

7 Reasons to Switch from Lacework to Uptycs

Is Lacework the right tool for you? Here's a list of things to consider when deciding if Uptycs is a better fit for your organization than Lacework.

	Uptycs	Lacework
False Positives	Uptycs takes into account diverse factors using a unique algorithm to score and prioritize risks so you only get the alerts that mean something.	Their ML-first approach buries you in alerts while they play catch up building a rules-based engine.
Detection in Real Time	Uptycs analyzes data in real time to give you immediate detections.	Lacework defaults to refreshing data on an hourly basis, leaving gaps open for attacks.
Laptop to Cloud Security	Uptycs covers cloud and critical attacker entry points like developer laptops—the point of access used when hackers breached both LastPass and CircleCI.	Only works for cloud workloads and some on-premises servers—not designed for traditional corporate environments.
Customization & Transparency	Uptycs gives flexible and powerful querying using SQL. Users can see and customize detection logic and allow-lists to prevent false positives.	Opaque detections and limited querying customizability. Users aren't able to see how detections work.
Cloud Threat Detection	Detects malicious use of cloud APIs for enumeration, privilege escalation, and data exfiltration with low false positives.	Relies on deviations from temporal baselines, which results in large numbers of false positive alerts.
MITRE ATT&CK Coverage	Offers robust ATT&CK-mapped detections and pre-built pivot queries to learn things like whether similar suspicious behavior has been seen on other hosts.	Limited context on the who/what/when/where and other potentially related events, leaving you to swivel to another tool.
Insights Across Cloud Accounts	Uptycs identifies risks across your cloud accounts and providers at scale.	Lacework machine learning isn't suited to providing unified insights across accounts.

About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

Shift your cybersecurity up with Uptycs.

