FOR IMMEDIATE RELEASE

MEDIA RELEASE

July 8, 2025

Tosibox Redefines OT Network Control with Launch of Advanced Network Traffic Analytics (TosiANTA)

Purpose-built solution delivers real-time visibility and anomaly detection for operational technology environments as industrial cyberattacks surge 49% year-over-year

Oulu, Finland / Irving, Texas --- Tosibox, the global pioneer in providing solutions to connect, protect and control OT networks, today announced the launch of TosiANTA (Tosibox Advanced Network Traffic Analytics), a breakthrough solution that fundamentally redefines what comprehensive OT network control means for industrial organizations facing an unprecedented cyber threat landscape.

Redefining Control in an Era of Escalating Threats

Industrial organizations today face a cybersecurity crisis that demands a complete redefinition of network control. Recent industry data reveals that 73% of organizations experienced intrusions impacting OT systems in 2024 - a dramatic 49% increase from 2023. With 83% of OT leaders reporting at least one security breach in the past three years and critical infrastructure experiencing over 420 million attacks between January 2023 and January 2024, traditional approaches to OT network management are failing.

"Our customers tell us they need real control over their industrial networks, and today we are redefining what that means," said Sakari Suhonen, CEO of Tosibox US. "TosiANTA delivers visibility into every device, protocol, and data flow—something most organizations have never achieved. This launch advances our mission to provide customers the fastest way to connect, protect, and control their critical infrastructure."

OT Network Control: Beyond Traditional Monitoring

TosiANTA addresses the fundamental problem that has left organizations without comprehensive OT network control: the inability to see, understand, and respond to their operational technology environments in real-time. While 45% of organizations now report financial impacts exceeding $500,000 from OT cyberattacks, and 49% experience more than 12 hours of operational downtime, traditional monitoring approaches create visibility gaps across OT infrastructure

TosiANTA Redefines OT Network Control by Delivering:

- Comprehensive Asset Visibility: Real-time discovery and monitoring of every connected device regardless of vendor, protocol, or location—achieving comprehensive visibility across OT infrastructure
- Comprehensive Behavioral Intelligence: Deep understanding of normal operations to instantly detect deviations, threats, and performance issues, moving beyond traditional monitoring that misses abnormal patterns
- Continuous Network Governance: Persistent oversight across your entire OT infrastructure, eliminating the language barriers that render traditional IT security tools ineffective in OT environments

Purpose-Built for Industrial Reality

Unlike traditional security tools adapted from IT environments, TosiANTA operates as a native module within the Tosibox Platform, requiring no additional appliances or infrastructure. This approach directly addresses the architecture gaps that prevent organizations from achieving true network control, enabling deployment in days rather than months.

"We selected TosiANTA for beta testing because we need granular visibility for both security investigations and operational optimization," said Chris Isbell, OT Manager at Howard Energy Partners. "The ability to extend our cybersecurity governance program into the OT environment with detailed reporting and integration capabilities aligns very well with our network monitoring goals."

"We're testing TosiANTA to enhance our network visibility and operational insights," said Nate Ferrara, I&E and SCADA Consultant at Civitas Resources. "The potential to automatically discover assets and improve our network intelligence could significantly optimize our field operations, especially as we continue expanding through acquisitions."

Addressing the Control Crisis

With ransomware remaining the dominant threat - including 68 documented cyberattacks in 2023 that caused physical consequences to industrial control systems - and only 56% of organizations maintaining OT-specific incident response plans, the need for redefined network control has never been more urgent. TosiANTA enables organizations to move from reactive security postures to proactive network governance.

The solution eliminates the three fundamental barriers preventing comprehensive OT network control:

1. Architecture Gaps: Organizations typically have visibility gaps across distributed OT infrastructure

2. Understanding Gaps: Traditional security tools built for IT environments can't comprehend industrial protocols
3. Time Gaps: Traditional monitoring approaches miss real-time threats in environments under constant attack

Immediate Availability and Implementation

TosiANTA is available immediately as part of the Tosibox Platform. Current Tosibox customers can deploy the solution in days with no additional hardware required, as TosiANTA activates on existing Tosibox infrastructure - a critical advantage in today's threat environment.

For more information or to schedule a demonstration of how TosiANTA redefines OT network control, visit www.tosibox.com.

##

About Tosibox

Tosibox is the global pioneer in providing solutions to connect, protect and control OT networks. Since 2011, the company has deployed solutions to manage hundreds of thousands of end point devices and physical infrastructure, securing the associated data. With U.S. headquarters in Irving, Texas and global headquarters in Oulu, Finland, Tosibox serves 800+ direct customers globally and works with 200+ partners. The company's purpose-built OT cybersecurity platform enables rapid deployment, comprehensive visibility, and robust security that simplifies compliance and delivers measurable cost savings.

Media Contact:

Margaret Herndon

pr@tosibox.com

214.454.1112