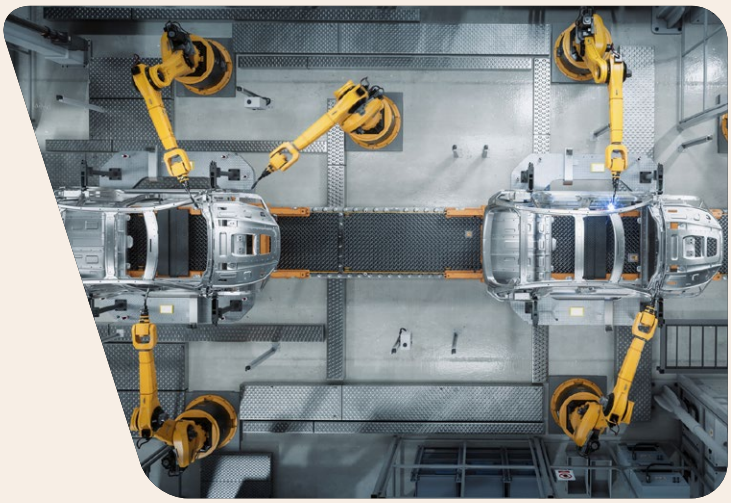
THE NEW STANDARD YOUR ORGANIZATION ISN'T MEETING



Sakari Suhonen is CEO of Tosi US, bringing over 20 years of experience leading B2B software companies. He has transformed organizations and driven exceptional growth, including spearheading Finland's first B2B enterprise SaaS company IPO. His deep understanding of OT environments and cybersecurity challenges has made him a trusted advisor to industrial organizations worldwide.

Sakari Suhonen
CEO
Tosi US
(formerly Tosibox US)

CEO INSIGHTS — REDEFINING CONTROL IN THE INDUSTRIAL AGE

Let me introduce you to a concept that's about to reshape how we think about industrial cybersecurity: what it really means to have control over your OT networks.

It's not what most executives think they have when they talk about their OT security. It's not remote access. It's not network segmentation. It's not even about having the latest security tools.

Real control over your industrial networks requires three fundamental capabilities that transform how you operate:

- **Complete Visibility:** Real-time, 100% visibility into every device, protocol, and data flow
- **Contextual Understanding:** Knowing not just what's happening, but whether it's normal
- **Immediate Action:** The ability to prioritize high-risk events and respond to critical anomalies within minutes, not hours

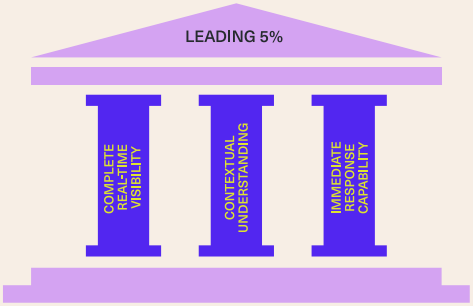
This is the new standard. And here's the uncomfortable truth: less than 5% of industrial organizations have achieved it.

THE DINNER THAT CHANGED MY PERSPECTIVE

Recently, I had dinner with the CISO of a major manufacturing company. His organization had invested millions in OT security, implemented remote access, segmented their networks, and trained their teams extensively. Yet when he asked his team to demonstrate what was actually happening on their factory floor network at that moment — the real-time data flows and device communications — they simply couldn't do it. His revelation crystallized what I've been seeing across the industry: Organizations believe they have control because they have access. But access without visibility isn't control — it's an illusion.

THE THREE PILLARS: WHAT SEPARATES LEADERS FROM THE VULNERABLE

After two decades in this industry, I've identified what distinguishes the 5% who have achieved genuine network control from the 95% who remain vulnerable.



1. First Pillar: Complete real-time visibility

You need to see everything — not just device inventories or network diagrams, but every conversation, every protocol, every data flow in real-time. One energy executive who achieved this discovered 30% more devices than they knew existed, including three that were already compromised.

2. Second Pillar: Contextual understanding

Visibility without context is just noise. You must understand what's normal for your specific environment. When you know that your PLC typically communicates with three specific IPs between 6 AM and 2 PM, any deviation becomes immediately significant.

But context goes deeper than patterns — it requires risk intelligence. Not all anomalies are created equal. A new connection from your HMI might be a routine update or a critical breach attempt. Without the ability to instantly distinguish between high-risk events that demand immediate action and low-risk anomalies that can be investigated during normal operations, your team drowns in alerts while real threats slip through.

3. Third Pillar: Immediate response capability

In OT environments, minutes matter. Your security posture must enable teams to cut through the noise, identify which events demand urgent attention, and act within minutes of detection. This is the difference between stopping an incident and explaining one.

WHY 95% OF ORGANIZATIONS FALL SHORT

Three fundamental barriers prevent organizations from achieving comprehensive control over their OT networks.

1. Architecture Gap

Most organizations monitor less than 20% of their OT network communications. They've installed cameras at the front door while leaving the windows open. Complete control requires comprehensive traffic monitoring — every packet, every protocol, every conversation.

2. Language Barrier

Industrial networks speak in Modbus, DNP3, Profinet, and dozens of proprietary protocols. Traditional security tools are deaf to these languages. Without protocol-aware monitoring, you're missing the actual content of your network's conversations. It's like monitoring your company's financial transactions but only seeing that money moved, not whether it was a legitimate vendor payment or embezzlement — you see the activity but miss the intent and context that defines the risk.

3. Time Gap

Periodic scans and manual checks belong to yesterday's security model. Modern OT security demands continuous, real-time monitoring. In flat OT networks where compromises cascade in minutes, yesterday's visibility is today's breach.

THE REAL COST OF OPERATING BELOW THE STANDARD

When you operate without comprehensive network control, you're not just accepting risk — you're inviting it:

- **Invisible Dwellers:** Sophisticated campaigns like Volt Typhoon target organizations without comprehensive visibility, living undetected in networks for months
- **Operational Blindness:** Without real-time visibility, every anomaly becomes a time-consuming mystery instead of a quickly resolved issue
- **Compliance Exposure:** Regulators now expect "continuous monitoring" — a core component of modern OT security
- **Alert Fatigue:** Without risk-based prioritization, critical threats hide among thousands of low priority events

THE PATH TO COMPREHENSIVE CONTROL

Achieving real control over your OT networks isn't about abandoning your current investments — it's about completing them.

Start by assessing your current state. Can you see all OT network communications in real-time? Do you understand normal behavior for every critical asset? Can you distinguish between high-risk and low-risk events automatically? Can you detect and respond to anomalies within minutes? Every "no" represents a gap between your current state and where you need to be.

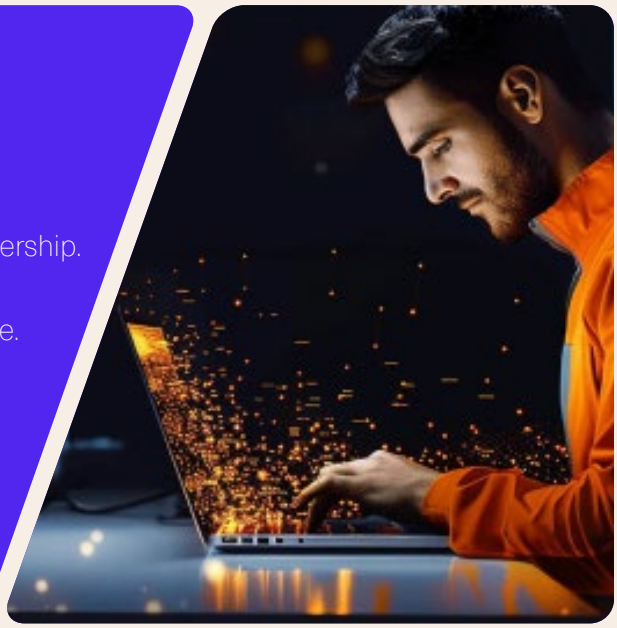
Building your foundation requires:

- Protocol-aware monitoring that understands industrial languages
- Behavioral baselines for all critical systems
- Risk-based prioritization that separates critical from routine
- Real-time detection and alerting capabilities
- Contextual analysis that distinguishes normal from abnormal

Implementation should be strategic and systematic. Start with critical assets and expand methodically. Close visibility gaps, establish baselines before threats emerge, train teams on new capabilities, and continuously refine your control posture.

THE EXECUTIVE MANDATE

Achieving comprehensive OT network control isn't a technical initiative—it's a business imperative that requires executive leadership. Your role is to set the standard by making complete visibility and control your organization's minimum acceptable security posture. Challenge your teams on visibility, not just access. Fund the capabilities that bridge the gap. And track your advancement toward complete visibility, contextual understanding, and immediate response.



THE FUTURE BELONGS TO THOSE WHO ACT

The industrial landscape is dividing into two categories: organizations with comprehensive control over their OT networks and those without. The difference isn't just about security — it's about operational excellence, competitive advantage, and business resilience.

Companies achieving this level of control report:

- 90% faster incident response times
- 75% reduction in unexplained production anomalies
- Confidence in their compliance posture
- Proactive threat detection instead of reactive incident response

Act now: The question isn't whether you'll need this level of control. It's whether you'll achieve it proactively or be forced to react after an incident.

The era of "good enough" OT security is over. Complete visibility, contextual understanding, and immediate response are now the minimum standard for industrial operations.

The technology exists today. The only variable is your decision to implement it.

Because in the end, if you don't have real control over your OT networks, you don't have control at all. You have access to systems you can't truly see, understand, or protect.

Sakari Suhonen is CEO of Tosi US, bringing over 20 years of experience leading B2B software companies. He has transformed organizations and driven exceptional growth, including spearheading Finland's first B2B enterprise SaaS company IPO. His deep understanding of OT environments and cybersecurity challenges has made him a trusted advisor to industrial organizations worldwide.

Connect with Sakari on LinkedIn to continue the conversation about achieving comprehensive control in your organization.

Sakari Suhonen
CEO
Tosi US
(formerly Tosibox US)

US HQ
1212 Corporate Drive
Suite 170
Irving, Texas 75038

GLOBAL HQ
Elektroniikkatie 2a
7th floor
90590 Oulu, Finland

CONTACT US