uptycs SRC CYBER SOLUTIONS LLP

Solution Brief

Uptycs for AWS

Secure AWS and connected assets from a single security console, policy framework, and data lake. Gain unified security and compliance visibility, risk-based prioritization, and rapid threat detection and remediation across AWS, hybrid multicloud, and your developer ecosystem.

Uptycs and AWS: Better together

Looking to migrate or expand in AWS? Uptycs can help ease your transition by providing you with security and compliance consistency across your data center and hybrid multicloud environments. Uptycs centralizes the functionality of multiple native and third-party security tools, automates data correlation and detection, and simplifies workflows for investigation, remediation, and threat hunting.

The agentless debate is over. Choice won.

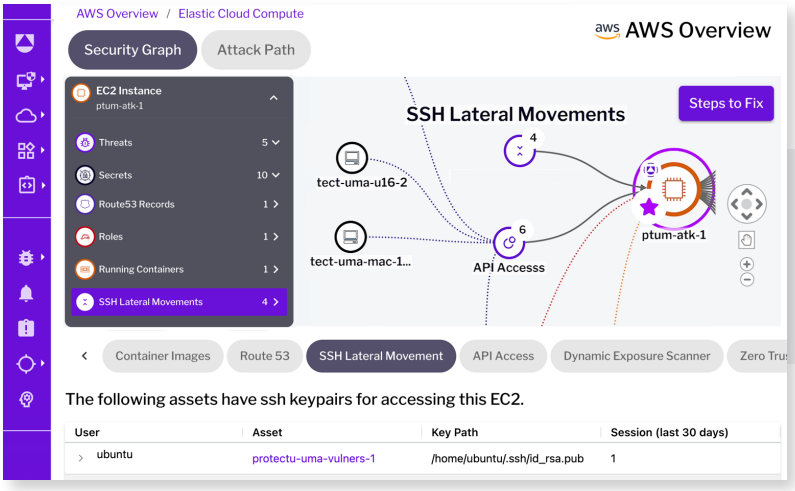
Secure your AWS environment with a trusted and proven partner. Uptycs has multiple AWS validations including being AWS SaaS QuickLaunch–enabled, meaning you get accelerated deployment. Start with wall-to-wall agentless coverage then add the Uptycs Sensor on critical workloads for runtime protection, advanced remediation, and forensics.

Uptycs has been validated in the following programs:

- AWS Security Software Competency
- AWS Container Security Competency
- AWS Graviton Partner
- AWS Public Sector Partner
- AWS Security Hub Partner
- AWS SaaS QuickLaunch Partner

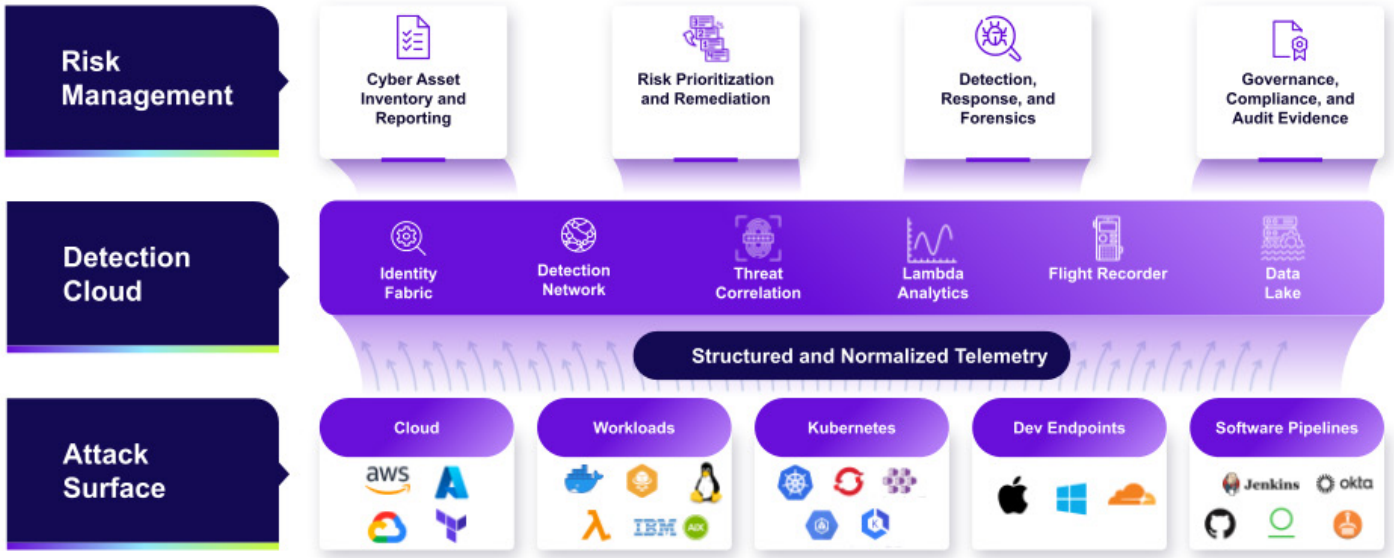
Detect, prioritize, and remediate risk

Get continuous, all-time visibility, correlating telemetry across your AWS environment and the development ecosystem. Uptycs prioritizes laptop to code to cloud vulnerabilities and threats by looking at available remediations, asset value, and the latest exploit data from threat intel feeds. Enjoy guided remediation of vulnerabilities and threats throughout the software development lifecycle and into production.



Go beyond point-in-time snapshots by leveraging Uptycs' real-time security graphs to continuously monitor the potential impact of security incidents – from laptop to code to cloud

> "We've gotten a significant ROI on our Uptycs investment by playing to its strengths - the single data model and backend analytics. It's one of the most powerful tools in our security arsenal."
>
> **Grant Kahn,** Director of Security Intelligence Engineering, Lookout



Shift up your AWS security

Don't settle for fragmented visibility

Gain comprehensive security visibility across your cloud and connected assets, including VMs, containers, Kubernetes, serverless, developer endpoints, GitHub repos, and CI/CD pipelines.

Ephemeral workloads can erase the origin of an attack. Uptycs blends 13 months of historical data with runtime insights so you not only know what's risky, but also if a threat actor has been active in your environment.

Supercharge SecOps with customizations

Customize out-of-the-box capabilities for your environment by tagging and grouping assets, refining threat analysis with detection as code, and creating custom dashboards focused on your most critical assets or business objectives. Encourage application owners and SecOps to work together through policy-based workflows and automations across your SDLC.

The result is the ability to quickly bring the right people together to reduce risk, fix vulnerabilities, or block or remove a threat.

Don't just detect. Remediate.

Use real-time detections mapped to the MITRE ATT&CK framework or YARA to identify and remove emerging threats and malware at scale. Remediate Kubernetes risk inside the cluster and across your container supply chain.

Investigate and respond to suspicious behavior or an active breach, and remediate down to the host or process level. Quickly kill, pause, and restart processes, disable users, quarantine hosts, and run remediation scripts.

Discover

Know what you have so you can protect it.

Deep asset inventory: discover, inventory, and map all AWS cloud resources, workloads, and users.

Instant graphical discovery: visualize networking and IAM relationships across all AWS services, accounts, and regions without having to toggle through multiple screens.

Full AWS support: continuously monitor AWS cloud workloads and services like Amazon EC2, S3, IAM, EKS, EBS, ECS, CloudTrail, Workspaces, Fargate, and more.

Audit

Identify what's wrong so you can fix it.

Risk correlation and prioritization: consolidate diverse AWS telemetry —such as CloudTrail, flow logs, S3 logs, EKS audit logs, and runtime data—into a unified data lake for correlated analysis to quickly identify and prioritize your highest risks.

Misconfiguration alerting and remediation: detect and alert on misconfigurations in real time, then trigger automatic or step-through remediations.

Full lifecycle vulnerability management: get comprehensive vulnerability detection, monitoring, prioritization, and image layer insight for VM, container workloads, and serverless running on AWS from build to production.

Compliance management: monitor compliance posture, capture evidence, and align to CIS Benchmarks, PCI, SOC 2, AWS well-architected framework, NSA Hardening Guidelines for K8s, and more.

Shift-left image scanning: continuously scan images throughout the SDLC with automated vulnerability, malware, and secrets scanning. Start with CI tools like AWS CodeBuild and move to container registries such as Artifactory.

Identity access monitoring: protect AWS resources from unauthorized access, misuse, and insider threats. Easily spot permission gaps and overly-permissive roles, and apply the principles of least privilege.

Visual attack path analysis: visualize anomalous activities across your AWS estate and connected assets to pinpoint lateral movement, privilege escalation, and unauthorized access.

Secure

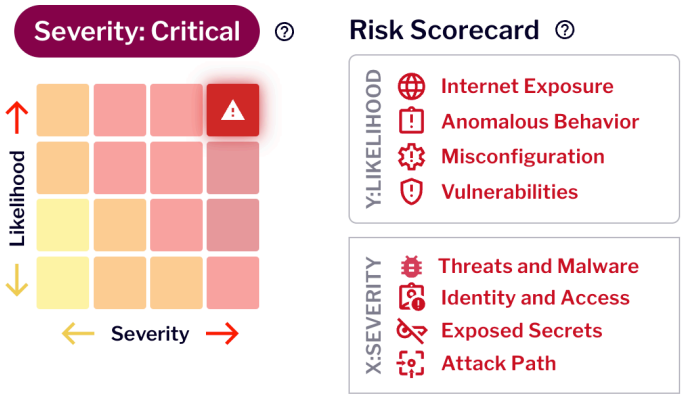
Respond to suspicious behavior so you can secure it.

End-to-end security: remediate vulnerabilities, fix misconfigurations, and mitigate threats across the SDLC and AWS runtime environment, starting with developer endpoints.

Threat detections: utilize real time threat detection that maps data plane threat information to the MITRE ATT&CK framework. Correlate threats with AWS cloud infrastructure misconfigurations for rapid threat mitigation.

eBPF workload security: minimize CPU and I/O footprint with the Uptycs Sensor for YARA file/memory scanning, container process blocking and remediation. Conduct forensic investigations, and live and historical queries across your AWS estate.

Predict potential threats: leverage anomaly detection across billions of events, formulate an assumed breach hypothesis and leverage advanced threat hunting to protect crown jewel data and services. Use a user-friendly interface to investigate issues, such as identifying cross-account suspicious activities and stolen GitHub AWS keys, to quickly achieve resolution.



Broad ecosystem support

Workloads	Amazon EC2, EKS, Lambda, ECS on Fargate, ECS on EC2 instances
Container Runtime	Docker, CRI-O, Containerd
Image Registries	Amazon ECR, JFrog Artifactory, Google GCR, Azure ACR, Private Docker Registry (Cloud + On-Prem)
CI Pipeline	AWS Codebuild, Jenkins, GitHub Actions, GitLab, Travis CI
IaC Scanning	AWS CloudFormation, Terraform, Helm, Kubernetes YAML, Dockerfile
Compliance Standards	AWS Well-Architected Framework, CIS, SOC2, PCI, NSA Hardening, HIPAA, ISO 2700, FedRAMP, and more
3rd Party SaaS	Identity Providers: Azure AD, Okta Code Repositories: GitHub ISVs: Axonius, Cortex XSOAR, Cribl, Datadog, Jira, PagerDuty, Panther, SafeBreach, ServiceNow, Slack, Splunk, Tarsal, Tines, Torq, QRadar, and more API-first: Add your own integrations leveraging Postman and Swagger
Developer Endpoints	macOS, Linux, Windows, Cloudflare ZTNA

aws PARTNER
- Container Security Competency
- Security Software Competency
- AWS Graviton Ready
- Public Sector Partner
- AWS Marketplace Seller

AICPA SOC — SOC 2 Type II Certified

MITRE Engenuity ATT&CK Eval TURLA 2023

CIS Benchmarks™ Certified

About SRC

At SRC Cyber Solutions LLP , we provide Next Generation , Highly Automated , User - Friendlyand scalable solution . Our robust solutions include Comprehensive Email Security , Automated Patching and Endpoint Management , Asset Risk Visibility and Management with Policy Enforcement (ARM), Third - Party Data Flow Security solutions, Agentless Micro Segmentation, Endpoint, Management, and, Compliance Platform and an Online Gamified Simulation Platform for Cyber Security Training attacks . Additionally , we provide a Cloud - Native Application Protection Platform (CNAPP) solution to ensure comprehensive security across cloud - native applications.

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

uptycs

www.srccybersolutions.com | +91 120 232 0960 /1 | sales@srccybersolutions.com