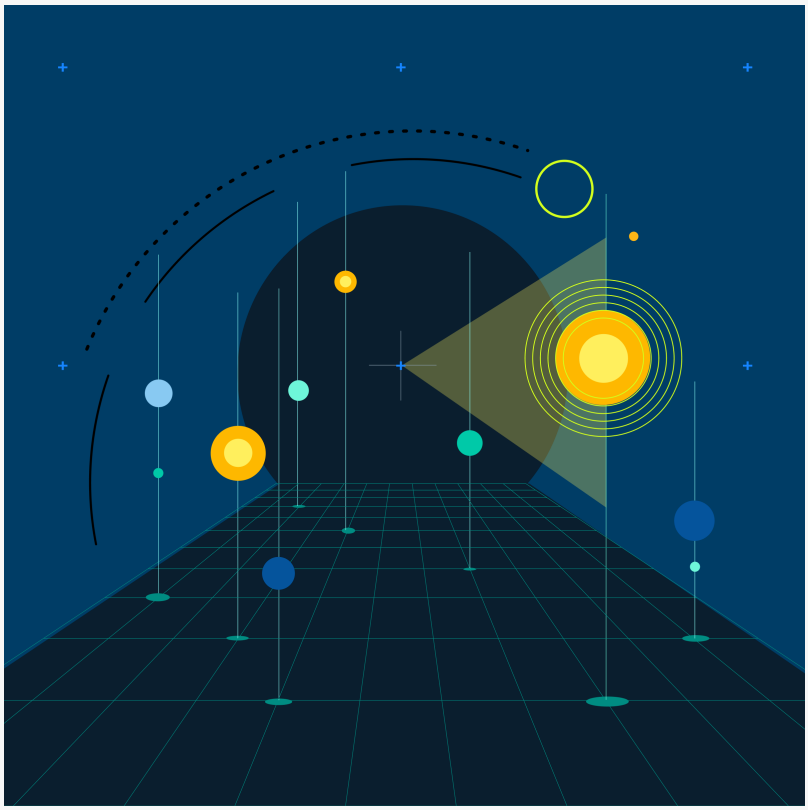
New Report Reveals a Widening Gap Between the Speed of AI-Driven Bot Threats and the Pace of Organizational Response

Survey of 300 Enterprise Leaders Exposes a Critical Governance Gap as AI-Driven Bots Become a Preferred Attack Vector



Hydrolix Bot Insights

PORTLAND, OR, UNITED STATES, June 3, 2026 /EINPresswire.com/ -- Today's cyberattackers are no longer breaking into enterprise systems. They're blending in. Powered by AI, modern bots mimic legitimate users with increasing precision, making identity the primary battleground in a threat landscape that is evolving faster than most organizations can track. Despite this shift, 45% of enterprises update their bot detection rules only weekly. A new research report from TechStudio™, an Energize Marketing® company, sponsored by Hydrolix, exposes just how wide that gap has become.

AI Bots in 2026: Risk, Readiness, and Governance draws on a survey of 300 enterprise leaders across North America, spanning IT security, engineering, infrastructure, site reliability engineering (SRE), IT operations, and bot management.

The report shows that the nature of AI-enabled attacks has fundamentally shifted. Rather than forcing entry through perimeter vulnerabilities, adversaries are using AI to automate reconnaissance, optimize targeting, and deploy bots that operate inside the behavioral envelope of legitimate users. Scraping operations have become more precise and persistent, enabling attackers to extract sensitive data while evading traditional detection mechanisms. Credential-based attacks (74%), DDoS attacks (51%), and AI-driven scraping (40%) remain the top threat vectors but their speed, scale, and sophistication have been transformed.

The economics of attack have shifted, too. AI has dramatically lowered the cost of executing an attack while increasing the volume, velocity, and likelihood of success. Yet the defensive posture of most enterprises has not kept pace: only 25% of organizations update detection rules continuously, while 45% do so only weekly.

"Zero trust has always been about verifying identity before granting access, and that principle doesn't change just because the actor is a bot," said Dr. Chase Cunningham (Dr. Zero Trust), Principal Analyst and Cybersecurity Strategist. "If anything, AI-driven bots demand even more rigorous identity verification than humans do, because they're faster, more persistent, and harder to distinguish from legitimate traffic. Organizations need to stop treating bots as a traffic category and start treating them as identity-bearing actors that require the same authentication, authorization, and continuous verification as any human user."

Simon Ouderkirk, VP of Product, Hydrolix

Hydrolix.io

Compounding the identity problem is an inability to classify intent. One in four enterprises (23%) cannot distinguish malicious bots from legitimate ones, a critical weakness when modern threats are engineered specifically to exploit that ambiguity. The report also shows that organizations increasingly rely on bots for uptime monitoring (51%) and SEO (48%). This means there can be a significant overlap between intended beneficial bot traffic and external threat traffic. Smart attackers know this and in some cases, actively design for it.

Nearly half of enterprises (43%) report that bots now account for 10–25% of their total traffic, a number lower than many industry reports, which only validates that even those who sit closest to managing bot traffic can't see all of it. Visibility and classification are no longer optional. They are the difference between an effective defense and a false sense of security.

"The most dangerous space in bot management is the gray area between beneficial and malicious automation," said Simon Ouderkirk, VP of Product, Hydrolix. "Legitimate bots and agents, and adversarial ones now look nearly identical in traffic logs. Attackers are deliberately

> The most dangerous space in bot management is the gray area between beneficial and malicious automation."
>
> *Simon Ouderkirk, VP of Product, Hydrolix*

exploiting that ambiguity, operating inside the behavioral envelope of trusted systems. Until organizations move beyond detection and invest in real classification, attribution, and governance, that gray area will keep getting larger and harder to defend."

The survey reveals a 56-point gap between perceived confidence and actual strategic maturity. Nearly four in five respondents (79%) believe they can detect bot activity, yet only 23% have proactive, governance-driven programs in place. Under half (44%) rely on reactive approaches, and a third depend on default CDN or WAF protections as their primary defense. The result is a defensive posture built on overconfidence. Only 33% report that their detection tools successfully blocked more than 50% of AI bot traffic in the last 12 months.

The consequences of this readiness gap are no longer confined to the security operations center. More than half of respondents (54%) expect AI bots to degrade customer experience within the next 12 months, and a third anticipate increased sensitive data exposure. Modern bots create subtle, persistent friction across the customer journey, including slower load times, disrupted transactions, and degraded personalization that erodes user satisfaction and revenue.

This elevation of bot management from a technical problem to a business-critical one reflects the scale at which these organizations operate. Nearly half manage between one million and 10 million monthly web visits, and more than 80% generate over $500 million in annual revenue. At that scale, unmanaged bot activity is not a tolerable risk. It is a material one.

The AI Bots in 2026: Risk, Readiness, and Governance report is now available here.

About Hydrolix: Hydrolix is a Portland, Oregon-based real-time data platform for operational intelligence at internet scale. Founded in 2018, Hydrolix delivers real-time analytics that surface insights in seconds across globally distributed data —from servers and microservices to AI agents—while enabling years of retention through next-generation compression. Trusted by Fox, ABC, and Paramount for mission-critical live events, Hydrolix has grown to over 650 customers globally in 24 months.

About TechStudio / Energize Marketing: TechStudio™ is a research division of Energize Marketing®, specializing in primary research for enterprise technology markets. The AI Bots in 2026 study was conducted in March 2026 across 300 enterprise leaders in the United States, with a 95% confidence level and ±5.6% margin of error.

MEDIA CONTACT(s):

Abby Ross
Head of Corporate Communications, Hydrolix
abby@hydrolix.io

Stacey Barker
Jade Umbrella PR
+1 323-833-8358
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
X
