uptycs

Solution Brief

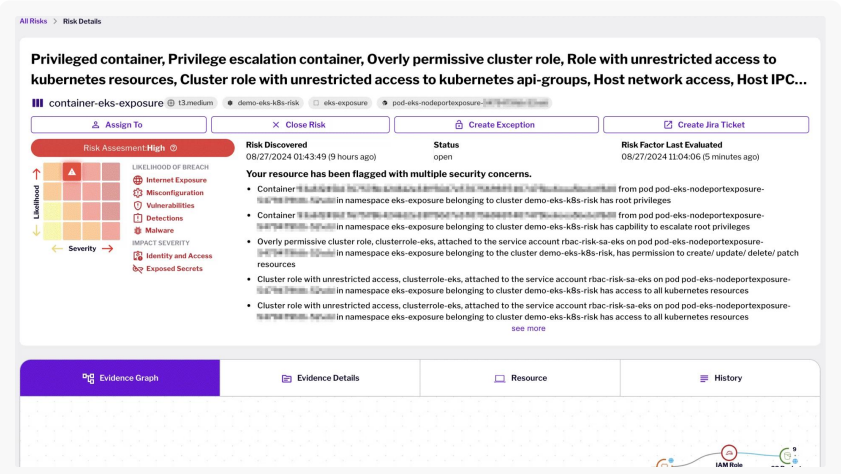
End-to-End Container and Kubernetes Security with Uptycs

Uptycs Container Security spans the entire container lifecycle, from development to runtime, delivering real-time protection, risk assessment, and security guardrails across platforms like Amazon ECS, Fargate, and Kubernetes. Organizations can detect vulnerabilities, prevent container breakouts, and secure workloads without disrupting development.

What We Do

Unified Development to Runtime Protection Across the Container Lifecycle

- **Contextual Risk Assessment:** Pinpoint and prioritize critical container risks by correlating data from security control planes, eBPF runtime activities, and cloud posture context. This enables teams to effectively mitigate vulnerabilities that could impact containerized workloads.
- **Runtime Threat Prevention:** Proactively halt container breakouts and privilege escalation attempts. Employ image provenance analysis and enforce unified admission policies to detect, remediate, and prevent insecure deployments throughout runtime environments.
- **Secure Development Gateways:** Conduct seamless unified scanning from CI/CD pipelines to runtime stages. Deploy secure image artifacts via policy-driven controls, reducing risk without impeding development workflows.



How We Do It

Runtime-First Container Security That Spans The Development Lifecycle

Uptycs combines runtime-first posture management with behavioral detection, response, and prevention throughout the development lifecycle, offering full image provenance and root cause analysis.

Effective Container Security Solutions for Cloud Environments

Gain full visibility across clusters, detect and mitigate risks, and enforce security policies throughout the container lifecycle.

Complete Visibility and Risk Assessment

- **Continuous Scanning:** Monitor hybrid and on-prem environments, including Amazon EKS/ECS, Fargate, and more.
- **Discovery and Prioritization:** Context-rich topology insights, eBPF threat correlation, and risk-based prioritization.

Real-Time Threat Detection and Response

- **Detection & Response:** Detect lateral movements, privilege escalations, and more.
- **Protection Engine: S**top attacks like ransomware and cryptominers.
- **Admission Controls:** Enforce deployment governance via Gatekeeper policies.

Flexible Guardrails for Development Pipelines

- **CI/CD and Registry Scanning:** Integrate security scans before deployment.
- **Image Security Policies**: Block vulnerable images with policy-driven controls.
- **Software Pipeline Posture:** Maintain security across repositories and runtime.

Secure Your Containers

Uptycs empowers security teams with holistic container and Kubernetes protection through advanced threat detection, real-time remediation, and integrated security controls across hybrid and multi-cloud platforms.

Success Stories

"Uptycs simplifies investigations and saves time—about 30% per investigation."

Sean McElroy
CSO Lumin Digital

"I would not want to do Security anywhere without this level of visibility"

Christ Castaldo
CISO Crossbeam

"Uptycs was deployed on a large scale as a key component of our Security posture."

Comcast
Vice President IT Security

Uptycs is the leading cloud security platform for large hybrid cloud environments. We extend security visibility from development to runtime, ensuring consistent protection and compliance across the application infrastructure. That's why enterprises like PayPal, Comcast, and Nutanix rely on Uptycs to secure the development ecosystems they use to build their applications and run their workloads.

uptycs

Secure Everything from Dev to Runtime

See Uptycs in action