FROST & SULLIVAN

FROST & SULLIVAN BEST PRACTICES AWARD

INFORMATION TECHNOLOGY / OPERATIONAL TECHNOLOGY SECURITY - GLOBAL

Company of the Year 2019

CLAROTY
Clarity for OT Networks

FROST & SULLIVAN
2019 BEST PRACTICES AWARD

Contents

Background and Company Performance

Industry Challenges

As the connected device and equipment landscape continues to grow, companies across sectors seek new ways to better secure and optimize their operational technology (OT) devices. Industrial control systems (ICS)—particularly the supervisory control and data acquisition (SCADA) systems used throughout the upstream and downstream operations lifecycle for industrial processes—are intrinsic to operations. Similarly, the use of smart OT devices in non-industrial buildings to improve the efficiency of building operations is on the rise. However, due to the rise of the Internet of Things (IoT) and the uptake of IoT technologies resulting in contractors' growing reliance on vendor remote access, Frost & Sullivan points out that the inherently non-secure nature of OT devices is further compromised. Outdated legacy software and hardware systems, weak authentication at the device level, employee error, and the presence of unprotected devices are among the typical entry points for cyber-adversaries to gain access to enterprises' networks.

Current automation systems are vulnerable to both targeted and non-targeted cybersecurity threats and attacks. Frost & Sullivan notes that any malicious presence detected, or security threat/high-stake changes made to OT devices, could result in the loss of lives and critical services, the destruction of property, and production downtime. Buildings in the healthcare, hospitality, finance, manufacturing, energy, utilities, and data center verticals are prime targets. As such, these security issues require real-time, constant threat monitoring of network traffic. Apart from the high-implied cost of cyber-attacks, some regulations also demand regular auditing of the systems by third-party service providers, thereby propelling the IT/OT Security market. However, Frost & Sullivan research suggests that the high complexity of the threat landscape and unclear return on investment (ROI) benefits are creating ambiguity hesitance among potential buyers.

Beyond security challenges, operational challenges also burden organizations. For instance, each enterprise typically has multiple siloed OT networks. As a result, there is no standard view of assets across an entire OT network environment, and traditional IT security monitoring products prove grossly insufficient on this front. Without a complete active inventory of assets on the network, it is impossible to monitor the behavior of its resources continually. Frost & Sullivan believes that vendors offering a technology platform that secures OT networks and provides an unmatched depth and breadth of OT visibility (without unnecessary alerts) will have the clear advantage needed to gain a leadership position in the market.

Frost & Sullivan's research also reveals that outsourcing of IT/OT security operations to managed security services (MSS) is a growing trend. Vendors respond by presenting subscription-based models to provide scalability and flexibility, enabling service alignment with end-user requirements. Market participants are focusing on building a comprehensive portfolio, providing end-users the ability to select modules best suited to their enterprise cybersecurity goals.

Notably, the smart building technology market for IT/OT security is in an early growth stage, primarily due to the limited awareness among enterprises for an integrated IT/OT security solution. However, Frost & Sullivan analysis predicts that enterprise adoption will improve significantly during the next three years to reach double-digit growth rates. Within a moderately fragmented market where vendors compete based on technological capabilities and experience, Frost & Sullivan expects rapid growth from regions such as Europe, the Middle East, and Africa (EMEA) and Asia-Pacific (APAC). The global IT/OT security for smart building technology market is poised to record a compounded annual growth rate (CAGR) of 37.0% from 2018 to 2022, as enterprises progressively recognize the cost impact of a cyberattack on buildings.[1]

Visionary Innovation & Performance and Customer Impact

Founded in 2014, Claroty is a leader in operational technology (OT) network protection. Headquartered in New York, United States (US) with supporting offices in Israel and Brazil, the company offers the only OT security solution that encompasses the entire spectrum of cybersecurity functions to its customers-namely to identify, detect, protect, and respond to threats. Its integrated and comprehensive platform provides industrial control networks with supreme and complete visibility of assets, high-level threat and anomaly detection, secure remote access, and risk assessments. In addition, the platform's secure remote access—a centralized management interface—expedites data integration with existing security systems to facilitate simple service deployments. By leveraging its elite team of researchers, engineers, and IT/OT cybersecurity experts, Claroty's 130 employees help industrial enterprises across 14 verticals to decrease the risk of cyberattacks.

Full-Spectrum and Unified Visibility Across Devices, Without Any Risk

Both industrial and non-industrial environments (such as the smart buildings technology segment) face difficulty when monitoring the range of assets on their network. The open architectures of OT systems, using standardized interfaces and connecting to both the Internet and internal corporate networks, results in exposure to third-party intrusions—a common attack vector—and massive disruption possibilities. Frost & Sullivan recognizes how Claroty's platform nicely fills these critical gaps by offering a fully integrated product suite enriched with advanced features to provide unparalleled depth, coverage, and scalability across a variety of domains.

Installed on a server or run as a virtual machine (VM), Claroty's continuous threat detection (CTD) software connects to a switched port analyzer (SPAN). After being plugged into the SPAN port, the CTD views the traffic and copies it—rather than asking questions to the assets on the network. As such, by leveraging deep packet inspection (DPI), Claroty does not leave a footprint on the industrial network; instead, the CTD safely monitors the IT/OT network traffic from the outside (i.e., passively). Since the platform works on a non-intrusive monitor mode, there is zero impact on a floater's existing critical ICS or OT systems.

[1] *Information Technology/Operational Technology (IT/OT) Security Convergence in the Smart Building Technology Market, Forecast to 2022* (Frost & Sullivan, July 2019)

Another valuable feature of CTD is that it automatically discovers, classifies, and profiles assets by more than just IP address, but also by the appropriate asset category (e.g., nested assets) and type of communication. In fact, an active asset inventory is built automatically, even before threat detection. Therefore, not only does Claroty's CTD profile the assets, but it also creates a deep profile of the network communication patterns (e.g., assets communicating over serial connections) and uses the information to generate a high-fidelity behavioral baseline model that characterizes legitimate traffic. Hence, the platform's unique network segmentation rapidly accelerates and reduces the cost of network segmentation projects by establishing baseline communications between assets in automatically designated virtual zones. As the system automatically tags assets with similar network traffic parameters into logical groups, CTD identifies the relationships between logical groups and generates granular communication policies. The policies assign permission levels to each zone, along with a specific level of trust to help the end-user understand the risk posed by every logical connection between the zones.

By leveraging artificial intelligence, Claroty's real-time CTD delivers advanced anomaly and signature-based detection for known and unknown threats. Its five detection engines generate different event baselines, and its machine learning (ML) alert algorithm correlates these events with patterns and behaviors on the network. Even though every change is logged in the system, only the highest fidelity alerts are delivered to the end-user for further review and investigation—improving both the user experience and security by eliminating the noise of unnecessary alerts that poses little or no risk. Enriched by Claroty's threat intelligence and furnished by Claroty's root cause analytics, Claroty's risk-based indicators and a proprietary scoring index contextualize and prioritize the ML-generated alerts in the user's queue. As a result, alerting sensitivities are customizable to the risk appetite of any enterprise. The Claroty platform's exciting new features also afford improved threat hunting and chain of events visibility through detailed alert scoring with contextual intelligence surrounding associated risks. A story graph visualizes the chain of events leading to alert generation, indicating relevant alerts and assets, alert severity, alert volume and more. Frost & Sullivan independent research concludes that Claroty clearly differentiates itself by delivering full-spectrum, unified visibility across IoT and OT devices at no risk to operations.

Delighting Customers With Dynamic Deployments

The advanced sensor-based architecture enables cost-effective deployments in remote, bandwidth or compute-constrained environments. As Claroty's solution requires no endpoint agents or endpoint configuration changes, there is no plant downtime for either installation or maintenance. It is deployable in many ways; from rack mount and DIN-rail form factors to hardened hardware and virtual appliances, container-based delivery models, embedded into select switches and routers, as well as within any partner's security infrastructure. System dashboards allow for status checks at each site, reducing the risk of user error during deploying, facilitating simple maintenance and driving rapid return on investment.

Strategic Partnerships Propel Global Growth

By entering partnerships with market-leading OT Equipment manufacturers and cybersecurity technology providers, Claroty strategically expands its technology integration ecosystem, enabling enterprises to leverage their current OT investments in technology, processes, and training. For example, Claroty collaborates with Schneider Electric — one of the largest OT equipment vendors — and Cisco, a global networking company. Furthermore, Claroty recently secured investments from leading OT equipment manufacturers, such as Rockwell Automation and Siemens. As these companies have the ability to truly influence the value chain as channel partners and customers, Clarity obtains a huge competitive advantage. Therefore, Frost & Sullivan applauds Claroty's strategic drive to gain these go-to-market partners who will support its global growth in the converged IT/OT security industry.

Claroty's Stellar Business Performance and Increased Market Penetration

Due to Claroty's industry-agnostic products, the company thrives in serving a heterogeneous mix of verticals with deployments in more than 20 countries across six continents. In 2019, Claroty accelerated in terms of growth and scalability. Strengthened by the recent appointment of former U.S. Navy Admiral Michael S. Rogers as Chairman of the Claroty Board of Advisors, the company sets the stage for further achievements in the field. In 2018, Claroty showcased its market understanding and competitive edge by its stellar financial performance due to the uptake of its technology. The company reported a 97% year-on-year growth in bookings and a 100% year-on-year increase in deals. According to Claroty, its overall headcount surged with 60% to support its penetration in 5 new verticals.

Conclusion

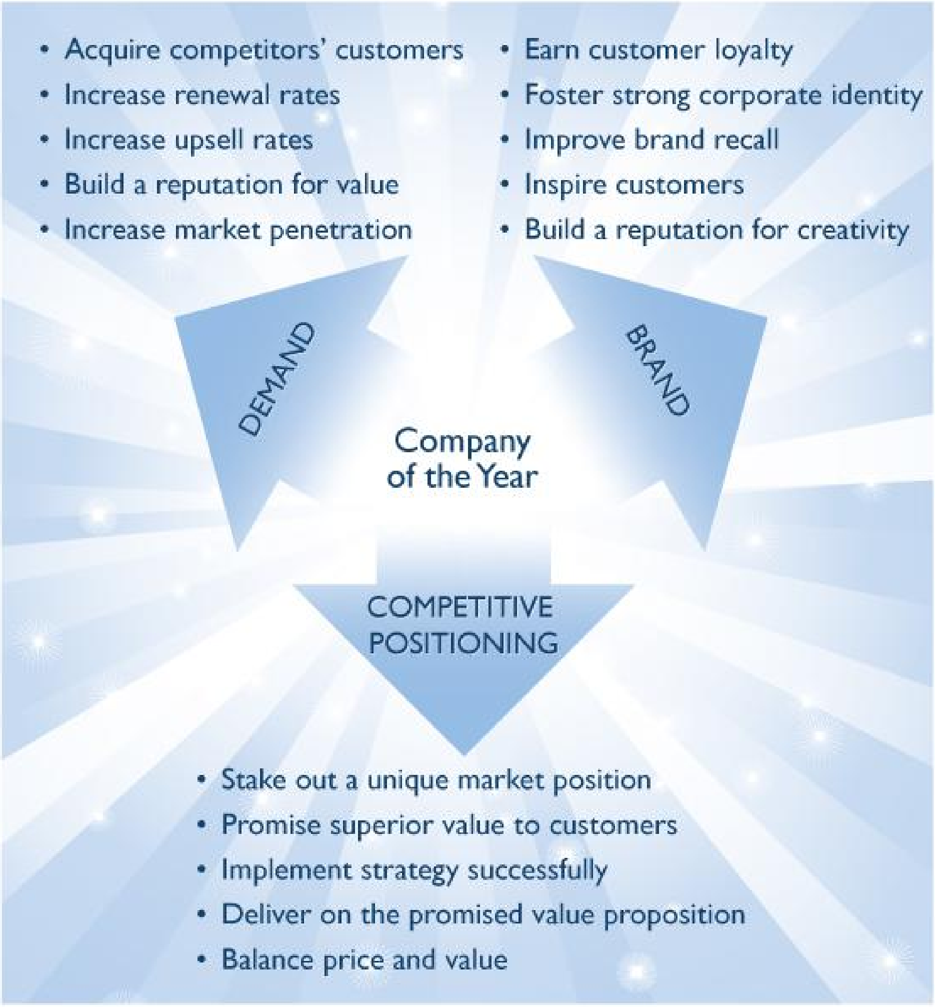
The rise in the digitalization of building operations and connected devices has led to automated work environments, ensuring safety, comfort, productivity, and operational efficiency for enterprises. However, the abundance of connected devices provides an expanded cyberattack surface that extends beyond IT networks to OT devices, increasingly targeting buildings, particularly in the healthcare, hospitality, finance, manufacturing, energy, utilities, and data center verticals.

Claroty's superior suite of industry-agnostic products provides unified visibility into industrial networks, enabling unparalleled cyberthreat protection, detection, and response for both IoT and OT devices across 14 verticals. Recent advancements of its continuous threat detection software combine extended coverage with faster deployment features and a new machine learning alert algorithm to offer rapid time-to-value – all without the distracting noise of unnecessary alerts. Frost & Sullivan analysis concludes that dynamic deployment, seamless integration, and remote access to enforce granular access policies all uncontestably cement the company's global position as a leader in the converged IT/OT security market.

With the range of integrations embedded in the platform, and the company's stellar business performance bolstered by its growth and scale, Claroty earns the 2019 Frost & Sullivan Global Company of the Year Award.

Significance of Company of the Year

To receive the Frost & Sullivan Company of the Year Award requires a market participant to demonstrate excellence in growth, innovation, and leadership. This excellence typically translates into superior performance in three key areas—demand generation, brand development, and competitive positioning—that serve as the foundation of a company's future success and prepare it to deliver on the 2 factors that define the Company of the Year Award: Visionary Innovation and Performance, and Customer Impact.


• Acquire competitors' customers
• Increase renewal rates
• Increase upsell rates
• Build a reputation for value
• Increase market penetration
• Earn customer loyalty
• Foster strong corporate identity
• Improve brand recall
• Inspire customers
• Build a reputation for creativity
DEMAND
BRAND
Company of the Year
COMPETITIVE POSITIONING
• Stake out a unique market position
• Promise superior value to customers
• Implement strategy successfully
• Deliver on the promised value proposition
• Balance price and value

Understanding Company of the Year

Driving demand, brand strength, and competitive differentiation all play critical roles in delivering unique value to customers. This three-fold focus, however, must ideally be complemented by an equally rigorous focus on Visionary Innovation and Performance to enhance Customer Impact.

Key Benchmarking Criteria

For the Global Company of the Year Award, Frost & Sullivan analysts independently evaluated two key factors—Visionary Innovation & Performance and Customer Impact—according to the criteria identified below.

Visionary Innovation & Performance

Criterion 1: Addressing Unmet Needs
Requirement: Implementing a robust process to continuously unearth customers' unmet or under-served needs, and creating the products or solutions to address them effectively

Criterion 2: Visionary Scenarios through Mega Trends
Requirement: Incorporating long-range, macro-level scenarios into the innovation strategy, thereby enabling "first-to-market" growth opportunity solutions

Criterion 3: Implementation of Best Practices
Requirement: Best-in-class strategy implementation characterized by processes, tools, or activities that generate a consistent and repeatable level of success.

Criterion 4: Blue Ocean Strategy
Requirement: Strategic focus on creating a leadership position in a potentially "uncontested" market space, manifested by stiff barriers to entry for competitors

Criterion 5: Financial Performance
Requirement: Strong overall business performance in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Impact

Criterion 1: Price/Performance Value
Requirement: Products or services offer the best value for the price, compared to similar offerings in the market.

Criterion 2: Customer Purchase Experience
Requirement: Customers feel they are buying the most optimal solution that addresses both their unique needs and their unique constraints.

Criterion 3: Customer Ownership Experience
Requirement: Customers are proud to own the company's product or service and have a positive experience throughout the life of the product or service.

Criterion 4: Customer Service Experience
Requirement: Customer service is accessible, fast, stress-free, and of high quality.

Criterion 5: Brand Equity
Requirement: Customers have a positive view of the brand and exhibit high brand loyalty.

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan analysts follow a 10-step process to evaluate Award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

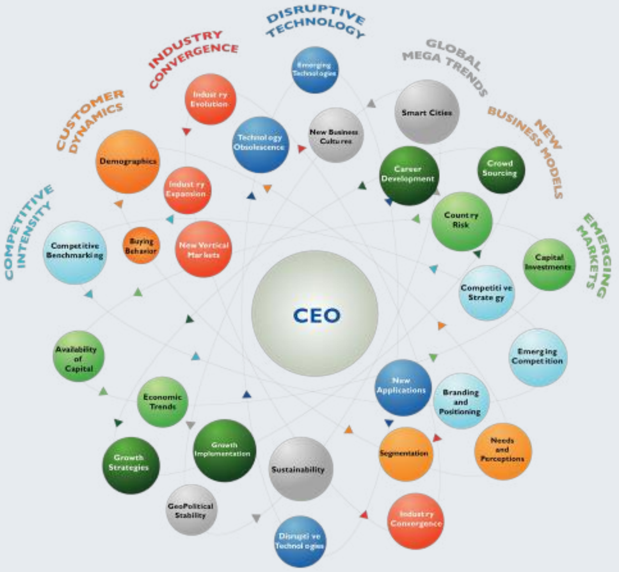
	STEP	OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	• Interview thought leaders and industry practitioners • Assess candidates' fit with best-practice criteria • Rank all candidates	Matrix positioning of all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	• Confirm best-practice criteria • Examine eligibility of all candidates • Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	• Brainstorm ranking options • Invite multiple perspectives on candidates' performance • Update candidate profiles	Final prioritization of all eligible candidates and companion best-practice positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	• Share findings • Strengthen cases for candidate eligibility • Prioritize candidates	Refined list of prioritized Award candidates
6	**Conduct global industry review**	Build consensus on Award candidates' eligibility	• Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates	Final list of eligible Award candidates, representing success stories worldwide
7	**Perform quality check**	Develop official Award consideration materials	• Perform final performance benchmarking activities • Write nominations • Perform quality review	High-quality, accurate, and creative presentation of nominees' successes
8	**Reconnect with panel of industry experts**	Finalize the selection of the best-practice Award recipient	• Review analysis with panel • Build consensus • Select winner	Decision on which company performs best against all best-practice criteria
9	**Communicate recognition**	Inform Award recipient of Award recognition	• Present Award to the CEO • Inspire the organization for continued success • Celebrate the recipient's performance	Announcement of Award and plan for how recipient can use the Award to enhance the brand
10	**Take strategic action**	Upon licensing, company able to share Award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess Award's role in future strategic planning	Widespread awareness of recipient's Award status among investors, media personnel, and employees

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation, and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.