Research Addresses the Threats of AI-Driven, Multi-System Attack Chains

Independent White Paper states Validian Runtime Security "directly limits the effectiveness of AI-driven, multi-system attack chains"

OTTAWA, ON, CANADA, May 7, 2026 /EINPresswire.com/ -- Validian Corporation has announced its unique ability to directly limit the effectiveness of AI-driven cyber attacks, including AI-driven multi-system attack chains.

> “Validian Runtime Security directly limits the effectiveness of AI-driven, multi-system attack chains.”
>
> *Rafael Gorgal*
>
> (RSAC, March 2026)

There have been two recent, massive paradigm shifts in the cyber-security landscape:

1. The newly recognized category of Runtime Security

2. A new class of AI-driven offensive capabilities highlighted by Claude Mythos AI that is raising concern across government and commercial sectors (April 2026)

The March 2026 RSAC conference in San Francisco formally established Runtime Security as a critical discipline for protecting applications and data after access—particularly in the face of AI-enhanced attackers and malware.

“Validian is the technology leader in Runtime Security because Validian invented it,” said Bruce Benn, president of Validian Corporation. “While the industry is only now shifting protection into the runtime, Validian has been an early pioneer in refining and advancing this approach.”

Traditional security measures focus on controlling access to networks and applications but do not protect application sessions or data once access has been granted, even when augmented with artificial intelligence — as has been evidenced by countless successful application and data breaches with significant economic damage. These measures include firewalls, VPNs, SSL-VPNs, intrusion and threat detection systems, MFA, identity and access management, zero trust network access (ZTNA), and cloud-native access points (CNAP).

Runtime Security is now recognized as a distinct and essential domain. It does not replace existing approaches but instead extends them—moving beyond perimeter and network

defenses and delivering protection that cannot be achieved through traditional methods alone.

At the same time, a new wave of AI-driven offensive capabilities—exemplified by Mythos AI—represents a significant shift in how vulnerabilities are identified, weaponized, and exploited.

Conventional defenses are not sufficient to counter these rapidly evolving threats. The scale and speed at which advanced AI systems can uncover weaknesses in production code have prompted governments and enterprises to form industry-wide coalitions focused on continuously identifying, prioritizing, and remediating these emerging risks.

"But "continuously remediating" means continuously tracking, patching and fixing," commented Bruce Benn, president of Validian Corporation. "As other AI morphs into these new AI-driven offensive cybersecurity capabilities, and falls into the hands of malicious State Actors and other attackers, this "wave of vulnerabilities" will become a relentless tidal wave, with a multitude of new vulnerabilities identified and weaponized and with speed like never before, which will overload and overwhelm vulnerability patching systems."

"This is going to create a defender backlog problem, where remediation capacity cannot match discovery volume" says a recently published white paper titled "Executive Briefing: Mitigating Mythos-Class Cyber Threats " authored by Rafael Gorgal, a highly respected independent cybersecurity expert, which then opines that:

Validian Runtime Security "directly limits the effectiveness of AI-driven, multi-system attack chains".

The white paper is available at https://s4-sa.com/english/f/executive-briefing-mitigating-mythos-class-cyber-threats.

About Validian Corporation

Validian is the technology leader in Runtime Security because Validian invented Runtime Security. Validian Runtime Security is runtime-native, data-centric security —and it’s genuinely different from how most cybersecurity is implemented today. As security moves into the runtime, ValidianProtect leads by securing the applications and the data itself—delivering continuous protection and control at the moment it matters most, when cyber attacks successfully breach systems, networks and devices - when the networks and devices are otherwise compromised by malware, attackers, malicious insiders and zero-day vulnerabilities - and even by AI-driven multi-system attack chains.

Visit www.Validian.com for more information on Validian's Runtime Security solutions.

Safe Harbor Statement

Investors should carefully consider the information contained in this news release before making an investment in the shares of the company. Information contained in this news release contains "forward looking statements", which can be identified by the use of forward-looking terminology such as "believes," expects," "may," "should," or "anticipates" or negative thereof or given that the future results covered by such forward -looking statements will be achieved. The preceding matters constitute cautionary statements identifying important factors with respect to such forward-looking statements, including certain risks and uncertainties that could cause actual results to vary materially from the future statements. Other factors could also cause actual results to vary materially from the future results covered in such forward-looking statements.

Bruce Benn
Validian Corporation
email us here
