2018 North American OT Network Protection Platform Entrepreneurial Company of the Year Award
## Contents

Background and Company Performance ................................................................. 3  
  *Industry Challenges* ......................................................................................... 3  
  *Entrepreneurial Innovation and Customer Impact* ........................................... 3  
  *Conclusion* ......................................................................................................... 7  

Significance of Entrepreneurial Leadership .......................................................... 8  
Understanding Entrepreneurial Leadership ............................................................ 8  
  *Key Benchmarking Criteria* .............................................................................. 9  

Best Practices Award Analysis .............................................................................. 9  
  *Decision Support Scorecard* .............................................................................. 9  
  *Entrepreneurial Innovation* ............................................................................. 10  
  *Customer Impact* ............................................................................................ 10  
  *Decision Support Matrix* .................................................................................. 11  


The Intersection between 360-Degree Research and Best Practices Awards ........... 13  
  *Research Methodology* ..................................................................................... 13  

About Frost & Sullivan ............................................................................................ 13
Background and Company Performance

Industry Challenges

In light of the world’s increasingly connected industrial landscape, companies across sectors seek new ways to better secure and optimize their operational technology (OT) networks. Industrial control systems (ICS), particularly the supervisory control and data acquisition (SCADA) systems that are used throughout the upstream and downstream operations lifecycle to run industrial processes are intrinsic to operations. However, due to the inherently non-secure nature of OT networks (e.g., unprotected ICS protocols, weak authentication) that developed with the rise of the Industrial Internet of Things (IIoT) where OT networks have become increasingly connected and reliance on vendor remote access by contractors has grown, these automation systems are now vulnerable and at risk of both targeted and non-targeted cyber-security threats and attacks. Frost & Sullivan points out that any malicious presence detected or security threat/high-stake changes made to OT networks represent serious risks that could result in loss of lives and critical services, destruction of property, and downtime of an entire plant. Frost & Sullivan notes that these security issues, therefore, require real-time, constant threat monitoring of ICS network traffic.

Beyond security challenges, operational challenges burden organizations. For instance, each manufacturer typically has multiple OT networks that are siloed. As a result, there is no common view of assets across an entire OT network environment, and traditional IT security monitoring products prove grossly insufficient on this front. Part of the challenge stems from the fact that without a complete active inventory of assets on the network, there is no way to constantly monitor the behavior of their resources.

Frost & Sullivan believes that vendors that offer a technology platform that can not only secure OT networks, but also provide deep visibility into them so industrial companies will know what assets are on the network and efficiently address both security and operational challenges, will have the clear advantage needed to gain a leadership position in the market.

Entrepreneurial Innovation and Customer Impact

Market Disruption

Strongly committed to helping cyber security professionals and shop floor teams (engineers and operators) protect their ICS, SCADA, and IIoT assets, Claroty, founded in 2014, offers a single holistic OT security platform. The company, leveraging its elite team of researchers, engineers, and IT/OT cyber security experts, has effectively matched its capabilities to the needs of OT environments through a unique combination of cyber-security products: Continuous Threat Detection, Secure Remote Access, and Enterprise Management Console.
Continuous, Non-intrusive Threat Detection and Risk Assessment Software

Lacking full visibility, many industrial environments face difficulty when it comes to monitoring the varied range of assets on their network. Frost & Sullivan observes how Claroty successfully addresses this issue.

Claroty’s continuous threat detection software, installed on a server or run as a VM, connects to a SPAN port on a switch. The first thing continuous threat detection does after being plugged into the SPAN port is view the traffic and take a copy of it - rather than ask questions to any of the assets on the network. As such, by using deep packet inspection (DPI), Claroty does not leave a footprint on the industrial network; instead, it safely monitors the ICS 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.

What makes the continuous threat detection software both innovative and appealing is that it automatically discovers, classifies, and profiles the assets not just by IP address, but also by appropriate asset category (e.g., nested assets) and type of communication. In fact, an active inventory of assets is automatically built, even before getting to threat detection. Therefore, not only does it profile the assets that are out there, but 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.

In other words, what Claroty’s customers enjoy the most is a quick, complete, and deep real-time view of their OT networking infrastructure that reveals what type of assets they have on their industrial network (asset discovery addresses internal audit requirements), and to whom and how these assets are speaking internally as well as externally. Security professionals get a unified view of the assets across OT networks that differ from each other in automation equipment and communication protocols used, and are separately managed by their respective contractors. The resulting volume of actionable insights derived can be used to uncover network configuration issues, vulnerable assets, and insecure connections (to name just a few issues), and give customers the power to proactively fix them.

Another major value proposition that Claroty provides is risk assessment. Customers can now understand what is on the network and just how risky certain assets and connections are. By highlighting the high-risk or vulnerable assets/insecure connections, customers can assess the security posture and focus their efforts on securing those assets on their connected infrastructure.

Frost & Sullivan applauds Claroty for demonstrating powerful entrepreneurial innovation that now enables industrial companies to gain deep, unified visibility into OT networks, as well as to discover and monitor those assets that need immediate attention.
Competitive Differentiation & Market Gaps

Once the software has learned the network behavior and built a baseline model, it then provides continuous real-time monitoring that will highlight suspicious/malicious activity and critical changes on the network. If it detects suspicious behavior (i.e., any violation of or deviation from the baseline model), context-rich alerts are generated and sent to the security and control teams.

Superior Protocol and Vendor Support

Frost & Sullivan considers the industry best practice implemented by Claroty as its ability to support a wide range of protocols — IP network protocols, industrial network protocols — and a number of major ICS vendors. A clear differentiator for Claroty from a product standpoint is the level at which this company analyzes the protocols; the information it can pull out is far better than what is achievable from other competing products. Other solutions on the market may be able to find an anomaly or give a bunch of alerts for every anomaly found (i.e., polling), yet Frost & Sullivan feels that Claroty is strikingly different, as its product can discern what kind of OT industrial conversations take place, rather than simply offering information (such as IP address A is talking to IP address B, three times a day).

Some of the alerts generated by Claroty’s products are for configuration upload/download, mode change, and firmware upgrade notice, but where the company nicely fills the market gap is in providing context-rich alerts that give security administrators an understanding about what happened and what assets were tampered with. This helps them to effectively respond in real-time and maintain the safety and reliability of industrial processes. The alerts are rich in context to the extent of displaying the exact code change that was made to a controller, thereby making it simpler for the security and controls team to restore the right settings.

Analyzing protocols at a deep level also means that Claroty can spot threats early in the kill chain — before the attack gets underway — when the attacker is getting the footprint on the network. This is due to the fact that Claroty is watching the whole network. In essence, as soon as an attacker tries to get a footprint on a server or does some reconnaissance on the network, Claroty will detect the activity as anomalous traffic right away and provide the SOC with context-rich alerts about what is going on or what kind of logic change was made on a controller. The differentiator, again, between companies that do polling versus Claroty, is that Claroty sees the whole attack life cycle and spots something early on by deeply analyzing the protocols.
Secure Remote Access

ICS are now based on open architectures using standardized interfaces and are connected to both the Internet and internal corporate networks. For instance, OT networks on offshore drilling ships are not air-gapped and are connected directly with the rig contractor’s main IT network, which is connected to the Internet. Essentially, they have begun to expand and cross traditional boundaries (i.e., internal networks), leaving them exposed to third-party intrusions — a common attack vector — and massive disruption possibilities.

Keeping in mind that unmonitored external users such as third-party workers, contractors, and remote employees can induce a threat to OT networks, Claroty offers Secure Remote Access, an access policy enforcement and control product. By connecting through this solution, not only is a direct interaction between external users and industrial assets eliminated, but authentication of all external users is established before they can perform any software upgrades, periodic maintenance, and other support activities on assets within ICS networks. Secure remote access enables network administrators to define policies that establish which individuals can enter (even at what time), which user needs access from a policy perspective, and what industrial assets they should have access to. Finally, it shows them only the devices they are allowed to touch. The administrator can watch these remote access sessions live and can stop/break the connection if they sense questionable activity. In addition, they can record the sessions (video recording of remote sessions) to return to later and audit. Overall, network administrators can safeguard the OT networks from external users.

Customer Impact

Security Teams Gain Real-time Situational Awareness Using Enterprise Management Console

With Claroty’s products deployed in multiple sites across the globe, the company focuses on working closely with its customers to ensure an enhanced service experience through its Enterprise Management Console which consolidates all data generated by its products. Claroty believes visual representation of performance is a powerful element of success. Therefore, it has built the console as a well-defined, intuitive, centralized management interface that ensures a holistic view of assets, activities and alerts, and access controls. Being suitable for SOC deployments, Enterprise Management Console was designed with interactive dashboards, so that the security team can easily compare multiple scenarios, visualize them fully, and understand the enterprise industrial control system security posture more thoroughly. Integration with security tools enables the console to send alert data to SIEM (Radar, Splunk), log management (Alert Logic, LogRhythm), and security analytics products (RSA Netwitness).
Support from Leading Investors Enhance Team Size, Working Capital, and Customer Engagement

With Fortune 500 companies as its customers Claroty has production deployments across 6 continents and 9 industry verticals, including oil and gas, electric utilities, water, chemical, manufacturing, and mining industries. Founded in 2014, the company draws its heritage from Team8 Security Foundry and is one of the more well-funded start-ups with a total investment of $32 million and support from investors such as BESSEMER, Innovation Endeavors, Red Dot, and MITSUI, to name a few.

Strategic Partnerships Help Secure Target Accounts and Provide Global Reach

Claroty has two of the largest industrial control vendors (Rockwell Automation and Schneider Electric) and one of the largest networking companies in the world (Cisco) as its strategic partners - and not just as marketing relationships. These companies chose Claroty from a competitive selection process and are building a business (a whole managed security services) around Claroty’s technology platform. Frost & Sullivan points out that this success is a clear differentiator that none of the other vendors in this space can claim.

Conclusion

Through its single, holistic, enterprise-class OT security platform comprising Continuous Threat Detection, Secure Remote Access, and an Enterprise Management Console, Claroty ramped up its capabilities to deliver unmatched product value and consolidate its position in the industrial cybersecurity market. Leveraging its industry expertise and technical knowledge in building the most complete OT security platform that supports all major ICS equipment vendors’ open and proprietary protocols, Claroty provides engineers, operators, and cyber security professionals with the deepest visibility into their OT networks and full protection by performing continuous, real-time monitoring.

With the platform’s benefits ranging from context-rich alerts, non-intrusive monitoring, access policy enforcement and control, and agentless deployment to a visually appealing centralized management interface, Frost & Sullivan firmly believes that Claroty has clearly enhanced the value proposition for its customers. With its strong overall performance, Claroty has earned the 2018 Frost & Sullivan Entrepreneurial Company of the Year Award.
Significance of Entrepreneurial Leadership

Ultimately, growth in any organization depends upon customers purchasing from a company and then making the decision to return time and again. In a sense, then, everything is truly about the customer—and making those customers happy is the cornerstone of any long-term successful innovation or growth strategy. To achieve these dual goals (customer engagement and growth), an organization must be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Entrepreneurial Leadership

Demand forecasting, branding, and differentiation underpin an entrepreneurial company’s journey toward forming deep relationships with customers and permanently altering the market with their actions.
Key Benchmarking Criteria
For the Entrepreneurial Company of the Year Award, Frost & Sullivan analysts independently evaluated two key factors—Entrepreneurial Innovation and Customer Impact—according to the criteria identified below.

Entrepreneurial Innovation
- Criterion 1: Market Disruption
- Criterion 2: Competitive Differentiation
- Criterion 3: Market Gaps
- Criterion 4: Blue Ocean Strategy
- Criterion 5: Passionate Persistence

Customer Impact
- Criterion 1: Price/Performance Value
- Criterion 2: Customer Purchase Experience
- Criterion 3: Customer Ownership Experience
- Criterion 4: Customer Service Experience
- Criterion 5: Brand Equity

Best Practices Award Analysis for Claroty
Decision Support Scorecard
To support its evaluation of best practices across multiple business performance categories, Frost & Sullivan employs a customized Decision Support Scorecard. This tool allows our research and consulting teams to objectively analyze performance, according to the key benchmarking criteria listed in the previous section, and to assign ratings on that basis. The tool follows a 10-point scale that allows for nuances in performance evaluation. Ratings guidelines are illustrated below.

The Decision Support Scorecard is organized by Entrepreneurial Innovation and Customer Impact (i.e., These are the overarching categories for all 10 benchmarking criteria; the definitions for each criterion are provided beneath the scorecard.). The research team confirms the veracity of this weighted scorecard through sensitivity analysis, which confirms that small changes to the ratings for a specific criterion do not lead to a significant change in the overall relative rankings of the companies.
The results of this analysis are shown below. To remain unbiased and to protect the interests of all organizations reviewed, we have chosen to refer to the other key participants as Competitor 2 and Competitor 3.

<table>
<thead>
<tr>
<th>Measurement of 1–10 (1 = poor; 10 = excellent)</th>
<th>Entrepreneurial Innovation</th>
<th>Customer Impact</th>
<th>Average Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entrepreneurial Company of the Year</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claroty</td>
<td>8.5</td>
<td>9.5</td>
<td>9.0</td>
</tr>
<tr>
<td>Competitor 2</td>
<td>8.0</td>
<td>8.0</td>
<td>8.0</td>
</tr>
<tr>
<td>Competitor 3</td>
<td>7.5</td>
<td>6.5</td>
<td>7.0</td>
</tr>
</tbody>
</table>

**Entrepreneurial Innovation**

**Criterion 1: Market Disruption**
Requirement: Innovative solutions that have genuine potential to disrupt the market, obsoleting current solutions and shaking up competition

**Criterion 2: Competitive Differentiation**
Requirement: Deep understanding of both current and emerging competition to create and communicate strong competitive differentiators in the market

**Criterion 3: Market Gaps**
Requirement: A clear understanding of customers’ desired outcomes, the products that currently help them achieve those outcomes, and where key gaps may exist

**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: Passionate Persistence**
Requirement: A deep belief in the “rightness” of an idea and a commitment to pursuing it despite seemingly insurmountable obstacles

**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.

**Decision Support Matrix**

Once all companies have been evaluated according to the Decision Support Scorecard, analysts then position the candidates on the matrix shown below, enabling them to visualize which companies are truly breakthrough and which ones are not yet operating at best-in-class levels.
## 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.

<table>
<thead>
<tr>
<th>STEP</th>
<th>OBJECTIVE</th>
<th>KEY ACTIVITIES</th>
<th>OUTPUT</th>
</tr>
</thead>
</table>
| 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 recipient | 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 is 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.

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.