Orchid

A Buyer’s Guide to Application-First Visibility

Uncovering Identity Dark Matter

Introduction

Executive Summary

Most IAM leaders believe they have strong visibility into their environments. They have centralized authentication. They have corporate policy. They pass audits.

But every year, new breaches prove the same painful truth: attackers do not go through the front door. They find the unmonitored applications, the orphaned accounts, the forgotten service credentials, the hidden authorization paths and the missing or weak controls. They now even look for the “harvest now, decrypt later” data. These blind spots form what we call Identity Dark Matter: the unseen but powerful forces shaping risk across your enterprise.

Traditional sources of IAM data such as your current IAM stack, CMDBs, audit reports, activity logs, or even modern network-based discovery tools offer only an indirect and incomplete picture. They describe how a subset of systems should work, not how identity actually functions inside each and every application - basically just scratching the surface and giving a false sense of security.

The only way to significantly reduce Identity Dark Matter is to go straight to the source: the applications themselves. By analyzing applications at the binary level, organizations can uncover every app, every account, every identity flow, and every control (or lack thereof),

Discover hidden applications outside the IAM perimeter.

Map forgotten accounts and unused credentials.

Analyze authorization policies coded directly into applications.

Tie identity controls directly to compliance, security and best practice frameworks.

Confidently reduce exposure and prove it.

The Problem

Blind Spots in Identity

Indirect Sources = Incomplete Visibility

Most IAM programs rely on information aggregated from:

- The existing identity stack, which excludes unmanaged applications.
- CMDBs and asset inventories, which often miss legacy or shadow apps.
- Audit reports, which only validate what is sampled and tested.
- Logs and network traffic, which capture activity but not configuration or intent.
- Application documentation or owners, which quickly go stale.

Each of these is at least one step removed from the actual controls coded and deployed in applications. That means they cannot give you a complete or current picture of your identity posture.

Examples of Identity Dark Matter

Forgotten apps

Legacy or shadow systems left out of IAM scope but still authenticating users, storing data, and serving part of the organization.

Orphaned accounts

Accounts that remain active even after the owner leaves, need passes, or a provisioning error occurs.

Local credentials

Hardcoded service accounts or local admin users never tied back to central IAM.

Shadow AuthN and AuthZ paths

Hidden rules or bypasses coded into applications, often undocumented.

Privilege drift

Permissions that accumulate over time, unmonitored and unchecked.

Weak controls

Variants of technologies that check compliance boxes but leave organizations exposed.

The Problem

Blind Spots in Identity

The Consequences

Compliance risk

Time consuming audit processes- for **PCI, HIPAA, GDPR, NYDFS**, and similar- that often fail to satisfy auditors and typically leave organizations exposed despite “compliance”.

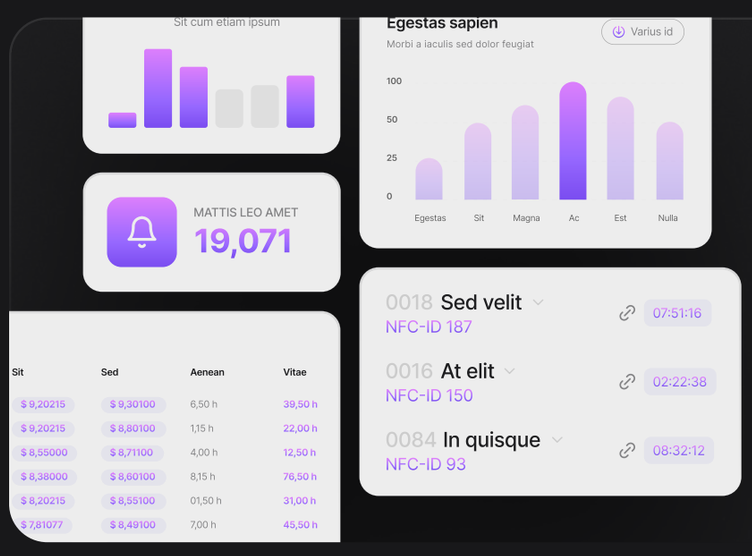
Operational cost

IAM activities are **high effort**, low outcome processes that **drain resources, burden teams, and often remain incomplete.**

Security exposure

Threat actors exploit the very blind spots **your IAM program cannot see**, resulting in cyber compromise and all that entails.

Industry Snapshot

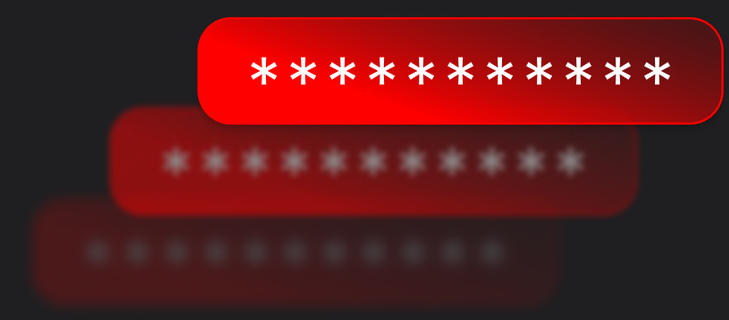


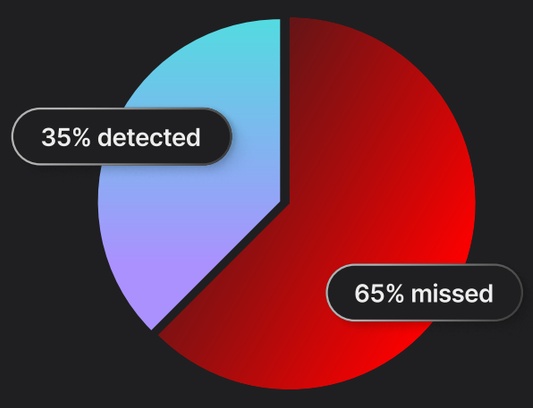
One Missed App = 1.1M Exposed

In July 2025, Allianz Life disclosed a breach impacting 1.1 million customers after attackers exploited OAuth permissions in a CRM integration. A single overlooked application gap put customer data at risk.

16 Billion Logins Lost

One of the largest credential leaks ever, discovered in 2025, exposed 16 billion login credentials collected by infostealer malware, highlighting the sheer scale of identity exposure





Check Point Cloud Security Report

65% of Incidents Go Undetected - Check Point’s 2025 Cloud Security Report found that only 35% of incidents are detected by monitoring tools, leaving the majority discovered by third parties or end users

These are just a few examples that underscore the cost of indirect and incomplete visibility as well as the urgent need for direct, application-level insight.

The Solution

Application-First Visibility

Go Straight to the Source

Instead of working from secondhand data, application-first visibility examines applications directly at the binary, runtime, and configuration level.

Mapping **all authentication flows** (SAML, OAuth, OIDC, Kerberos, LDAP, custom auth).

Discovering **all applications**, including those self-hosted, whether centrally registered or unmanaged.

Extracting **all authorization logic** (roles, policies, entitlements) from inside the app.

Correlating **all accounts and credentials** (users, service accounts, local logins).

Assessing **all controls**, not just their application, but also their strength.

Benefits for IAM Leaders

Accuracy

Direct evidence from applications, not assumptions from logs.

Completeness

Visibility into shadow IT, legacy apps, and unmanaged identities.

Confidence

Audit ready data, straight from the source, tied directly to compliance controls.

Actionability

Proactive discovery of gaps for prioritized remediation with evidence you can prove.

The Solution

Application-First Visibility

Real-World Scenarios

A global bank discovered 30% more applications than were listed in their CMDB once direct application scans were run.

A healthcare provider uncovered hundreds of orphaned accounts tied to retired staff, including some with privileged access.

A retail enterprise found local service accounts with domain admin rights running in production systems, entirely invisible for IAM tools.

A paper manufacturer found (despite regular security assessments) identity exposures within a label printing application that could allow a threat actor to break their strict segmentation.

Alignment with Best Practices

Zero Trust requires continuous, context-rich visibility at the app layer.

Continuous Assurance is now expected by regulators who want real-time, not annual, validation of IAM controls.

Least Privilege is impossible without knowing every entitlement and control in use.

What Good Looks Like: Buyer's Checklist

10 Questions every IAM leader should ask to understand the size of Identity Dark Matter

Pro Tip: Each "no" answer reflects dark matter in your identity and a blind spot in your identity program.

/ 01

Can I see all applications in my environment, including those we host ourselves, not just the ones registered in IAM / CMDB or kept modern by others as SaaS?

Only 31% of CISOs indicated that they have even a mostly current application inventory.

/ 02

Do I know every authentication flow and protocol in use, not just the primary one that may be compliant with corporate policy, regulations and best practices?

On average, an enterprise application has 2.4 identity flows coded into it.

/ 03

Can I map all authorization policies inside each application, not just the most common ones covering the majority of users?

It is very common to find an explosion of groups within directory services, not to mention additional authorizations coded natively in an application.

/ 04

Can I identify orphaned, inactive, over-privileged and service or otherwise unused accounts, not just those managed in the primary directory?

44% of organizations report more than 1,000 orphaned accounts, as well as 26% of all accounts that have gone unused for 90+ days.

/ 05

Do I have visibility into local credentials and alternate shadow identity paths?

Nearly half of enterprise applications have credentials hard-coded directly within the application.

/ 06

Can I demonstrate which apps/flows/ accounts are covered by which controls, especially when required by compliance frameworks (PCI, HIPAA, GDPR, NYDFS, SOX)? And do I know the strength of each control?

Most organizations can demonstrate, through documentation, which applications are covered by identity controls; but not which applications or flows are not covered.

/ 07

Can I continuously monitor for drift- changes made to go live, through patches or as part of major upgrades- in permissions or policies?

It is estimated that 5% of applications get patched each month, resulting in substantial drift over time.

/ 08

Can I prioritize remediation based on risk and compliance impact? More importantly, can I assign, track and confirm their completion?

Today, IAM teams are at the mercy of application developers to remediate issues and have to take them at their word that it's been completed.

/ 09

Can I prove compliance with policy, process and resolution with evidence directly from applications and user activity?

Compliance is most commonly demonstrated through documentation or self-certification, rather than looking at each application itself.

/ 10

Can I scale this across thousands of apps in hybrid and multi-cloud environments?

According to CISOs, the average enterprise hosts 80% of applications themselves, with 20% managed by SaaS providers.

Buyer Action Plan

01

Assess your current visibility.

Use the checklist to measure the line of sight offered by your **CMDB**, **IAM**, and log-based tools.

02

Identify the gaps.

Which apps are unmanaged? Which accounts or permissions cannot be tracked? Which identity flows are overlooked? Which controls are too weak, or missing altogether?

03

Evaluate new approaches.

Look for solutions that **provide application-first visibility**, not just log aggregation or asset mapping.

04

Build the internal case.

Position the **ROI** in terms of:

- **Compliance readiness** (reduced audit friction).
- **Risk reduction** (fewer breach entry points).
- **Operational efficiency** (faster remediation).

05

Pilot and expand.

Start with a critical business unit or compliance scope. Show hidden findings. **Build momentum**.

About Orchid Security

Orchid Security delivers an Identity Control Plane designed to simplify and strengthen identity and access management (IAM).

Our platform continuously discovers enterprise applications, automatically analyzes authentication and authorization flows- comparing them against regulatory requirements and cybersecurity frameworks- and streamlines resolution that includes augmenting native capabilities and onboarding into IAM systems with little to no effort or coding.

By uncovering and addressing “identity dark matter” hidden across environments, Orchid helps organizations reduce cybersecurity risk, lower operational costs, and meet compliance requirements at scale. Backed by Intel Capital and Team8, Orchid is already trusted by Fortune 500 and global 2000 organizations across industries.

Orchid Security is trusted by

To learn more about our customers, visit orchid.security/customer-stories

Compliance Certificates

- CSA STAR Level 1
- GDPR
- HIPAA
- ISO/IEC 27001
- ISO/IEC 27701
- SOC 2 Type 2

To learn more about our commitment to security and privacy, visit trust.orchid.security/