Uptycs

Uptycs for Cloud Infrastructure Security

Harden your hybrid and multi-cloud infrastructure against 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 Security Analytics platform incorporates cloud workload protection, cloud security posture management, and cloud infrastructure entitlements management in one common solution, so you can eliminate blind spots, detect threats, and ensure compliance.

Cloud Security Posture Management

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 their cloud-based assets and resources across accounts, and 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?"

Uptycs

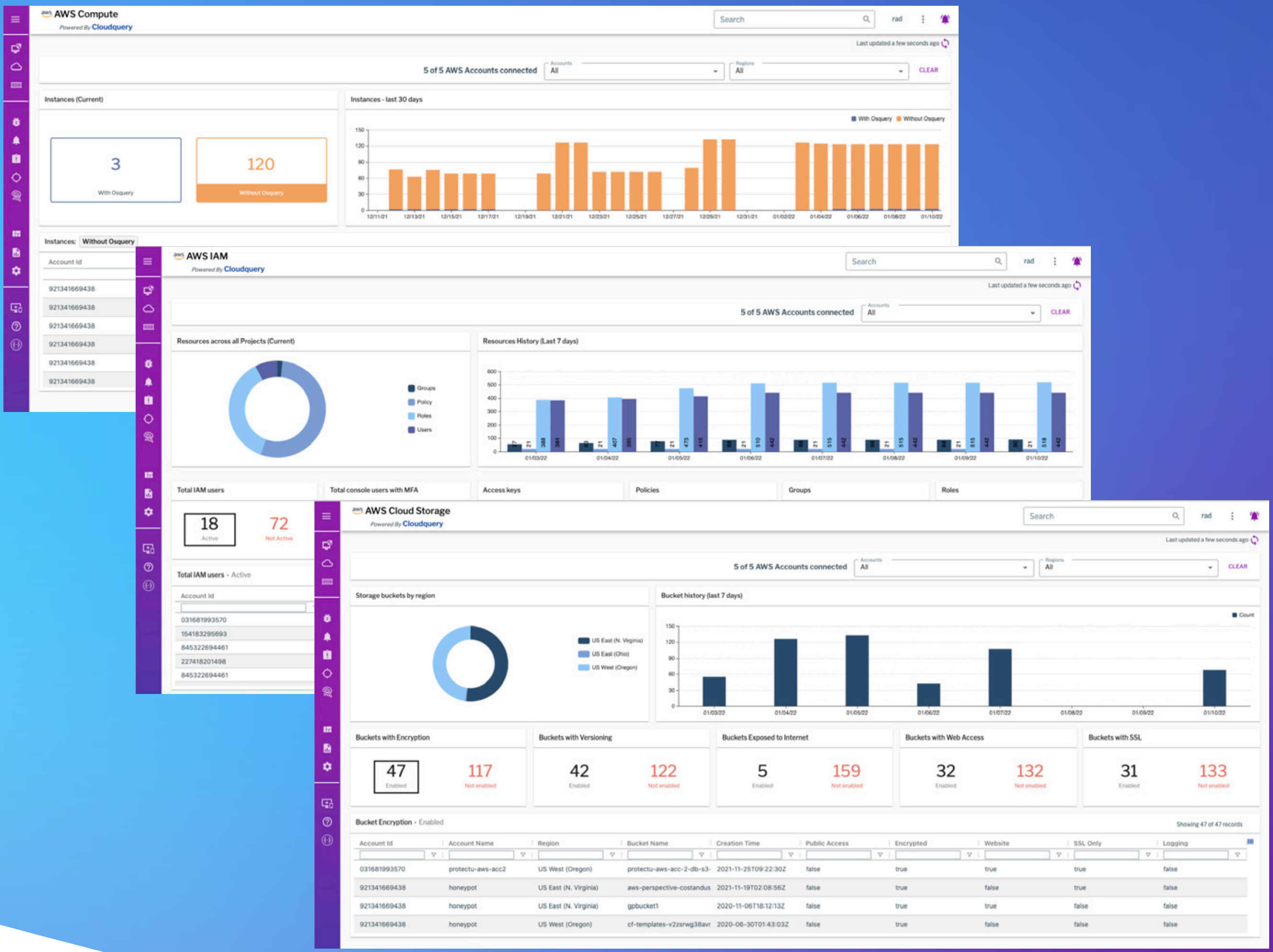
Visibility features

- **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 of the services from a cloud provider.

- **Insights dashboards.** Easily spot security issues with continuously updated snapshots of critical metrics for key services.

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



AWS Compute
Powered By Cloudquery

Last updated a few seconds ago

5 of 5 AWS Accounts connected — Accounts: All — Regions: All

Instances (Current)

3 With Osquery

120 Without Osquery

Instances - last 30 days

Instances: Without Osquery

Account Id
921341669438
921341669438
921341669438
921341669438
921341669438
921341669438

AWS IAM
Powered By Cloudquery

Last updated a few seconds ago

5 of 5 AWS Accounts connected — Accounts: All

Resources across all Projects (Current)

Resources History (Last 7 days)

Total IAM users: 18 Active, 72 Not Active

Total console users with MFA

Access keys

Policies

Groups

Roles

Total IAM users - Active

Account Id
031681993570
154183295693
845322694461
227418201498
845322694461

AWS Cloud Storage
Powered By Cloudquery

Last updated a few seconds ago

5 of 5 AWS Accounts connected — Accounts: All — Regions: All

Storage buckets by region

Bucket history (last 7 days)

Buckets with Encryption	Buckets with Versioning	Buckets Exposed to Internet	Buckets with Web Access	Buckets with SSL
47 Enabled, 117 Not enabled	42 Enabled, 122 Not enabled	5 Enabled, 159 Not enabled	32 Enabled, 132 Not enabled	31 Enabled, 133 Not enabled

Bucket Encryption - Enabled

Showing 47 of 47 records

Account Id	Account Name	Region	Bucket Name	Creation Time	Public Access	Encrypted	Website	SSL Only	Logging
031681993570	protectu-aws-acc2	US West (Oregon)	protectu-aws-acc-2-db-s3-	2021-11-25T09:22:30Z	false	true	true	true	false
921341669438	honeypot	US East (N. Virginia)	aws-perspective-costandus	2021-11-19T02:08:56Z	false	true	false	true	false
921341669438	honeypot	US East (N. Virginia)	gpbucket1	2020-11-06T18:12:13Z	false	true	true	false	false
921341669438	honeypot	US West (Oregon)	cf-templates-v2zsrwg38avr	2020-06-30T01:43:03Z	false	true	false	false	false

404 WYMAN ST.
WALTHAM,
MA, 02451

SCHEDULE YOUR DEMO TODAY:
www.uptycs.com/demo

Uptycs

Continuously Assess Cloud Security Posture

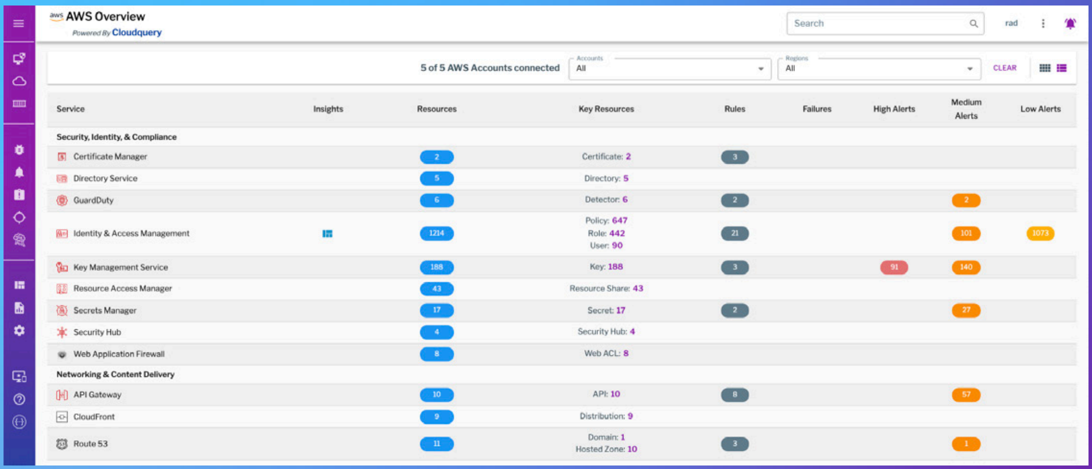
For Security teams, the growth of cloud usage can be nerve-wracking because it's so easy for developers and other users to make unintentional mistakes. Uptycs makes it easy for Security teams to ensure that their cloud resources are adhering to best practices.

Uptycs alerts teams to risks, like insecure configurations, tracks configuration history, and provides details that engineers need to quickly remediate issues. For example, 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 the 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.



5 of 5 AWS Accounts connected

Accounts: All

Regions: All

Service	Insights	Resources	Key Resources	Rules	Failures	High Alerts	Medium Alerts	Low Alerts
Security, Identity, & Compliance								
Certificate Manager		2	Certificate: 2	3				
Directory Service		5	Directory: 5					
GuardDuty		6	Detector: 6	2			2	
Identity & Access Management	▦	1214	Policy: 647 Role: 442 User: 90	21			101	1073
Key Management Service		188	Key: 188	3		91	140	
Resource Access Manager		43	Resource Share: 43					
Secrets Manager		17	Secret: 17	2			27	
Security Hub		4	Security Hub: 4					
Web Application Firewall		8	Web ACL: 8					
Networking & Content Delivery								
API Gateway		10	API: 10	8			57	
CloudFront		9	Distribution: 9					
Route 53		11	Domain: 1 Hosted Zone: 10	3			1	

404 WYMAN ST.
WALTHAM,
MA, 02451

SCHEDULE YOUR DEMO TODAY:
www.uptycs.com/demo

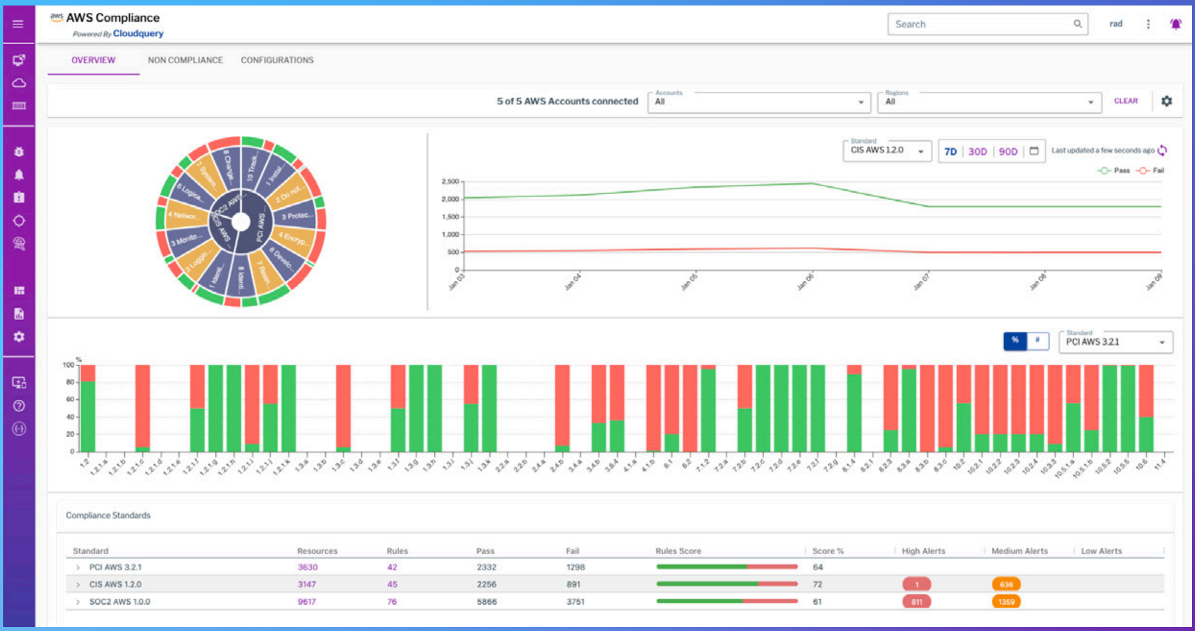
Uptycs

Ensure Compliance in the Cloud

Uptycs makes demonstrating compliance with detailed evidence much faster, with regular checks of your cloud environments against various standards including CIS Benchmarks, PCI-DSS, and SOC 2. Users can view summary visualizations of compliance posture and have the ability 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.

Comply features

- **Overview dashboards.** Track compliance posture with visual summaries of compliance over time, evidence, and snapshots of cloud resource configuration.
- **Historical trends.** Demonstrate improvement in compliance posture with compliance history by resource.
- **Customize standard checks.** Easily make adjustments based on your environment with parameterization and other customization options.
- **Easy remediation.** Make it easy to fix issues with one-click and automated remediation.
- One-click compliance reporting.



5 of 5 AWS Accounts connected

Accounts: All

Regions: All

Standard: CIS AWS 1.2.0

Standard: PCI AWS 3.2.1

Compliance Standards

Standard	Resources	Rules	Pass	Fail	Rules Score	Score %	High Alerts	Medium Alerts	Low Alerts
PCI AWS 3.2.1	3630	42	2332	1298		64			
CIS AWS 1.2.0	3147	45	2256	891		72	1	636	
SOC2 AWS 1.0.0	9617	76	5866	3751		61	811	1359	

404 WYMAN ST.
WALTHAM,
MA, 02451

SCHEDULE YOUR DEMO TODAY:
www.uptycs.com/demo

Detect and Investigate Cloud Threats

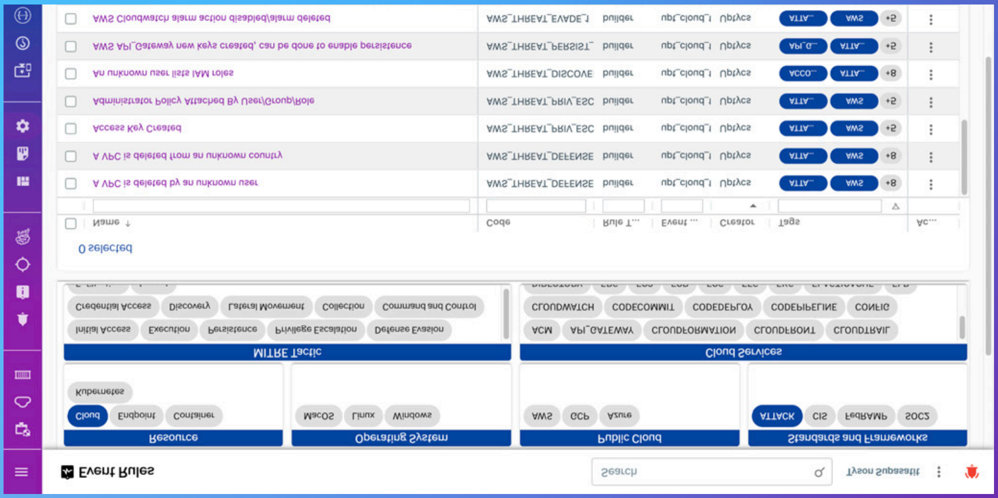
With Uptycs, Security teams can rapidly identify threat activity targeting their cloud environments and then dig into rich host-based and container-based data to answer difficult questions that come up during the course of investigation.

Uptycs offers several powerful detection and investigation capabilities for the cloud:

- Uptycs ingests network flow logs and matches IPs and domains against its threat intelligence platform to detect threats in the cloud.
- Uptycs ingests activity logs so that users can trace user activity during incident investigation.
- Uptycs offers in-depth analysis of your cloud identity activity with insight into access decisions, suspcious behavior and more so Security, Incident Response, and Compliance teams are better able to detect and investigate unauthorized access, misuse and insider threat.

Secure features

- **Detect cloud threat behavior.** Generate alerts based on malicious and unauthorized user behavior, such as cryptocurrency mining.
- **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 that analysts have better context during triage and investigations.



Name ↑	Code	Rule T...	Event ...	Creator	Tags	Ac...
A VPC is deleted by an unknown user	AWS_THREAT_DEFENSE	builder	upt_cloud_t	Uptycs	ATTA... AWS +8	⋮
A VPC is deleted from an unknown country	AWS_THREAT_DEFENSE	builder	upt_cloud_t	Uptycs	ATTA... AWS +8	⋮
Access Key Created	AWS_THREAT_PRIV_ESC	builder	upt_cloud_t	Uptycs	ATTA... AWS +5	⋮
Administrator Policy Attached By User/Group/Role	AWS_THREAT_PRIV_ESC	builder	upt_cloud_t	Uptycs	ATTA... AWS +5	⋮
An unknown user lists IAM roles	AWS_THREAT_DISCOVE	builder	upt_cloud_t	Uptycs	ACCO... ATTA... +8	⋮
AWS API_Gateway new keys created, can be done to enable persistence	AWS_THREAT_PERSIST_	builder	upt_cloud_t	Uptycs	API_G... ATTA... +5	⋮
AWS Cloudwatch alarm action disabled\alarm deleted	AWS_THREAT_EVADE_1	builder	upt_cloud_t	Uptycs	ATTA... AWS +5	⋮

404 WYMAN ST.
WALTHAM,
MA, 02451

SCHEDULE YOUR DEMO TODAY:
www.uptycs.com/demo

Cloud Identity Security

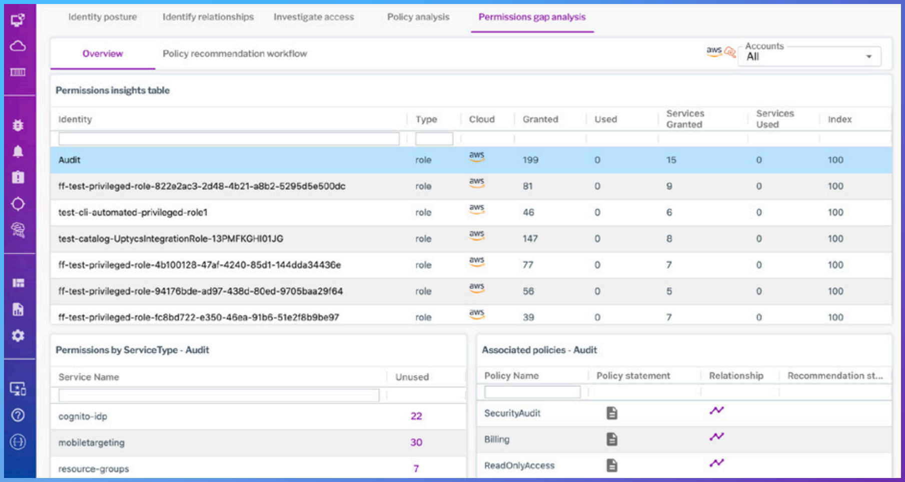
With organizations' ever-expanding cloud usage, it is a growing challenge to keep track of cloud identities and their privileges. Uptycs delivers a breakdown of your cloud identity risk and governance based on identity types, credentials, activity and identity-specific control plane misconfiguration. With Uptycs, Security teams are better able to protect their 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, 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 cloud identity infrastructure to spot identity misconfiguration and permissions gaps so you can continuously improve toward attaining least privilege and zero trust access, minimizing the damage that can be caused by privilege exploitation. With permissions gap analysis, you can understand how many permissions an identity has and how those permissions are used.



Permissions insights table

Identity	Type	Cloud	Granted	Used	Services Granted	Services Used	Index
Audit	role	aws	199	0	15	0	100
ff-test-privileged-role-822e2ac3-2d48-4b21-a8b2-5295d5e500dc	role	aws	81	0	9	0	100
test-cli-automated-privileged-role1	role	aws	46	0	6	0	100
test-catalog-UptycsIntegrationRole-13PMFKGHI01JG	role	aws	147	0	8	0	100
ff-test-privileged-role-4b100128-47af-4240-85d1-144dda34436e	role	aws	77	0	7	0	100
ff-test-privileged-role-94176bde-ad97-438d-80ed-9705baa29f64	role	aws	56	0	5	0	100
ff-test-privileged-role-fc8bd722-e350-46ea-91b6-51e2f8b9be97	role	aws	39	0	7	0	100

Permissions by ServiceType - Audit

Service Name	Unused
cognito-idp	22
mobiletargeting	30
resource-groups	7

Associated policies - Audit

Policy Name	Policy statement	Relationship	Recommendation st...
SecurityAudit	🗎	⁓	
Billing	🗎	⁓	
ReadOnlyAccess	🗎	⁓	

404 WYMAN ST.
WALTHAM,
MA, 02451

SCHEDULE YOUR DEMO TODAY:
www.uptycs.com/demo

Measure Identity Risk and Governance Posture

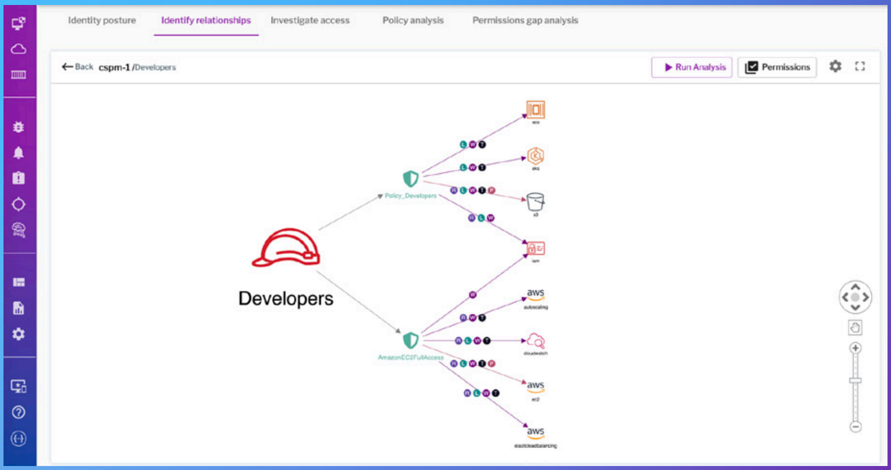
By analyzing your identity and access management (IAM) policies, Uptycs measures the overall identity risk posture for your cloud accounts based on factors such as root account configuration, credentials rotation, possibility of privilege escalation, and credential exposure. Similarly, Uptycs also measures 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 governance 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 is critical to make attackers' jobs 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 that you can prioritize your efforts on tuning the most risky policies. Analysts can also use Uptycs to examine the users and roles bound to a policy, and the specific permissions that may lead to privilege escalation or exposure.

Map Identities and Relationships

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



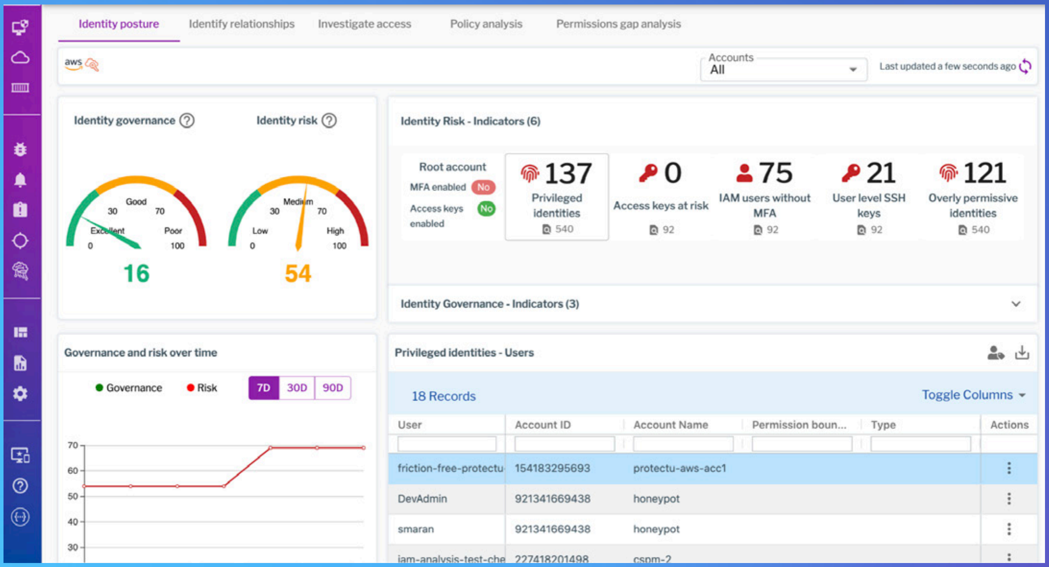
404 WYMAN ST.
WALTHAM,
MA, 02451

SCHEDULE YOUR DEMO TODAY:
www.uptycs.com/demo

Detect and Investigate Identity Misuse

Without proper visibility into cloud identities and their entitlements, it can be impossible to keep track of who exactly 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 so 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 principals / Top 10 Services denied based on specific time windows. Drill down into trends for a specific user/service and spot any anomalies from the regions based on historical data. Establish identity provenance based on user activity data.



User	Account ID	Account Name	Permission boun...	Type	Actions
friction-free-protectu	154183295693	protectu-aws-acc1			⋮
DevAdmin	921341669438	honeypot			⋮
smaran	921341669438	honeypot			⋮
iam-analysis-test-che	227418201498	cspm-2			⋮

About Uptycs

Uptycs provides the first unified, cloud-native security analytics platform that enables both endpoint and cloud security from a common solution. The solution provides a unique telemetry-powered approach to address multiple use cases—including Extended Detection & Response (XDR), Cloud Workload Protection (CWPP), and Cloud Security Posture Management (CSPM). Uptycs enables security professionals to quickly prioritize, investigate, and respond to potential threats across a company's entire attack surface.

404 WYMAN ST.
WALTHAM,
MA, 02451

SCHEDULE YOUR DEMO TODAY:
www.uptycs.com/demo