

Uptycs for AWS

Safeguard your entire AWS estate, from macOS to EKS, on a single unified platform. Get started with instant-on agentless coverage, then shift up to dynamic runtime protection and advanced remediation capabilities using the Uptycs Sensor.

Uptycs and AWS: Better together

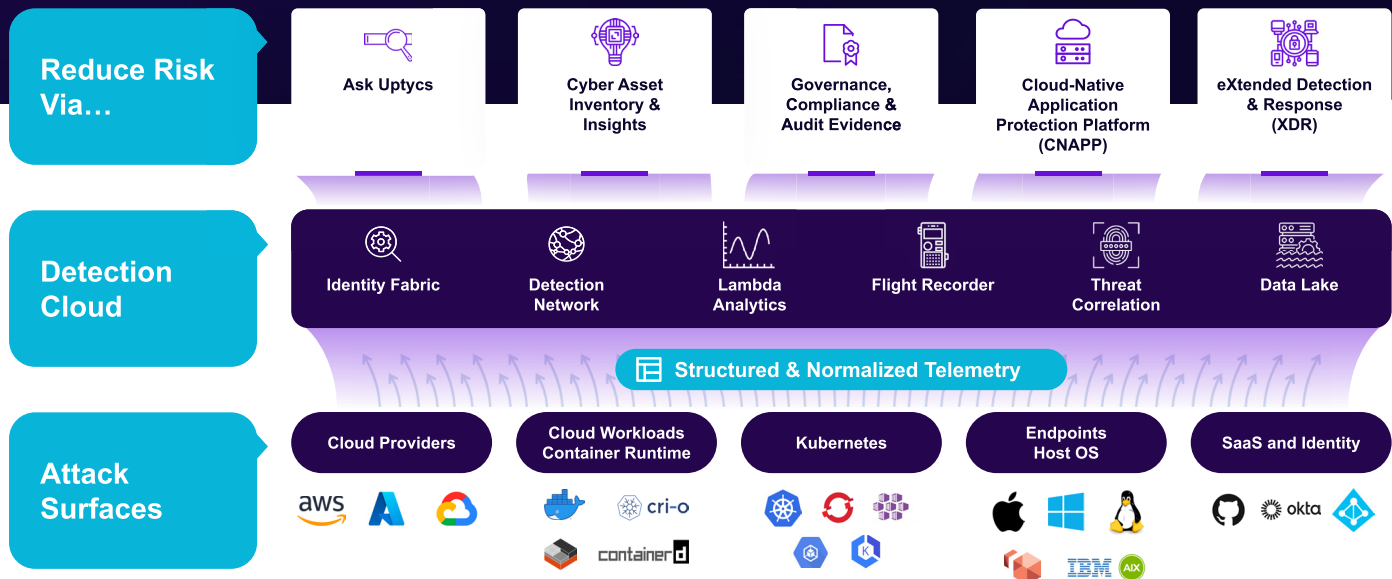
By integrating with native AWS services and developer workspaces, Uptycs enhances AWS security capabilities while also serving as a cloud security early warning system, stopping threat actors before they ever reach your cloud.

Uptycs, an AWS Security Competency Partner and Public Sector Partner, also offers managed detection and response services (MDR) to bolster your existing team.

Secure your AWS estate and connected assets

Unlike siloed tools, Uptycs delivers connected insights by streaming normalized and structured telemetry into your Uptycs Detection Cloud. This eliminates the need to navigate through disparate data sources, perform ETL functions, or learn multiple UIs.

What's more, Uptycs provides a powerful search tool, deep asset inventory, and the compliance, CNAPP, and XDR capabilities you need to stay vigilant and be ready for what's next.



Shift up your AWS security

Visualize and prioritize risk for AWS

Go beyond basic security graphs to identify cloud-wide vulnerabilities, implement preventative measures, and execute remediations.

Reduce dwell time with real-time attack path analysis and monitoring.

Take control of your cloud identities

Better protect your AWS resources from unauthorized access, misuse, and insider threats.

Easily spot permission gaps and overly-permissive roles, and apply the principles of least privilege.

Quickly detect and respond to cloud threats

Rapidly identify and respond to malicious use of AWS APIs, privilege escalation, remote code execution, data exfiltration, and more.

Enlighten your team with plain-language explanations of cloud security events.

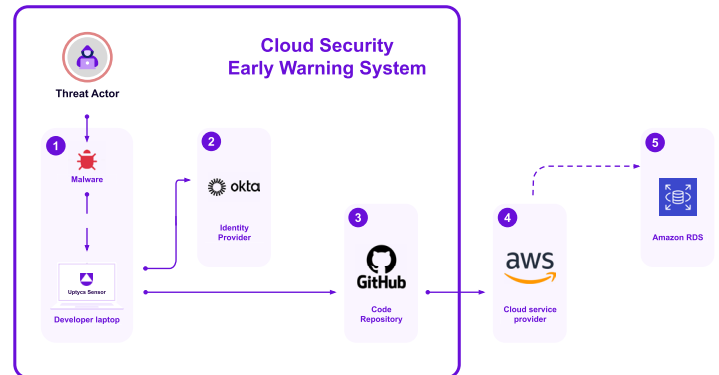
Secure your cloud workloads - both control plane and data plane

Track cloud asset inventory, monitor compliance, detect and remediate vulnerabilities and threats, ensure image security, and scan for secrets from the CI/CD pipeline to production. Gain comprehensive security visibility across your cloud assets, including VMs, containers, Kubernetes, and serverless.

Full lifecycle cloud-native application security – from laptop to cloud

Major cloud breaches often start with the developer's laptop. Uptycs helps you correlate threat activity across developer machines, source code repositories, identity providers, and cloud infrastructure in one unified platform.

Collect and analyze developer identity information from Okta and audit logs from GitHub to reveal suspicious behavior as the developer moves code in and out of repositories and into AWS.



Ensure cloud compliance

Comply with industry standards by leveraging Uptycs' validation against CIS Benchmarks, PCI-DSS, SOC 2, and the AWS well-architected framework, as well as environment-specific checks, such as NSA Hardening Guidelines for K8s.



"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

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, delivering a more cohesive security posture across your entire enterprise

Shift up your cybersecurity with Uptycs.

