

Can AI Defend Itself Against Attack?

The new frontier of cyber resilience is not firewalls—it’s AI.

Swipe for insights →

THE DATA

28

Zero-Day Vulnerabilities

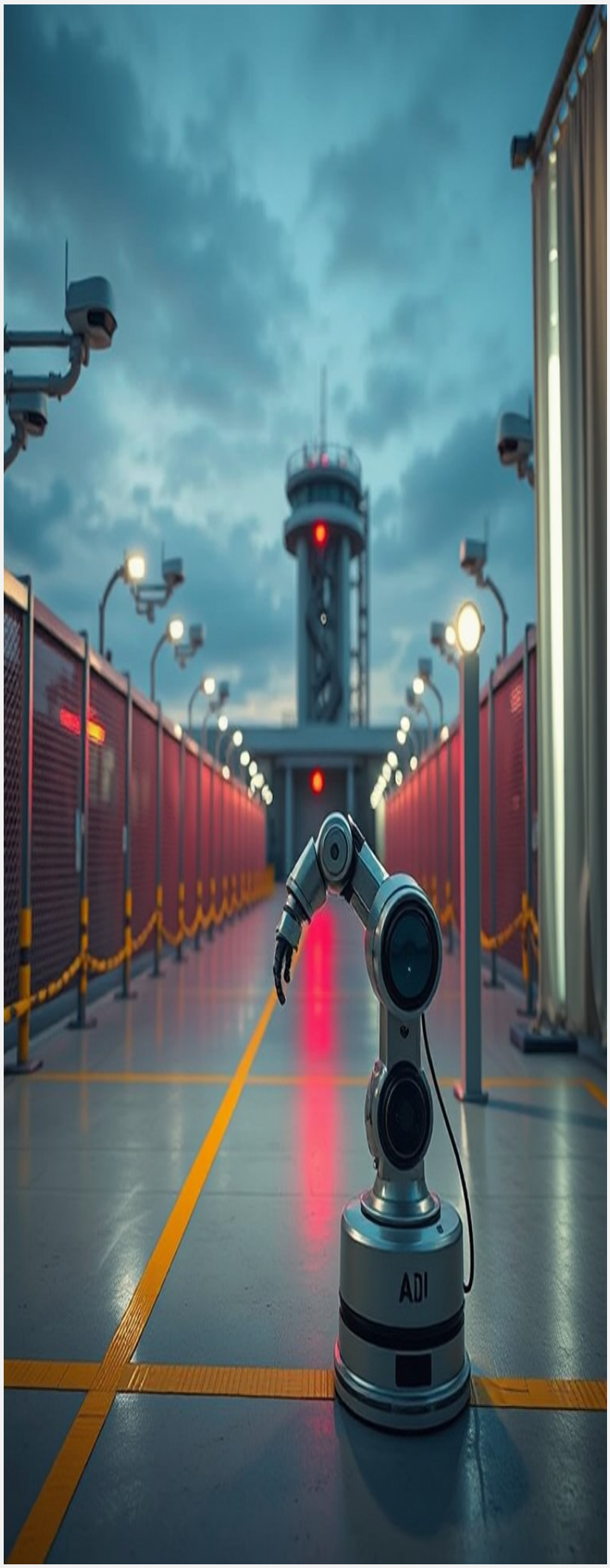
This surge in undetected vulnerabilities reveals a systemic gap in AI-driven physical systems. As robotics become embedded in infrastructure, supply chains, and public services, unpatched flaws could enable large-scale disruptions. The speed of discovery outpaces the ability to secure systems, exposing a critical vulnerability in the AI safety lifecycle.

Source: IEEE Spectrum · Published November 16, 2026
https://spectrum.ieee.org/zero-day-robotics-vulnerabilities-vicone-security

01

AI Security Is a Race Against Time

The current model of post-deployment patching is obsolete. Real-time, AI-powered monitoring and self-healing systems must be baked into the architecture from the start, not retrofitted after compromise.



02

Ethics Must Precede Deployment

Without mandatory risk assessments and independent audits, even the most advanced AI defense can become a vector of attack. The most dangerous AI isn’t the one that fails—it’s the one that appears secure but is engineered to be compromised.

George Arnold Alexander III, MPA

Partner, ALEX Companies
Associate Broker, Alexander Tiffany Southwest, LLC
Licensed Broker in TX, CO, NC, AL

george@alex.realestate · +1 713.918.9951

ALEX

ALEX Intelligence
deep intelligence

ALEX Real Estate
genius real estate

ALEX Advisory
uncontested strategy

ALEX Cares
purposeful philanthropy