

SOLUTION BRIEF


04/21/2022



Cloud Identity and Entitlement Analytics

Reduce your cloud risk profile through least-privilege and entitlements monitoring

404 Wyman Street
Suite 357
Waltham, MA 02451
www.uptycs.com



“ Today, it’s estimated that the ratio of user identities to machine identities is 1:5, with projected growth to 1:20 in the next five years.

The Unspoken Cloud Problem

As IaaS and PaaS services continue to expand, managing cloud identities becomes an increasingly complex but critical component of cloud infrastructure—in both its operation, and its security.

Traditional Identity Access Management solutions help with user identities in on-premises contexts, but aren’t equipped to handle the fast growth in identity capabilities within cloud environments, and don’t offer the visibility needed to effectively measure and reduce identity risk. Today, it’s estimated that the ratio of user identities to machine identities is 1:5, with projected growth to 1:20 in the next five years.

With so many identities accessing your cloud infrastructure for a multitude of reasons, it’s easy for their privileges to get a little out of control. In fact, Gartner suggests that by 2023, 75% of security failures will result from inadequate management of identities, access and privileges, up from 50% in 2020.¹

Cloud Identity Has Taken The Driver’s Seat

The damage that an over-privileged identity can cause, whether it be accidental or malicious, includes data breaches, compliance failures, and service disruptions, and the extent of that damage depends entirely on what that identity has access to. That’s why having a solution that measures your cloud identity risk, offers remediation guidance, and continuously monitors for privilege escalation is fundamental.

Uptycs’ Cloud Identity and Entitlement Analytics continuously monitors cloud identity infrastructure to spot identity misconfiguration and permissions gaps so customers can effectively implement least privilege and zero trust access, minimizing the damage that can be caused by privilege exploitation.

The Cloud Identity and Entitlement Analytics offering is part of the broader Uptycs’ security analytics platform that delivers the capabilities you need to defend cloud-native applications, including cloud security posture management (CSPM) and cloud workload protection (CWPP).



Implement Least Privilege

Recent research by Gartner found that more than 95% of accounts in IaaS use, on average, less than 3% of the entitlements they are granted.² Each unnecessary entitlement an identity has represents an opportunity for security failure. This is why organizations strive for least-privilege access policies, whereby identities only have the entitlements and permissions needed to do their intended jobs. But it's hard to know which permissions to shave off when you don't know which it needs to function.

Uptycs performs permission gap analysis on your cloud identities and breaks down how many identities have unused permissions, how many permissions each identity has and how they are used, and offers policy recommendations based on the findings. This way, you're able to effectively implement least privilege policy without disrupting workflow.

Audit and Compliance Support

To better understand the potential extent of damage a cloud identity could cause, you need to be able to see the services, resources and accounts it is able to connect with, and which actions it's able to perform with that access. Uptycs provides identity mapping and relationship graphing, which visualizes the connections your identities have across accounts and ranks them based on their risk, so you know at-a-glance exactly what an identity can do.

Visualize Identity Relationships

In the event of an audit, compliance teams need to be able to look into permissions configurations to make sure they're adhering to regulatory requirements. Uptycs empowers auditors to ask identity-specific questions and answers through the relationship map, and reachability queries show all users who can access a particular service.

Rapidly Respond to Security Events

Being able to act quickly in response to a security event is vital. Uptycs helps establish identity provenance for access decisions, like the who, what, when and where, so Security teams can quickly identify the origin of an event and any affected resources or assets.

Uptycs Cloud Identity and Entitlement Analytics Key Benefits

- Visibility into identity control plane-related risk
- A view on how well the organization follows the AWS Well-Architected Framework and security best practices for entitlements policy
- Help customers continuously improve on the Principle of Least Privilege
- Provide actionable policy recommendation and help automate
- Interactive way to visualize, explore, and understand relationships between identities and resources
- Visually investigate entitlements for resources or identities
- Automated way of identifying risky cloud IAM policies
- Associating Users/Roles to those risky policies to take remediation actions
- A powerful analytics engine and data pipeline
- Data summarizations and visualizations that solve for multiple solutions

Uptycs' Cloud Security Platform Delivers

- Real-time and historical service and resource inventory
- View into critical service insights
- Multi-cloud coverage
- Audit checks across multiple services
- Vulnerability and misconfigurations discovery
- Continuous, real-time compliance
- Support for multiple standards with customization
- Real-time alerting based on threat data

¹Gartner, "Managing Privileged Access in Cloud Infrastructure," Paul Mezzera, June 09, 2020

²Gartner, "Innovation Insight for Cloud Infrastructure Entitlement Management," Henrique Teixeira, Michael Kelley, Abhyuday Data, June 15, 2021