Datasheet

uptycs

Uptycs for Cloud Infrastructure Security

Harden your hybrid and attack by proactively identifying and remediating insecure configurations and other risks.

Why Uptycs?

As organizations move further along on their cloud journey, they often find themselves outgrowing niche tools and in need of more unified visibility. Disparate cloud security solutions only deliver pieces of an organization's entire cloud infrastructure picture, leaving you unaware of security risks and compliance issues.

The Uptycs unified CNAPP and XDR platform incorporates cloud workload protection, cloud security posture management, cloud infrastructure entitlements management, and cloud detection and response so you can eliminate blind spots, detect threats, and ensure compliance.

Simplify Cloud Asset & Resource Inventory

You can't secure what you can't see. Uptycs gives you connected insights across all of your cloud environments so you get a complete view of your cloud estate and the answers you need, fast.

Users can group and tag cloud-based assets and resources across accounts, as well as run queries and reports for information-like service configurations. In a single place, you can answer questions about your cloud environment such as, "What cloud-based assets do I have running and where?" and "What are my cloud service configurations?"

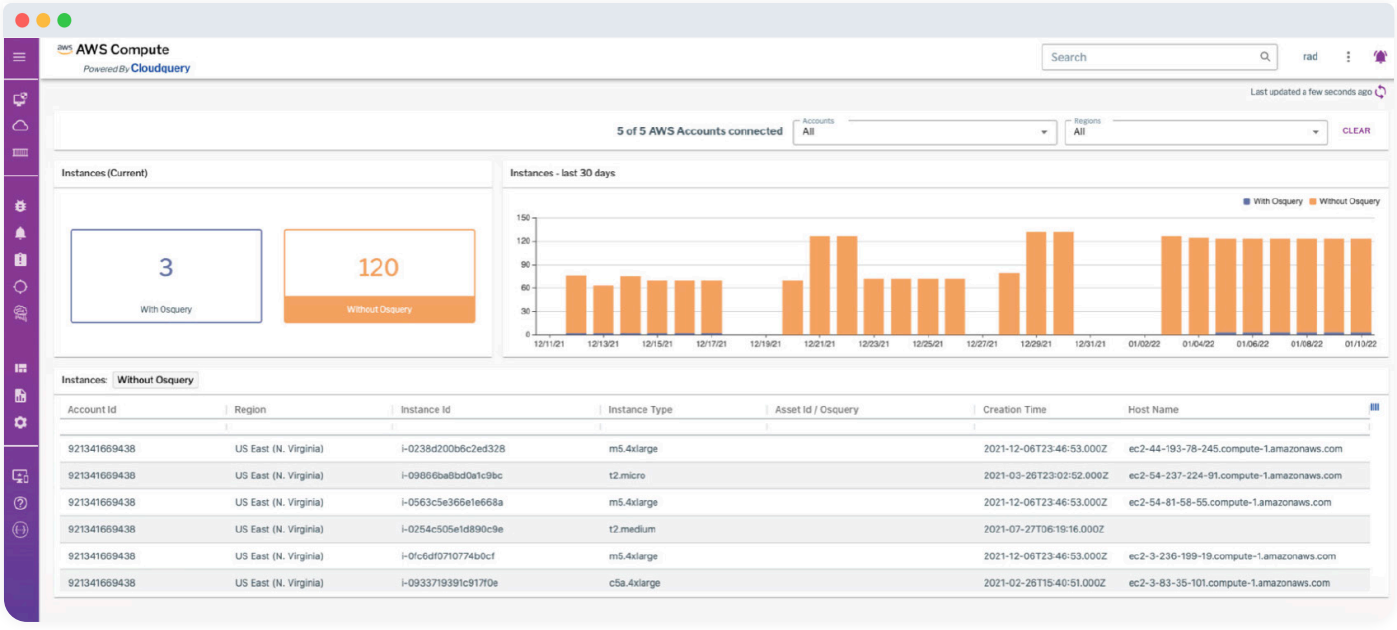
Visibility Features

Continuously updated cloud inventory – Configuration details for resources from AWS, Azure, and GCP. Real-time monitoring using API polling and event-driven monitoring for instantaneous detection of changes in the cloud.

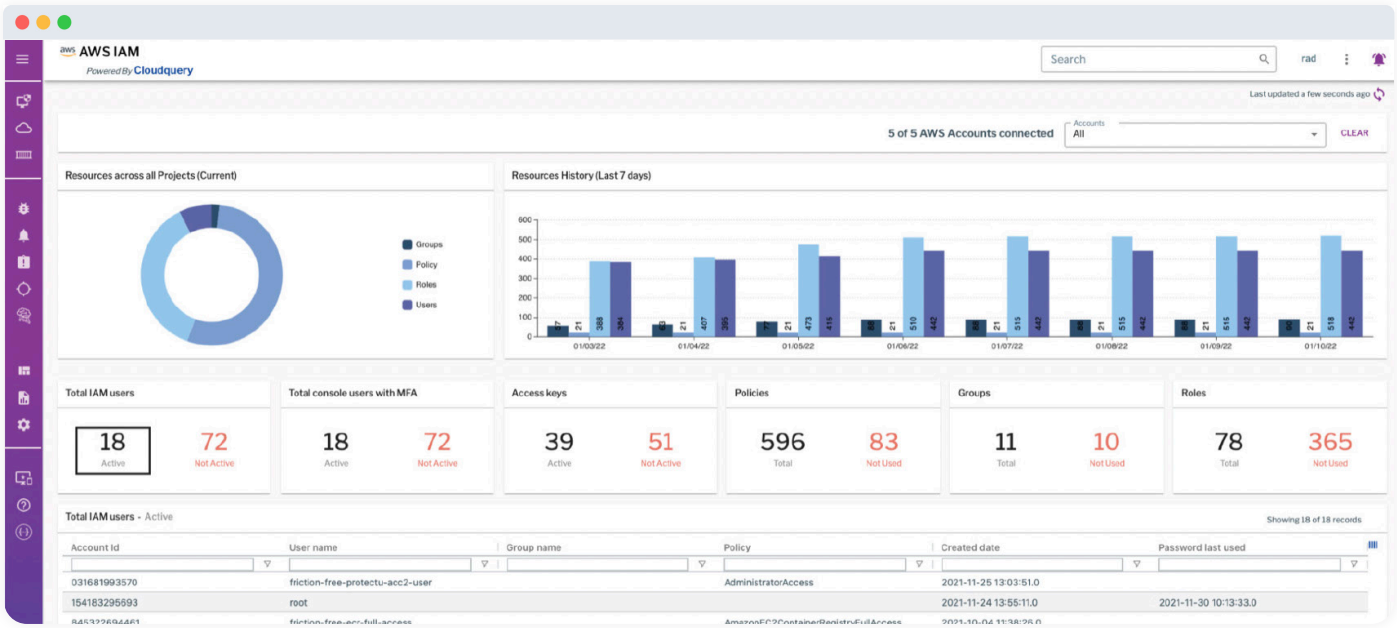
Everything in one view – Get a complete inventory snapshot across all cloud provider accounts and services.

Insights dashboards – Easily spot security issues with continuously updated snapshots of critical metrics for essential services.

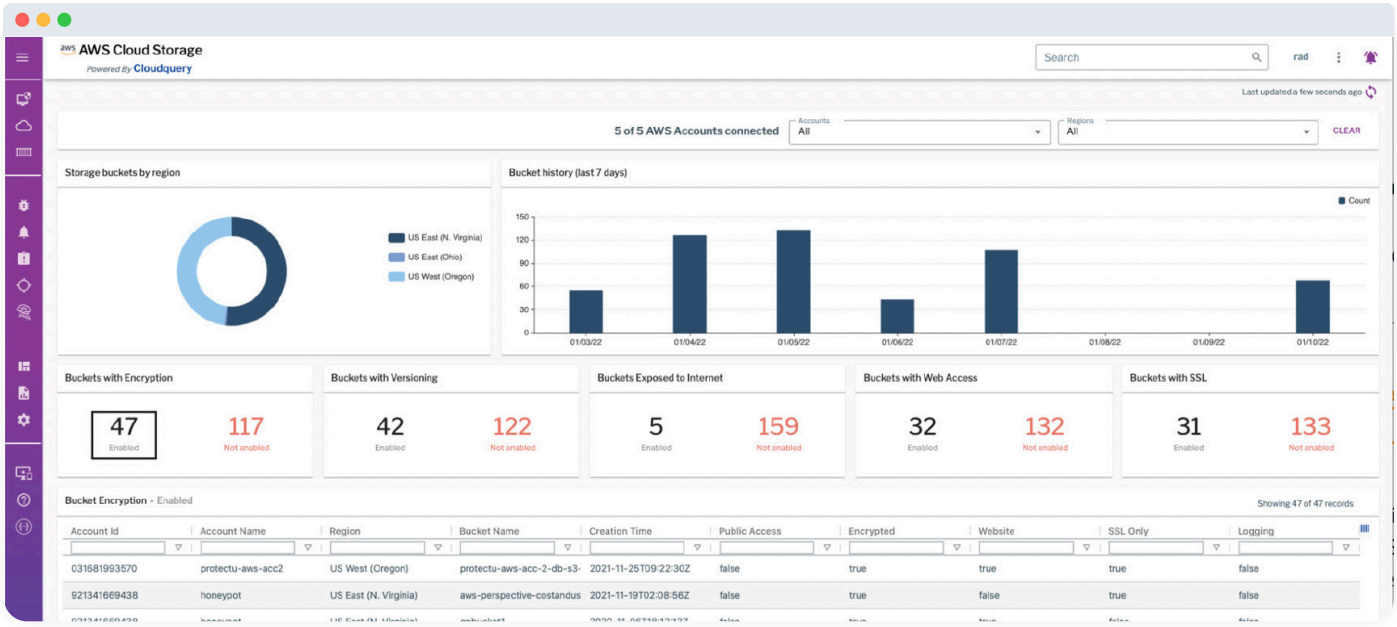
Identify issues across key resources – Highlight relationships across resources—including alerts and non-conformance—using built-in and custom rules.



Compute Insights - Know what you have running, and drill down to details from here.



Cloud IAM dashboard - Key metrics related to identity and access management in one place.



Insights for cloud storage - Know what you have and quickly identify what needs attention.

Continuously Assess Cloud Security Posture

For security teams, the growth of cloud usage can be nerve-racking because it's so easy for developers and other users to make unintentional mistakes. Uptycs makes it easy for Security teams to ensure their cloud resources are adhering to best practices.

Uptycs alerts teams to risks such as insecure configurations, tracks configuration history, and provides details that engineers need to quickly remediate issues, e.g., multi-factor authentication (MFA) for users, user activity logging on resources, and unauthorized API activity.

With Uptycs in place to monitor for risk and alert in real time,security teams can strike a balance between protecting data and applications and enabling developers and operations teams to respond quickly.

Audit Features

Implement best-practice guardrails – Run hundreds of audit checks based on cloud best practices to avoid unintentional misconfiguration.

Highlight possible vulnerabilities – Explore service and resource relationships through graphical tools, including alerts and non-compliant configurations.

Build custom checks – Easily address unique use cases with an easy-to-use rule builder for custom checks.

Works with your tools – Send alert notifications based on audit checks to third-party systems, including email, Slack, PagerDuty, and other HTTP destinations.

Easy remediation – Fix misconfigurations to follow best practices with remediation guidance.

Ensure Compliance in the Cloud

Uptycs makes demonstrating compliance with detailed evidence much faster using, with regular checks of your cloud environments against many standards that include CIS Benchmarks, PCI-DSS, and SOC 2. Users can view summary visualizations of compliance posture and are able to drill down into non-compliant resources, associated evidence, and remediation guidance. They can instantly see the latest failed configuration checks, most non-compliant resources, time to resolve non-compliance, and more.

Compliance Features

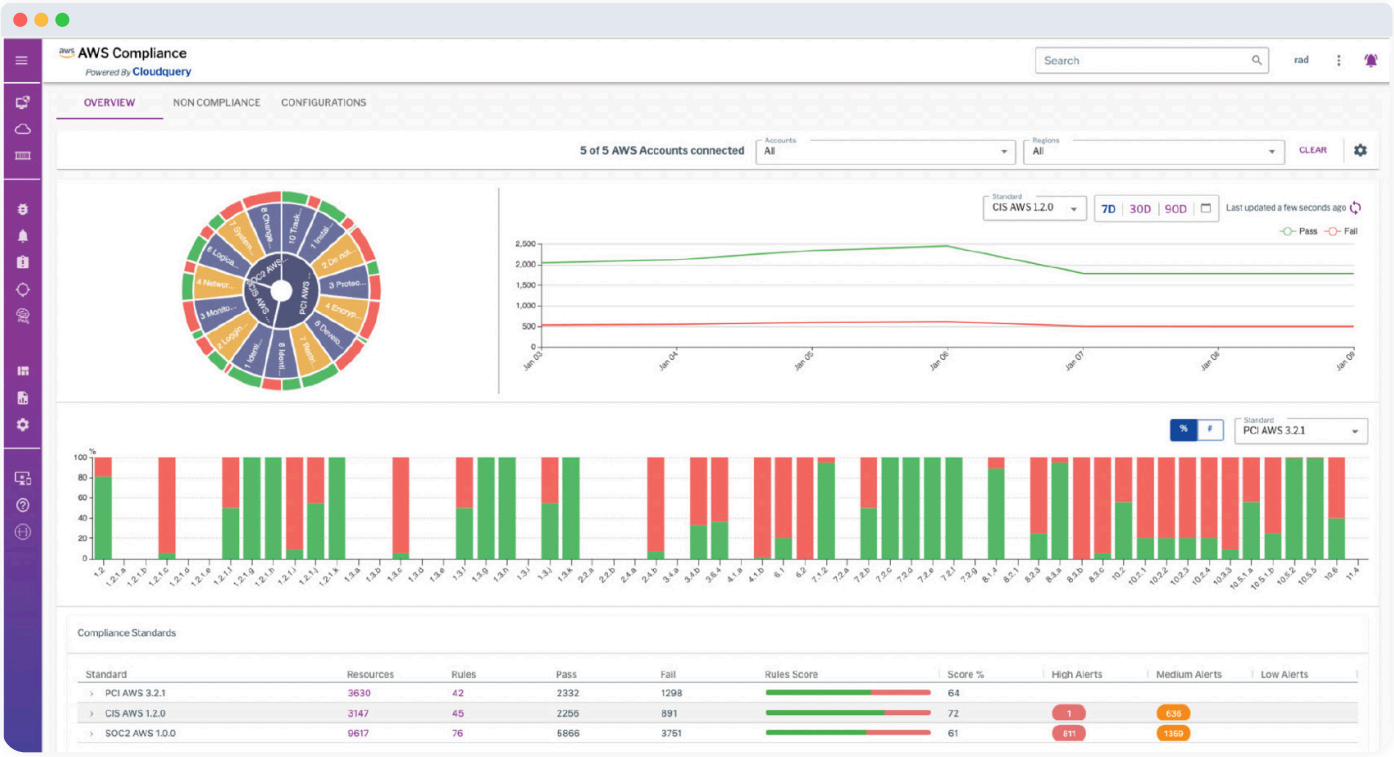
Overview dashboards – Track compliance posture with visual summaries of compliance over time, related evidence, and snapshots of cloud resource configuration.

Historical trends – Demonstrate improvement in your compliance posture with associated resource history.

Customize standard checks – Easily make adjustments based on your environment using parameterization and other customization options.

Easy remediation – Make it easy for teams to fix issues with one-click and automated remediation.

One-click compliance reporting.



Compliance dashboard - Monitor and enforce the standards you require.

Cloud Threat Detection and Response

With Uptycs, security teams can rapidly identify threat activity targeting cloud environments and dig in to answer difficult questions that come up during the course of investigations.

Uptycs offers several powerful cloud detection and investigation capabilities:

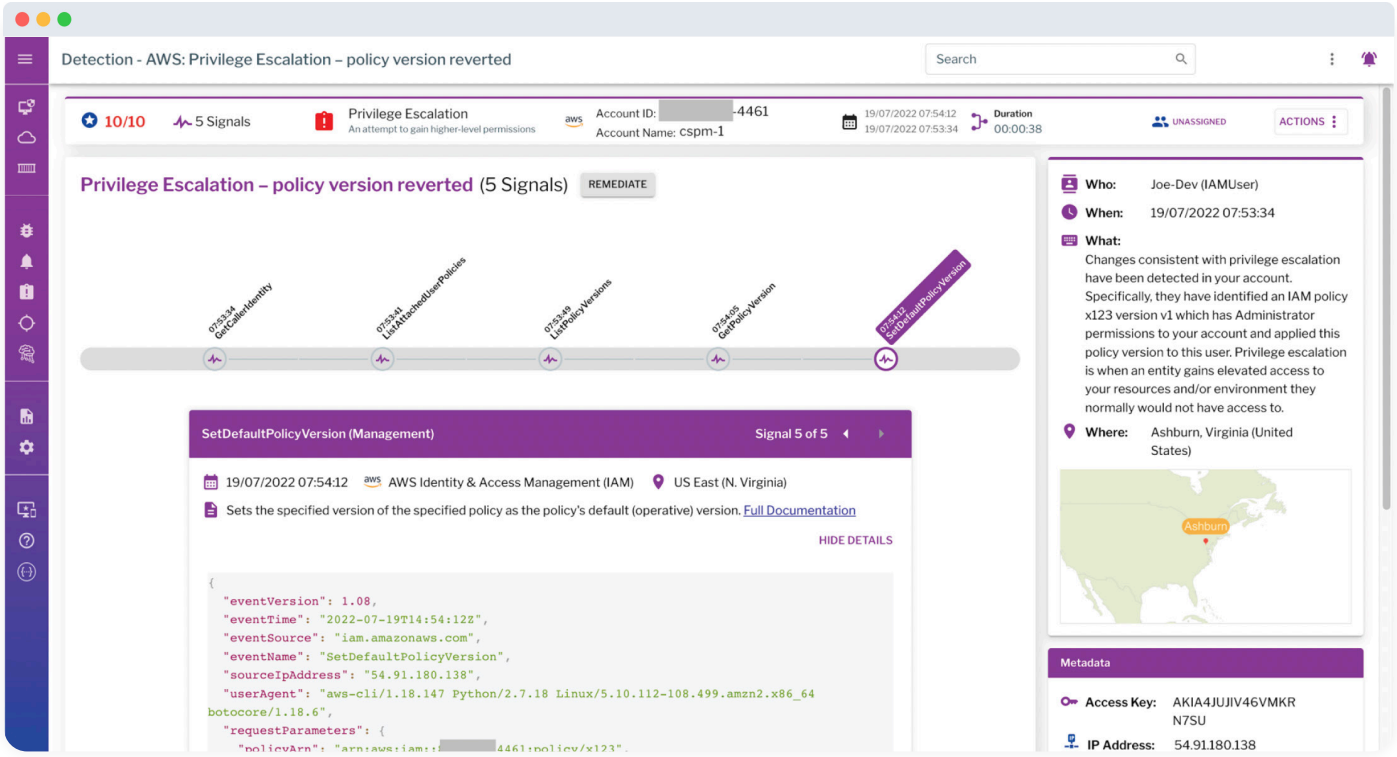
- Uptycs ingests network flow logs, matches IPs and domains against its threat intelligence platform to detect threats in the cloud.
- Uptycs ingests activity logs so analysts can trace user activity during incident investigation.
- Uptycs offers in-depth analysis of your cloud identity activity. Insight into access decisions, suspicious behavior and more. Security, incident response, and compliance teams are better able to detect and investigate unauthorized access, misuse, and insider threats.

Secure Features

Detect cloud threat behavior – Generate alerts based on malicious use of the cloud provider API for discovery, privilege escalation, remote code execution, data exfiltration, and more.

Threat intelligence – Compare Uptycs threat intelligence against observed domains and IP addresses from flow logs to detect communication with known command-and-control servers and API calls from known malicious IP addresses.

MITRE ATT&CK for IaaS coverage – Detect and map attack techniques and sub-techniques described by MITRE so analysts have better context during triage and investigations.



Cloud threat detection details - Get the context you need and follow the steps of the attack.

Cloud Identity and Entitlement Analytics

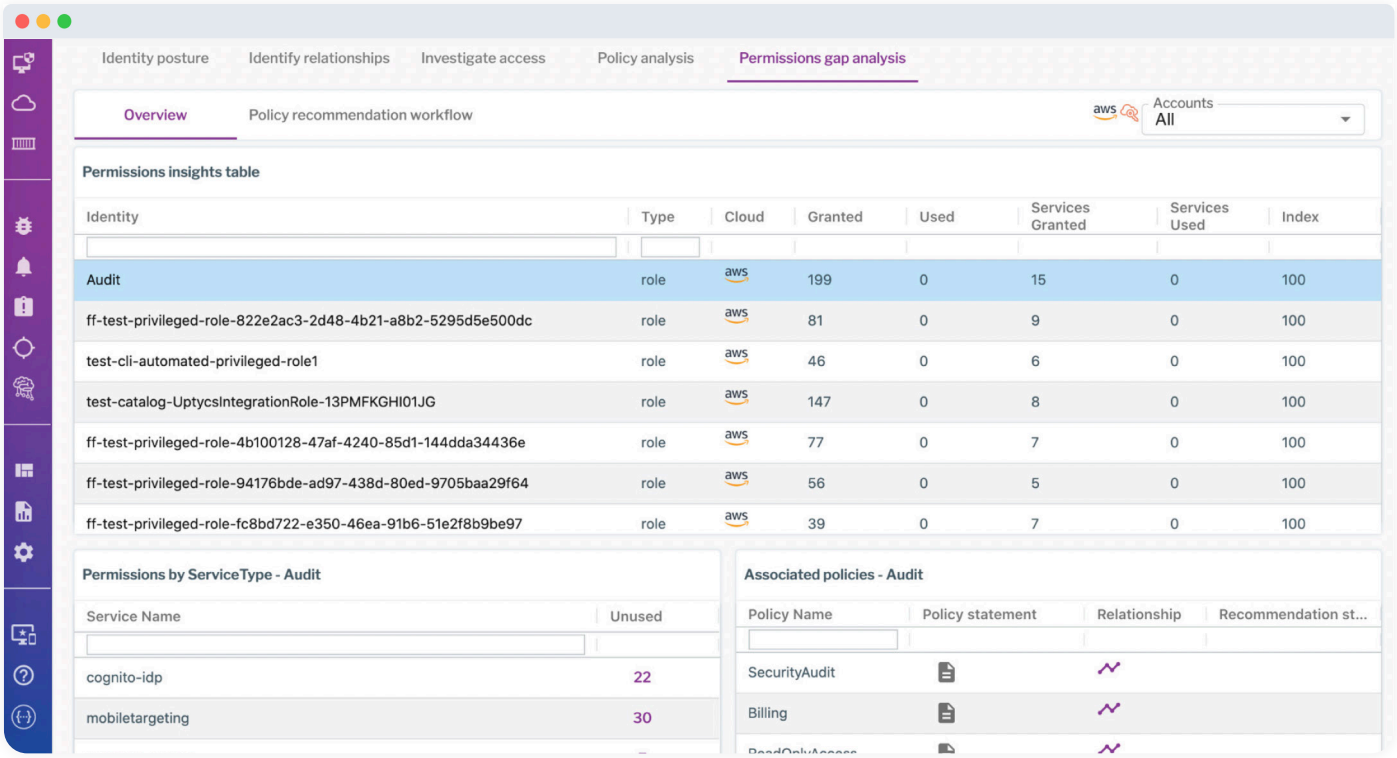
With organizations' ever-expanding cloud usage, it's a growing challenge to keep track of cloud identities and their privileges. Uptycs delivers a breakdown of your cloud identity risk and governance based on identity types, credentials, activity, and identity-specific control plane misconfiguration. With Uptycs, Security teams are better able to protect your cloud resources and infrastructure from unauthorized access, misuse, and insider threat.

Uptycs also provides permission gap analysis and identity mapping to see which assets an identity has access to, which permissions are granted to them, and which are actually being used. By seeing exactly how an identity interacts with your infrastructure, you're able to better establish least privilege and zero-trust permissions, thus reducing potential for misuse.

According to the *Managing Privileged Access in Cloud Infrastructure* report by Gartner, "by 2023, 75% of security failures will result from inadequate management of identities, access and privileges, up from 50% in 2020."

Monitor Least Privilege

With organizations' ever-increasing reliance on the cloud, IaaS and PaaS capabilities continue to expand, making it challenging to keep track of cloud identities and their privileges. Uptycs continuously monitors your cloud infrastructure to spot identity misconfiguration and permission gaps. This empowers you to continuously improve toward attaining least privilege and zero-trust access, thereby minimizing damage caused by privilege exploitation. Such analysis lets you easily understand how many permissions an identity has and how they're being are used.



Permission gap analysis - Identify overly-permissive roles and remediate immediately.

Measure Identity Risk and Governance Posture

By analyzing your identity and access management (IAM) policies, Uptycs measures the overall risk posture for your cloud accounts based on root account configuration, credentials rotation, possibility of privilege escalation, and credential exposure. Similarly, Uptycs also measures overall identity governance (or hygiene) based on how well your cloud accounts follow best practices such as the AWS Well-Architected Framework. The factors that influence your score include permission boundary configuration, orphaned roles/identities, and overly permissive identities.

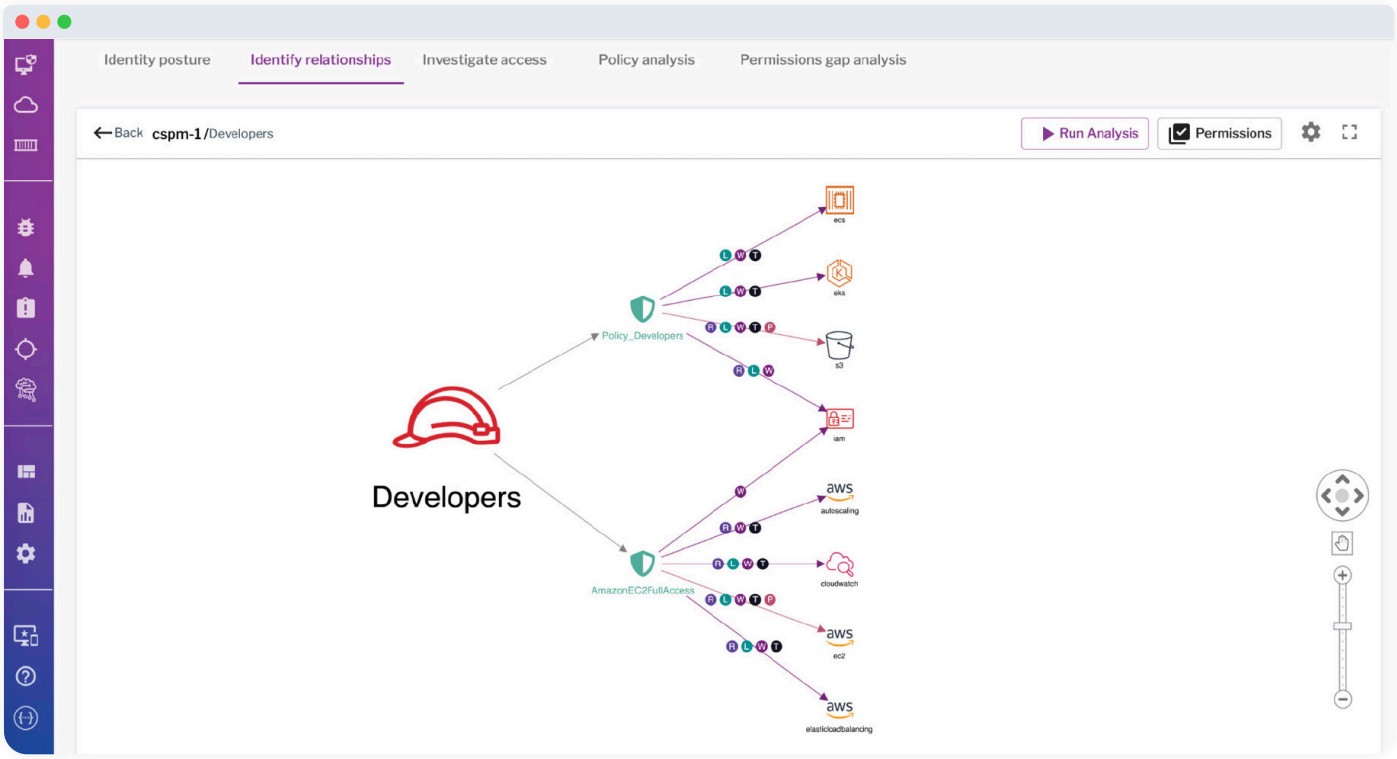
Harden IAM Policies

To gain a foothold in your cloud environment, attackers first target user access keys and passwords. That's why it's critical to make their task more difficult by appropriately limiting your IAM policies to avoid credential exposure, privilege escalation, resource exposure, and excessive privileges.

Uptycs continuously analyzes your IAM policies and creates risk profiles so you can prioritize efforts in tuning the most risky policies. Analysts can also use Uptycs to examine users and roles bound to a policy as well as specific permissions that could lead to privilege escalation or exposure.

Map Identities & Relationships

Uptycs maps how resources, identities, and policies are related in a visual graph. Filters let you easily get to questions without having to write complex queries. You can view relationships across accounts, rank connections based on risk, and see the impact a user can have on an asset or critical service. Such visualization helps your team understand who has access to what resources and with what level of permissions—in other words, the impact they can create on a service, or how much damage an attacker could inflict if they have compromised an identity.



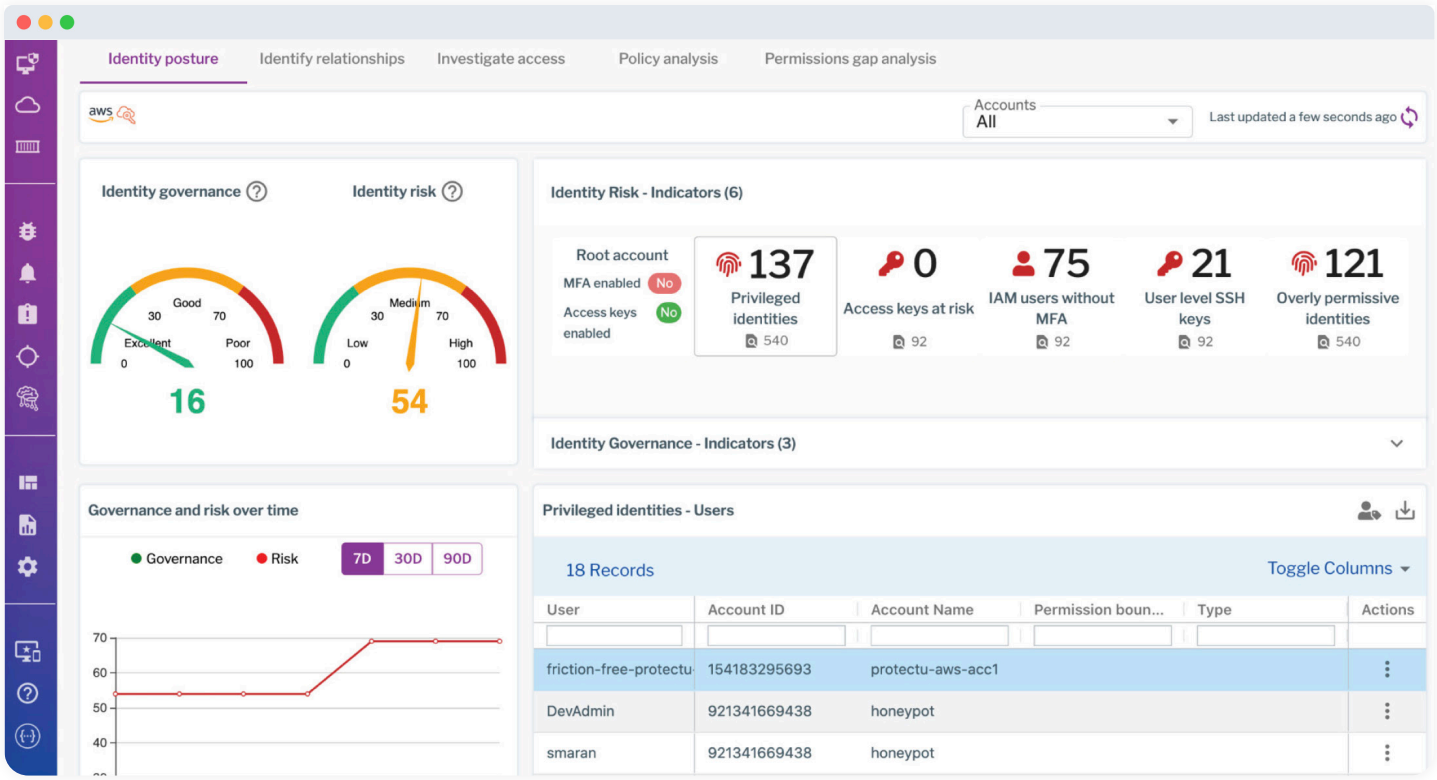
Identity relationship mapping - A picture is worth a thousand words. Use the map to understand relationships and navigate to investigate.

Detect and Investigate Identity Misuse

Without proper visibility into cloud identities and their entitlements, it can be impossible to keep track of exactly who has access to which assets, what kinds of action they can take, or the damage an identity can cause with unauthorized access. Uptycs offers in-depth analysis of your cloud identity activity with insight into access decisions, anomalous behavior, and more. Security, incident response, and compliance teams are better able to detect and investigate unauthorized access, misuse, and insider threat.

Identity posture breakdown – Extend risk and governance to identities with risk scores, inventory of privileged identities, and dashboards showing risky access keys, users without MFA, overly permissive identities, and more.

Access investigation – See top 10 IAM principles / top 10 services denied based on specific time windows. Drill down into trends for a specific user/service to spot any anomalies from the regions based on historical data. Establish identity provenance based on user activity data.



IAM dashboard - At a glance, know your IAM security posture and get key insights.

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