Uptycs
Unified CNAPP and XDR

uptycs

Get faster threat detection and remediation

Instead of having to buy and integrate separate security tools for cloud, containers, servers, and workspaces, Uptycs normalizes your security data close to its collection point, then streams it up into your Uptycs Detection Cloud—your security data lake that's part of your Uptycs subscription.

Now that you control your security data, you can instantly access the correlated insights you care about most and take decisive action.

Secure laptop to cloud from a single UI

Major breaches often start from a developer's laptop. It's critical to be able to detect malware and vulnerabilities on your developers' laptops and reveal any suspicious behavior as they move code in and out of repositories and into the cloud.

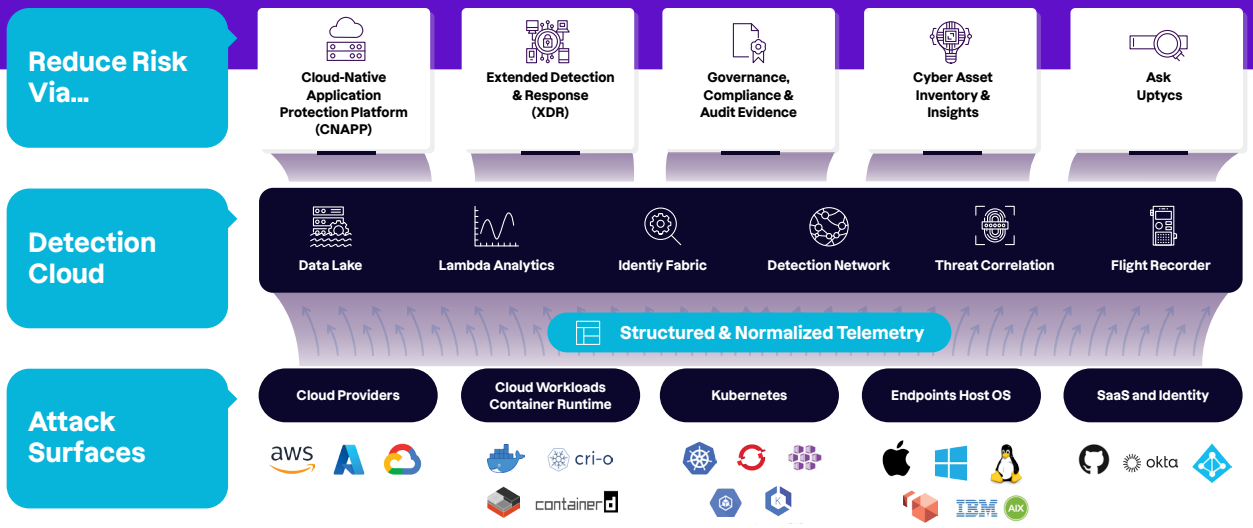
Only Uptycs can give you a cloud security early warning system that identifies and stops threat actors before they can access crown jewel data and services in the cloud.

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.



Shift up your cybersecurity

Go beyond point-in-time visibility

Identify enterprise-wide vulnerabilities, implement preventative measures, and execute remediations.

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

Instantly search across your live infrastructure or investigate historical states going back up to 13 months.

Increase DevSecOps efficiency with customizations

Tag and group assets, tailor threat analysis via detection as code, and create custom dashboards based on your most critical assets or business outcomes.

The result is less noise, and an ability to bring your teams together to reduce the time it takes you to fix a vulnerability, or block or remove a threat.

Don't just detect. Defend.

Investigate and respond to suspicious behavior or an active breach. Dig deeper with remediations down to the host or process level.

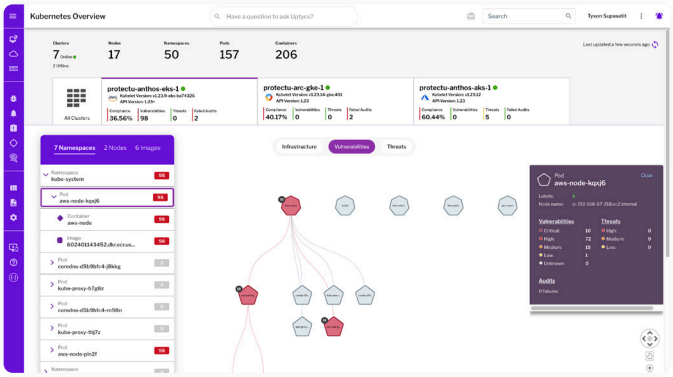
Leverage detection rules mapped to the MITRE ATT&CK framework or use YARA to identify emerging threats and malware at scale.

Choose Uptycs MDR for outsourced detection and response.

Full lifecycle cloud-native application security (CNAPP)

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

- Secure cloud workloads with full attack path visibility across hosts, VMs, containers, Kubernetes clusters, and serverless.
- Identify, prioritize, and fix misconfigurations, policy violations, and compliance issues, and detect active threats with anomaly and behavior-based detections.
- Simplify cloud identity risk and governance, and defend against unauthorized access, misuse, and insider threats.
- Enjoy deep support for AWS, Azure, and Google Cloud. Start with instant-on agentless coverage then add runtime protection for advanced remediation and forensics.

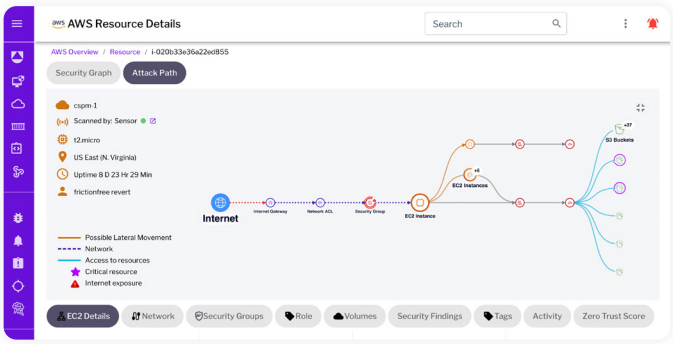


Get deep visibility into K8s and container security, including inventory, compliance, vulnerabilities, and threats.

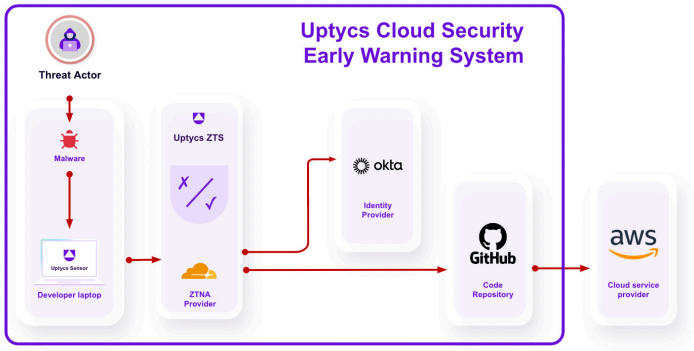
Extended Detection and Response (XDR)

Protect the developer laptops that build your applications to the Linux servers that run them. 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.

- Maintain blazing fast response times with the Uptycs osquery-based agent (with eBPF on Linux), minimizing the memory, CPU, and disk I/O footprint.
- Leverage purposeful, rich security telemetry that goes beyond basic events to include browser extensions, file system files, Augeas lens, DNS lookups, sudoers list, and disk encryption.
- Meet compliance mandates with support for CIS benchmarks, DISA STIG, FedRAMP, HIPAA, ISO 27001, NIST, PCI, and SOC 2.
- Enjoy deep support for both macOS and Windows workspaces, rare Linux distros, IBM AIX, Linux on Z, HPC environments, and more.



Master your threat operations with real-time security graph and attack path analysis and monitoring.



Stop threat actors before they access your cloud. Configure access rules in Cloudflare / ZTNAs based on the Uptycs Zero Trust Score.

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 enterprise–wide security posture. Choose Uptycs MDR for fully managed detection and response.

Shift your cybersecurity up with Uptycs. Visit Uptycs.com

uptycs