CYBERARK

DATA SHEET

CYBERARK CLOUD ENTITLEMENTS MANAGER™

THE CHALLENGE

As cloud adoption increases, so does the attack surface, in the form of increasing permissions for human and machine identities to access critical cloud resources. Especially at scale, the dynamic nature of cloud identities, infrastructure, applications and services often leads to misconfigurations that cause identities to collect excessive and unused permissions. Attackers and malicious insiders can exploit these permissions to gain access to critical cloud infrastructure, steal or alter sensitive data, or interrupt cloud-hosted services.

In cloud environments, rapidly accumulating permissions pose a significant challenge for Cloud Security teams. These stakeholders can quickly become responsible for managing thousands of identities and services across separate cloud platforms, each with their own permissions models.

As organizations accelerate cloud adoption, many Security and Operations teams lack the cross-platform visibility and controls needed to efficiently manage permissions and follow best practices by implementing the Principle of Least Privilege Access. This challenge is exacerbated by the shared responsibility model of cloud providers, in which customers are responsible for secure configuration of Identity and Access Management (IAM) controls in their unique environments.

Particularly in large scale and multi-cloud environments, an inconsistent approach to managing identities and permissions can quickly become a major security risk and impediment to operational efficiency.

THE SOLUTION

CyberArk Cloud Entitlements Manager is a SaaS solution that reduces risk by implementing Least Privilege across cloud environments. From a centralized dashboard, Cloud Entitlements Manager provides visibility and control of permissions across an organization's cloud estate. Within this single display, Cloud Entitlements Manager offers easily deployable remediations based on Least Privilege to help organizations strategically remove excessive permissions without disrupting cloud operations.

Cloud Entitlements Manager collects data on IAM entities and applies artificial intelligence (AI) to assign an exposure level score for each unique identity, environment, and platform. This allows organizations to continuously assess their permissions exposure and identify the fastest paths to risk reduction.

SPECIFICATIONS

Supported Cloud Platforms and Services

- Amazon Web Services (AWS)
- AWS Elastic Kubernetes Service
- Microsoft Azure
- Google Cloud Platform (GCP)

Onboarding

- Immediate, automatic onboarding of cloud accounts
- Zero-footprint, cloud-hosted solution
- AI-driven recommendations rapidly available
- Less than 1 hour to full deployment and solution value

Key Features

- Continuous, cloud-agnostic visibility and control
- Single, centralized dashboard for all environments
- Granular, AI-powered recommendations to efficiently implement Least Privilege
- Exposure Level Analysis for proactive, measurable risk reduction

HOW IT WORKS

As a cloud-hosted SaaS solution, Cloud Entitlements Manager offers immediate value through rapid deployment. In just five minutes, users can install the solution. Within an hour, they can leverage intelligent recommendations to remediate excessive permissions across their AWS, AWS EKS, Azure, and GCP environments.

Cloud Entitlements Manager uses the IAM services of each platform to identify and map permissions across the enterprise's cloud estate. Advanced detection capabilities can also uncover additional configuration risks not typically tracked by the cloud providers' IAM tools, such as Shadow Admins, users with specific sensitive permissions that grant them the ability to escalate privileges in the cloud.

Next, Cloud Entitlements Manager collects usage data for all existing permissions to identify excessive and unused permissions that can be removed with minimal disruption to ongoing operations. The solution uses this data to weigh permissions by the scope of allowed access, automatically calculating a quantifiable exposure level score reflecting the total permissions risk of each environment. Cloud Entitlements Manager can then reduce this risk by using AI to generate granular, immediately deployable JSON policy remediations that remove only excessive or unused permissions, mitigating risk without impacting necessary access for ongoing tasks.

These AI-powered recommendations are informed by the principle of Least Privilege and account for the unique risks of each provider. Enforcing Least Privilege helps organizations follow cloud security best practices and meet leading compliance frameworks. In addition, API and Webhook integrations incorporate Exposure Level scores into workflows for security tools, enhancing their value.

BENEFITS

- **Gain cloud-agnostic visibility of permissions risk.** From a centralized dashboard, navigate and control all permissions to access resources across AWS, AWS EKS, Azure and GCP environments. Interactively map and visualize access relationships between identities and resources. Measure exposure level for full platforms and individual entities, and apply granular policy remediations, all from a single centralized display.
- **Implement Least Privilege throughout the cloud estate.** Identify hidden, unused and misconfigured permissions unique to each cloud platform. Act swiftly to remove excessive permissions for human and machine identities. Proactively defend against external adversaries and insider threats.
- **Operate cloud permissions securely and efficiently.** Leverage AI-powered recommendations to rapidly and easily remediate permissions. Granular, code-level policy remediations provide a consistent process for removing entitlements across platforms, applying least privilege to assist with compliance efforts without disrupting users or operations.
- **Proactively reduce risk and measure progress.** Use dynamic, environment-specific Exposure Level scores to determine the fastest paths to risk reduction. Quantify risk reduction over time with historical Exposure Level data. Apply Least Privilege to demonstrate compliance with industry and regulatory frameworks.
- **Integrate with existing CyberArk solutions.** Unify security intelligence to onboard and manage identities and defend against compromised identities in cloud environments through integration with CyberArk Privilege Cloud®.

WHY CYBERARK

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust Cyberark to help secure their most critical assets.