uptycs

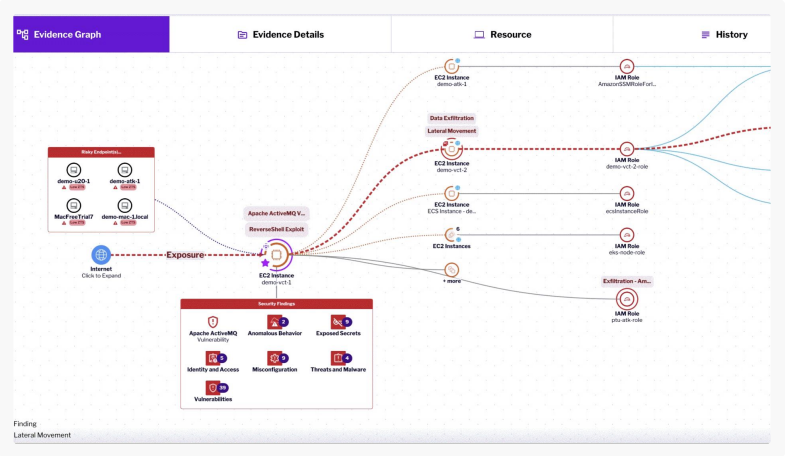
Solution Brief

Secure and Monitor Every Cloud Workload in Real-Time with Uptycs

Securing workloads across hybrid and multi-cloud environments is challenging. Uptycs Cloud Workload Protection (CWPP) simplifies this with unified visibility, proactive risk management, and real-time threat detection. Our platform provides end-to-end protection, from workload discovery and vulnerability assessment to automated remediation and forensic analysis.

Streamlining Cloud Workload Security

As organizations adopt cloud-first strategies, maintaining security and control becomes complex. Uptycs CWPP offers a comprehensive approach to securing hybrid cloud environments through visibility, risk assessment, and threat detection, enabling security teams to safeguard workloads at scale, regardless of the number of assets.



Proactive Cloud Workload Security

From discovery to real-time monitoring, Uptycs CWPP ensures comprehensive protection:

- **Secure Hybrid Cloud Workloads at Scale:** Use agentless discovery to identify vulnerabilities during deployment and lightweight agents for in-depth threat detection across VMs, containers, and serverless functions.
- **Establish Trustworthy Pipelines:** Integrate image scanning and policy enforcement to block untrusted code.
- **Real-Time Attack Prevention:** Stop cryptominers, reverse shells, and lateral movement with automated threat responses.

Core Capabilities of Uptycs CWPP

Fleet-Level Discovery and Visibility

Achieve 360° visibility into cloud assets with scalable monitoring using eBPF technology to track processes, network interactions, and file changes

- **eBPF Asset Insights:** Monitor workload activities for granular fleet visibility.
- **Software Inventory and SBOM:** Maintain compliance and understand software risks.
- **Secrets and Certificates Scanning:** Identify unencrypted secrets and expired certificates.

Runtime Risk and Threat Detection

Continuously identify and mitigate risks using behavioral and anomaly-based detection engines.

- **Behavioral & Anomaly-Based Detection:** Utilize YARA-based signatures for rapid threat identification.
- **Attack Path Analysis:** Trace attacks and highlight misconfigurations and malicious code.

Real-Time Response & Remediation

Quickly mitigate threats with automated detection capabilities.

- **Uptycs Rule Engine:** Enforce policies to block suspicious processes.
- **Bulk Remediation:** Customize actions and enforce policies for large-scale responses.

Threat Hunting and Forensics

Conduct thorough investigations into past threats.

- **File and Process Carving:** Retrieve files and perform retrospective analysis.
- **YARA Scanning:** Discover malware based on unique signatures.

Ideal Solution for Complex Cloud Environments

Uptycs CWPP is designed for organizations looking to enhance security across hybrid and multi-cloud environments. This solution benefits:

- **Enterprises:** Managing mixed workloads with uniform security policies.
- **Teams:** Running containerized applications needing advanced runtime security.
- **Security Teams:** Focused on forensic investigations of sophisticated attacks.

Benefits of Uptycs Cloud Workload Protection

- **Unified Workload Visibility:** Comprehensive visibility across VMs, containers, and clusters.
- **Reduced Risk Exposure:** Prioritize vulnerabilities based on real-time data.
- **Scalable Security Operations:** Protect workloads at scale with high-performance eBPF technology.
- **Enhanced Response and Remediation:** Minimize impact with automated actions and advanced analysis.
- **Simplified Compliance:** Built-in compliance checks for seamless audits.

Unified Protection for Cloud Workloads with Uptycs

Uptycs Cloud Workload Protection delivers a unified solution that scales with your cloud footprint, providing complete visibility and robust protection. Whether securing VMs, containers, or serverless workloads, Uptycs CWPP empowers teams to proactively manage risks and respond to threats in real time, maintaining a strong security posture across all environments.