CLAROTY

SOLUTION BRIEF

INDUSTRIAL CYBERSECURITY FOR OIL & GAS

How Claroty empowers oil & gas companies to drive resilience by protecting all cyber-physical systems (CPS) in their operational technology (OT) environments.

PART I: Inside the Industrial Cybersecurity CHALLENGE in Oil & Gas

The sector is facing complex economic, environmental, and geopolitical conditions

- Global Fuel Shortages
- Volatile Barrel Prices
- Source Depletion
- Sustainability Needs
- Geopolitical Tensions

These conditions are motivating many companies to accelerate digital transformation

Automation

Rigs, refineries, and pipelines are replacing once-manual tasks with computerized automation, precision drilling, and other key systems to increase efficiency, safety, and uptime.

IT/OT Connectivity

Cloud migrations and remote work are extending connectivity from IT to OT via MES, remote maintenance, and ERP solutions to improve productivity, streamline audits, and enhance control.

Cyber-Physical Systems (CPS)

All oil & gas segments are embracing Industry 4.0 by augmenting their already-automated, connected OT environments with more CPS to boost throughput while lowering costs.

Digital transformation is inadvertently exposing oil & gas operations to cyber attacks

Most oil & gas companies still rely considerably on aging OT infrastructure with legacy (and thus unpatched, unsecured) systems. The challenge is that the cost of updating equipment – as well as the significant downtime that that often requires – in pipelines, refineries, and offshore facilities, among others, is typically more than the expected commercial output of the life of the facility. These conditions can make updates or replacements tough to justify.

At the same time, the sector continues to embrace digital transformation – resulting in legacy systems becoming increasingly intertwined with new, internet-connected technologies and cyber-physical systems (CPS). This ever-growing connectivity is inadvertently expanding the attack surface for many oil & gas companies, thereby exposing their OT infrastructure to cyber threats. This unfortunate reality has repeatedly manifested in the form of ransomware and other attacks that exploit security weaknesses in the CPS on which the availability, integrity, and safety of oil & gas operations and infrastructure rely.

Governments are increasingly urging and requiring oil & gas companies to secure OT

The NotPetya, Colonial Pipeline, and ARA Refinery ransomware attacks are merely a few of the seemingly countless and highly disruptive cybersecurity incidents that have affected oil & gas in recent years. Upticks in the frequency and impact of such incidents has since elicited robust responses from governments globally in the form of new regulations that encourage – or, in many cases, mandate – that oil & gas companies take action to secure their CPS and OT infrastructure. Key regulations include:

NIS2 Directive (EU)

TSA Directive (US)

The SOCI Act (Australia)

CISA CPGs (US)

Since OT is distinctly different from IT, securing OT requires a different approach

OT environments – and the CPS that underpin them – in all segments of the oil & gas sector are fundamentally different from their IT counterparts, which is why securing OT requires a unique, nontraditional approach. Some of these differences include:

	Purpose	Top Priorities	Typical Composition	Patching Frequency	Compatibility
IT:	*Control the Flow of Information*	*Confidentiality, Integrity, Availability*	✓ ✓ ✓ *Standard Protocols & IT Systems*	*Very Frequent*	*Compatible with IT Security Tools*
OT:	*Control Physical Processes*	*Safety, Availability, Reliability*	? ? ? *Proprietary Protocols & Legacy OT Systems*	*Relatively Rare*	*Incompatible with IT Security Tools*

PART II: Introducing the Industrial Cybersecurity SOLUTION for Oil & Gas

The Claroty Approach to Securing OT: Key Principles for Oil & Gas Companies

Recognizing that securing the OT environments that underpin oil & gas operations can be a complex and challenging endeavor, Claroty has tailored our industrial cybersecurity portfolio to reflect three principles that help streamline and optimize this journey.

1. Gain visibility into all CPS in OT

Visibility is foundational to securing OT— which is why all segments of the oil & gas sector must attain a complete, inventory of all OT, IoT, and BMS assets and other CPS across all drilling sites, pipelines, plants, and refineries.

It's also why Claroty is proud to deliver the industry-leading visibility our oil & gas customers need to secure the OT environments on which their critical assets and operations rely.

2. Integrate IT Tools with OT

Since most CPS in upstream, midstream, and downstream oil & gas use proprietary protocols and legacy systems, they are incompatible with IT solutions — but that doesn't mean such solutions have no place in OT.

Rather than require customers to expand their already-extensive tech stacks, Claroty integrates with them. As a result, customers can simply extend their IT tools and workflows to OT.

3. Extend IT controls to OT

Unlike their IT counterparts, it is common for OT environments in all segments of the oil & gas sector to lack essential security controls and consistent governance – especially across different sites and regions.

After providing visibility into all CPS and integrating IT tools and workflows with OT, Claroty extends existing IT controls to OT — unifying security governance and driving resilience across IT and OT.

How Claroty Empowers Oil & Gas Companies to Drive Resilience from IT to OT

Claroty's industrial cybersecurity portfolio and team of domain experts empower upstream, midstream, and downstream oil & gas companies to extend — and further optimize — the following cybersecurity use cases and governance areas from IT to OT:

Vulnerability Management

Network Segmentation

Endpoint Protection

Secure Remote Access

Threat Detection

Asset & Change Management

The above use cases and capabilities also further empower oil & gas customers to more-easily and effectively satisfy regulatory requirements, implement industry standards, best practices, and frameworks, streamline audits, and minimize noncompliance.

NIS2

TSA

SOCI

CPGs

NIST CSF

IEC 62443

Why 7 of the World's 10 Largest Oil & Gas Companies Trust Claroty

Leading oil & gas companies globally trust Claroty to protect the critical CPS on which the safety, security, and mobility of our society depend. Here are a few of the key factors that set Claroty apart and have been integral in enabling us to earn this trust:

40+

Awards

Our comprehensive cybersecurity platform has earned dozens of accolades for seamlessly enhancing the safety, security, and efficiency of OT, IoT, IIoT, BMS, and other CPS.

420+

Disclosures

Our award-winning Team82 researchers have disclosed more vulnerabilities than any other group, enhancing our customers' protections while drive security industry-wide.

Top 3

Industrial Automation Vendors

The Top 3 automation vendors (Rockwell Automation, Schneider Electric, and Siemens) invest in, partner with, and are loyal customers of Claroty, validating our leadership.

About The Claroty Portfolio

Unlike generic solutions, Claroty's industrial cybersecurity portfolio is purpose-built for the unique security and operational needs of the oil & gas sector. Complementary strategic guidance from Claroty's domain experts further enables oil & gas customers to not only secure OT – but also drive business value throughout their industrial cybersecurity journey. Solutions include:

Claroty xDome

Claroty xDome is a highly flexible, modular, SaaS platform purpose-built for all use cases & types of CPS on the entire industrial cybersecurity journey.

Claroty CTD

Claroty Continuous Threat Detection (CTD) is an on-premises solution that offers robust cybersecurity controls for critical infrastructure environments.

Claroty SRA

Claroty Secure Remote Access (SRA) delivers frictionless, reliable, secure remote access and management for internal and third-party OT personnel.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for asset visibility, asset and change management, risk and vulnerability management, network segmentation, endpoint protection, threat detection, secure remote access, and more.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.