

TXONE NETWORKS RECEIVES THE 2023 COMPETITIVE STRATEGY LEADERSHIP AWARD

*Identified as best in class in the Taiwan
operational technology security industry*



Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. TXOne Networks excels in many of the criteria in the operational technology (OT) security space.

AWARD CRITERIA	
<i>Strategy Innovation</i>	<i>Customer Impact</i>
Strategy Effectiveness	Price/Performance Value
Strategy Execution	Customer Purchase Experience
Competitive Differentiation	Customer Ownership Experience
Executive Team Alignment	Customer Service Experience
Stakeholder Integration	Brand Equity

Industry Challenges

As a major original equipment manufacturer (OEM) and original design manufacturer (ODM) manufacturing country, Taiwan plays a critical role in the semiconductor industry supply chain and production of technology products globally. The Taiwanese government actively supports smart manufacturing development and industrial transformation as factory equipment and OT systems increasingly connect to the internet to take advantage of smart technology and automation capabilities.

However, the proliferation of connected devices expands the attack surface and exposes the OT environment to potential security risks. The growing number of cyberattacks targeting manufacturing and critical infrastructures signals a pressing need for greater awareness about the potential losses to the OT environment for recovery.

Despite the risk of substantial losses or reputational damage, the security maturity level in the manufacturing sector remains not up to par, with most industry players only adopting basic cybersecurity processes such as antivirus or firewalls to secure their operations. It is paramount for organizations to adopt a robust OT security strategy to obtain complete visibility of their assets and industrial IoT devices within or across sites, protecting networks pervasively while ensuring business continuity.

Strategy Effectiveness and Competitive Differentiation

Founded in 2019, TXOne Networks offers zero-trust framework-based OT cybersecurity solutions designed to ensure the reliability and safety of industrial control systems (ICS) and OT environments. Its

ICS-native solutions backed by OT zero-trust policies help to protect the asset life cycle across applications, equipment, control, and network in the OT environment. By adopting a zero-trust framework throughout its offerings, TXOne Networks applies a "never trust, always verify" approach at every stage of the onboarding process and protection of critical assets. This helps to secure OT environments and reduce threats that could pose a significant risk to these systems. The company develops zero-trust-based OT technologies that go beyond traditional OT security approaches other OT security players adopt in Taiwan.

"To secure both legacy systems and modern devices in today's OT environment, TXOne Networks analyzes more than 200 ICS protocols, including popular protocols in the semiconductor industry, SECS/GEM, and supports thousands of software applications in the OT environment through its network defense product line, showcasing its ability to prevent attackers from exploiting legacy and unpatched systems. TXOne Networks stands out among competitors because of its strong support for ICS protocols and software applications over legacy and modern operating systems, allowing it to offer a protection level other OT network security competitors find hard to replicate."

– Vivien Pua
Senior Industry Analyst

Its OT-centric solutions come with situational security awareness capabilities surpassing what other endpoint detection and response (EDR) or extended detection and response (XDR) solutions offer. Frost & Sullivan lauds TXOne Networks's commitment to bolstering its product line with advanced capabilities to address the growing requirements for more robust OT security.

TXOne Networks adopts a vertically focused go-to-market strategy as it believes there is no one-size-fits-all OT security solution due to the level of complexity in OT environments, especially in large organizations. Different OT verticals often have unique requirements and need solutions adapted to their environments. By listening to the needs of major manufacturers, the company designs its solutions to fit into their daily operations and comply with regulatory requirements and industry standards. The high level of technology

customization enables TXOne Networks to differentiate itself from other market players that put their IT security products into ruggedized hardware and offer them as standardized OT security solutions.

The company has a strong presence in the semiconductor, automotive, pharmaceutical, and aviation industries. For example, TXOne Networks works with semiconductor companies to implement the OT zero-trust cybersecurity defense architecture and streamline cybersecurity compliance to adhere to stringent Semiconductor Equipment and Materials International (SEMI) standards. It implements network and endpoint protection to ensure the reliability, accuracy, and stability of semiconductor fabrication plants to prevent potential operational production disruptions. The use cases of serving large Taiwanese customers successfully position TXOne Networks as an expert in the OT security space.

Strategy Execution

The Industry 4.0 evolution and need to create smarter operation outcomes in Taiwan see an increased proliferation of connected industrial devices across industrial systems and data transmission to business networks. The connection between physical processes and the internet exposes previously air-gapped industrial networks to cyber threats. As OT systems converge with IT systems as part of the broader digital transformation trend in the industrial sector, there is a critical need to manage this convergence with OT-centric cybersecurity solutions.

TXOne Networks offers three layers of OT security protection to cover the entire lifecycle of OT assets. This includes security inspection, endpoint protection, and network defense. Security inspection allows customers to instantly scan the asset, even if it is air-gapped, using an antivirus engine on a portable USB drive. With this device, no software installation is required. Endpoint protection easily secures ICS endpoints and protects both modern patchable devices and legacy unpatchable devices. Network defense provides OT-native network segmentation to protect against vulnerabilities in unpatched and legacy endpoints through asset shielding. In contrast to other cybersecurity products, TXOne products can operate without an internet connection, which sets it apart from competitors. Its multi-layered protection also provides end-to-end security, differentiating the company from other OT security players that typically focus on a single aspect: network security, security inspection, or endpoint security.

Diverse protocols, customized systems, and the range of vulnerabilities and weaknesses of legacy industrial networks increase the complexity of managing OT cybersecurity. TXOne Networks recognizes that OT security management can be challenging for organizations owing to the large number of assets running on legacy systems and the low visibility of assets in OT environments. The company addresses these pain points by offering virtual patching to protect and reduce the risk of compromising unpatchable legacy systems and securing endpoints even when updates are not possible. The company also provides the ICS protocol-based trust list to give organizations more granular control over their legacy assets.

To secure both legacy systems and modern devices in today's OT environment, TXOne Networks analyzes more than 6000 combinations of ICS protocol granular setting, including popular protocols in the semiconductor industry, SECS/GEM, and recognize more than 8000 of software applications in the OT environment through its product lines, showcasing its ability to prevent attackers from exploiting legacy and unpatched systems. TXOne Networks stands out among competitors because of its strong support for ICS protocols and software applications over legacy and modern operating systems, allowing it to offer a protection level that other OT network security competitors find hard to replicate.

Customer Purchase and Service Experience

A preferred choice of industrial customers in Taiwan, TXOne Networks leverages the strengths of its key distributors, including global cybersecurity companies like Trend Micro, to strengthen its value proposition to customers. The company adopts a two-tier service model, tapping into its key distributors' vast distribution network to maximize its reach in the market. The two-tier service model also allows the company to leverage the strengths of its other local distributor and channel partner network ecosystem to engage and support customers. TXOne Networks boasts one of the broadest market penetration, securing more than 2,000 customers across multiple manufacturing sectors in Taiwan. To cater to the customized requirements of its large customers, the company also provides direct customer support and creates products that fit well into the customer's OT environment and protect their assets the way they want.

TXOne Networks's extensive customer reach is a source of competitive differentiation that other OT-focused security vendors are unable to keep pace with owing to their smaller network of distributors to achieve effective customer engagement.

“TXOne Networks has a strong track record of supporting leading companies in the manufacturing, pharmaceutical, automobile, and aviation sectors, setting it apart from competitors lacking the expertise to support large-scale OT security deployments.”

– Vivien Pua
Senior Industry Analyst

Adopting OT cybersecurity is an ongoing, cross-department conversation for organizations. Close collaboration between security teams, engineers, and operators that manage and understand OT systems is required to reduce OT cybersecurity risks effectively. TXOne Networks focuses on establishing regular communication practices, including customer listening tours to encourage an open dialog between the company’s product managers and different stakeholders on the customers’ end. The company prioritizes

responsiveness and has a dedicated customer support engineer team to help drive customer satisfaction by proactively managing and resolving their technical issues. In addition, its content communication team, including security researchers, developers, and marketing personnel, regularly creates security content or articles to strengthen customer engagement and education. Its annual security report showcases TXOne Networks’s domain expertise in OT security through in-depth analysis of ICS-related vulnerabilities, cyber threats, and OT environment trends.

Brand Equity

TXOne Networks has a strong track record of supporting leading companies in the manufacturing, pharmaceutical, automobile, and aviation sectors, setting it apart from competitors lacking the expertise to support large-scale OT security deployments. Within Taiwan’s semiconductor industry, the company serves six of the top 10 manufacturing equipment companies, four of the top 10 fabrication plants, and four of the top 10 packaging and testing facilities. While in the pharmaceutical industry in Taiwan, the company serves five of the top 10 companies in the country. TXOne Networks has a well-established brand name in the Taiwanese OT security market, and its products remain a top-of-mind choice among leading companies across various verticals.

As a result of its solid brand equity, the company was asked by SEMI, a global industry association representing the semiconductor and electronics industry, to contribute to the security standard SEMI E187, launched in 2022, a specification to secure semiconductor fab equipment, including operations and maintenance. The involvement of TXOne Networks in drafting the cybersecurity standard to improve the cybersecurity of the semiconductor industry underscores its ability to help companies implement their OT security strategy in line with global standards.

Conclusion

TXOne Networks stands out among OT security competitors in Taiwan because of its vertical-specific go-to-market strategy, flexible approach to better address customer needs, unwavering commitment to innovation, dedication to providing high-quality customer services, and a well-established brand reputation. This strategic combination has enabled the company to gain a competitive edge in the market and remain the top-of-mind choice among leading organizations in the country.

With its strong overall performance, TXOne Networks earns Frost & Sullivan’s 2023 Taiwan Competitive Strategy Leadership Award in the OT security industry.

What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy Leadership Award recognizes the company with a stand-out approach to achieving top-line growth and a superior customer experience.

Best Practices Award Analysis

For the Competitive Strategy Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Strategy Innovation

Strategy Effectiveness: Effective strategy balances short-term performance needs with long-term aspirations and overall company vision

Strategy Execution: Company strategy utilizes Best Practices to support consistent and efficient processes

Competitive Differentiation: Solutions or products articulate and display unique competitive advantages

Executive Team Alignment: Executive team focuses on staying ahead of key competitors via a unified execution of its organization's mission, vision, and strategy

Stakeholder Integration: Company strategy reflects the needs or circumstances of all industry stakeholders, including competitors, customers, investors, and employees

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

