identity, policy, evidence

ENTERPRISE SYSTEM
Decision and retained record

03 FOUR ARCHITECTURE DISTINCTIONS

Access Versus Surface — ENTRY

Blue and Red describe trusted access; product surfaces describe where work runs.

Capability Versus Authority — AUTHORITY

Product analysis or proposals do not supply target or change authority.

Evidence Versus Decision — RECORD

Findings and artifacts support review; they do not record the final disposition.

OpenAI Versus Luminity — BOUNDARY

OpenAI supplies the program and products. Luminity designs the client operating model.

ARCHITECTURE RULES

- Keep access distinct
- Name the runtime identity
- Retain the evidence
- Bind action to authority

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://openai.com/daybreak/ · verified Nov 13, 2026

OpenAI Select Partner

Managed and Programmable Daybreak Surfaces

Surface choice changes the trigger, runtime, evidence store, and review method; current access and target authority remain separate.

01 WHICH SURFACE IS BEING CONSIDERED?

Defense Factory	MANAGED
Daybreak Plugin	MANAGED
Security Review	MANAGED
CLI and Security in CI	PROGRAMMABLE
TypeScript SDK and OpenAI API	PROGRAMMABLE
Access and target authority	CONFIRM

Managed surfaces → Programmable surfaces

02 HOW SURFACE CHOICE CHANGES OPERATION

Target · repository, pull request, app

Runtime · remote, local, pipeline

Evidence · shared or app-owned

Select — Match the use

Trigger — Request, event, command

Run — Managed or application-owned

Review — Retain evidence and disposition

RUNTIME
Remote, local, pipeline, or application

EVIDENCE
Shared product record or app-owned logs

OWNER
Team, repository, pipeline, or application

03 FOUR SURFACE DISTINCTIONS

Managed Versus Programmable — MODE

Managed products supply an operating experience; programmable paths require application controls.

Local Versus Remote — RUNTIME

Plugin and CLI can work locally; Defense Factory and APIs use connected or remote execution.

Shared Versus App-Owned Evidence — EVIDENCE

Product surfaces may retain shared findings; SDK and API callers own response logs.

Product Review Versus App Review — OWNER

Review may occur in a product, repository, pipeline, or application.

DO NOT ASSUME

- Same entitlement
- Same runtime
- Same evidence store
- Same decision authority

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://openai.com/daybreak/ · verified Nov 13, 2026

OpenAI Select Partner

Governed Cyber Work Across the Stack

The stack produces useful evidence when the workflow keeps target authority, review, change authority, and verification explicit.

EVIDENCE AND AUTHORITY PATH



CONTROL RECORDS AROUND THE DECISION

Target Record

System, owner, permission, scope, revision

Coverage Record

Examined, excluded, interrupted, incomplete

Validation Record

Evidence tested against current context

Change Evidence

Patch, tests, risk, review, deployment

Disposition Receipt

Reviewer, decision, owner, next step, location

AUTHORITY LIMIT

Analysis and proposed fixes support a decision. A named person or approved process authorizes consequential action.

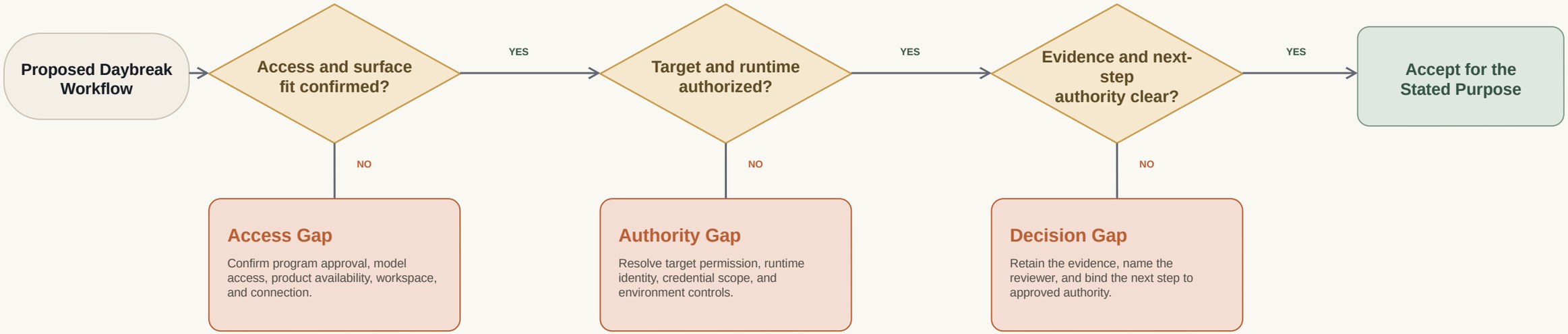
© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://openai.com/daybreak/ · verified Nov 13, 2026

OpenAI Select Partner

Daybreak Stack Acceptance

Accept a Daybreak-enabled workflow only for the documented product purpose, approved target, reviewed evidence, and authorized next step.



REQUIRED OVERLAYS

Access and Surface
Program, product, workspace, connection

Target and Scope
Owner, permission, revision, limits

Runtime Controls
Identity, credentials, network, audit

Evidence Package
Coverage, findings, artifacts, validation

Decision and Authority
Reviewer, disposition, owner, next step

ARCHITECTURE RULE — **Keep access, execution, evidence, and authority distinct.**

OPENAI BOUNDARY — Product access and generated artifacts do not establish enterprise approval.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://openai.com/daybreak/ · verified Nov 13, 2026

OpenAI Select Partner