

Waratek Appoints Apostolos Giannakidis as Chief Technology Officer

Veteran runtime security architect to lead Waratek's technology strategy as enterprises confront a new wave of AI-generated code vulnerabilities and exploits

DUBLIN, IRELAND, June 15, 2026 /EINPresswire.com/ -- [Waratek](#), the leader in runtime application security, today announced the appointment of Apostolos Giannakidis as Chief Technology Officer. In his new role, Giannakidis will lead Waratek's technology vision, product strategy, and security research as the company expands its runtime protection platform to address the surge in software vulnerabilities and exploits introduced by AI-generated code.



Apostolos Giannakidis is Waratek's new CTO.



Waratek logo

WARATEK

A former AppSec Vice President at JPMorgan Chase and a Principal Product Security Engineer at Microsoft, Giannakidis is a globally recognized thought leader in the AppSec community with more than two decades of technical expertise building and researching innovative technologies that protect production applications from the inside. He has authored security research and disclosures on the JVM and enterprise runtime environments, contributed to the body of work on runtime instrumentation and virtualization-based protection, and is a frequent speaker at international security conferences on application security, vulnerability exploitation, threat modeling and defensive runtime techniques.

His deep engineering background — spanning runtime instrumentation, bytecode-level security controls, virtual patching, and the detection and prevention of memory- and injection-class exploits — directly maps to the threats now emerging from AI-assisted software development. As enterprises ship code at unprecedented velocity using generative AI tools, vulnerabilities are being introduced faster than traditional scanners, SAST/DAST testing, and human review can catch them. Waratek's runtime approach neutralizes those vulnerabilities where they actually execute, without requiring code changes.



AI is collapsing the time between a vulnerability being written and a vulnerability being exploited. Runtime security is now more important than ever before."

*Apostolos Giannakidis,
Waratek CTO*

Waratek's platform applies security policy directly inside the application runtime, blocking exploits — including zero-days and AI-introduced flaws — at the point of execution. With Giannakidis at the helm of technology, Waratek will accelerate investment in runtime defenses purpose-built for an environment in which:

- AI coding assistants are dramatically increasing the volume of insecure code reaching production.
- Attackers are using AI to discover and weaponize vulnerabilities at machine speed.

- Legacy perimeter and signature-based security tooling cannot keep pace with the rate of new zero-day exploits.
- Compliance and regulatory pressure is intensifying around demonstrable, in-application controls.

Giannakidis will work closely with Waratek's engineering, research, and customer-facing teams to further extend the company's runtime protection capabilities across modern Java, .NET, and emerging runtimes, and to deepen integrations with the platforms enterprises rely on to deliver software securely at AI-era speed.

Leadership commentary

"We aren't just building security; we're architecting the future of AI protection," said Doug Ennis, Executive Chairman and CEO, Waratek. "The team is thrilled to have Apostolos on board to lead our technical strategy as we solidify our position as the premier Runtime AI Defender platform. We're moving fast, and with his expertise, we're built to win."

"AI is collapsing the time between a vulnerability being written and a vulnerability being exploited," explained Giannakidis. "Traditional AppSec defenses are no longer sufficient to protect against these dynamic, non-deterministic AI threats. Runtime security is now more important than ever before."

"Runtime is where attacks actually happen, and it's where we can apply context-aware defenses. It is the critical, foundational security control that allows organizations to safely adopt AI and proactively neutralize AI-generated zero-day exploits. I am thrilled to join Doug and lead Waratek's engineering and product teams as we deliver the next generation of intelligent RASP and IAST solutions."

About Waratek

With headquarters in Dublin and Chicago, Waratek provides runtime application security that protects enterprise software from exploits at the point of execution — including vulnerabilities introduced by AI-generated code. Waratek's platform applies security controls directly inside the application runtime, eliminating entire classes of exploits without code changes, signatures, or intrusive agents. The world's most security-conscious organizations rely on Waratek to defend mission-critical applications and meet evolving compliance requirements. Learn more at www.waratek.com.

Doug Ennis

Waratek

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/919771624>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.