Enterprise Strategy Group by TechTarget

SHOWCASE

MARCH 2024

Securing Game Tech From Developer Laptops to Gameplay

Melinda Marks, Practice Director, Cybersecurity

Abstract: Video games are evolving rapidly, both with the increasing demand for online gaming experiences and with the technology innovations making it easier for developers to efficiently build and release new games. While cloud services and modernized development processes enable organizations to efficiently produce games for wider audiences, gaming applications and software are often an attractive target for hackers looking for ways to gain access to valuable data or resources. Game tech organizations need to ensure they can secure their development processes—starting with developer endpoints—to protect their applications and enable secure gaming experiences.

Increased Security Risk as Gaming Development Scales

The gaming industry has been growing rapidly, especially considering the recent, increasing demand for interactive forms of entertainment, including console games, mobile games, e-sports, and online betting and gambling. PwC's *Global Entertainment & Media Outlook 2023–2027* report estimates the global gaming industry will be worth $312 billion by 2027.[1]

Cloud services, including Amazon Web Services (AWS), play a key role in this rapid evolution, helping developers and gaming companies maximize their productivity and innovation. By utilizing cloud-native technologies and processes, including continuous integration/continuous delivery (CI/CD) pipelines and Kubernetes for automating deployment, scaling, and management of containerized applications, developers can focus their time and effort on developing feature-rich games instead of building and managing their computing infrastructure.

Cloud-native technologies also enable global participation in game development and gaming, bringing a wider variety of games to market for widespread audiences. However, because the software involves transactions with customers for usernames, passwords, financial transactions, or other valuable items or resources, they can be popular targets for hackers.

Security Needs to Start With Developers

While this is an exciting time for gaming, organizations with game tech need a proactive approach to managing security risk without disrupting development. To gain a competitive advantage, they often accommodate global game development talent, supporting remote workers who may be using multiple devices.

Security teams need an effective way to manage security posture with visibility and controls in place, helping them manage risk across developer machines, source code repositories, cloud identities, and cloud infrastructure for secure development. This is an important part of driving efficiency for security teams to identify and stop threats before an attacker can access crown-jewel data and services in the cloud.

[1] Source: PwC, "Perspectives from the Global Entertainment & Media Outlook 2023–2027," June 2023.

This Enterprise Strategy Group Showcase was commissioned by Amazon Web Services and is distributed under license from TechTarget, Inc.

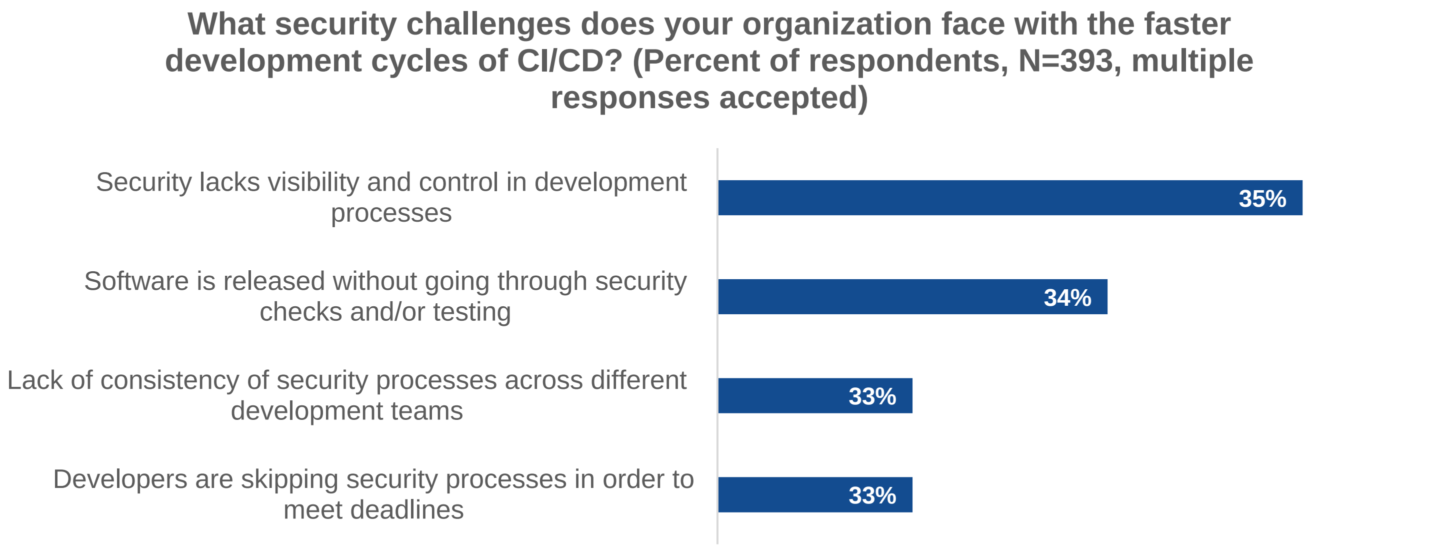
Optimizing Operational Efficiency for Cloud Threat Detection and Response

Cloud gaming development enables a faster cadence of releases and updates, creating challenges for application security teams responsible for protecting customer and company data. Recent research by TechTarget's Enterprise Strategy Group on cloud threat detection and response (TDR) showed that organizations need to optimize their security operational efficiency for effective TDR that can keep up with the faster development cycles associated with cloud services.

Organizations with game tech need to safeguard customers' personally identifiable information, including user data and payment details, as consumers download, buy, and use games.

As shown in Figure 1, the top challenges resulting from faster release cycles include lack of visibility and control in development processes (cited by 35% of respondents), software being released without going through security checks and testing (34%), a lack of security process consistency (33%), and developers skipping security processes to meet deadlines (33%).[2]

Figure 1. Top Security Challenges Associated With Faster Development Cycles



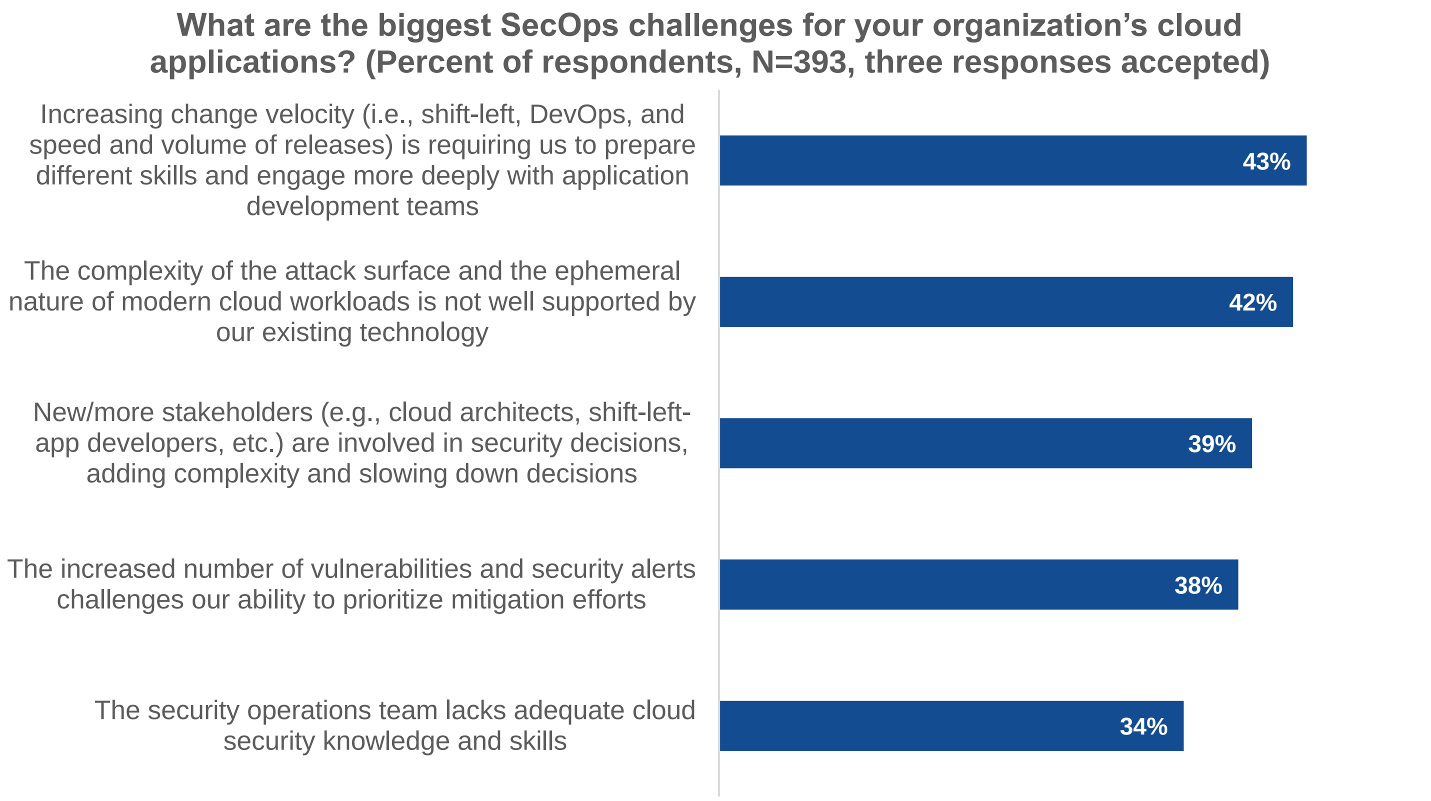
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

These issues increase the attack surface area and threat vectors, creating challenges for security teams that need to protect gaming applications running in the cloud.

As shown in Figure 2, the research also indicates that the biggest security operations (SecOps) challenges result from the higher velocity and volume of releases (cited by 43% of respondents), the added complexity of the attack surface combined with the ephemeral nature of workloads (42%), collaboration with new and greater numbers of stakeholders (39%), the increase in the number of vulnerabilities and alerts (38%), as well as lacking cloud security knowledge and skills (34%).[3]

[2] Source: Enterprise Strategy Group Research Report, *Cloud Detection and Response*, December 2023.
[3] Source: Ibid.

Figure 2. Biggest SecOps Challenges for Cloud Applications



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The gaming industry also faces unique compliance challenges due to global distribution and varying regulatory requirements. Organizations with game tech need to safeguard customers' personally identifiable information, including user data and payment details, as consumers download, buy, and use games. So, security teams need an effective solution to address these challenges while supporting faster software development.

Introducing Uptycs With AWS for Game Tech

Uptycs enables secure gaming by giving game tech organizations a centralized platform with a unified data model to drive secure game development and security operations efficiency. It enables the definition of posture controls for secure game development, while providing the visibility needed for applications across cloud environments, spanning both the software development lifecycle (SDLC) and the runtime environments.

For example, Uptycs helps gaming companies ensure that their development teams and business units follow the right processes with end-to-end security controls across their software pipelines, answering key questions including:

- Did the developer image go through the security controls across the SDLC? If not, what was missed?
- Was the image deployed from a trusted registry?
- Did the developer bypass/not use the enterprise registry and instead deploy from registries such as DockerHub?

Integrated with AWS services and developer endpoints, Uptycs helps game tech organizations secure their development ecosystems through runtime and ensure they can respond quickly to threats and attacks. Uptycs provides:

- **Scanning of images across CI and registries** for vulnerabilities, malware, and secrets, correlating findings across the SDLC. This helps security teams rapidly detect and respond to vulnerabilities by identifying which parts of their SDLC, CI registry, and runtime applications are affected.
- **Risk visualization and prioritization.** For faster risk mitigation and reduced dwell time, it features vulnerability identification and implementation of preventative measures as well as attack path analysis and monitoring.
- **Control of cloud identities.** To protect AWS resources from unauthorized access, misuse, and insider threats, it identifies permission gaps and overly permissive roles and applies least privilege principles.
- **Rapid cloud threat detection and response.** This includes faster response to malicious use of APIs, privilege escalation, remote code execution, and data exfiltration, accompanied by clear explanations of security events.
- **Compliance with industry standards.** Uptycs offers validation against Center for Internet Security benchmarks, PCI DSS, SOC 2, ISO 27001, and the AWS well-architected framework. It also offers environment-specific checks, such as NIST or National Security Agency hardening guidelines.

This is all within a platform that can reliably scale from hundreds to millions of workloads. In addition, Uptycs offers managed detection and response services with 24/7 monitoring and guidance from its expert team for on-premises and cloud systems.

Conclusion

While the global gaming market is booming, online games can be an attractive target for hackers to exploit to acquire valuable information. Therefore, it's important for organizations to proactively take measures for secure development and to safeguard their customers' gameplay.

Organizations should consider Uptycs for a unified security solution integrated with AWS services and developer endpoints. Because its capabilities span from endpoints, where the code is developed, to the cloud, where the applications run, using Uptycs with AWS for game tech provides comprehensive visibility for threat detection, along with capabilities to expedite investigation and response. With the ability to scale, Uptycs can help game tech companies support business growth with secure development, while enabling them to respond quickly and effectively to threats and attacks.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
🖥 www.esg-global.com