sonraí security

Cloud Permissions Chaos

Unlocking AWS Innovation by Fixing Identity First

Unlocking Identity Center: The Fast Track to AWS Managed App Adoption

AWS managed applications promise faster innovation, but too often companies never get past the starting line. The reason isn't a lack of interest; it's identity. AWS Identity Center is designed to provide essential access controls, but in practice, it often becomes the bottleneck. Migration projects drag on, access models clash with legacy IAM, and business timelines slip while teams try to retrofit access.

Cloud leaders are discovering that identity, not infrastructure, is the gating factor for AWS adoption. Traditional identity models simply don't scale to modern, cloud-driven innovation. As a result, developers are left waiting, security teams are uneasy about uncontrolled privileges, and the business struggles to experiment at cloud speed.

This eBook explores the unexpected identity barrier at the heart of AWS managed application adoption, why it exists, what it costs, and how forward-looking organizations are rethinking their approach to IAM in order to move faster, stay secure, and unlock the full value of AWS.

Key Insight
#1

Identity Center is a Top Adoption Blocker

Companies eager to take advantage of AWS managed applications often find their momentum stalled by identity. AWS Identity Center, designed to unify and control access, too often becomes the very thing that slows innovation down.

Instead of enabling agility, Identity Center can trigger lengthy migration projects and complicated access realignments before any trials can begin. Developers wait to experiment, security teams wrestle with risks of broad standing privileges, and business initiatives slip as identity infrastructure lags behind.

"Identity-first security: This approach to security design makes identity-based controls a foundational element of an organization's protection architecture."

Source: Gartner 2024 Planning Guide for Security

63% of orgs lack AI governance policies

Source: IBM's Cost of a Data Breach Report 2025 - The AI Oversight Gap

Conclusion

The result is a paradox: the very control meant to safeguard access becomes a bottleneck to cloud adoption. Organizations that don't address this friction risk delaying critical innovation, undermining their ability to move at cloud speed, and creating exposure as permission sprawl grows unchecked.

Key Insight
#2

Permission Sprawl is the Hidden Risk

The most dangerous IAM risks aren't loud, they're invisible. Excessive permissions pile up quietly until they turn into an open door for attackers.

Temporary access often becomes permanent. Roles granted for speed are never revisited. Over time, organizations end up with thousands of over-permissioned accounts that no one tracks, until an auditor flags a violation or an attacker slips through. According to the IBM Cost of a Data Breach Report 2025, "excessive permissions and delayed adoption of identity-first security approaches left organizations more vulnerable to attackers and prolonged breach lifecycles."

99% of cloud identities are overly permissive

62% of organizations have cloud resources publicly exposed

Source: Identity And Access Management: The First Line Of Defense -By Palo Alto Networks and Unit 42 ARES

Conclusion

Unchecked permission sprawl doesn't just make compliance harder, it expands the blast radius of every breach. Identity-first security means shrinking that risk before it becomes an exposure.

Key Insight
#3

Security Incidents Amplify Operational Friction

IAM complexity doesn't just invite risk, it slows business down. When access is messy, every initiative takes longer than it should.

Developers wait for credentials instead of building. Security teams spend cycles reviewing entitlements instead of improving defenses. Business leaders see timelines slip as projects get stuck behind identity roadblocks. According to the IBM Cost of a Data Breach Report 2025, "security incidents had a ripple effect that led to data compromise and operational disruptions." That same ripple effect applies when IAM delays stall adoption.

60+
AWS accounts in 6 days

Source: Sonrai and Global Atlantic – AWS Customer Story

Conclusion

The cost of IAM complexity isn't measured only in breaches. It's measured in lost time, stalled innovation, and missed opportunities. Streamlined access means innovation and security can move forward together.

Key Insight
#4

Identity-First Security Requires a New Approach

Most organizations adopted cloud faster than their IAM could keep up. Technology alone isn't enough, organizations need new ways to align security, operations, and business priorities.

Many companies still view IAM as a technical afterthought, bolted on instead of built in. This leaves gaps between what developers need, what security requires, and what business leaders expect. As Gartner notes in its 2024 Planning Guide for Security: "Organizations are forced to cultivate more effective communications with IAM teams to help establish identity-first security strategies."

5min

Relay disabled unused AWS regions org-wide in 5 minutes

Source: Relay Network – Customer Story

Conclusion

The future of IAM isn't about tools, it's about coordination. By treating identity as a shared business priority, companies can replace friction with trust and move faster in the cloud.

Key Insight
#5

From IAM Chaos to Cloud Control in Days

The challenges outlined so far aren't theoretical. Leading enterprises are already proving that IAM transformation doesn't have to be slow or disruptive. With automation-first approaches, they're enforcing least privilege and eliminating hidden risks across sprawling AWS estates in record time.

Global Atlantic once managed IAM manually across 60+ AWS accounts, burdened by zombie identities, over-privileged roles, and little visibility. After deploying Sonrai's Cloud Permissions Firewall, they achieved full IAM automation and least privilege enforcement in just 6 days, without disrupting developer workflows.

Relay Network, facing region-level exposure, applied identity-based guardrails to disable unused AWS regions across its organization in under 5 minutes.

These outcomes are not outliers, they illustrate what becomes possible when organizations shift from reactive cleanup to proactive identity governance.

> "Zero trust is now a key design principle for IT systems as a result of its maturity."
>
> **Source:** Gartner 2024 Planning Guide for Security

Conclusion

The lesson is clear: IAM doesn't have to be a bottleneck. With the right architecture and automation, organizations can move from chaos to control in days, and unlock innovation at cloud speed.

Conclusion

The real barrier to AWS innovation isn't technology, it's outdated assumptions about identity. Too many organizations delay adoption of managed applications, convinced IAM modernization must come first.

Companies are already proving otherwise, achieving least privilege in days, running secure trials without waiting on migrations, and turning identity from a bottleneck into a business accelerator.

The takeaway is simple: don't wait for perfect IAM to innovate. Start with what you have, secure what matters, and move at the pace your business demands. Don't let Identity Center be your #1 adoption blocker.

So, are you blocked by Identity Center?

You don't need to wait on migrations or fight permission sprawl to start innovating.

Most IAM and permissions tools only scratch the surface. Sonrai Cloud Permissions Firewall is different: it enforces least privilege by design, using native AWS IAM, no org-wide rebuild required. That means:

- Secure, scoped access without waiting on Identity Center migrations
- Automated remediation that eliminates permission sprawl before it creates exposure
- Guardrails that accelerate projects instead of slowing them down
- Alignment across developers, security, and business leaders with a single source of truth

Here's how to get started

Launch a scoped CPF trial via AWS Marketplace, securely in minutes.

With Sonrai, you unify visibility, automate action, and shrink risk across every AWS account, while enabling adoption of Amazon Q, Bedrock, and other managed apps at cloud speed.

About the Company

Sonrai Security is a leading public cloud identity and access management solutions provider. With a mission to empower enterprises of all sizes to innovate securely and confidently, Sonrai Security delivers identity, access, and permissions security for companies running on AWS.

The company is renowned for pioneering the Cloud Permissions Firewall, enabling one-click least privilege while supporting developer access needs without disruption. Trusted by leading companies across various industries, Sonrai Security is committed to driving innovation and excellence in cloud security.

Learn more at **sonraisecurity.com**

- Founded in **2017**
- Headquartered in **New York City**
- **AWS Security Competency Partner**