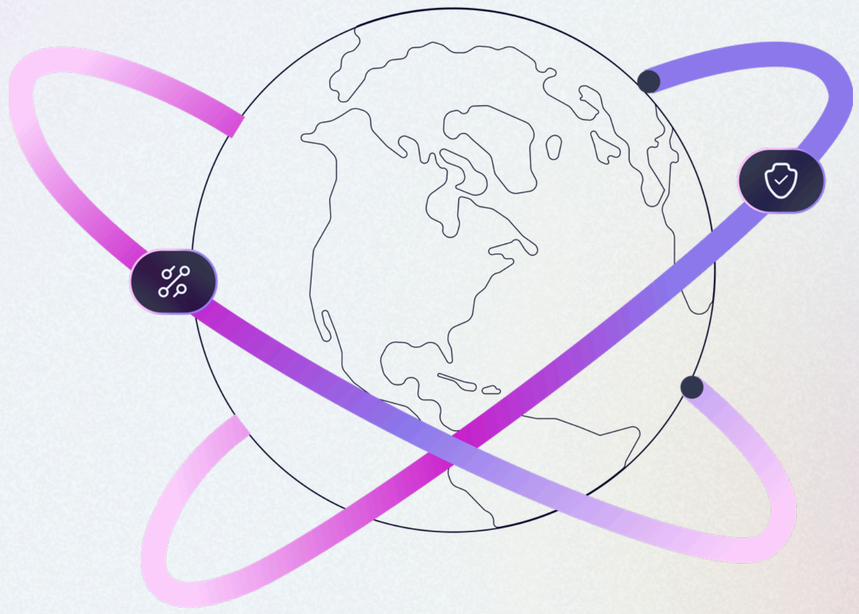
britive

>_ SOLUTION BRIEF

Cloud-Native Privileged Access Management

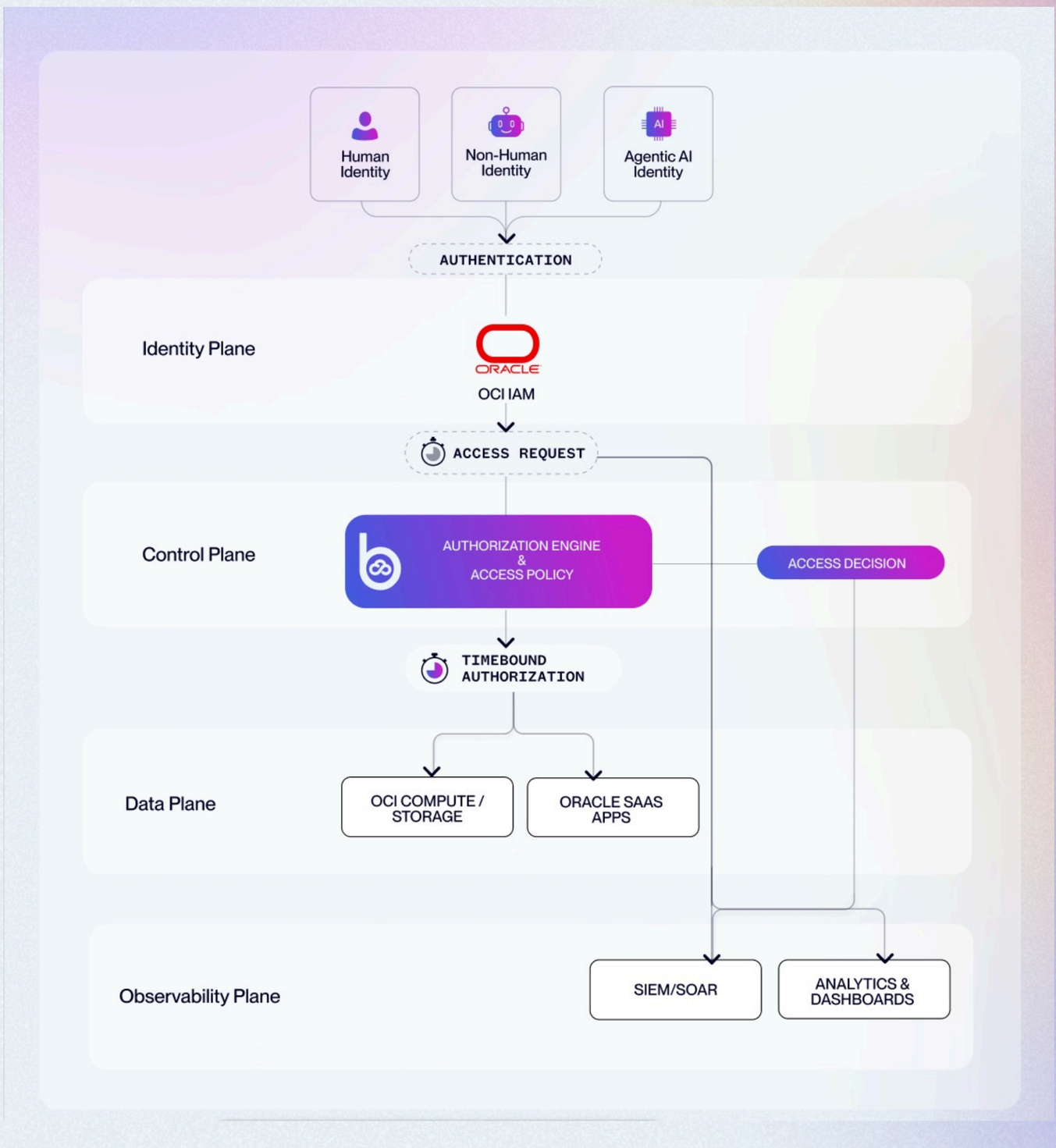
for Oracle Cloud Infrastructure (OCI)



Britive integrates directly with Oracle Cloud Infrastructure's (OCI) native IAM and API framework to deliver ephemeral, just-in-time (JIT) privileged access for both human and non-human identities. Through API-level integration, Britive manages OCI resource permissions dynamically, provisioning and revoking them in real time without requiring agents, proxies, or network reconfiguration.

Britive connects via OCI's Identity Domains, Policies, and Dynamic Groups to:

- Discover and inventory all OCI identities, roles, and entitlements.
- Enforce Zero Standing Privileges (ZSP) by assigning access only at request time.
- Provide audit-ready visibility into who accessed which OCI resources, when, and for how long.
- Apply consistent policy-as-code controls across OCI, AWS, Azure, and GCP from a single platform.



SECURING ACCESS FOR INDUSTRY LEADERS

RxBenefits · fiserv. · MARQETA · GAP · Forbes · ThermoFisher SCIENTIFIC · PROCORE · TOYOTA · cityblock

THE CHALLENGE: STATIC PRIVILEGE MODELS

Modern OCI environments mix infrastructure, platform services, and Oracle SaaS apps.

Each layer comes with its own IAM logic, service accounts, and admin roles, creating hidden standing access.

What breaks:

- Standing privileges persist across tenancy and SaaS tiers.
- Native IAM + OAM tools handle user login but not runtime privilege changes.
- Manual provisioning and ticket-driven access slow DevOps teams.
- Hard-coded credentials in OCI scripts and SaaS connectors expand attack surface.

The result: over-provisioned access and delayed governance that no longer fits Zero Trust or compliance needs.

BRITIVE'S SOLUTION: RUNTIME AUTHORIZATION AT EVERY LAYER

Britive replaces static roles and vault-based secrets with Just-in-Time (JIT) authorization and Zero Standing Privileges (ZSP). Access is created dynamically, scoped by policy, and deleted when the task completes.

Unified Access Model	One policy framework across OCI IaaS, PaaS, and Oracle SaaS (ERP, HCM, EPM).
No Agents or Connectors	Native API integrations via OCI IAM and SaaS APIs.
Runtime Policy Evaluation	Access decisions are enforced continuously based on context (identity, role, data sensitivity, time, and risk).
Ephemeral Access & Roles	Credential, access, and tokens exist only upon request at runtime. Nothing stored, nothing vaulted to achieve Zero Standing Privileges (ZSP) at scale.
Audit at Cloud Speed	Every OCI access request, approval, and revocation logged for instant "who-had-what-when-and-why" for real-time visibility and compliance mapping.

KEY OUTCOMES

ELIMINATE STANDING PRIVILEGES

- Replace static keys and roles with ephemeral, just-in-time access.
- Enforce Zero Trust and least-privilege by default.
- Remove persistent admin rights across OCI.

UNIFY MULTI-CLOUD GOVERNANCE

- Manage OCI, AWS, Azure, and GCP from one platform.
- Apply consistent, policy-based access controls everywhere.
- Eliminate tool sprawl and manual configurations.

ACCELERATE SECURE ACCESS

- Automate provisioning and revocation in real time.
- Enable self-service access through chat or APIs.
- Keep DevOps and cloud teams moving fast, securely.

STRENGTHEN COMPLIANCE & VISIBILITY

- Centralize logs and audit trails across OCI.
- Prove Zero Standing Privileges for SOC 2, PCI, ISO, etc.
- Simplify audits with full access transparency.