uptycs

Datasheet

Uptycs CNAPP for Hybrid Cloud Security

Unify your hybrid cloud security – from dev to runtime

Uptycs is the top Cloud-Native Application Protection Platform (CNAPP) choice for security teams collaborating with developers to safeguard critical application pipelines, mitigate risks, and defend runtime environments in the hybrid cloud.

Uptycs consolidates cloud security silos into a unified platform, providing a single security console, policy framework, and data lake. This unification enables greater automation, simplifies policy enforcement, and extends security coverage, all while reducing costs.

Data is your power, not a headache

We tackled the cybersecurity data challenge first to give you deeper context so you can prioritize what truly matters.

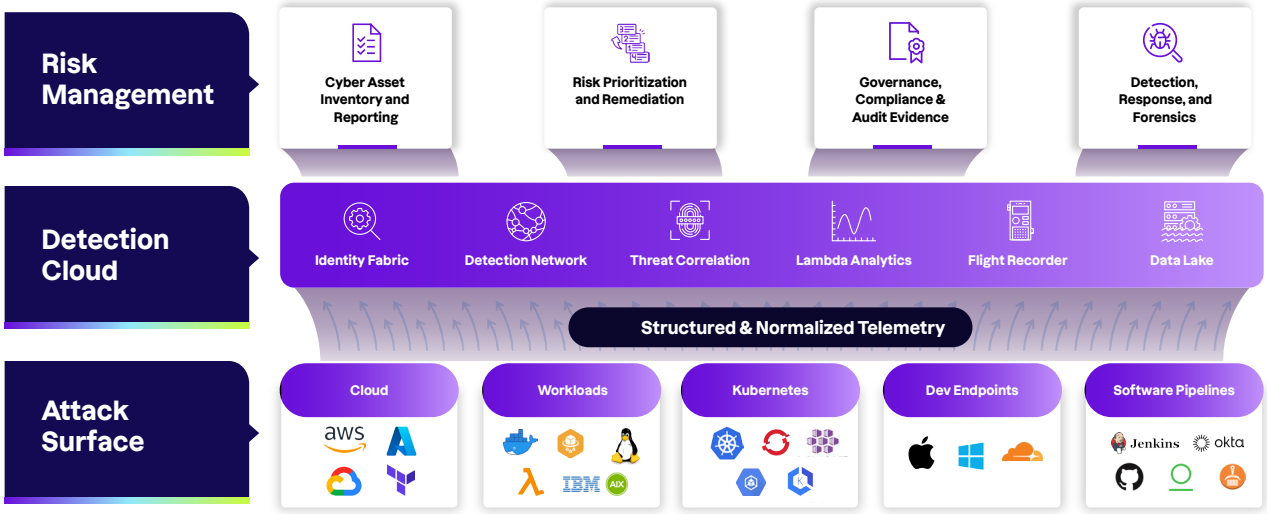
Uptycs' modern architecture normalizes security telemetry close to its collection point, and then streams it into your detection cloud, so you can query your attack surface like a database. No black boxes, no ETL, and no need to put in a support ticket to get new insights.

Uptycs helps you do three things really well:

1. Discover
Tell you what you have so you can protect it.

2. Audit
Identify what's wrong so you can fix it.

3. Secure
Respond to suspicious behavior and take appropriate actions to secure it.



Supercharge your SecOps

Cloud means hybrid cloud

Secures public and private cloud, Kubernetes, rare Linux distros, IBM LinuxONE, developer endpoints, and the software pipeline.

Scales from hundreds to millions of workloads with proven reliability.

Deeper data delivers better insights

Correlates real-time insights with historical data to prioritize the threats and vulnerabilities that matter.

Provides 13-month lookback for compliance and forensic analysis, and 'Ask Uptycs' for on-the-fly investigations.

Remediation requires cloud speed

Slashes MTTR by 50% with real-time ATT&CK-mapped detections and blast radius visibility from laptop to code to cloud.

Choose Uptycs MDR for outsourced detection and response.

Full lifecycle cloud-native application protection

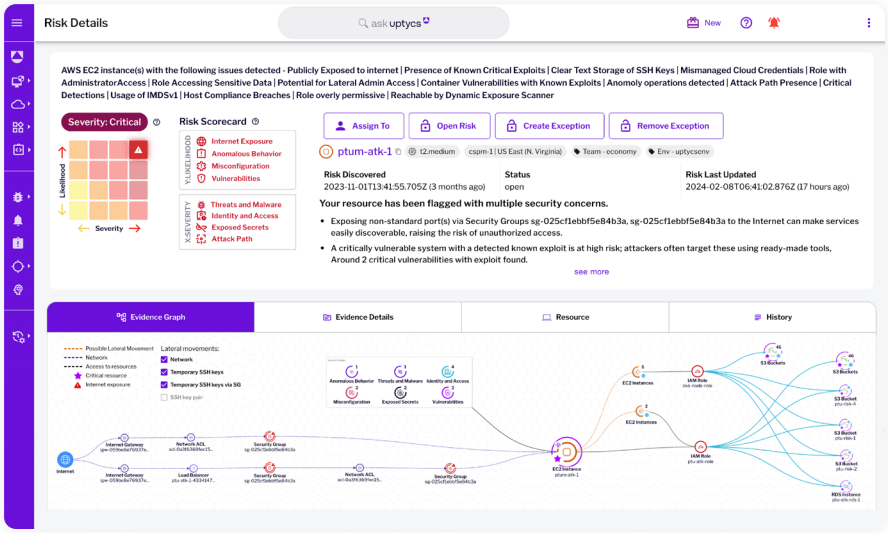
Detect malware or suspicious behavior on developer laptops, identify vulnerabilities early in the build process, verify secure configurations, and continuously monitor in production.

- Prioritize security findings across your hybrid cloud workloads (VMs, containers, clusters, and serverless), and cloud infrastructure (databases, data stores, object storage) through exposure scanning, full attack path analysis, and correlation of security signals
- Detect active threats to workloads with anomaly and behavior-based detections. Identify, prioritize, and fix misconfigurations and policy violations in Infrastructure as Code (IaC)
- Simplify the maintenance of least privilege access and reduce IAM risks with full visibility into policies, users, and roles. Detect identity-specific threats through Identity Threat Detection and Response (ITDR) capabilities
- Get deep support for AWS, Azure, and Google Cloud. Start with instant-on, agentless coverage, then add the Uptycs Sensor for runtime protection, advanced remediation, and forensics
- Gain full visibility into your software development pipeline's posture and apply guardrails throughout your software development lifecycle (SDLC)
- Fully protect your cloud with visibility of all cloud-connected assets, empowering you to understand your blast radius should a developer's laptop be compromised
- Meet compliance mandates with support for CIS benchmarks, HIPAA, ISO 27001, NIST, PCI, and SOC 2 across your cloud infrastructure and workloads running within the cloud

Protect your critical workloads, wherever they run

Replace multiple agents and tools with Uptycs for unified threat detection and response, vulnerability scanning, security hygiene, compliance, cyber asset management, file integrity monitoring (FIM), and ad hoc investigation and threat hunting.

- Enjoy deep support for rare Linux distros, IBM LinuxONE, Linux on Z, IBM Power, AIX, HPC environments, and more
- Enjoy blazing-fast response times with the Uptycs osquery-based agent with eBPF, designed to minimize its memory, CPU, and disk I/O footprint
- Leverage rich security telemetry that goes beyond basic events to include file system files, Augeas lens, DNS lookups, sudoers list, and disk encryption



Go beyond isolated incidents to see the bigger picture. Ensure that every action taken is a step towards a more secure and resilient environment.

About Uptycs

Uptycs is the leading cloud security platform for large hybrid cloud environments, protecting workloads wherever they run, while extending security visibility from development to runtime — all from a single security console, policy framework, and data lake. That's why PayPal, Comcast, and Nutanix rely on Uptycs to secure their mission-critical workloads.

Shift up your cybersecurity. Learn more at Uptycs.com

uptycs