Application: 6291

Adversa AI

Page: General Information

Provide information about the company to be considered for the award. If you will be nominating an individual, specify the nominee's employer.

Name of Organization/Company

Adversa AI

[redacted]

Additional Contacts

I would also like to have others receive emails about the disposition of our entries.

Page: Entry Information

Entry Title

Adversa AI

Category

E04. Technology Breakthrough of the Year - Artificial Intelligence

Technology Breakthrough of the Year Submission Format

Written Answers

a. Briefly describe the organization that achieved the nominated technology breakthrough: its history and past performance (up to 200 words). Required

Adversa AI is a AI security startup pioneering Security and Safety testing for AI by experts in cybersecurity, machine learning, and neuroscience, the company recognized early that the rise of GenAI and Agentic AI would introduce a new class of threats—ones that traditional cybersecurity tools could not address.

Since its inception, Adversa AI has focused exclusively on securing AI systems themselves, not just the infrastructure around them. The company's core product, the Adversa AI Red Teaming Platform, is the world's first patented, end-to-end solution for stress-testing AI behavior under adversarial conditions. Unlike conventional approaches that secure access or networks, Adversa AI simulates how AI models respond to real-world threats like prompt injections, jailbreaks, and behavioral manipulation.

The company has built the world's largest repository of AI attack scenarios and technnology to automatically invent new ones and works with Fortune 500 enterprises, Big 4 consulting firms, and AI-native startups across the U.S., Europe, MENA, and Asia. Its work is recognized by Gartner, IDC, Wavestone, and over 20 global awards. The team actively contributes to global standards at NIST, OWASP, CoSAI, and IEEE.

Adversa AI is not just building tools—it's shaping the future of secure and responsible AI.

b. Outline the nominated technology breakthrough. Be sure to describe it in terms that someone with limited knowledge of the technology can understand and appreciate (up to 250 words). Required

Adversa AI has achieved several major milestones in product development, market validation, and global influence. In early 2023, the company launched its fully automated Adversa AI Red Teaming Platform, designed to secure GenAI, and later became world's first to test Agentic AI systems by simulating real-world attacks. The platform uses AI Hacking Agents to detect known and unknown vulnerabilities across the full AI lifecycle—including adversarial input detection, prompt injection testing, jailbreak prevention, and compliance validation.

The technology behind the platform demonstrated that within minutes of public release, the platform uncovered critical flaws in leading AI models from OpenAI, DeepSeek, and X.AI, and others, validating its real-world value. Since launch, it has been adopted by tier-1 U.S. banks, Big 4 consulting firms, and AI-native startups worldwide.

Throughout 2023, Adversa AI expanded its proprietary AI threat database by more than 1,000 new attack scenarios, enabling precise, contextual testing tailored to each client's risk profile. The platform also added support for multimodal input, multilingual scenarios (including hieroglyphs), and autonomous agents.

The company contributed to the NIST AI Risk Management Framework, joined CoSAI's governance board to lead AI Agents Security. It also received 10+ new awards and analyst recognition from Gartner and IDC.

Adversa AI's platform has become a foundation for secure AI deployment—transforming AI security from theory into enterprise-grade practice.

c. Explain why the technology breakthrough you have highlighted is unique or significant (up to 250 words). Required

What makes Adversa AI's achievements unique is not just the technology—it's the fact that they are delivering solutions to problems that most organizations only recently discovered. While many security providers attempt to retrofit AI models into traditional infrastructure protections, Adversa AI builds AI-native defenses that simulate the way real attackers interact with AI systems—at the model layer.

Its platform is not a toolset for penetration testers, nor a passive monitoring system. It is a fully-automated, continuously evolving Red Teaming engine that tests GenAI and Agentic AI systems in real time—before those systems reach production. Adversa AI was the first to publicly demonstrate the ability to detect zero-day vulnerabilities in major models within minutes of release, outperforming in-house and academic efforts.

The company's ability to win the trust of high-stakes clients, influence industry standards, and deliver measurable protection shows that this is not just an innovation—it's a foundational shift in how AI will be secured moving forward. Adversa AI's success marks a paradigm shift in how risk is managed in an AI-first world.

d. Reference any attachments of supporting materials throughout this nomination and how they provide evidence of the claims you have made in this nomination (up to 250 words). Optional

To support the achievements described in this nomination, we were included in almost all the most important lists for AI Cybersecurity solutions by OWASP, CSA, OECD, and top analysts' reviews such as Gartner, IDC, and Wavestone as well as 20+ Awards in Cyber and AI.

1. IDC Innovators: AI Security, 2024
Adversa AI was selected as one of only four global vendors in IDC's "AI Security Innovators" with at least 10x less funding than each of others https://www.idc.com/getdoc.jsp?containerId=US51886324

2. Wavestone AI Security radar 2024 https://www.wavestone.com/en/insight/radar-2024-safety-solutions-ia/

3. Gartner AI TRISM 2024, Representative vendor in Gartner Market Guide.
https://www.gartner.com/en/documents/4623399

4. Inclusion in the OECD Catalogue of Tools & Metrics for Trustworthy AI (Dec 2024)
This catalogue serves as a global benchmark for AI solutions that align with OECD AI Principles, including safety, fairness, robustness, and human rights alignment. https://oecd.ai/en/catalogue/tools/adversa-ai-red-teaming-platform

5. Inclusion in CSA (Cloud Security Alliance) list of innovative AI and cloud security solutions designed to tackle today's biggest challenges. https://cloudsecurityalliance.org/csa-startup-showcase/registry

6. Inclusion in the OWASP list of tools as the only AI Red Teaming tool that can test for all types of OWASP for LLM Weaknesses. https://genai.owasp.org/solution/adversa-ai-red-teaming-platform/

[redacted]

[REDACTED FOR PUBLICATION]

[redacted]

Would you like to add an additional webpage link?

Yes

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted])

Would you like to add an additional webpage link?

Yes

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]the_download.unpaid.engagement&utm_term=*%7CSUBCLASS%7C*&utm_content=*%7CDATE:m-d-Y%7C*)

Supporting Document

No File Uploaded

Would you like to add an additional supporting document?

By your submission of this entry to The Stevie Awards, you verify that you have read and agreed to abide by the regulations, terms and conditions of the competition (https://www.asia.stevieawards.com/rules-and-terms-conditions-competition).

Terms and Conditions

I Agree