OASIS Coalition for Secure AI Welcomes EY, Protect AI, Trend Micro, and Zscaler as Newest Premier Sponsors

Industry Leaders Strengthen Coalition to Drive Innovation in AI Security

BOSTON, MA, UNITED STATES, September 19, 2024 / EINPresswire.com/ -- The Coalition for Secure AI (CoSAI), an OASIS Open Project that launched on 18 July 2024, is announcing the addition of EY, Protect AI, Trend Micro, and Zscaler as its newest Premier Sponsors. These industry leaders join CoSAI's expanding alliance of organizations, which now includes more than 30 partners dedicated to advancing the security of artificial intelligence (AI). Together, they support CoSAI's mission to develop and share open-source methodologies, standardized frameworks, and tools for secure AI development and deployment.

CoSAI is a collaborative open-source initiative designed to give all practitioners and developers the guidance and tools they need to create Secure-by Design AI systems. Three strategic workstreams have been established within CoSAI, with plans to add more over time: software supply chain security for AI systems, preparing defenders for a changing cybersecurity landscape, and AI risk governance.

In addition to welcoming new Premier Sponsors, CoSAI is pleased to introduce its latest General Sponsors: Blinder, Cranium, Cyware, Dell Technologies, Fr0ntierX, Harvey, HiddenLayer, Invariant Labs, Lasso Security, Legit Security, Logitech, Mozilla, Styrk AI, Thomson Reuters, TrojAI, and VE3. These organizations further diversify and strengthen CoSAI's community of stakeholders committed to advancing AI security.

"Joining CoSAI underscores the EY organization's dedication to fostering innovation while at the same time enhancing the security and integrity of AI technologies," said Yang Shim, EY Americas Technology Consulting Leader. "By working alongside other industry leaders, we aim to contribute to the development of robust frameworks that will empower enterprises and individuals to shape the future with confidence through the secure integration and deployment

of AI," added Kapish Vanvaria, EY Americas Risk Leader.

"At Protect AI we are on a mission to create a safer AI-powered world. As the prevalence of AI within organizations grows, so must the ability to secure it," said Ian Swanson, CEO and Co-founder, Protect AI. "We are proud to join CoSAI as a Premier Sponsor. Through this collaboration, we aim to help shape the development of frameworks and standardized MLSecOps processes that enhance the security, safety, and trust for AI applications across industries."

Eva Chen, CEO at Trend Micro, said, "We are dedicated to leading the charge in securing AI deployment, ensuring that security is seamlessly embedded from the ground up. Our collaboration with CoSAI reflects our commitment to pioneering efforts that not only protect organizations but also leverage AI to enhance security and uphold the trust of consumers. By bringing together industry leaders, we aspire to set new standards for the integrity and safety of AI systems, driving positive change across both the industry and broader society."

"Zscaler is proud to join CoSAI to collaborate with industry leaders. Our collective aim is to establish best practices that ensure AI technologies are not only innovative but also trustworthy," said Deepen Desai, Chief Security Officer, Zscaler. "This partnership will enable Zscaler to leverage the power of AI in order to deliver the most advanced security solutions for our customers. Through this collaboration, we're striving to set a new standard for AI-driven security that prioritizes transparency, reliability, and excellence."

These Premier and General Sponsors will join forces with CoSAI's founding Premier Sponsors – Google, IBM, Intel, Microsoft, NVIDIA, and PayPal – and founding General Sponsors, including Amazon, Anthropic, Cisco, Chainguard, Cohere, GenLab, OpenAI, and Wiz. With the support of these industry leaders and experts, CoSAI is poised to make significant strides in establishing standardized practices that enhance AI security and build trust among stakeholders globally.

Participation

Everyone is welcome to contribute technically as part of the CoSAI open-source community. OASIS welcomes additional sponsorship support from companies involved in this space. Contact join@oasis-open.org for more information.

See a list of CoSAI General Sponsors' quotes here.

About CoSAI:
CoSAI is an open ecosystem of AI and security experts from industry-leading organizations dedicated to sharing best practices for secure AI deployment and collaborating on AI security research and product development. CoSAI's scope includes securely building, integrating, deploying, and operating AI systems, focusing on mitigating risks such as model theft, data poisoning, prompt injection, scaled abuse, and inference attacks. The project aims to develop

comprehensive security measures that address AI systems' classical and unique risks. CoSAI operates under OASIS Open, the international standards and open source consortium.

About OASIS:
OASIS is one of the most respected, nonprofit open source and open standards bodies in the world. It advances the fair, transparent development of open source software and standards through the power of global collaboration and community. OASIS is the home for worldwide standards in AI, cybersecurity, supply chain, IoT, privacy, and other technologies. Many OASIS standards go on to be ratified by de jure bodies and referenced in international policies and government procurement. www.oasis-open.org

Media inquiries:
communications@oasis-open.org

Carol Geyer
OASIS
+1 941-284-0403
carol.geyer@oasis-open.org
Visit us on social media:
LinkedIn
YouTube
Facebook
X
