Otterize

AWS IAM Automation

DATASHEET

AWS IAM Automation

Requirements

- **Streamline workload IAM management:** Improve security posture by adhering to least privilege semantics, and reduce manual configuration overhead.
- **Automate** policy creation, enforcement, and audit to reduce manual effort and errors.
- **Define standards and repeatable frameworks** to manage the lifecycle of workload IAM configurations across diverse platforms and hyperscalers.
- **Visibility:** Gain insights into access patterns and proactively identify potential security risks.
- **Compliance:** Automate the generation of audit reports and evidence of compliance with regulatory requirements.

Devs

- **Simplified access controls:** Easily manage IAM permissions for applications and services without requiring deep IAM expertise.
- **Faster time to production code deployment:** Enable self-service access management to reduce reliance on DevOps or security teams.
- **Integration with existing workflows:** Support existing development tools and processes, such as GitOps and CI/CD pipelines.
- **Self-documentation:** Create a comprehensive and actionable map of your application architecture in a declarative and visual format, identifying all services involved, regardless of their type and location.

Platform

- **Seamless integration:** Build an agnostic automation framework for IAM, using existing AWS infrastructures, including cloud services, Kubernetes, and third-party tools.
- **Support GitOps workflows:** With a declarative approach, manage IAM policies as code using GitOps practices for better version control and collaboration.
- **Scalability:** Handle IAM management across large and complex environments with multiple accounts and regions.

SecOps

- **Understand service permissions:** Clearly identify the IAM permissions required for applications consuming serverless and PaaS services in AWS.
- **Enforce least privilege:** Automatically generate and enforce least privilege IAM policies based on observed application behavior.
- **Detect and respond to threats:** Monitor access patterns, identify anomalies, and automatically trigger alerts for potential security incidents.
- **Automate remediation:** Automatically revoke or modify excessive permissions to mitigate risks proactively.
- **Simplify compliance audits:** Generate comprehensive audit reports and demonstrate adherence to regulatory requirements.

Drivers

- **Simplification of DevSecOps workflows**

  Managing IAM policies at scale becomes exponentially complex as environments grow, leading to misconfigurations, inconsistent policies across teams and services, and difficulty in understanding the impact of changes. This complexity translates to higher operational costs due to increased time spent on manual configuration, troubleshooting, and resolving security incidents caused by IAM errors.

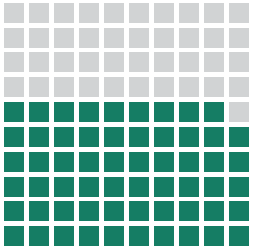
  Multi-Cloud Environments: The challenge is compounded in multi-cloud environments where each provider has its own IAM model, terminology, and best practices. This creates additional overhead for managing, maintaining, and securing access across different platforms, especially when considering extending AWS IAM roles to workloads outside of AWS using IAM Roles Anywhere.hybrid infrastructures, which demand new approaches to security.

- **Developer Productivity:** Manual IAM configuration forces developers to spend valuable time navigating complex IAM concepts and syntax, rather than focusing on building and delivering applications. This can lead to frustration, delays, and potential security vulnerabilities due to rushed or incomplete configurations. This friction slows down innovation and time-to-market for new products and features, hindering the company's ability to stay competitive and respond to changing market demands.

- **Reduce attack surface and Increase Visibility:** Overly permissive IAM permissions, even unintentional, can provide attackers with a foothold into your environment, potentially leading to data breaches, compromised systems, and reputational damage. Additionally, the lack of visibility into who has access to what can make it diffcult to detect and respond to security incidents promptly. Security breaches can result in significant financial losses due to regulatory fines, legal fees, customer churn, and the cost of remediation. It can also severely damage a company's reputation and customer trust.

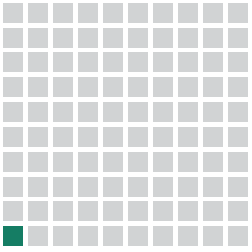
- **Compliance:** Meeting regulatory requirements for access controls, such as those mandated by PCI DSS, HIPAA, GDPR and DORA, involves meticulous documentation, auditing, and continuous monitoring of IAM configurations. Manual processes are often insufficient to keep up with the pace of change, leading to compliance gaps and potential penalties. Non-compliance can lead to costly fines, legal action, and loss of business opportunities, especially in regulated industries where demonstrating robust security controls is essential.

Key Figures and Data



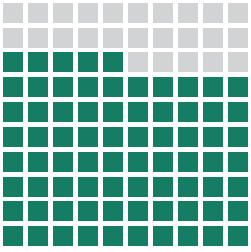
59%

of security professionals highlight misconfiguration of cloud platforms as the biggest security threat. (Checkpoint Cloud Security Report, 2023)



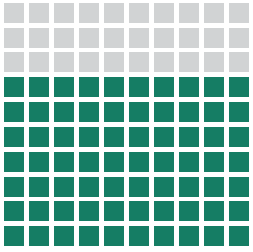
1%

Across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), workload identities are using only 1% of their granted permissions. (Microsoft 2023 State of Cloud Permissions Risks Report)



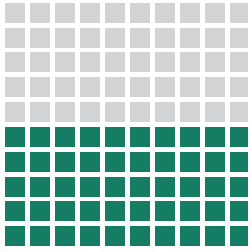
75%

Gartner predicts that by 2026, 75% of organizations will adopt a digital transformation model predicated on cloud as the fundamental underlying platform. (Gartner press release, 2023)



70%

Over 70% of AWS customers are using one or more serverless solutions (Datadog State of Serverless Report, 2023)



50%

Kubernetes is more popular than ever for managing and deploying containers, with nearly 50% of container organizations using it. (Datadog Container Report, 2022)

Benefits

- **Improved Security for Complex Architectures:** Otterize understands the intricate relationships between microservices, containers, serverless and cloud PaaS services. This allows for the creation of more granular and precise IAM policies that adhere to least privilege principles, significantly reducing the attack surface of modern applications. Otterize also proactively identities new services integrated into your application architecture, automatically creating and enforcing least-privilege IAM policies for these services before they are even deployed to production.

- **Increased Developer Velocity in Hybrid Environments:** Otterize simplifies IAM management across hybrid architectures, enabling developers to focus on building and deploying applications instead of struggling with complex IAM configurations across multiple platforms. Automated ChatOps notifications and GitHub pull requests enable efficient communication and collaboration between development and security teams, ensuring that security considerations are addressed early in the development lifecycle.

- **Reduced Operational Overhead for Microservices:** Managing IAM policies for numerous microservices can be overwhelming. Otterize automates policy generation and enforcement, scaling seamlessly with your microservices architecture to minimize manual effort and potential errors. The self-documenting nature of Otterize's automated workflows provides a clear and up-to-date understanding of the access permissions required by each service.

- **Global Compliance in Multi-Cloud Environments:** Otterize understands the unique IAM requirements of different cloud providers and services, simplifying compliance across your multi-cloud environment. It provides audit report generation and proactively identities and automates remediation for potential compliance gaps, ensuring you meet regulatory requirements.

Competitive Advantage

- **Application-Aware IAM:** Otterize's deep understanding of application architectures, including microservices, containers, and PaaS components, allows you to generate IAM policies that precisely align with the specific permissions needed by each component. This level of granularity and security automation are unmatched by traditional workload IAM solutions.
- **Hybrid and Multi-Cloud Expertise:** Otterize seamlessly integrates with and manages IAM policies across various cloud platforms and on-premises infrastructure. This makes it ideal for organizations with hybrid architectures and those leveraging multiple cloud providers.
- **Developer-First Approach:** Otterize prioritizes developer experience by streamlining IAM management and enabling self-service access control. This fosters collaboration between developers and security teams and accelerates development cycles.
- **Automated Remediation and Continuous Monitoring:** Otterize goes beyond static policy enforcement by continuously monitoring application behavior and automatically remediating potential security risks in real time. This proactive approach ensures that your IAM configurations remain secure and up-to-date.

Key Features

- **Policy-as-Code Declarative Intents with IBAC:** Allows you to define and manage IAM policies in a declarative format using code, simplifying the management of complex access controls and enabling the use of Identity-Based Access Control (IBAC) to further enhance security.
- **Automated IAM Policy Generation:** Generates least privilege IAM policies based on observed application behavior, including newly integrated services.
- **Continuous Monitoring and Enforcement:** Monitors access patterns and enforces IAM policies in real time, proactively identifying changes in application architecture.
- **GitOps Integration:** Supports GitOps workflows for managing IAM policies as code, ensuring version control and enabling seamless rollback if needed.
- **Slack and GitHub Integrations:** Enables developers to manage access requests and approvals directly from their preferred tools.
- **Security Insights and Alerts:** Provides detailed visibility into access patterns and proactively alerts you to potential security risks, including changes in application architecture that may require new IAM policies.
- **Compliance Reporting:** Simplifies compliance reporting by automatically generating audit reports.
- **Automated ChatOps Notifications:** Sends notifications through ChatOps channels (e.g., Slack) to alert relevant teams about changes in application architecture and newly generated IAM policies.
- **Automatic GitHub Pull Requests:** Creates pull requests in GitHub for newly generated IAM policies, allowing for review and approval before merging into the main branch. This ensures that all changes are properly documented and auditable.
- **Cross-Cluster Visibility:** Provides a centralized view of IAM permissions and access patterns across multiple Kubernetes clusters, enabling you to easily identify and address security risks in complex environments.