Uptycs

# Cross-Platform File Integrity Monitoring

FOR DOCKER, MACOS, LINUX, WINDOWS

LIVE & HISTORICAL QUERYING

FLEET VISIBILITY

INTRUSION DETECTION & INCIDENT RESPONSE

VULNERABILITY MONITORING

AUDIT & COMPLIANCE

UNIVERSAL, OPEN-SOURCE OSQUERY AGENT

WWW.UPTYCS.COM

## Overview: Uptycs Security Analytics Platform

With Uptycs, gain a consolidated view for monitoring and securing your cloud, on-premises, or hybrid infrastructure by moving from several point solutions to a single, unified view of your security analytics. By pairing the single universal agent, osquery, with a scalable security analytics platform, Uptycs enables a unified view for:

**Fleet Visibility** | **Intrusion Detection** | **Vulnerability Monitoring** | **Audit & Compliance**

Uptycs collects, aggregates and analyzes your endpoint (workstation, workload, container, virtual machine, or server) telemetry, making it available for live and historical query using SQL.

## The Power of Osquery for File Integrity Monitoring

Uptycs for FIM offers a highly scalable way to detect and reconcile changes to files across macOS, Linux, and Windows.

FIM is offered as a precisely configurable module of the Uptycs Osquery-Powered Security Analytics Platform. Uptycs enables security teams to deploy FIM alongside additional components of their global security program, reducing point solution requirements and management overhead. Combined with our dead-simple audit and compliance reporting, you're not only regulatory compliant, you can easily prove it, too. With Uptycs for FIM, you get:

- Full visibility across operating systems
- Continuous, event-based monitoring
- Flexible and precise configuration options
- Highly performant file change analysis
- Context-rich alerting

**Simplified Reconciliation**
Uptycs collects and stores a rich set of endpoint telemetry -- including process ID, process name, and the user account that modified a given file -- providing the context data required to easily resolve and reconcile normal business activity from malicious file modifications.

**Precision & Performance**
Our flexible configuration options enable controls over which files you want to monitor on which systems. Easily tag assets and deploy FIM only to the desired subset of your operating environment. Performance is further optimized by the unique way that Uptycs monitors file changes at the operating system level, reducing computing overhead by avoiding the need to analyze every single file directory.

**Alerting & Integration**
Uptycs offers real-time alerting for modifications made to your monitored files. Alerts provide helpful context by including machine name, Host IP, file path modified, action taken, and more. Alerts can be forwarded to Slack, Pagerduty, email, etc to fit into your existing response workflows. Uptycs also integrates with your SOAR and SIEM solutions.