

New Research Highlights Key Security Gaps in Enterprise Mobile Networks

Report reinforces need for next-generation capabilities to protect 5G and other wireless networks

TAIPEI, March 3, 2025 /PRNewswire/ -- CTOne, a Trend Micro™ company, today announced the availability of a new research report that highlights the need for next-generation security solutions to protect enterprise private 5G and public mobile networks. With the enterprise attack surface risk expanding rapidly, CTOne's next-generation solution delivers crucial security for organizations leveraging mobile-edge AI devices and applications. At Mobile World Congress (MWC) Barcelona 2025, CTOne will showcase key new mobile network security capabilities that empower organizations to fully unlock the potential of private, public, and hybrid mobile networks while more effectively managing enterprise attack surface risk.

Join CTOne and Trend Micro at Mobile World Congress Barcelona in [booth 4A50, Hall 4](#) from March 3-6, 2025:

https://resources.trendmicro.com/Mobile_World_Congress_MWC_2025_LP.html

The new research*, in partnership with Trend Micro, highlights that a lack of communications technology (CT) expertise could be exposing private 5G networks to vulnerabilities, despite the growing adoption of AI-powered security tools. The research reveals that only 20% of global organizations have a dedicated CT team to manage and secure their communications networks. In many cases, the responsibility for CT security falls to the CTO (43%) or CIO (32%).

Jason Huang, CEO of CTOne: "Organizations deploying private 5G are seeing the real benefits that next-generation wireless can deliver. As shown in our new research, they are also realizing that they need to secure those networks as a part of managing their enterprise attack surface risk. CTOne's new solutions for protecting enterprise wireless change the game, addressing both enterprise skills gaps as well as potential threats to wireless deployments."

At the conference, CTOne and Trend Micro will demonstrate cybersecurity solutions for protecting next-generation mobile networks, integrating the protection of IT, OT, and CT environments. Organizations will be able to experience end-to-end zero trust capabilities for private and public wireless networks, edge AI endpoints in public 5G, and optimized operational capabilities for scaling mobile applications.

At MWC 2025, CTOne will also showcase its tailor-made solution – CTOne SecureRAN— for protecting AI-powered O-RAN systems. SecureRAN is designed to drive better security outcomes and ensure sustainable O-RAN deployments, providing robust protection for critical O-RAN assets and AI-driven applications.

**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.*

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 CTOne

For further information: CTOne Inc., Press@ctone.com

<https://newsroom.trendmicro.com/2025-03-03-New-Research-Highlights-Key-Security-Gaps-in-Enterprise-Mobile-Networks>