How CISOs should approach their identity security programs: a first principles guide

Contents

1. Introduction: cutting through the identity security noise

Identity security has become an acronym factory, but only three pillars matter: IAM, IGA and PAM.

CISOs are drowning in acronyms: IAM, IGA, PAM, CIEM, ITDR, ISPM, NHIs, agentic identities and whatever comes next quarter. Every few months, a new product category is created, usually by vendors and analysts rather than practitioners. The result is a landscape full of overlapping tools, conflicting claims and unclear value.

Most of these acronyms are not solving new problems. They are repackaging slices of old ones. Complexity has often been rewarded in the market, but for security leaders it is a liability. If you strip away the noise and think from first principles, identity security is straightforward: protect sensitive company assets from misuse by the workforce. Everything else is a tactic.

Once you frame the problem this way, you see something powerful: there are only three platforms that matter, IAM, IGA and PAM. these are not full-blown solutions…they are capabilities. Useful signals, perhaps. But not something that deserves to exist as a standalone pillar in your architecture. And the reason these other acronyms keep popping up is because the core three pillars in many organizations are still anchored in an on-premise world. As organizations move critical workloads to the cloud and adopt hundreds of SaaS apps, core platform vendors haven't kept up with the new stack—even though the use cases remain the same.

This does not mean you only need three tools. No vendor, legacy or modern, fully addresses all the needs of a single platform. But you do need a three-pillar framework that anchors your identity strategy and helps you separate what is essential from what is noise. The sections that follow break down what each platform does, why they matter and how to use this lens to cut through vendor sprawl, close real gaps and simplify your identity stack without losing control.

2. Identity security from first principles

At its core, identity security exists to protect sensitive company assets from misuse by the workforce. Three words matter here: protecting, assets, workforce.

A note on scope

When we talk about identity security in this paper, we mean workforce identity: every human, non-human, or agentic identity that can access company assets. Customer identity and device identity are separate domains, each with their own platforms and challenges.

Protecting = authentication + least privilege authorization

To protect something, you must first know who is requesting access and then enforce the right level of access. Authentication verifies who an identity is, solved by IAM. Authorization governs what they can access, when and why, solved by IGA and PAM.

These jobs serve different personas. IAM is typically owned by enterprise IT or IAM teams. Their priority is ensuring reliable connectivity so identities can log in to the systems they need without disruption. If SSO or MFA fails, the business stops. Their success is measured by keeping access available, not by minimizing privileges.

IGA and PAM, on the other hand, are the domain of security and GRC teams. Their priority is control and risk reduction, ensuring users have only the access they need and that sensitive systems are protected from abuse.

Assets = applications and infrastructure

Not all assets are equal. Low-blast-radius apps include collaboration tools, HR systems, CRMs and internal business apps. High-blast-radius systems include cloud provider consoles, production databases, CI/CD pipelines and domain controllers.

For the first group, security teams focus on coverage and compliance, ensuring periodic access reviews and revoking stale access. This is the domain of IGA. For the second, they need precision and observability, enforcing short-lived access, monitoring sessions and integrating with engineering workflows. This is the domain of PAM. That is why IGA and PAM emerged as distinct categories.

Workforce = every identity that can access an asset

"User" is no longer enough. Today's workforce includes employees, contractors, vendors, service accounts, workloads, IAM roles and AI agents. These identities authenticate with passwords, keys, or tokens, but the underlying issue is the same: they can access assets. If they can access assets, they must be governed by the identity program. Agentic identities are still emerging, but the principle remains the same. Any solution that stops at "users" is solving yesterday's problem.

3. IAM—the authentication layer

IAM is the front door to your environment. Its job is to establish trust at login.

A mature IAM program handles storing and managing identities, authenticating with credentials and factors such as passwords, MFA, passkeys, API keys, OAuth tokens and TLS certificates, enabling SSO and federation and syncing directories between HR, IT and SaaS systems. The goal is to establish trust at login, reliably and at scale.

IAM teams, usually within enterprise IT, optimize for connectivity and uptime. Connectivity means authentication works across all applications and systems. Uptime means login services are always available. If authentication fails, productivity halts. Their success is measured by reliability, not by reducing privileges.

IAM's job ends after trust is established. It does not provision access, elevate privileges, monitor sessions, or validate appropriateness. Those belong to IGA and PAM. Keeping this boundary clear ensures IAM remains lean and dependable.

4. IGA and PAM—two different classes of assets

Once an identity is authenticated, the job shifts from who you are to what you can do. This is where least privilege comes in and where the landscape splits into two distinct control planes.

IGA: Governance at scale

IGA governs access to the broad majority of business applications, such as HR systems, CRMs, finance tools and collaboration platforms. These apps are important, but not catastrophic if misused. Core IGA functions include provisioning and deprovisioning based on roles and HR events, periodic access reviews and certifications, detecting and removing stale entitlements and reporting on access. The persona is GRC or compliance teams. The goal is coverage and audit readiness.

PAM: Precision for high-impact systems

PAM governs access to high-value assets such as production cloud consoles, domain controllers, privileged Unix accounts, production databases and CI/CD pipelines. Core PAM functions include just-in-time access elevation, session monitoring and recording, fine-grained controls for admin actions and vaulting or rotation of shared credentials. The persona is security engineering or operations, often working closely with DevOps. The goal is to minimize blast radius continuously.

Why they are separate

IGA and PAM both enforce least privilege, but the stakes, controls and owners differ. IGA is designed for broad governance across a large number of lower-blast-radius applications where the main priority is compliance, auditability and coverage at scale. PAM is designed for high-blast-radius systems where the priority is technical depth, precision and continuous control. The personas are also different: IGA is led by GRC and compliance teams, while PAM is led by security engineering and operations. Merging them into one platform requires a clear understanding of use cases and the difference in ownership, which is why they have remained distinct.

5. Understanding the stack—where (and why) gaps emerge

By the late 2000s, the typical enterprise stack paired Active Directory for IAM, SailPoint for IGA and CyberArk for PAM. Over time, several shifts created gaps in this model.

- **SaaS explosion:** Enterprises now run hundreds of SaaS apps, each with unique RBAC models. Legacy IGA and PAM were not built for federated governance at this scale.
- **Ephemeral infrastructure:** Containers, serverless and cloud resources spin up and down in seconds. Older PAM assumed static servers and long-lived credentials.
- **API-driven operations:** Privileged actions increasingly happen through APIs, while traditional PAM controlled access at the network layer.
- **Non-human identity growth:** Service accounts, cloud roles, workloads and AI agents require lifecycle governance, but legacy IAM, IGA and PAM were designed for humans first.
- **Vendor fragmentation:** Point tools emerged to fill gaps, marketed as new acronyms such as CIEM, ITDR and ISPM.

Today's hybrid enterprises mix on-prem, SaaS and cloud-native systems. Legacy IAM, IGA and PAM platforms were designed for narrower environments and those assumptions break down. Vendors increasingly overlap in features, but the functional distinctions between IAM, IGA and PAM remain critical for clarity of ownership and architecture. CISOs should map every asset to IAM, IGA, or PAM and flag high-blast-radius systems that remain uncontrolled. Fill gaps by extending a pillar, not adding a new control plane

Continuous posture assurance—closing the loop

Modern identity programs can't stop at provisioning and access enforcement. They also need continuous assurance that access posture in the environment still matches policy intent.

This is where many legacy IGA and PAM deployments fall short. They were designed for static environments, where quarterly access reviews and periodic audits were considered "good enough". In a SaaS- and cloud-first world, that model breaks down. New entitlements appear daily. Service accounts proliferate. AI agents and workloads request access autonomously. Drift happens constantly.

A modernized IGA/PAM stack must therefore include continuous posture monitoring:

- Detecting orphan accounts or dormant privileges as soon as they appear, not months later.
- Watching for anomalous usage patterns that indicate risk (e.g., a bot behaving outside its expected scope).
- Validating that zero-standing-privilege and least-privilege models actually hold in practice.
- In other words: governance can't just be point-in-time. It has to be continuous, context-aware and risk-driven. Extending IAM, IGA and PAM with posture assurance capabilities ensures intent, enforcement and reality remain aligned, even in highly dynamic environments.

New acronyms are often marketed as platforms, but most are capabilities that belong inside IAM, IGA or PAM.

- ITDR identifies suspicious activity, but it does not govern access. It belongs in XDR or SIEM, integrated with IAM telemetry.
- CIEM identifies excessive permissions in cloud platforms. It should be a capability inside cloud-aware IGA or PAM.
- ISPM highlights overprivileged accounts or stale access. It fits best as part of IGA analytics.
- NHIs and agentic identities are identity types, not new platforms and must be covered across all three pillars.

These are valuable capabilities, but they are most effective when integrated into the core pillars rather than treated as standalone platforms.

7. Strategy for CISOs—rationalize...do not multiply

More platforms do not mean more control. They mean overlap, integration challenges and unclear ownership. Anchor on the three-pillar model and follow these steps.

1. Inventory control planes → List your IAM, IGA and PAM platforms.
2. Map coverage → Assign each system and vendor to a pillar.
3. Spot gaps → Identify uncontrolled high-blast-radius systems.
4. Extend, don't multiply → Fill gaps by extending pillars, not by adding new control planes.
5. Retire redundancy → Consolidate overlapping tools.

Why this matters based on your lens

- If you're a board member → This is how you ensure the organization is not overspending on tools that add confusion but don't reduce risk. Think of it as simplifying locks on the house: three strong locks are better than a dozen mismatched ones.
- If you're in IT → Less tool sprawl means fewer integration headaches, more uptime and cleaner login experiences for employees.
- If you're in security/GRC → Clear ownership of IAM/IGA/PAM makes audits easier and prevents finger-pointing when incidents occur.

Measuring maturity and outcomes

A rationalized three-pillar model only matters if it produces measurable improvements. CISOs should track outcome-driven metrics—and translate them into business impact:

- **Reduction in excessive entitlements**
  - Security lens: Measure the % of accounts with privileges broader than their peers.
  - Goal: Show a downward trend over time as IGA/PAM hygiene improves.
  - Business lens: Reduces the chance that one stolen credential leads to a costly breach headline.

- **Faster remediation of orphan accounts**
  - Security lens: Track average time from discovery of an account without an owner to remediation.
  - Goal: Move from weeks/months to days/hours through continuous monitoring.
  - Business lens: Proves to regulators and auditors that we're not leaving ghost accounts open to abuse.

- **Improved governance of non-human identities (NHIs)**
  - Security lens: Measure % of NHIs (service accounts, workloads, agents) with assigned owners and enforced policies.
  - Goal: Close governance gaps that adversaries often exploit.
  - Business lens: Prevents "shadow automation" from creating risks that could stall product launches.

- **Audit efficiency**
  - Security lens: Measure hours/days required to produce audit-ready evidence of who had access to what, when.
  - Goal: Reduce manual reconciliation by relying on native logs and automated reporting.
  - Business lens: Cuts compliance costs and frees staff for higher-value work.

- **Zero-trust alignment**
  - Security lens: Track the number of exceptions to just-in-time and zero-standing privilege policies.
  - Goal: Decrease exceptions while maintaining usability.
  - Business lens: Demonstrates that "zero trust" isn't marketing spin - it's measurable progress.

These kinds of metrics move identity security away from "busy work" and into a business outcome lens. They let CISOs prove progress, defend budget and - most importantly - demonstrate that the identity program is actively reducing organizational risk.

They also give boards clear evidence that identity controls tie directly to reduced exposure and regulatory readiness. For IT teams, they validate that investments are improving uptime and reducing operational friction. For GRC and security operations, they provide a defensible trail that simplifies audits and sharpens risk oversight.

8. Simplify the landscape, focus on control

Identity security is not about collecting acronyms. It is about knowing who can access what, enforcing the minimum necessary access and proving it when challenged.

The three pillars, IAM, IGA and PAM, provide a clear and durable framework. Everything else is a capability to integrate, not a platform to own. The key is to modernize each pillar so it can handle cloud-first infrastructure, SaaS estates, non-human identities and ephemeral access patterns.

At the end of the day, identity security isn't about acronyms. Anchor on IAM, IGA and PAM, so you have an identity program that's clear, defensible and future-proof. One that is focused on proving continuously...that your human and machine workforce has the right access to the right assets at the right time.

The evolution of Privileged Access Management

If you're rethinking your identity stack, it helps to understand how we got here. This companion paper traces PAM's journey across three eras—vault-led, bastion-led and API-led—showing why older tools are struggling and what modern environments really need.

DOWNLOAD

Glossary

AI agent: An autonomous software process acting on behalf of a human or system, capable of authenticating, requesting access and performing actions.

Blast radius: The potential scope of damage if an identity is compromised or misused. High-blast-radius systems, such as production infrastructure, require stricter controls than low-blast-radius systems, such as HR portals.

CIEM: Cloud Infrastructure Entitlement Management: Identifies excessive or risky permissions in cloud platforms. Best integrated into cloud-aware IGA or PAM.

Control plane: A layer of security architecture that can directly grant, revoke, or change access to systems and resources.

Ephemeral access: Short-lived permissions granted for a specific task or time period, automatically revoked when no longer needed.

IAM: Identity and Access Management: The front door to your environment. Handles authentication and related services such as SSO and directory synchronization. Owned by IT or IAM teams, focused on connectivity and uptime.

IGA: Identity Governance and Administration: Governs entitlements for the majority of business applications. Covers provisioning, access reviews, compliance reporting and stale access cleanup. Owned by GRC or compliance-oriented security teams.

ISPM: Identity Security Posture Management: Flags overprivileged accounts, stale entitlements, or misconfigurations. Typically part of IGA analytics.

ITDR: Identity Threat Detection and Response: Detects suspicious identity activity, often integrated into XDR or SIEM. It does not grant or revoke access.

MFA: Multi-Factor Authentication: An IAM capability requiring more than one verification factor, such as password plus token.

NHI: Non-Human Identity: Any identity not tied to a human user, including service accounts, workloads and cloud IAM roles. Requires the same lifecycle governance and privilege controls as human identities.

PAM: Privileged Access Management: Provides just-in-time and least-privilege access for high-impact systems, with session monitoring, audit trails and governance controls. Owned by security engineering or operations.

Privilege creep: The accumulation of unnecessary or outdated access rights over time, often due to role changes or lack of periodic reviews.

SSO: Single Sign-On: An IAM capability that allows a user to log in once and access multiple systems without re-entering credentials.

RBAC: Role-Based Access Control: An authorization model that grants access based on predefined roles rather than individual assignments.

Glossary

AI agent: An autonomous software process acting on behalf of a human or system, capable of authenticating, requesting access and performing actions.

Blast radius: The potential scope of damage if an identity is compromised or misused. High-blast-radius systems, such as production infrastructure, require stricter controls than low-blast-radius systems, such as HR portals.

CIEM: Cloud Infrastructure Entitlement Management: Identifies excessive or risky permissions in cloud platforms. Best integrated into cloud-aware IGA or PAM.

Control plane: A layer of security architecture that can directly grant, revoke, or change access to systems and resources.

Ephemeral access: Short-lived permissions granted for a specific task or time period, automatically revoked when no longer needed.

IAM: Identity and Access Management: The front door to your environment. Handles authentication and related services such as SSO and directory synchronization. Owned by IT or IAM teams, focused on connectivity and uptime.

IGA: Identity Governance and Administration: Governs entitlements for the majority of business applications. Covers provisioning, access reviews, compliance reporting and stale access cleanup. Owned by GRC or compliance-oriented security teams.

ISPM: Identity Security Posture Management: Flags overprivileged accounts, stale entitlements, or misconfigurations. Typically part of IGA analytics.

ITDR: Identity Threat Detection and Response: Detects suspicious identity activity, often integrated into XDR or SIEM. It does not grant or revoke access.

MFA: Multi-Factor Authentication: An IAM capability requiring more than one verification factor, such as password plus token.

NHI: Non-Human Identity: Any identity not tied to a human user, including service accounts, workloads and cloud IAM roles. Requires the same lifecycle governance and privilege controls as human identities.

PAM: Privileged Access Management: Provides just-in-time and least-privilege access for high-impact systems, with session monitoring, audit trails and governance controls. Owned by security engineering or operations.

Privilege creep: The accumulation of unnecessary or outdated access rights over time, often due to role changes or lack of periodic reviews.

SSO: Single Sign-On: An IAM capability that allows a user to log in once and access multiple systems without re-entering credentials.

RBAC: Role-Based Access Control: An authorization model that grants access based on predefined roles rather than individual assignments.

P0 SECURITY

Contact Us

Email: info@p0.dev
Web: www.p0.dev

P0 Security is the unified access privilege platform built for modern cloud infrastructure. Where legacy IAM, PAM, and IGA tools fall short — particularly around non-human identities, ephemeral infrastructure and developer velocity — P0 delivers orchestration and governance, visibility and risk posture across all cloud environments.

With an agentless, API-native architecture, P0 helps teams enforce least privilege by default through short-lived, just-in-time access for both human and machine identities. Security and platform teams rely on P0 to reduce blast radius, streamline audits and eliminate manual provisioning without slowing down development.

P0 is trusted by leading organizations in fintech, healthcare, AI and cloud-native tech, with full enterprise deployments completed in under 60 days. Learn more at www.p0security.dev.

WP-CIISOISP_0825