Industrial Networks Secured

Our Mission

Claroty was conceived to secure and optimize OT networks that run the world's most critical infrastructures.
Claroty empowers the people who run and protect industrial control systems to make the most of their OT networks. By discovering the most granular elements, extracting the critical data, and formulating actionable insights, Claroty provides extreme visibility and brings unparalleled clarity to OT networks.

Your Result

Better security, efficiency and integrity for your critical OT environments.

www.claroty.com

CLAROTY
Clarity for OT Networks

Case Study
Oil & Gas

Forward

The oil and gas industry has long been in the crosshairs of ICS\SCADA cyber security threats. These advanced automation networks, collectively known as operational technology, or OT networks, are used throughout the entire upstream and downstream operations lifecycle. The extensive use of these automation systems significantly increases productivity, but at the same time it provides an additional attack surface that threat actors can leverage to inflict material harm.

This document focuses on the offshore exploration drilling sub-segment within the upstream oil and gas operations which is executed by rig contractors for exploration and production (E&P) companies. The rapidly changing liability landscape in offshore drilling, combined with increased recognition of cyber risk, is driving E&P companies to compel rig contractors to implement sound cyber security programs on their vessels as a prerequisite to a drilling contract. This in turn has created an equally strong business imperative for rig contractors to develop cyber security policies and procedures and to seek solutions that align with the unique needs of their OT systems.

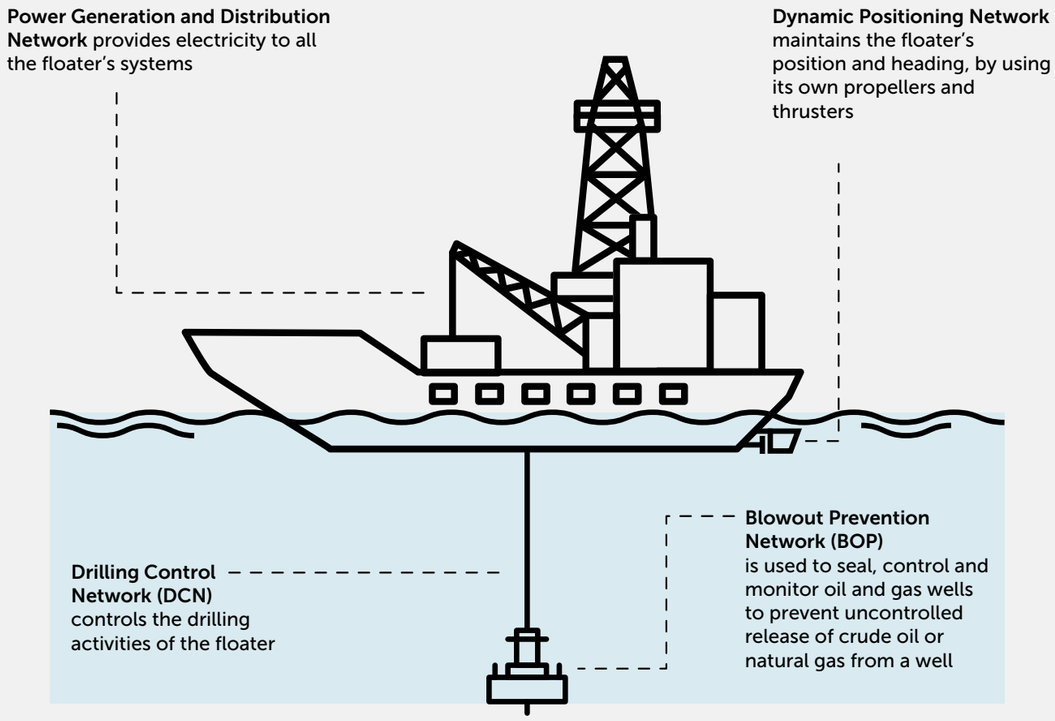
Claroty was conceived to secure and optimize operational networks running critical processes like the multiple integrated OT systems that offshore drilling vessels rely upon. Therefore, Claroty was the ideal partner for a rig contractor that sought not only to comply with E&P contractual requirements, but to take a leading role in transforming the cyber security posture of its vessels.

In this case study, we provide a detailed analysis of the unique offshore drilling OT attack surfaces and operational challenges, and walk through one of Claroty's offshore installations. This concrete example will serve to illustrate the broader cyber security and operational challenges that characterize the oil and gas industry.

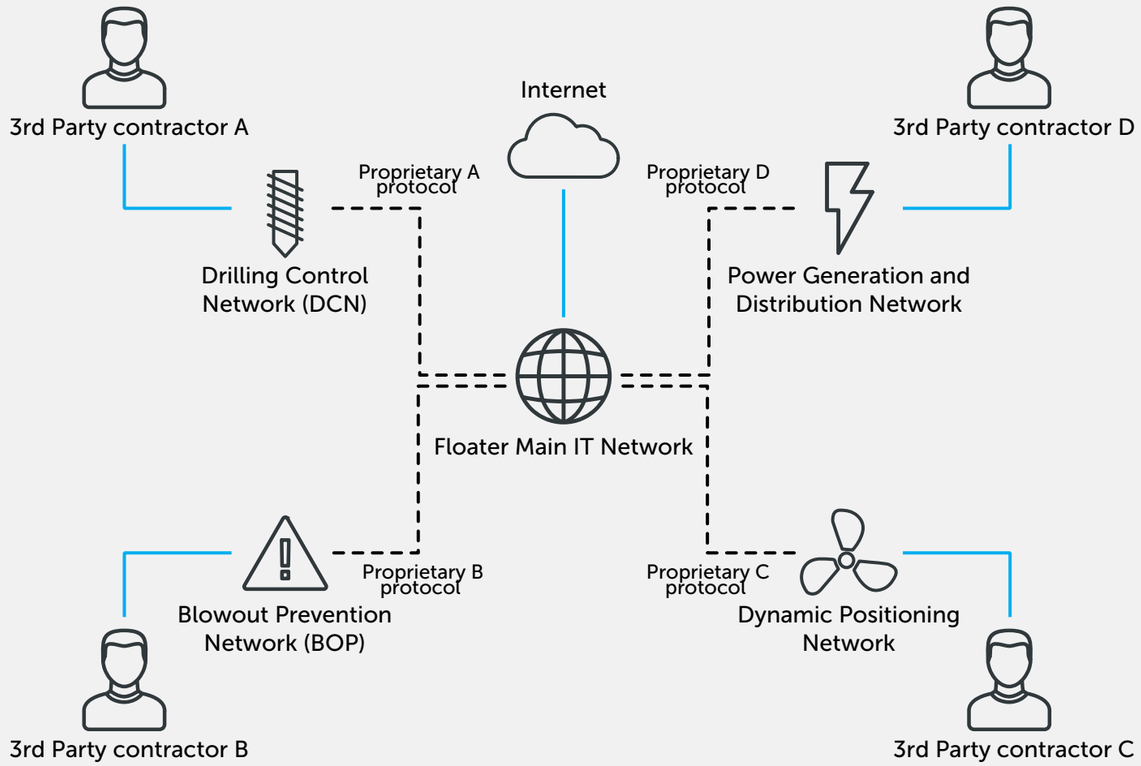
Offshore Rigs Overview

Mobile Offshore Drilling units (MODUs), used in the exploration and development of wells, are divided into Jack-ups that reside in shallow water sea beds and floaters (drilling ships and semisubmersibles) for mid and deep water drilling. Standard drilling ship and semisubmersibles typically include four major independent OT networks that are each managed by an external contractor and differ from each other in automation equipment and communication protocols utilized.

Floater Systems Overview



Floater Network Diagram



Security and Operational Challenges

The fragmentation and management of the floaters' OT networks causes the following structural security vulnerabilities:

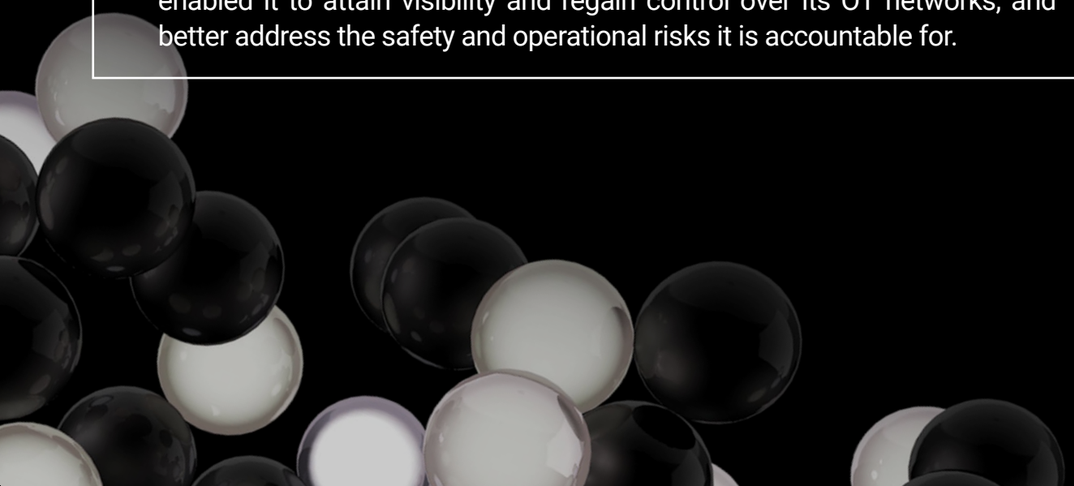
- Remote access required by the network contractors for maintenance activities introduces a new attack surface. Compromising a privileged third-party account to gain an initial foothold on the network is a common attack vector that has been utilized numerous times in targeted attacks.
- Further, the drilling ships' OT networks are not air-gapped. They are connected directly with the rig contractor's main IT network which is connected to the Internet.

It is clear that these structural vulnerabilities pose a significant risk. However, this risk cannot be soundly managed by the rig contractor for two reasons:

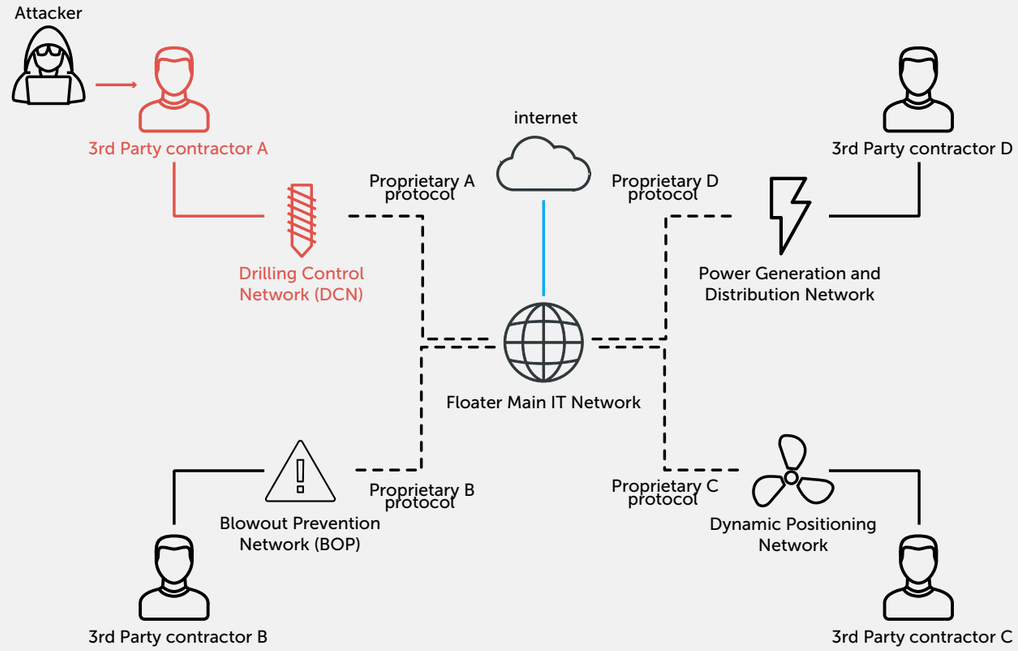
Each network is separately managed by its respective contractor in a complete silo. Therefore, there is no unified view of all assets across the entire OT network environment.

From the technology perspective, traditional IT security monitoring products do not provide visibility into the entire scope of proprietary OT protocols that are utilized by the assets throughout the floater's networks.

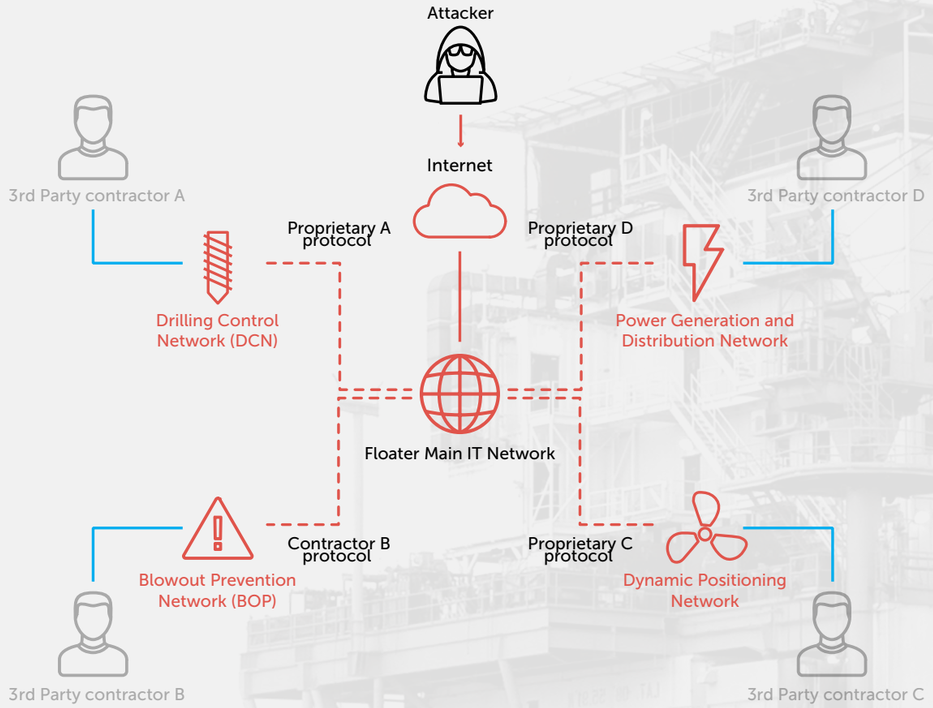
Acknowledging these challenges, the rig contractor sought a solution that enabled it to attain visibility and regain control over its OT networks, and better address the safety and operational risks it is accountable for.



OT Network Attack 1: Compromise the 3rd Party Contractor



OT Network Attack 2: Compromise the Floater IT Network



Claroty Solution

Preparatory Steps

OT Contractor Approval
The external management of the OT networks requires a preliminary approval stage. This includes rigorous testing in each vendor's lab to validate that the Claroty platform would not cause any operational disruption.

Claroty has undergone this process with all of the Drillship OT Contractors: NOV (for Siemens and Rockwell equipment), ABB and Kongsberg.

OT Network / Components	Drilling Control	Blowout Prevention	Dynamic Positioning	Power
Contractor	National Oilwell Varco (NOV)	National Oilwell Varco (NOV)	Kongsberg	ABB
Automation Vendor	Siemens	Rockwell	Kongsberg	ABB
Protocols	S7	AAdvance Ethernet\IP –CIP Modbus	Kongsberg Proprietary Protocol	MMS Satbus
Networking Vendor	Siemens	Hirschman	Cisco	Moxa

Deployment Process - Network Infrastructure Assessment

The Claroty platform can be deployed on top of any networking infrastructure. However, Claroty's recommended best practice is to connect to managed switches capable of relaying replicated traffic over a SPAN port. In this case, the DCN and BOP networks had managed switches prior to our arrival. Unmanaged switches in the power network were replaced based on the OEM's recommendation.

Passive monitoring is executed by connecting to SPAN ports on managed switches. This configuration replicates all the traffic these switches relay. When assessing the network to determine which switches to tap, the following considerations are made:

Top priority: Coverage of all traffic that directly involves level one assets (PLCs), including all connections of PLCs with level two (engineering workstations, HMIs) and above (various network servers). It is paramount that all traffic that directly impacts physical process is replicated and monitored.

Secondary priority: Following the completion of level-one communication coverage, the assessment team searches for level-two and-above, which includes strategic switches such as intersection points between network segments and working zones. A common example is the intersection point between the IT and OT networks.
The number of monitored switches is derived from the network topology. A network that features a main switch that aggregates all the traffic can be monitored from this single point. In a network that is more segmented, or features independent level one clusters, Claroty will port-mirror each of the relevant switches. The guideline is to balance between maximum coverage and minimum redundant traffic.

The replicated traffic that the SPAN port relays can be pushed through the existing network wiring. However, Claroty's recommended best practice is to have this data sent through dedicated cabling for the following reasons:

- Physically decoupling the replicated traffic ensures that there is zero impact on the actual traffic.
- Switches, by design, treat SPAN traffic as low priority when there are bandwidth constraints. Routing the monitored traffic to a dedicated physical route ensures that it is always prioritized, ensuring full real-time visibility.

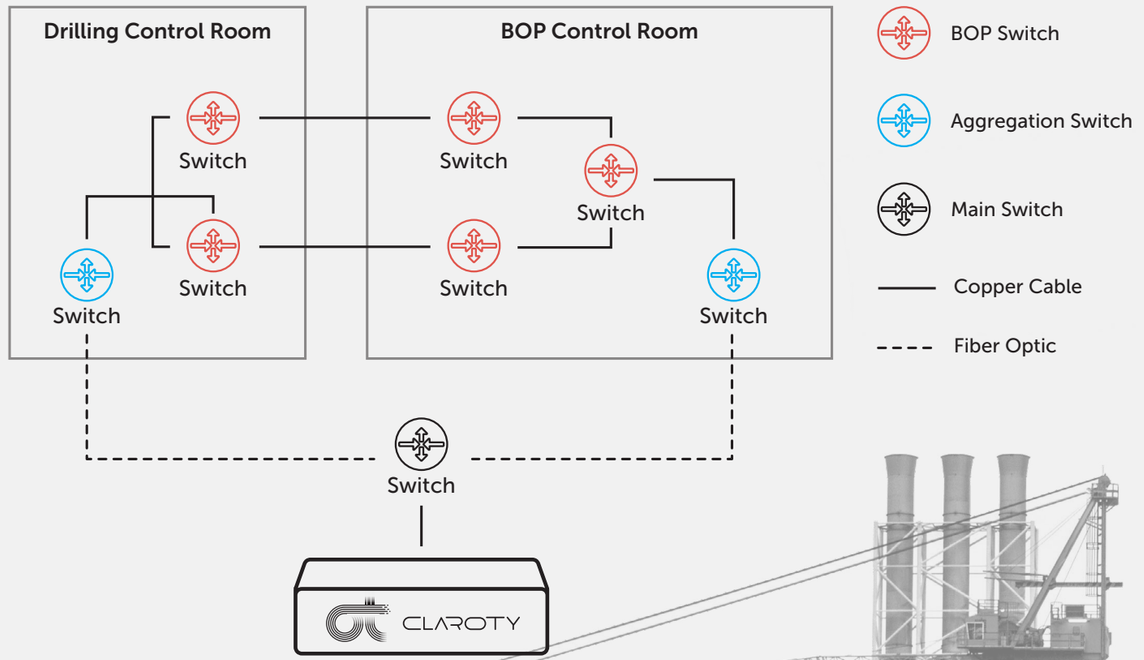
Let us see how Claroty has implemented these concepts in the drilling ship's BOP network (other networks were all subject to similar process):

The BOP network features a ring topology with five SPAN-configured switches in two physical locations (see diagram). There are three switches in the BOP control room and two in the drilling control room.

In order to relay the replicated traffic to the Claroty appliance, each group was connected to a nearby aggregation switch by a copper cable–the default choice for short distance communication.

A fiber optic cable is drawn from each aggregation switch to a main switch that relays the entire aggregated traffic to Claroty virtual appliance.

BOP Network Diagram



Deployment Process - From Training to Operational Mode

Real Time Network Topology

Initially, Claroty is configured to run in training mode. During this time it learns the networks' standard behavior and establishes a comprehensive behavioral baseline. This learning period enables the Claroty team to review aggregated findings with the customer and to share immediate insights. These insights cover various aspects, from pure security findings such as insecure remote connections, inadequate segmentation or week passwords, to various network misconfigurations that can impact operational workflow.

Network Behavior

Claroty discovers network assets (PLC, HMI, engineering stations and networking gear), gathers detailed data about each asset and profiles the communication patterns between assets each time the asset communicates on the network. Different assets generate traffic in varying time intervals depending on the specific function and environment. The common timeframe that is required for the entire set of OT assets to generate their routine traffic is approximately 2-3 weeks.

Anomalies Detection

Once the training mode is completed, Claroty shifts into operational mode where it raises an alert when it detects deviations from the baseline, critical changes (such as PLC configuration download or mode change) or distinct malicious activity. All OT network data is now visible and controlled from a single screen, enabling the rig contractor to track changes and respond to security and operational alerts.

End-to-End Security

During the learning period it is important to acknowledge the possibility that the environment might be already compromised. The Claroty deployment team ensures that any malicious presence is detected and eliminated, so that it is not incorporated into the baseline.

Deployment Process - Connect to Security Operation Center

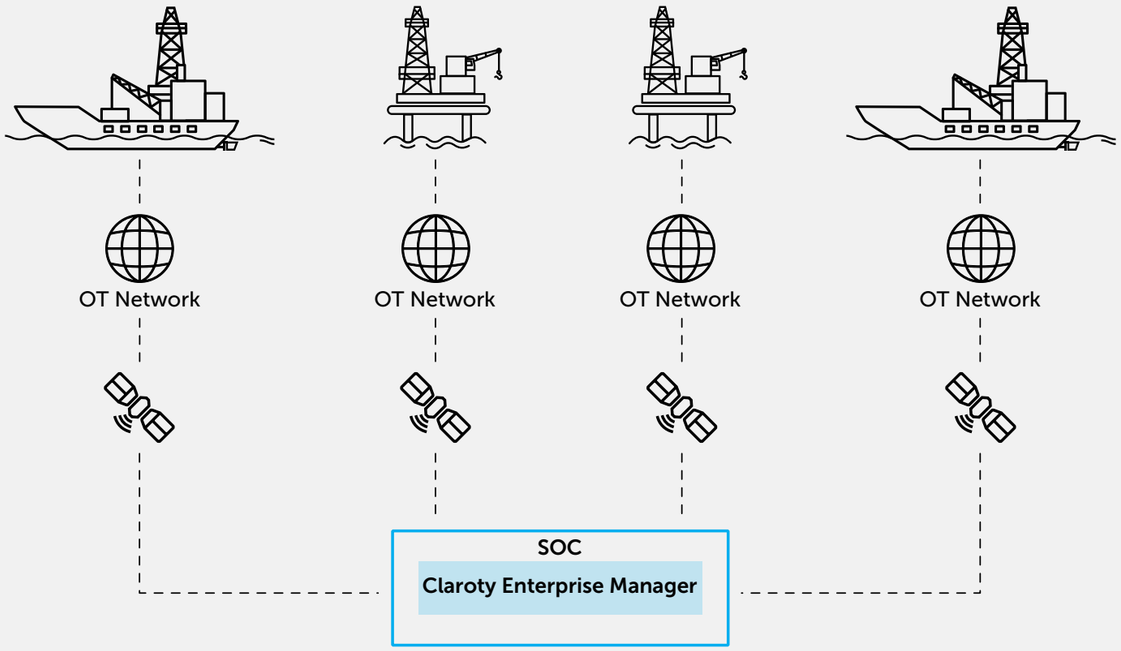
The final deployment step is to extend the successful on-site installation to a central site management interface, where the customer can gain full view of the security posture across multiple vessels.

The various vessels on the rig contractor 's fleet communicate with the onshore HQ via satellite connection. To provide a consolidated multi-site view, Claroty runs on top of the existing satcom network. Claroty utilizes a proprietary approach to overcome two important satcom constraints – relatively low-bandwidth and frequently dropped connections.

The data Claroty generates on site is continuously replicated and sent over SSH through the existing satellite connection to the Claroty Enterprise Manager residing in the rig contractor's onshore SOC.

Claroty Enterprise Manager is a central management console deployed in the SOC that provides a single aggregation and management interface across multiple remote sites.

Vessels connected to Enterprise Manager



End Result - Post Deployment Status

Onshore Secure Operations Center

24x7x365 continuous monitoring solution on several drilling ships around the globe

Advanced Security Monitoring & Detection System

Real-Time Monitoring Console

Secure Remote Access (for Vendors)

Customer Quotes:

"The technology that Claroty has provided within their software applications, has given us visibility into ICS networks that never before existed."

"Claroty solutions have placed us at the forefront within our industry, by proactively monitoring our ICS networks in real time and providing controlled, accountable and secure remote access for our system vendors."

"The solutions that Claroty has provided to us, are the tools that we were lacking to verify/enforce compliance with our ICS policies and procedures."