TOSIBOX

Sakari Suhonen
CEO, Tosibox, US

Sakari Suhonen, CEO of Tosibox US, is a proven leader in OT cybersecurity and network automation. With over 20 years leading B2B software companies, he has transformed organizations and driven exceptional growth, including spearheading Finland's first B2B enterprise SaaS company IPO. His business acumen and innovative approach have established him as a respected executive with a consistent track record of delivering results.

The 5 Non-Negotiable Capabilities Your OT Network Security Solution Must Have

A thought leadership article for OT and IT security professionals

As operational technology (OT) environments become increasingly connected and critical to business operations, the challenge of securing these systems has never been more complex—or more urgent. With the OT cybersecurity market projected to reach $21.6 billion by 2028, organizations are investing heavily in security solutions. But with so many options available, how do you ensure you're selecting a solution that will truly protect your critical infrastructure?

After years of analyzing successful OT security implementations across industries, five critical capabilities have emerged as non-negotiable requirements. These capabilities separate solutions that merely check boxes from those that deliver real, operational security value.

1 Autonomous Asset Discovery & Management

The foundation of any OT security program is knowing what's connected to your network. Traditional manual inventory processes fall short in today's dynamic environments, where devices are constantly added, removed, or modified. Your security solution must provide autonomous discovery capabilities that work without disrupting operations.

Why this matters: Recent Gartner research on CPS Protection Platforms identifies "Asset Discovery" and "Asset Pedigrees and Attributes" as critical capabilities, with both weighted at 20% importance for the foundational use case of discovering and mapping CPS assets. Organizations cannot secure what they cannot see.

Key requirements:

- Passive discovery methods that don't interfere with production systems
- Comprehensive asset classification including device types, versions, and configurations
- Continuous monitoring that automatically updates asset inventories
- Integration with vulnerability databases to identify security exposures
- Support for both modern and legacy industrial protocols

The best solutions go beyond simple device enumeration to provide rich contextual information about each asset's role, connections, and security posture. This foundation enables everything else in your security program—you can't protect, segment, or monitor what you don't know exists.

2 Non-Intrusive Network Traffic Analysis

OT environments demand security solutions that understand the unique constraints of operational technology. Unlike IT networks, OT systems prioritize availability and real-time performance. Your security solution must provide deep network visibility without introducing latency or disrupting critical processes.

Why this matters: Effective OT network traffic analysis requires a fundamentally different approach than traditional IT security monitoring. Rather than relying on deep packet inspection that can introduce latency and security concerns, the most effective solutions use metadata-based analysis that provides complete visibility while respecting privacy and operational constraints.

Key requirements:

- Passive, non-intrusive monitoring with zero operational interference
- Metadata-based analysis that respects data privacy
- Built-in deployment requiring no external appliances or sensors
- Detection of anomalies through behavioral pattern analysis
- Coverage of both North-South and East-West traffic flows

Effective OT network traffic analysis goes beyond simply monitoring data flows—it understands the operational context of communications and can distinguish between legitimate operational changes and potential security threats.

3 Zero Trust Architecture with Multi-Factor Authentication and Granular Segmentation

The traditional "castle-and-moat" security model fails in modern OT environments. As industrial systems become more interconnected, organizations need security architectures that verify every access request and limit lateral movement through granular segmentation.

Why this matters: Zero trust principles, when properly implemented in OT environments, provide defense-in-depth protection while maintaining operational efficiency. This approach is particularly critical as remote access to OT systems becomes more prevalent.

Key requirements:

- Cryptographic device authentication with physical key-based MFA
- Encrypted tunnels that create no visible attack surface
- Role-based access control (RBAC) with time-based restrictions
- Network invisibility with no public IP requirements
- Automated security updates with zero-touch management

Implementing Zero Trust in OT requires more than traditional IT security approaches. The best solutions establish cryptographic trust relationships between devices before any communication occurs, eliminating visible attack surfaces through encrypted tunnels that require no public IP addresses. This approach provides the security benefits of air-gapped systems while enabling the operational connectivity essential for modern industrial environments.

4 Purpose-Built Design for OT Operations

OT security solutions must be designed specifically for industrial environments, not merely adapted from IT security products. Purpose-built solutions understand the unique constraints, protocols, and operational priorities of industrial systems.

Why this matters: Generic IT security solutions often fail in OT environments due to fundamental differences in requirements. OT systems prioritize availability over confidentiality, run on specialized protocols, and have vastly different operational lifecycles compared to IT systems.

Key requirements:

- Native understanding of industrial protocols and systems
- Design that respects OT operational priorities (safety, availability, real-time performance)
- Features aligned with industrial workflows and responsibilities
- Minimal operational overhead and resource consumption
- Integration with existing OT tools and processes

Purpose-built solutions recognize that OT security isn't just about preventing cyberattacks—it's about enabling secure operations while maintaining the availability and performance critical to industrial processes.

5 Infrastructure & Protocol Agnostic Implementation

Your OT security solution must work with your existing infrastructure, not replace it. The reality of industrial environments is diversity—multiple vendors, protocols, and generations of equipment all operating together. Your security solution must embrace this heterogeneity.

Why this matters: Forklift upgrades are rarely feasible in industrial environments. Organizations need security solutions that can protect existing assets while supporting future technologies and protocols.

Key requirements:

- Support for diverse industrial protocols and systems
- Seamless integration with existing network infrastructure
- Vendor-agnostic approach that doesn't lock you into specific platforms
- Ability to protect legacy systems alongside modern equipment
- Scalable architecture that grows with your operations

The best solutions act as a security overlay that works with your existing infrastructure rather than requiring wholesale replacement or extensive modifications to your operational environment.

Implementation Considerations

When evaluating OT security solutions against these capabilities, consider these practical factors:

Start with asset discovery

You can't secure what you don't know exists. Begin with solutions that provide comprehensive asset visibility.

Prioritize operational impact

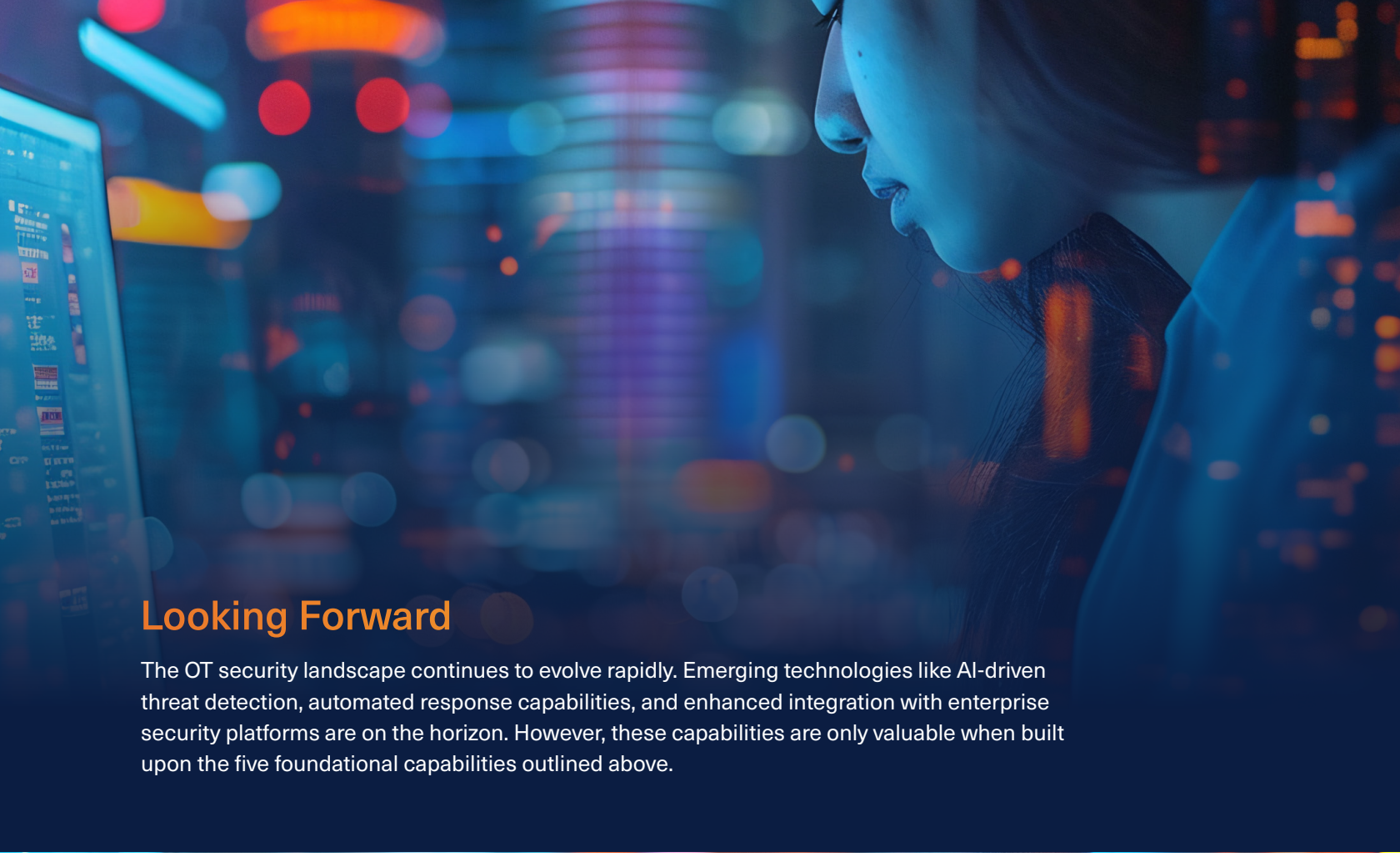
Any security solution that disrupts operations will face resistance and may be circumvented. Choose solutions that enhance rather than hinder operational efficiency.

Plan for scalability

Your security solution should grow with your operations. Look for architectures that can scale across multiple sites and accommodate future expansion.

Consider operational context

The best OT security solutions understand that security decisions must account for operational impact. Look for solutions that provide operational context alongside security insights.



Looking Forward

The OT security landscape continues to evolve rapidly. Emerging technologies like AI-driven threat detection, automated response capabilities, and enhanced integration with enterprise security platforms are on the horizon. However, these capabilities are only valuable when built upon the five foundational capabilities outlined above.

The organizations that successfully secure their OT environments are those that choose solutions based on these fundamental capabilities rather than getting distracted by flashy features or vendor marketing. By focusing on autonomous asset discovery, non-intrusive monitoring, zero trust implementation, purpose-built design, and infrastructure agnostic deployment, you'll build a security foundation that can adapt to whatever threats and technologies the future brings.

Remember: OT security isn't a destination—it's an ongoing journey. The five capabilities described here provide the foundation for that journey, but success requires continuous attention, regular assessment, and adaptation to changing threats and operational requirements.

As the industrial world becomes increasingly connected and threats continue to evolve, these capabilities will become even more critical. Organizations that prioritize them today will be better positioned to secure their operations tomorrow.

Sakari Suhonen
CEO, Tosibox, US

Sakari Suhonen, CEO of Tosibox US, is a proven leader in OT cybersecurity and network automation. With over 20 years leading B2B software companies, he has transformed organizations and driven exceptional growth, including spearheading Finland's first B2B enterprise SaaS company IPO. His business acumen and innovative approach have established him as a respected executive with a consistent track record of delivering results.