uptycs

Solution Brief

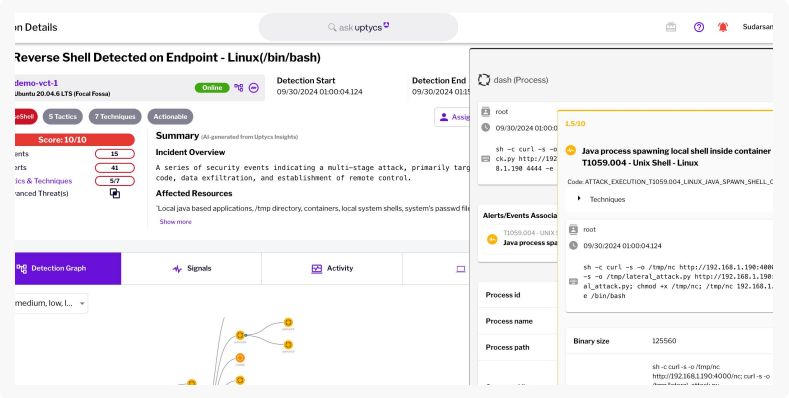
Defend Against Cloud Threats at Cloud Scale with Uptycs

Uptycs Cloud Threat Prevention offers comprehensive, multi-layered security to protect against sophisticated cloud threats. Using advanced analytics, machine learning, and automation, it empowers organizations to detect hidden risks, automate incident response, and safeguard cloud environments from breaches. By continuously analyzing cloud activities, Uptycs ensures emerging threats are swiftly addressed to minimize risk exposure.

What We Do

Detect and prevent threats at cloud speed using advanced analytics

- **Proactive Threat Defense:** Utilizes AI/ML to detect and respond in real time, continuously assessing workloads for malicious patterns to defend against threats.
- **Advanced Threat Hunting:** Proactively seeks hidden threats like APTs and zero-day vulnerabilities through techniques such as anomaly detection and YARA rules for swift response.
- **Automated Threat Response:** Integrates automation for incident response, reducing dwell time and enhancing efficiency through tailored workflows.



How We Do It

Proactive Threat Defense with Uptycs

Uptycs defends cloud environments by analyzing workload behaviors, detecting patterns indicative of attacks, and applying ML/AI techniques to surface zero-day threats. This proactive posture mitigates risk, reduces potential data breaches, and streamlines incident response.

Broad Observability for Threat Detection

- **Context-Aware Detection:** Analyze cloud workloads using eBPF telemetry and cloud logs to detect deviations and alert security teams.
- **Pattern Analysis:** Map adversary tactics, techniques, and procedures (TTPs) to develop robust countermeasures.
- **Breach Prevention:** Prevent data exfiltration, cryptomining, and other malicious activities.
- **Threat Intelligence Augmentation:** Enrich existing intelligence sources for efficient triage of malicious activities.

Contextual Threat Analysis and Hunting

- **Proactive Hunting:** Identify hidden threats, APTs, and zero-day vulnerabilities, enabling faster detection and response to sophisticated attacks before they escalate.
- **Behavioral Analysis:** Gain a deeper understanding of attacker methods through Uptycs' security graph, providing insights to predict and counter future tactics.
- **Incident Response Optimization:** Enhance workflows with in-depth forensics and historical data mapping, ensuring a comprehensive and informed response to security incidents.

Automated Response Capabilities

- **Streamlined Workflow Integration:** Integrate Uptycs with SIEM, SOAR, and other tools to automate response and reduce mean time to remediate (MTTR).
- **Reduced Dwell Time:** Leverage Uptycs threat books to quickly identify and address incidents.
- **Customizable Response Strategies:** Equip IR teams to tailor responses to diverse cloud threats.

Protect Your Cloud

Uptycs equips organizations with robust threat detection, automated response, and proactive strategies to stay resilient against emerging cloud threats. By continuously analyzing cloud activity and integrating advanced threat intelligence, Uptycs helps detect and mitigate risks before they escalate.

With its comprehensive defenses, Uptycs ensures a strong security posture, enabling teams to maintain operational efficiency and confidently protect cloud assets against evolving threats in multi-cloud environments.

Success Stories

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

Comcast
Vice President IT Security

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

Steve Shedlock
Incident Response Team Lead SEI

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