Security Gaps Imperil Private 5G Networks Amid AI Boom

New research reveals next-gen private wireless network deployments are surging, but lack of proactive security measures raises serious concerns

DALLAS, March 3, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released new joint research with CTOne* warning that a lack of communications technology (CT) expertise could be exposing private 5G networks to compromise, despite the widespread adoption of AI security tools.

To learn more about Trend and CTOne's activities at MWC Barcelona 2025, please visit: https://resources.trendmicro.com/Mobile_World_Congress_MWC_2025_LP.html

Rachel Jin, Chief Enterprise Platform Officer at Trend: "Not all AI security is created equal, and some organizations are putting themselves at risk due to lack of know-how. Proactive attack surface management is crucial for private 5G networks, where any oversight can open the door to compromises. Security leaders must combine AI-powered protection with a deep understanding of technology and cyber risk to safeguard these critical environments."

Private 5G networks are booming thanks to their use across critical industries including energy and utilities, military, logistics, healthcare, and smart manufacturing. 100% of Trend survey respondents revealed they are either currently using them (86%) or evaluating their deployment (14%).

IT and cybersecurity professionals also appear to understand the potential benefits of AI-powered security in these environments: nearly all said they are either currently using (62%) or planning to use (35%) such tools for private 5G networks.

They view the following AI-powered capabilities as essential in this regard:

- Predictive threat intelligence (58%)
- Continuous, adaptive authentication (52%)
- Zero trust enforcement (47%)
- Self-healing networks featuring AI automation (41%)

Jim Frey, Principal Analyst, Networking for ESG: "Organizations are finding great operational value from private 5G networking, often as a part of AI projects. But they must ensure that their security operations center is prepared to monitor and protect this emerging communications technology. Cybersecurity providers that can deploy proactive risk management, attack path prediction, and other proactive measures will be well positioned to help protect private 5G and AI architectures."

More than nine in ten organizations currently using AI security admit to facing challenges in deploying the tech to private 5G networks. High costs (47%), concerns over false positives/negatives (44%), and a lack of internal expertise (37%) were most frequently cited.

A lack of in-house CT know-how is reflected in the fact that just a fifth (20%) of global organizations have a dedicated team for securing their communications networks. In many cases, responsibility for CT security lies with the CTO (43%) or CIO (32%).

Jason Huang, CEO at CTOne: "As enterprise use of private and public mobile networks accelerates, we are seeing new challenges that demand specialized CT security capabilities. Organizations need the ability to secure end-to-end combined broad visibility that fits with SecOps needs, enabling them to manage their enterprise attack surface risk as it expands to support new wireless applications."

On average, less than a fifth (18%) of organizations' security budget is currently allocated to private 5G networks, despite the critical services they support and the highly sensitive data flowing through these networks.

Trend's research revealed that organizations may be unwittingly exposing themselves to cyber and compliance risks by failing to safeguard use of AI for traffic monitoring/analysis.

Specifically, only around half or fewer respondents said that they:

- Ensure compliance with data privacy regulations like GDPR (54%)
- Encrypt data at rest and in transit (51%)
- Deploy strict access controls for AI models (50%)
- Use data anonymization techniques (44%)

**Trend Micro & CTOne commissioned Sapio Research to survey 800 managers or above, with decision making authority over IT and / or cybersecurity across the US, UK, Japan, France, Germany, Italy and Spain. All respondents work in companies of 250+ employees and either currently use a private 5G network or are evaluating deployment*

250+ employees and either currently use a private 5G network or are evaluating deployment.

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.

About CTOne
CTOne, a global cybersecurity leader in communication technology (CT), helps organizations better manage their ever-expanding attack surface risk. As a subsidiary of cybersecurity leader Trend Micro, CTOne leverages 35+ years of experience to bridge the IT/CT expertise gap with an AI-powered solution for mobile deployments. With deep threat and attack expertise combined with comprehensive security for mobile deployments, CTOne delivers visibility and protection across mobile endpoints and network infrastructure in support of enterprises using private 5G for competitive advantage. Always on guard, CTOne helps organizations securely drive digital transformation, reduce operating costs, increase productivity, and avoid losses from CT-related attacks. https://www.ctone.com

SOURCE Trend Micro

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

---