AI on the Frontline: Global Firms Back Innovation, Brace for New Cyber Threats

New Trend Micro research reveals widespread AI adoption in cybersecurity strategies, but mounting concerns cyber risk exposure

DALLAS, July 1, 2025 /PRNewswire/ -- Global AI cybersecurity leader Trend Micro Incorporated (TYO: 4704; TSE: 4704) published new research* today revealing that while organizations are embracing artificial intelligence to strengthen their cyber defenses, many are increasingly concerned about the technology's potential to expand their attack surface and introduce new risks.

To learn more about Trend's latest research, visit:https://www.trendmicro.com/explore/aichangingcyberrisk

Rachel Jin, Chief Enterprise Platform Officer at Trend: "AI holds enormous promise for strengthening cyber defenses, from identifying anomalies faster to automating time-consuming tasks. But attackers are just as eager to leverage AI for their own purposes, and that creates a rapidly shifting threat landscape. Our research and real-world testing make it clear that security must be built into AI systems from the outset. There is simply too much at stake to treat this as an afterthought."

According to the study, 81% of global businesses are already using AI-driven tools as part of their cybersecurity strategy, with a further 16% actively exploring implementation. Nearly all respondents (97%) are open to using AI in some capacity. Over half are already relying on it for essential processes such as automated asset discovery, risk prioritization and anomaly detection. AI and automation are now considered top priorities for improving cybersecurity over the next 12 months by 42% of surveyed organizations.

This optimism also comes with significant risk. An overwhelming 94% of businesses believe that AI will negatively impact their cyber risk exposure within the next three to five years. Over half expect a surge in the scale and complexity of AI-driven attacks, which they say will force them to rethink and reshape existing cybersecurity strategies. Many point to the risk of sensitive data exposure, uncertainty around how data is processed and stored by AI systems, the potential for proprietary data to be exploited by untrusted models, as well as increased compliance pressures and monitoring challenges stemming from a proliferation of new endpoints, APIs and shadow IT.

The tension between opportunity and risk was evident at Trend's Pwn2Own event in Berlin, where the AI category was introduced for the first time. The results offered a compelling snapshot of where AI security currently stands.

Twelve entries targeted four major AI frameworks, with the NVIDIA Triton Inference Server receiving the most attention. Chroma, Redis, and the NVIDIA Container Toolkit were also successfully exploited, in some cases using just a single bug to achieve full compromise. In total, seven unique zero-day vulnerabilities were uncovered in the AI frameworks. The vendors now have 90 days to patch the flaws before technical details are made public.

As AI becomes more deeply integrated in enterprise IT environments, Trend urges security leaders to proactively evaluate the evolving risk landscape and embed rigorous security practices into every stage of AI adoption.

**Trend Micro commissioned Sapio Research to interview 2250 individuals with responsibility for IT and/or cybersecurity—across multiple verticals, organization sizes and 21 countries in Europe, North America and APAC.*

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, Trend's platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 70 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---