Access hygiene for AWS

The fast track to building the secure identity foundation every modernization project depends on

The challenge

Modernization starts with foundation

In order to modernize, you must first strengthen the foundation. Most enterprise environments today aren't purely cloud or on-prem. They're hybrid or multi-cloud, spanning AWS, Azure, GCP and legacy infrastructure.

At the same time, **machine identities** and **agentic AI** are being introduced into these environments faster than organizations can adapt their access governance. The result is a tangle of over-privileged roles, unmanaged credentials and orphaned accounts that quietly increase risk and stall modernization.

Before scaling development teams, deploying automation agents, onboarding new contractors, or integrating newly acquired companies, every organization needs a verified understanding of its current identity posture.

Conducting this level of cross-functional due diligence internally - while balancing ongoing initiatives - can take months and often bottlenecks innovation.

P0 Security's **Access Hygiene Blueprint (AHB)** accelerates foundational due diligence, providing DevOps, Security and IAM teams a verified baseline for implementing just-in-time access, short-lived credentials and posture-based authorization.

The service

Establish your access hygiene baseline

The **Access Hygiene Blueprint for AWS** is a fixed-fee, 12-week professional engagement designed to uncover, remediate and verify the true state of your AWS identity environment.

Our experts analyze, rationalize and certify your access model, creating a measurable, least-privileged and auditable foundation for continuous privilege management and automation through the P0 platform.

What's included in the service

1. User management and federation

Eliminate unmanaged and non-federated identities across all AWS accounts.

INCLUDES

- Configuration of AWS Identity Center (if not already in use)
- Full inventory of IAM users, groups and federation status
- Removal of inactive or non-federated users (>90 days)
- Assignment of verified owners for all active identities
- **Federation compliance report** (before/after view)

OUTCOME

- 100% AWS accounts integrated with your IdP (e.g. Microsoft Entra ID)
- ≥ 95% human users federated
- No static break-glass accounts

2. Authentication hardening

Replace static credentials with identity-based, short-lived authentication mechanisms.

INCLUDES

- Enforcement of MFA for all federated users
- Detection and removal of static AWS access keys
- Migration of workloads to IAM Roles using STS tokens
- Identification of static SSH, database and Kubernetes credentials
- **Authentication hardening report** detailing findings and remediation

OUTCOME

- 0 user static keys remaining
- ≥ 90% workloads using IAM roles
- All remaining credentials owned and tracked

3. Authorization rationalization

Right-size privileges and enforce least-privilege access across all identities.

INCLUDES

- Inventory and classification of all IAM roles and permission sets
- Identification of privileged identities (human and workload)
- Consolidation of duplicate roles and implementation of tiered model (basic_user, owner, break_glass)
- Policy cleanup to remove wildcard permissions
- **Role rationalization and least privilege report** with before/after metrics

OUTCOMES

- ≥ 20% reduction in privileged IAM roles
- 100% role ownership established
- ≤ 5% of users with standing owner/break-glass access

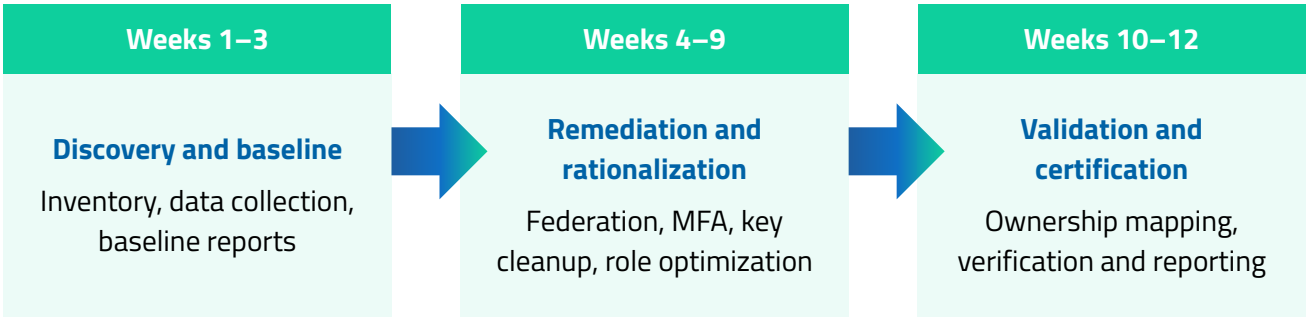
4. Authentication hardening

Extend access hygiene across every AWS subsystem:

- **Compute:** EC2, Lambda, EKS (SSH/ sudo access)
- **Data:** RDS, DynamoDB, Redis
- **Storage and networking:** S3, VPCs, Security Groups
- **Control plane:** IAM, Secrets Manager, CloudFormation

Each engagement concludes with a **certified blueprint**, a visual map of every privileged relationship and ownership link in your AWS environment.

Engagement timeline



The entire process is completed in three months with minimal disruption to production workloads.

Deliverable	Description	Verified outcome
Federation compliance report	**Inventory of users and federation status**	**100% federated accounts**
Authentication hardening report	**MFA and STS compliance summary**	**Zero static credentials**
Authorization rationalization blueprint	**Tiered roles and least-privilege policy set**	**20% fewer privileged roles**
Access DNA and Identity Graph - hygiene summary	**Visualization of privileged relationships**	**100% ownership mapping**

Where modernization begins

With the Access Hygiene Blueprint, you have everything you need to ensure your AWS environment is **ready for modernization**. It's the prerequisite to:

- Implementing **just-in-time access** for human and workload identities
- Enforcing **continuous least privilege** through the P0 platform
- Automating **secrets rotation and credential governance**
- Safely scaling **machine identity and AI-driven automation** across hybrid and multi-cloud infrastructure

Reach out to learn more!
Book time with our team.

Establishing your Access Hygiene Blueprint gives you measurable proof of progress.

When paired with modern PAM capabilities, here are some typical metrics you could expect to see:

- **Federation coverage**: percent of identities federated through the primary IdP (target ≥ 95%).
- **Static credential ratio**: percentage of static keys or passwords remaining (target = 0%).
- **MSPR** (Mean Standing Privilege Reduction): percentage reduction in permanent privileged roles across human and machine identities.
- **Access ownership coverage**: percent of identities with a verified owner (target = 100%).

Getting started is simple…but success requires everyone at the table.

The Access Hygiene Blueprint works best when teams align on a shared goal: building a secure, federated identity foundation that accelerates every initiative, from AI adoption to cloud migrations to M&A integrations.