ESET previews new AI security features to secure chatbot communications and AI workflows

DUBAI , DUBAI, UNITED ARAB EMIRATES, April 20, 2026 /EINPresswire.com/ -- ESET, a global leader in cybersecurity, today announced upcoming AI protection capabilities designed to safeguard how employees interact with AI tools. Demonstrated at RSAC 2026 and set to launch later this year, the new features will expand visibility in the ESET PROTECT Platform to investigate emerging risks tied to everyday AI usage and agentic AI adoption across an enterprise.

“As companies rely more on AI for productivity and automation, they face growing risks around sensitive data exposure, compliance violations, and misleading outputs,” said Juraj Jánošík, ESET Director of Artificial Intelligence. “Agentic AI is shifting the security battlefield back to the endpoint. ESET has spent over 30 years building leading endpoint protection powered by AI and machine learning, so we’re uniquely positioned to help organizations secure this next wave of AI right where it starts.”

As AI tools become embedded in everyday workflows, many employees are using open cloud chatbots without IT oversight, creating “shadow AI” risks and exposing sensitive data such as internal documents, API keys, secrets, and credentials. ESET addresses this through various technologies that get as close to the source as possible, one of which is a secure browser technology that intercepts AI interactions and analyzes both prompts and responses in real time, helping prevent data exposure and detect malicious or misleading content before it impacts users.

In demonstrations at RSAC 2026, the new AI protection feature flagged malicious URLs submitted through chatbot prompts, logging activity at the endpoint and surfacing it in the ESET PROTECT Platform for investigation. The same approach applies to prompt injection attempts, scripts, and

sensitive data inputs, enabling organizations to block or monitor activity in accordance with their policies. Security teams will gain visibility into how AI tools are used across their organization through ESET PROTECT Platform logging, helping them investigate risks and enforce policies more effectively.

As organizations expand their use of agentic AI tools, the attack surface is extending beyond chatbot interactions to include emerging AI supply chain risks. These include compromised AI frameworks and tools, such as trojanized components in widely used libraries like LiteLLM, as well as autonomous agents like OpenClaw that can execute actions on a system with limited oversight. ESET has already been protecting its customers from supply-chain attacks through compromised libraries delivered via standard repositories but is noting a rise in these types of attacks and remains committed to further research and development relating to AI tools.

As part of its broader AI security innovation, ESET launched a free ESET AI Skills Checker at RSAC 2026. Available to non-ESET customers and built on the same technology as ESET's endpoint security products and ESET LiveGuard, the scanner analyzes AI skills for hidden instructions, malicious code, and risky behavior, using multilayered inspection and cloud-based sandboxing. It is currently available as a built-in feature for existing ESET Endpoint users.

For more than 30 years, ESET has pioneered lightweight, high□performance endpoint security powered by machine learning and artificial intelligence. These new capabilities extend that foundation by helping organizations defend against today's rapidly shifting threat landscape, where cybercriminals increasingly harness AI to scale attacks, target employees, and automate sophisticated social engineering.

As the only dedicated cybersecurity member of the Agentic AI Foundation (AAIF), ESET is also working to secure emerging AI agent communication protocols through collaboration with industry leaders like OpenAI, Amazon, Microsoft, and Anthropic. Together, the group is working to establish trusted standards, secure protocol designs, and best practices for AI agent interoperability.

Learn more about why businesses choose ESET at https://www.eset.com/us/business/why-eset/.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class

research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here