FOR IMMEDIATE RELEASE

MEDIA RELEASE

April 21, 2026

The Weakest Link in OT Security: Tosi Identified It Two Months Before the Federal Advisory

A 2026 benchmark study from Tosi found vendor remote access to be the weakest OT security capability across every sector. A joint federal advisory issued on April 7 named the same vulnerability as the entry point for cyber-attacks on US critical infrastructure.

Oulu, Finland / Irving, Texas – Tosi's 2026 State of OT Security Report, published ahead of a recent U.S. federal advisory, **identified vendor remote access as the single weakest capability across every industry surveyed**. On April 7, six government agencies issued a joint advisory that confirmed the same vulnerability as the entry point for cyber-attacks on American critical infrastructure that had been carried out since at least March 2026. The entry method was simple: the attackers connected to the internet-exposed industrial controllers using the manufacturer's own software, because there was nothing controlling the access.

Tosi's report, released in February 2026, was conducted as an independent benchmark study of 77 U.S. enterprises across water and wastewater, energy, manufacturing, financial services, retail, and real estate. Vendor remote access emerged as the single weakest capability across every sector. The most alarming finding: manufacturing, one of the industries named in the advisory, scored just 1.67 out of 5 on vendor access to plant floor systems, the lowest score of any individual question in the entire dataset.

"The actors connected to internet-facing industrial controllers the same way a legitimate vendor would, because there was nothing in place to tell the difference," said Sakari Suhonen, CEO of Tosi U.S. "The advisory confirmed that attacks on critical infrastructure were already underway in March. Our research, conducted independently in February, found the same structural gap. Two separate efforts, looking at the same problem, reaching the same conclusion."

The advisory's primary recommendation is to place a secure gateway in front of industrial controllers so they are no longer directly reachable from the internet. Tosi Gateways are purpose-built for exactly this: they sit between the public internet and the plant floor, ensuring that no industrial device is ever directly exposed.

The City of Sandusky, Ohio, a municipal water and wastewater operator, is among the utilities that have deployed the Tosi platform.

"Tosi allows the City of Sandusky to keep our wastewater and drinking water networks securely isolated while still allowing for quick support from vendors and remote staff when needed," said Matthew DeVries, IT Manager, City of Sandusky.

The gap between having tools and enforcing controls is where most organizations remain exposed. "The organizations at the top of our maturity scale have one thing in common: they have turned deployed tools into enforced controls," Suhonen said. "What the advisory describes is not a novel threat. It is a known gap that has not been closed."

Tosi's 2026 State of OT Security Report also revealed that one in three U.S. organizations takes hours or longer to revoke vendor access after a job is complete. One in eight takes days or weeks. Furthermore, remote access

turned out to be the only capability where the U.S. trails Europe, scoring 6.47 out of 10 versus 6.62 for European respondents.

The full overview of the U.S. part of the report containing a detailed description of scores per capability is available here.

About the 2026 State of OT Security Report

Primary research conducted in February 2026 with 77 security and operations professionals at U.S. enterprises exceeding $1 billion in annual revenue. The full global study includes 135 respondents across the U.S., UK/Ireland, Germany, Benelux, and Finland.

About Tosi

Tosi (formerly Tosibox) is the global pioneer in Cyber Physical Systems platforms for OT networks. Since 2011, the company has deployed solutions to connect, visualize, and control hundreds of thousands of industrial devices. With headquarters in Irving, Texas and Oulu, Finland, Tosi serves 800+ customers globally and operates with 150+ partners. The company's integrated platform enables rapid deployment, comprehensive visibility, and unified control that delivers OT security that scales.

Media Contact:

Agata Radlak
E-mail: pr@tosi.net