

Uptycs and AWS: GameTech/Real Money Gaming

A unified golden thread to protect your enterprise from laptop to cloud

The GameTech industry—an ecosystem that encompasses everything from console and mobile games to Esports and online betting and gambling—is one of the fastest growing industries in the world, projected to generate a combined \$500+ billion by 2030. However, just as the popularity of online gaming has surged, so has the number of cyberattacks targeting gametech companies and infrastructure. With billions of dollars at stake, cybercriminals see the industry as a veritable goldmine.

GameTech in the Crosshairs: Complexity & Compliance

Gaming companies rely on complex cloud infrastructure, making them vulnerable to attacks.

As online gaming in all of its forms continues to flourish, GameTech security teams must protect an ever-expanding attack surface, from developer laptops to the cloud.

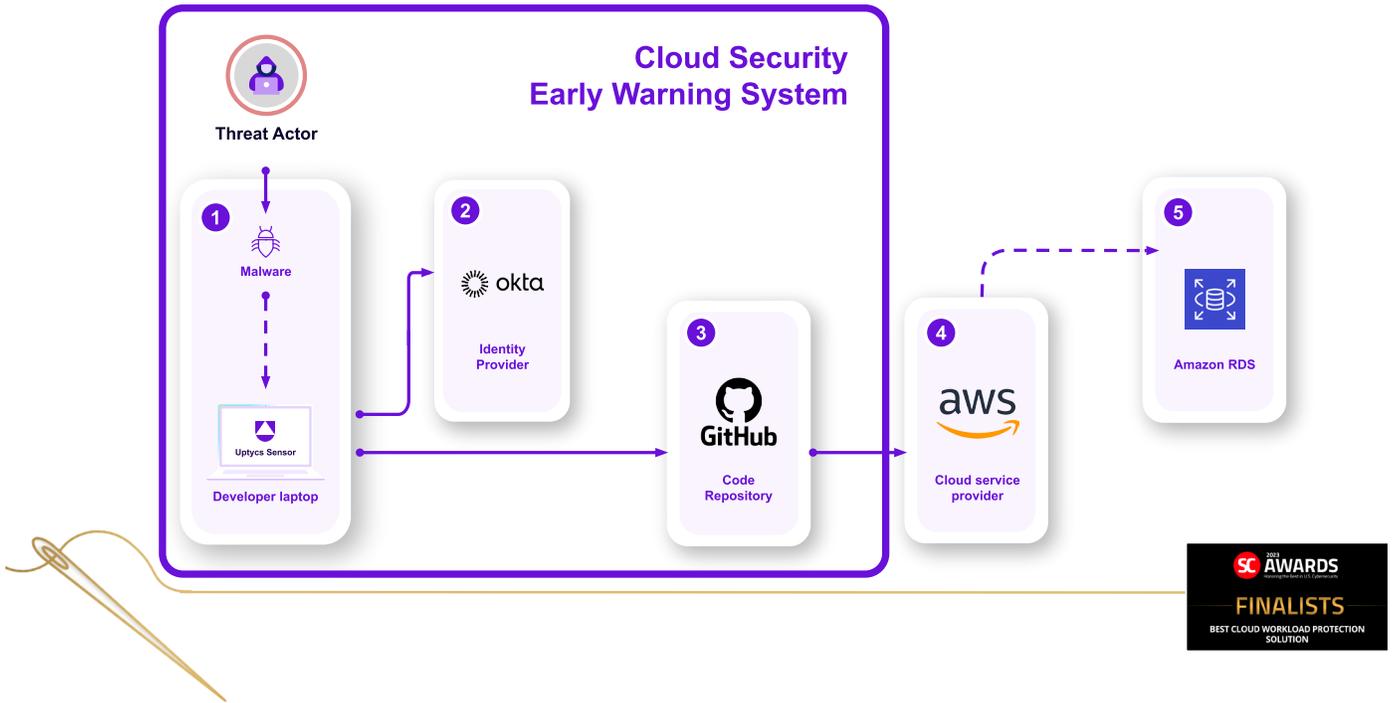
The gaming industry faces unique compliance challenges due to global distribution and varying regulatory requirements. Safeguarding customers' personally identifiable information, including user data and payment details, is of utmost importance.

The Uptycs Golden Thread: From Laptop to Cloud

Modern GameTech publishers need an “early warning system” to identify and stop threat actors before they can access crown jewel data and services in the cloud. Defending this environment requires what we call the Uptycs Unifying Golden Thread to correlate threat activity across developer machines, source code repositories, identity providers, and cloud Infrastructure — all in one unified platform.

Whether you are a single studio or a large publisher, Uptycs can integrate with your native AWS services and developer workspaces to stop threat actors before they ever reach your cloud.

Uptycs' unifying golden thread — from laptop to cloud



Shift up your AWS security

Visualize and prioritize risk for AWS

Go beyond basic security graphs to identify cloud-wide vulnerabilities, implement preventative measures, and execute remediations.

Reduce dwell time with real-time attack path analysis and monitoring.

Take control of your cloud identities

Better protect your AWS resources from unauthorized access, misuse, and insider threats.

Easily spot permission gaps and overly-permissive roles, and apply the principles of least privilege.

Quickly detect and respond to cloud threats

Rapidly identify and respond to malicious use of AWS APIs, privilege escalation, remote code execution, data exfiltration, and more.

Enlighten your team with plain explanations of cloud security events.

MDR: You keep working. We'll keep you secure.

Stay focused on what matters. Uptycs' Managed Detection and Response (MDR) service strengthens your security ops and continuously contains potential threats, so you're free to get things done. Our MDR includes 24x7 monitoring and response with our expert team for on-prem and cloud systems.

Platform or Problem at the Perfect Price Point

Uptycs has you covered if you are looking for a fully managed platform or trying to solve a specific pain point (Audits, Linux or Container Security at Scale, Real-Time YARA Scanning, Mac EDR, etc.). Also, we have a very flexible pricing model that fits all budgets.

Not Just AWS, No Problem

Protect digital assets spread across heterogeneous infrastructure through a platform that covers hybrid cloud, multi-cloud, containers, laptops, and servers from a single platform, UI, and data model.

You can't secure what you can't see. Uptycs helps you identify and prioritize risks across all of your cloud environments—AWS, Azure, and GCP—so you get a complete view of your cloud estate and the answers you need,



Ensure Cloud Compliance

Comply with industry standards by leveraging Uptycs' validation against CIS Benchmarks, PCI-DSS, SOC 2, ISO27001 and the AWS well-architected framework, as well as environment-specific checks, such as NIST or NSA Hardening Guidelines for K8s.

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, delivering a more cohesive security posture across your entire enterprise

Shift up your cybersecurity with Uptycs.

