uptycs

Solution Brief

Uptycs for Cloud Native Applications

Build security into your cloud native applications from development to production with one integrated platform.

> As organizations build out their cloud deployments, they often purchase niche tools to meet specific needs. But this disconnected approach results in confusion and complexity. Uptycs provides a cloud-native application protection platform (CNAPP) to solve your most-pressing cloud security challenges in a single product.

Why Uptycs?

Make Better Risk Decisions

Make better risk decisions about vulnerabilities and threats–derived from risk signals emanating from a large volume and variety of security and IT data. Data which enterprises must control. No black boxes!

Cover Your Modern Attack Surfaces

Protect digital assets spread across heterogeneous infrastructure through a platform that covers hybrid cloud, containers, laptops, and servers from a single platform, UI, and data model. Extensibility must be based on standardized telemetry and open standards.

Harden, Detect, and Respond

Eliminate tool, team, and infrastructure silos, and consolidating identity and policy management, and security intelligence so that you can prioritize vulnerabilities for remediation, and speed up MTTD and MTTR.

Uptycs Can Help:

- Consolidate disparate tools to create a unified security front against threats across all of your cloud native attack surfaces
- Gain visibility into your microservices
- Scan images for vulnerabilities, sensitive data, and misconfigurations

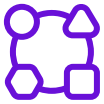
Uptycs Cloud Native Application Security Use-Cases

Streamline security controls across build, infrastructure, and workloads

Streamline your security controls with a centralized platform to manage VMs, containers, and Kubernetes security policies and configurations. Automate security checks and testing, reducing the need for manual intervention.

Gain visibility into your cloud native application lifecycle

Gain better visibility into the security posture of your application by providing real-time monitoring and analytics. This enables you to identify potential security threats and vulnerabilities and take immediate action to mitigate them.



Simplify integration across your development pipeline

Integrate easily with your existing DevOps tools and workflows, so you can seamlessly integrate security into your development pipeline. This eliminates the need for separate security tools and processes, making your development process more efficient and streamlined.

Achieve cloud native compliance

Ensure compliance with various industry standards and regulations by providing pre-defined policies and compliance rules. This ensures that your application meets the necessary security standards and requirements without requiring you to spend extra time and resources.

Reduce risk in your cloud native environment

Provide proactive security measures and automated security controls, to reduce the risk of security breaches and data loss. This also helps you minimize the impact of security incidents, reducing downtime and associated costs.

Uptycs Cloud Native Application Security Capabilities

Uptycs helps you unify your cloud native security efforts with:

CWPP

Cloud Workload Protection Platform

Cloud workloads are meant to run anywhere—in private cloud, public cloud, or hybrid. Uptycs provides security teams comprehensive visibility and control across all of their workloads, whether hosts, VMs, containers, microVMs, or serverless functions. And with both agentless and agent-based deployment options, you can get the most complete view of your environment in the way that works best for your security and operational needs.

KSPM

Kubernetes Security Posture Management

When Kubernetes and container deployments scale up, it becomes difficult to inventory and monitor your fleet. To make Kubernetes security simpler, Uptycs offers a single place to get clear visibility and control across your K8s clusters in Google GKE, AWS EKS, Azure AKS, Kubernetes, OpenShift, VMware Tanzu, and Google Anthos.

CSPM

Cloud Security Posture Management

You can't secure what you can't see. Uptycs helps you identify and prioritize risks across all of your cloud environments—AWS, Azure, and GCP—so you get a complete view of your cloud estate and the answers you need, fast.

CIEM

Cloud Infrastructure Entitlements Management

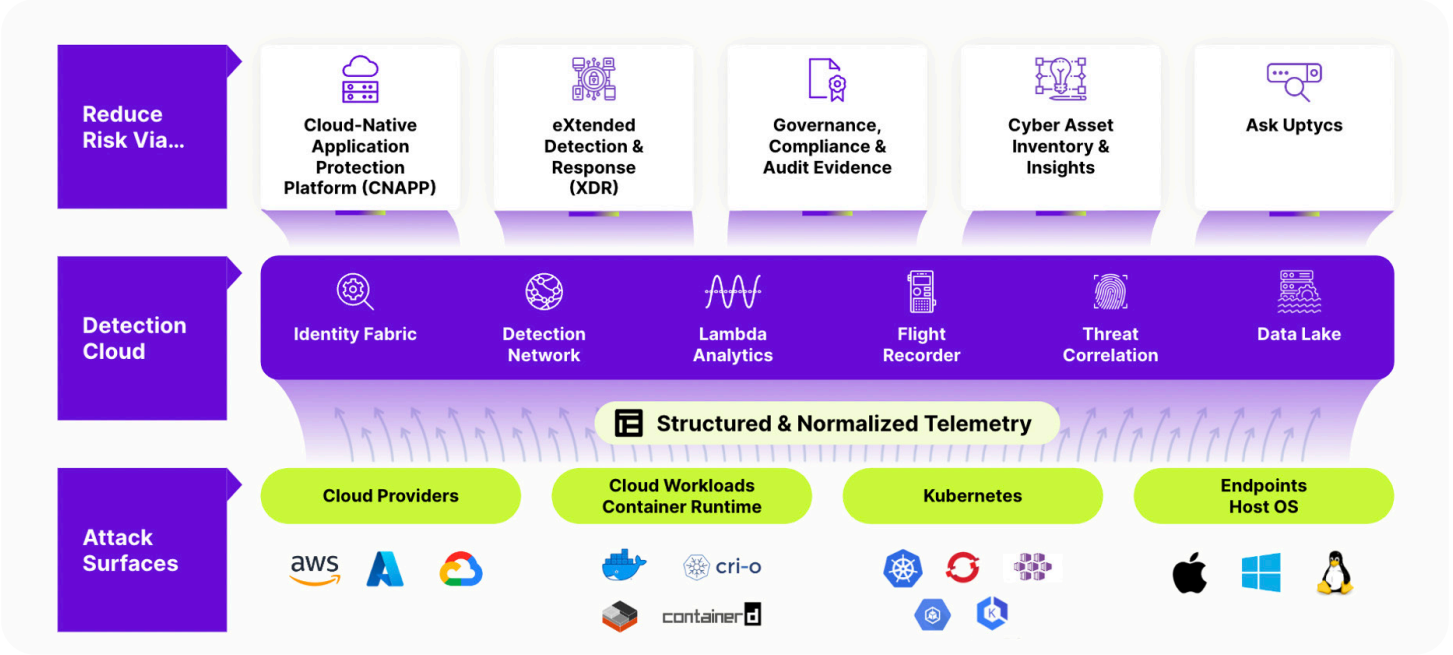
With organizations' ever-expanding cloud usage, it is a growing challenge to keep track of cloud identities and their privileges. Uptycs delivers a breakdown of your cloud identity risk and governance based on identity types, credentials, activity and identity-specific control plane misconfiguration.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

CDR

Cloud Detection and Response

Hardening, detecting, and responding to risks and threats in the cloud requires the ability to gain deep visibility into your applications and infrastructure, rapidly surface critical alerts, and instantaneously respond to the next zero-day. Uptycs protects against account compromise, insider threat, and access misuse with one platform for visibility and data-driven analytics to detect, investigate, and mitigate threats in the cloud.

The Uptycs Solution



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