Orchid

Solution Brief: Uncovering Identity Dark Matter

- See What Others Don't, Secure What Others Can't

From Problem to Action

In our Buyer's Guide to Identity Dark Matter, we showed how every enterprise carries a hidden layer of identity risk: unseen applications, unmanaged accounts and authentication paths your IAM stack does not track.

This brief outlines the next step: how Orchid transforms blind spots into visibility, evidence, and control.

The Challenge

Enterprises run thousands of applications, built at different times, by different developers, to meet different requirements. Your IAM stack, CMDB, or SIEM can show what they know and your app documentation or latest owner will reflect what they think they know.

But what about what they do not know?

Lurking outside the stack and deep inside each application are exposures invisible to most tools. We call this Identity Dark Matter:

Legacy and Shadow Apps

Old, incompatible, or overlooked during onboarding.

Orphaned and Local Accounts

Hardcoded, over-privileged, or leftover after users leave.

Hidden Authentication Paths

Alternate or emergency login methods, often undocumented, that no one monitors.

Identity Control Drift

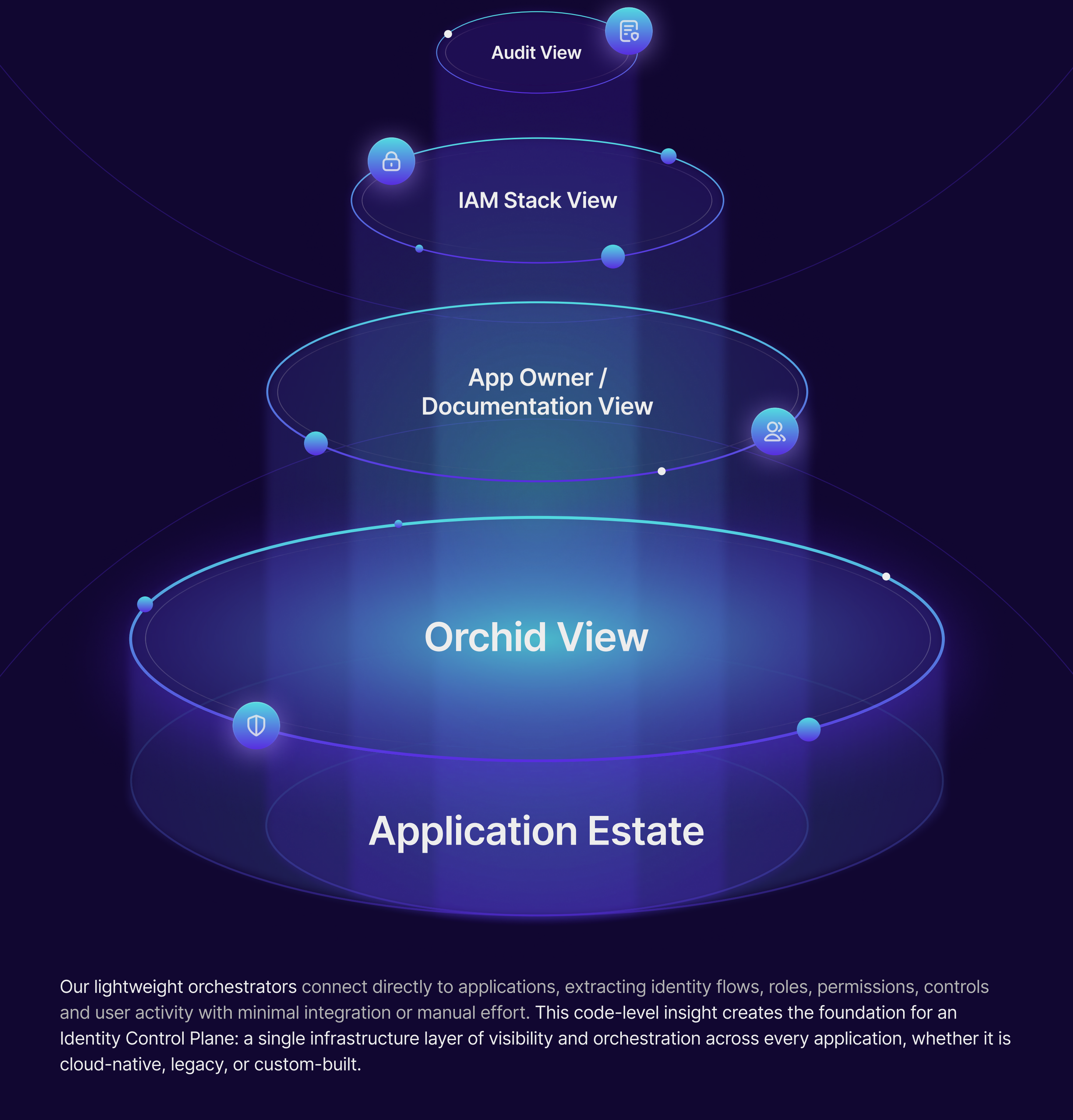
What is coded into apps does not always match IAM policy over time.

User Activity

Permissions show what is possible, not what actually happened.

The Orchid Approach

Just as telescopes infer the presence of dark matter by looking beyond what the eye can see, Orchid detects identity dark matter by looking beyond what IAM stacks show or documentation says. Traditional identity tools and processes rely on configurations, surveys, or self-attestations. Orchid goes deeper. We extract the truth from its source: the application itself.



Our lightweight orchestrators connect directly to applications, extracting identity flows, roles, permissions, controls and user activity with minimal integration or manual effort. This code-level insight creates the foundation for an Identity Control Plane: a single infrastructure layer of visibility and orchestration across every application, whether it is cloud-native, legacy, or custom-built.

Here is what makes Orchid different

By combining continuous discovery, analysis, and orchestration, Orchid bridges the gap between policy and reality. The result is visibility you can trust and enforcement you can prove.

Govern Without Bottlenecks

Remove dependency on app owners. Orchid pre-populates governance questionnaires, accelerates onboarding, and enables integrations with a single click.

Prove Compliance

Generate evidence directly from applications and map it to regulatory standards like PCI, HIPAA, GDPR, SOX, NYDFS, NIST, and ISO. Auditors see reality, not assumptions.

Expand your view

Go beyond the stack to discover unmanaged apps, legacy code, and hidden logic that live outside IAM tools. Orchid builds a dynamic inventory so nothing is overlooked.

Graph Authentication Flows

Visualize every login path, including undocumented or fallback methods. See what is actually coded, not just what is configured.

Assess Authorization Logic

Surface the full picture of accounts, roles, and permissions buried in application code. No manual reviews, no self-certifications, no guesswork.

Track Remediation

Assign, track, and confirm resolution of exposures with full accountability. Issues no longer get lost or avoided when thrown “over the fence” to developers.

Understand Activity

Move beyond what is supposed to be possible. Orchid shows how accounts and permissions are actually used in real time.

Use Cases and Benefits

Infrastructure

Build a dynamic app inventory with automated risk ratings.

Map app identity data to frameworks and onboarding workflows.

Enable one-click integrations into IAM and governance tools.

Audit and Compliance

Out-of-the-box reports with evidence from application binary.

Provide auditors with proof that the policy matches reality.

Identify abandoned, over-privileged, and local accounts.

Incident Response

Surface hidden credentials and permission chains.

Visualize identity flows in real time.

Accelerate investigations with user activity evidence.

The Bottom Line

Orchid Security is the only agent-based platform built for application-first identity visibility and orchestration.

- **Discover** every app, flow, and control, managed or unmanaged.
- **Eliminate dark matter**: shadow apps, orphaned accounts, hidden paths, and drift.
- **Map evidence to standards**, including PCI, GDPR, HIPAA, NYDFS, SOX, NIST, and ISO.
- **Track remediation to closure**, often without requiring code changes.
- **Provide real-time, auditable truth** across your identity stack.

Proof in Practice

Leading enterprises across industries are redefining identity with Orchid:

COSTCO WHOLESALE

repsol

HUB

↳ See how Orchid brings the unseen into focus. Visit orchid.security/customer-stories