uptycs

Solution Brief

Cloud Identity Entitlement Analytics

Reduce your cloud risk profile through least privilege and entitlements monitoring

> *"Today, it's estimated that the ratio of user to machine identities is 1:5, with projected growth of 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 (IAM) 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 they don't offer the visibility needed to effectively measure and reduce identity risk. Today it's estimated that the ratio of user 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]

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

Cloud Identity Has Taken the Driver's Seat

The damage that an overprivileged identity can cause—whether it be accidental or malicious—includes data breaches, compliance failures, and service disruptions. 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 infrastructure to spot identity misconfiguration and permission gaps so you can effectively implement least privilege and zero trust access, thereby minimizing the damage that can be caused by privilege exploitation.

Our Cloud Identity and Entitlement Analytics offering is part of the broader Uptycs' security analytics platform. It 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 superfluous entitlement represents an opportunity for security failure. This is why organizations strive for least-privilege access policies, whereby workers have only those entitlements and permissions needed to do their intended job. But it's hard to know which permissions to shave off when you don't know which it needs to function.

Uptycs performs gap analysis on your cloud identities to break down how many identities have unused permissions, how many permissions each identity has and how they're used, then 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 damage extent a cloud identity could cause, you need to assess the services, resources and accounts it can connect with, and which actions it's able to perform with said access. Uptycs provides identity mapping and relationship graphing, which visualizes the connections your identities have across accounts. It ranks them based on 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 review permission configurations to verify each adheres to regulatory requirements. Uptycs empowers auditors to ask identity-specific questions and obtain answers through the relationship map, with reachability queries showing all users who can access any given 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 i.e., the who, what, when, and where, so security teams can quickly identify the origin of an event and any affected resources or assets.

Key Benefits of Uptycs Cloud Identity and Entitlement Analytics

- Visibility into identity control plane-related risk
- A view of how well your organization follows the AWS Well-Architected Framework and security best practices for entitlements policy
- Help you continuously improve on the Principle of Least Privilege
- Provides actionable policy recommendation and helps you to automate
- Interactive way to visualize, explore, and understandrelationships 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
- Provides a powerful analytics engine and data pipeline
- Data summarizations and visualizations that solve for multiple solutions

Our 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

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

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

About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive, enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

Shift your cybersecurity up with Uptycs.

uptycs