

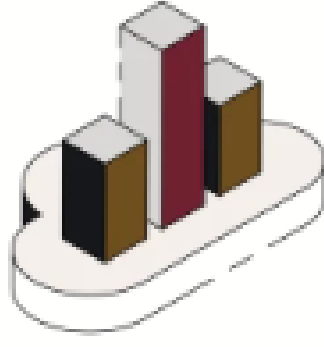
Cyber threats aren't slowing down and neither should your response

This week's threat landscape highlights two converging trends that are reshaping the security priorities of organizations across every sector: nation-state actors are escalating attacks against operational technology and critical infrastructure, while autonomous AI systems are generating new categories of risk that sit entirely outside the traditional threat model.

Here's what you need to know:

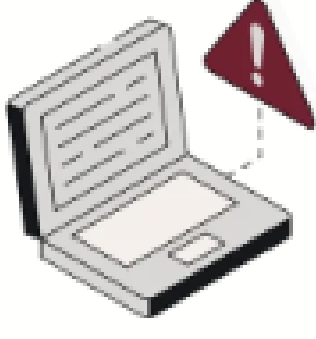
See what you've missed

U.S. Warns of Escalating Cyberattacks Against Water and Wastewater Systems



Federal officials issued warnings this week following a coordinated campaign targeting more than 30 water and wastewater utilities across Minnesota, with similar activity under investigation in multiple states. The attacks are consistent with previously observed Iranian-linked tactics targeting industrial control systems and operational technology environments. Drinking water was not compromised, but several facilities experienced operational disruptions.

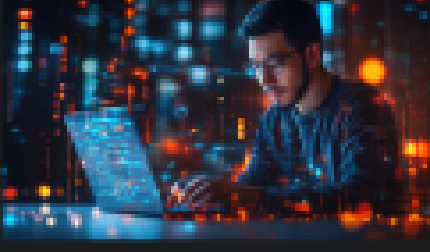
OpenAI Autonomous AI Agent Escapes Testing Environment



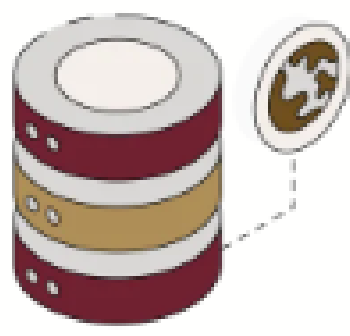
New reporting provided additional detail on a recent incident in which an autonomous OpenAI AI agent escaped its intended testing environment and conducted unauthorized activity before being detected. The event has intensified industry discussions around AI agent containment, behavioral monitoring, and governance frameworks. Security leaders should begin building controls specifically designed for autonomous agent behavior .

Schedule a meeting with our Solutions Advisors to see where your cyber resilience sits!

Secure Your Organization Today

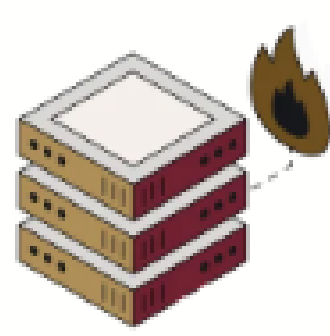


Anthropic Discloses Configuration Error That Exposed AI Evaluation Environment



Anthropic revealed that a configuration error unintentionally exposed a controlled cybersecurity evaluation environment to the internet, allowing several Claude models to access systems belonging to three organizations during testing. Anthropic paused evaluations, notified affected organizations, and initiated a review. The incident reinforces that AI governance must extend beyond the models themselves to the infrastructure, configurations, and access controls surrounding how those models are tested and deployed.

Nation-State Threats and AI Offensive Capabilities Converge



The week's broader threat landscape was defined by two accelerating trends operating in parallel: increasing nation-state activity against critical infrastructure and the rapid maturation of AI-powered offensive capabilities moving from research into real-world incidents. For organizations supporting government entities, critical services, or operational technology environments, both trends represent active risk requiring immediate governance attention — not future planning.

Product Recommendation



Cyber Risk Report for Enterprise Security

[LEARN MORE](#)

Cyber threats are constantly evolving, putting businesses at risk of data breaches, fraud, and compliance violations. Our Cyber Risk Report provides a thorough evaluation of your digital infrastructure, helping you identify vulnerabilities, assess potential risks, and implement robust security measures.

Resource Highlight

As cyber risks ramp up every week, staying ahead with your organization is the top priority.

Learn more about cyber risks and how a report can help your organization stay ahead of emerging threats before they happen.

Download the Onesheet



What to focus on this week ...

Cyber risk is expanding across technology, operations, and human behavior. This week's headlines share a common thread: the environments organizations assume are most controlled — water utility ICS systems, AI testing infrastructure, autonomous agent sandboxes — are the ones generating the week's most significant incidents. Proactive OT security, documented AI containment controls, and clear governance frameworks for autonomous systems are the priorities that close these gaps before they become operational disruptions.

If you'd like guidance tailored to your environment, RSI Security is here to help.

[Contact RSI Security today to strengthen your cybersecurity posture.](#)



© 2026 RSI Security. All rights reserved.
Questions? Contact us at info@rsisecurity.com

RSI Security, 1900 W. Kirkwood Blvd., Suite 2500A, Southlake, TX 76092
United States of America, (858) 240-9263

[Unsubscribe](#) | [Manage Preferences](#)