Uptycs

# Uptycs for AWS Security

Uptycs combines data from AWS services with data from cloud-based hosts (containers and the EC2 instances they run on). This gives security teams an end-to-end view of their cloud workloads—and the environment they operate in—and helps them easily answer difficult questions about cloud hosts and resources. At a glance, they can spot misconfigurations and vulnerabilities, meet compliance reporting requirements, and detect and investigate threats in the cloud.

FOR ENDPOINTS, SERVERS, CONTAINERS, & CLOUD

AUDIT & COMPLIANCE

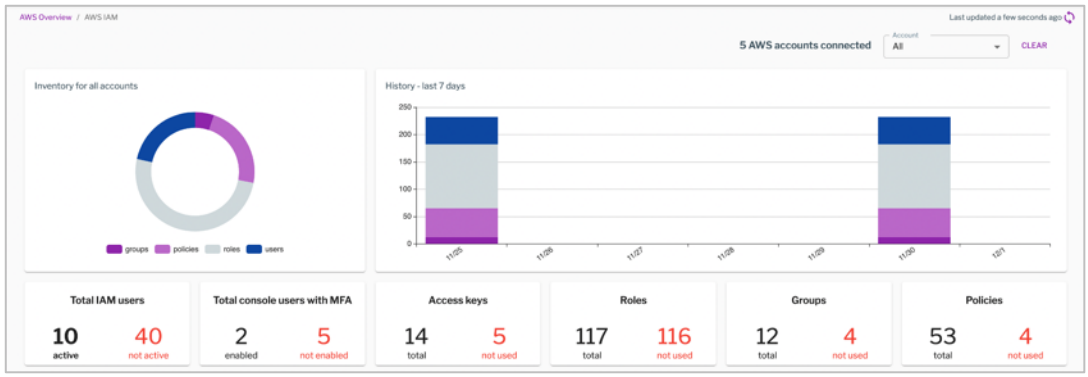
FLEET VISIBILITY

INTRUSION DETECTION

VULNERABILITY MONITORING

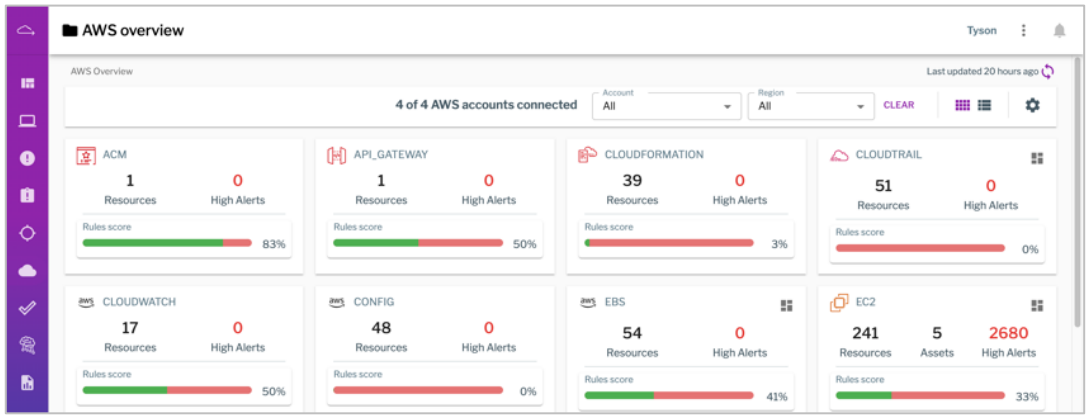
## Simplify Cloud Asset and Resource Inventory

You can't secure what you can't see. Uptycs' AWS offering gives you connected insights across all of your AWS accounts so you can get answers fast. Users can group and tag their cloud-based assets and resources across accounts, and run queries and reports. In a single place, you can answer questions about your entire cloud estate such as "What cloud-based assets do I have running and where?" and "What are my cloud service configurations?"




## Continuously Assess Cloud Security Posture

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 move fast. Uptycs makes it easy to ensure that AWS resources across accounts 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 such as MFA for users, CloudTrail logging on resources, and unauthorized API activity.




WWW.UPTYCS.COM

"As a cloud-based company running on AWS, finding a platform to solve all of our security needs across all of our accounts and services was a top priority. But finding a single solution that could solve for audit and inventory of our cloud assets, as well as endpoint detection and response, was a challenge—until we found Uptycs. Now we're able to do more with less, and save time, while maintaining a strong cloud security posture."

- KEVIN PAGE, CISO, FLEXPORT

WWW.UPTYCS.COM

# Uptycs for AWS Security

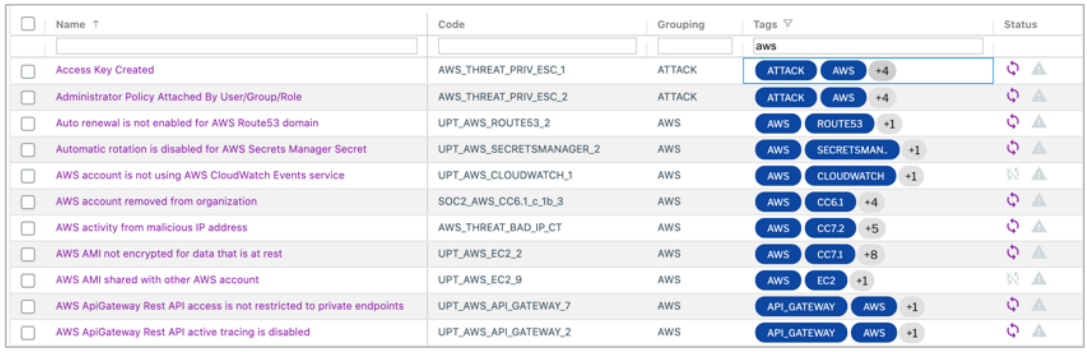
## Ensure Compliance in the Cloud

Uptycs makes demonstrating compliance with detailed evidence much faster. Security and compliance teams will know where they need to target their remediation efforts. 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. Uptycs currently supports CIS Benchmarks for AWS and SOC 2 out of the box and can add support for other standards.


## Detect and Investigate Cloud Threats

Uptycs provides connected insights across your hybrid environment so you can seamlessly investigate threats wherever they appear. Security teams can rapidly identify threat activity targeting their AWS environments and then dig into rich host-based and container-based data to answer difficult questions that come up during the course of investigation. They can implement and monitor least-privilege IAM policies in AWS, limiting the damage from compromised AWS credentials.

- Uptycs ingests IAM policy rules to perform security assessments, enable users to see permissions are being used by which entity (user and role) and when last used, and alert on policies with excessive permissions. Uptycs ingests IAM policy rules to perform security assessments. In the cloud, if attackers can gain access or escalate their privileges through IAM, then they have the keys to the kingdom. As one of our customers has said, "IAM is a firewall for the cloud," because if IAM configurations are insecure, then other preventative protections become less relevant.
- Uptycs ingests AWS CloudTrail and VPC Flog Logs and matches this information against its threat intelligence platform to detect threats in the cloud.
- To trace user activity during investigation, Uptycs also correlates activity on hosts and containers with AWS CloudTrail logs and VPC Flow Logs.



| Name | Code | Grouping | Tags | Status |
|---|---|---|---|---|
| | | | aws | |
| Access Key Created | AWS_THREAT_PRIV_ESC_1 | ATTACK | ATTACK AWS +4 | |
| Administrator Policy Attached By User/Group/Role | AWS_THREAT_PRIV_ESC_2 | ATTACK | ATTACK AWS +4 | |
| Auto renewal is not enabled for AWS Route53 domain | UPT_AWS_ROUTE53_2 | AWS | AWS ROUTE53 +1 | |
| Automatic rotation is disabled for AWS Secrets Manager Secret | UPT_AWS_SECRETSMANAGER_2 | AWS | AWS SECRETSMAN.. +1 | |
| AWS account is not using AWS CloudWatch Events service | UPT_AWS_CLOUDWATCH_1 | AWS | AWS CLOUDWATCH +1 | |
| AWS account removed from organization | SOC2_AWS_CC6.1_c_1b_3 | AWS | AWS CC6.1 +4 | |
| AWS activity from malicious IP address | AWS_THREAT_BAD_IP_CT | AWS | AWS CC7.2 +5 | |
| AWS AMI not encrypted for data that is at rest | UPT_AWS_EC2_2 | AWS | AWS CC7.1 +8 | |
| AWS AMI shared with other AWS account | UPT_AWS_EC2_9 | AWS | AWS EC2 +1 | |
| AWS ApiGateway Rest API access is not restricted to private endpoints | UPT_AWS_API_GATEWAY_7 | AWS | API_GATEWAY AWS +1 | |
| AWS ApiGateway Rest API active tracing is disabled | UPT_AWS_API_GATEWAY_2 | AWS | API_GATEWAY AWS +1 | |

**SEE IT LIVE!** www.uptycs.com/live-demo