CNAPP for Hybrid Cloud

Secure Everything from Dev to Runtime

Go Beyond Basic Posture Management.

Uptycs delivers outcome-driven cloud security with real-time detection, deep visibility, and automated prevention across your hybrid environment.

Security Outcomes, Built-In

A single pane of glass for cybersecurity professionals, covering **Inventory**, **Risk**, **Vulnerabilities**, **Compliance**, **Detections**, and **Response**. All correlated across cloud, containers, workloads, and CI/CD pipelines.

Discover & Monitor
See every asset from processes to software pages (SBOM)

Detect & Respond
Prioritize threats with enhanced correlated signals

Prevent & Harden
Enforce guardrails and streamline remediation

Use Cases Snapshot

Workload Protection
- Agentless scans + deep runtime visibility
- Rich telemetry: In memory running process view, file access and much more

Posture Management
- Detect config drift and access risk
- Custom checks and guided remediation

Detection & Response
- Real-time MITRE-mapped alerts
- Full attack path visibility
- Immediate remediation actions

Vulnerability Management
- Unified dashboard across clouds and workloads
- Context-aware, deep telemetry -driven risk prioritization
- Auto ticketing, SLA tracking, exceptions

Software Pipeline Security
- Scan images pre-deploy
- Trace vulns from build to runtime
- Enforce policy guardrails in CI/CD

Asset & Risk Management
- Agentless ephemeral assets discovery
- Prioritize with attack path + exposure correlation
- Historical data + forensic search (Ask Uptycs)

Why Uptycs?

Unified Risk Model
Cross-platform signals from cloud, workloads, endpoints, and identity – correlated in a single data model for smarter, faster prioritization.

Deep Runtime Telemetry
eBPF and osquery-based telemetry across processes, network, file, and software activity – delivering the rich signal needed for proactive defense and investigation.

Real-Time Response
Detect threats and take action instantly: block malware, quarantine hosts, kill processes, or trigger automated workflows.

Enterprise-Ready Scale
Secure hundreds of thousands of assets across hybrid and multicloud environments, with support for both agentless scans and lightweight sensors.

Single Pane of Glass
Unified visibility across cloud and on-prem assets from a single UI. No stitching together tools or toggling between consoles.

Configurable by Design
A highly customizable platform that adapts to your workflows, not the other way around. Create your own checks, rules, and integrations.

Built for Threat Hunters
Hunt across live and historical data with full context – process trees, network flows, file activity, identity, and more.

File Integrity Monitoring (FIM)
Industry-first FIM built into CNAPP. Track critical file changes across cloud workloads, containers, and servers – without bolting on third-party tools.

What Makes Uptycs Different

Deep + Wide Visibility
Unlike CNAPPs that rely on static scans, Uptycs leverages eBPF and osquery to correlate live process data with vulnerability posture. You see what's actually exploitable, not just what's installed.

Built for the Real World
Hybrid cloud. Containers. Kubernetes. Serverless. Uptycs secures it all, from the dev pipeline to production workloads.