

Container Security & Monitoring

FOR CONTAINERS, MACOS,
LINUX, WINDOWS

REAL-TIME, STREAMING &
HISTORICAL QUERYING

INTRUSION DETECTION





SECURE CONFIG

AUDIT & COMPLIANCE

UNIVERSAL, OPEN-SOURCE
OSQUERY AGENT

Overview: Uptycs SaaS Security Analytics Platform

Security & IT professionals juggle dozens of point solutions, each with proprietary agents, yet still field security blind spots created by service gaps for Linux, MacOS, container and cloud workloads. With Uptycs, a SaaS security analytics platform, endpoint and server workload states are ingested via osquery, a single open-source universal agent. Uptycs continuously streams and monitors system activity, transforming it into dashboards, reports and alerts that enable a comprehensive and proactive security posture for use-cases like:

-  Incident Investigation
-  File Integrity Management
-  Audit and Compliance
-  Vulnerability Management
-  Endpoint Detection and Response

Uptycs for containerd, CRI-O, and Docker

Uptycs is a host based monitoring solution that enables complete visibility into what containers are running, where, and which processes. The osquery agent is unique in that it can run on the host, in a VM, or as a privileged container. This means that unlike other container security offerings which run as plugins, Uptycs enables container monitoring in the widest variety of computing environments including those using managed container orchestration services.

Container Security & Monitoring

FOR CONTAINERS, MACOS,
LINUX, WINDOWS

REAL-TIME, STREAMING &
HISTORICAL QUERYING







INTRUSION DETECTION

SECURE CONFIG

AUDIT & COMPLIANCE

UNIVERSAL, OPEN-SOURCE
OSQUERY AGENT

With Uptycs for containers, you're a query away from historical and real-time visibility into several container attributes like:

-  Processes Running
-  Storage Volumes
-  Networks
-  Mounts
-  Ports
-  And More...

Intrusion Detection, Secure Configuration & Compliance for CI/CD

Gain real-time and historical forensic access - even to ephemeral assets - without significant impact to performance or storage.

Real-Time: Query your live infrastructure and customize alerts to monitor for suspicious activity.

Historical: The Uptycs Flight Recorder incorporates proprietary data compression techniques enabling both event and state recreation in a comprehensive and cost-effective manner. The depth and timeframe of detail captured enables more thorough compliance and hardening for CI/CD environments.

