WHITE PAPER

SUPPORTING THE MITRE ATT&CK FOR ICS FRAMEWORK

This paper examines the extent that The Claroty Platform can detect the adversary techniques listed in the MITRE ATT&CK for ICS framework

CLAROTY

CONTENTS

INTRODUCTION

What is MITRE ATT&CK for ICS?

The MITRE ATT&CK for ICS framework is a detailed compilation of the techniques and corresponding tactics that adversaries may use while operating in industrial control system (ICS) networks.

The framework aims to help operational technology (OT) and information technology (IT) security practitioners alike better understand and describe ICS adversary behavior both pre- and post-compromise.

The MITRE Corporation released the framework in January 2020 to augment its existing and widely used ATT&CK Knowledge Base, which also includes the ATT&CK for Enterprise and ATT&CK for Mobile frameworks.

As the newest framework, ATT&CK for ICS crucially addresses what its two predecessors did not: adversary behaviors that are typically only observed in the later stages of cyber attacks on ICS networks.

What is the purpose of this paper?

This paper details the extent that The Claroty Platform — which includes Claroty's Continuous Threat Detection (CTD) and Secure Remote Access (SRA) products, as well as the numerous security controls they provide for OT environments, including ICS networks — can detect the ICS adversary techniques that correspond with each of the 11 tactics in the MITRE ATT&CK for ICS framework.

It is important to recognize that while this report focuses solely on the detection of ICS adversary techniques, detection is only one component of the cybersecurity and cyber risk management lifecycle.

The Claroty Platform aligns with guidelines set forth by NIST and other regulatory frameworks that follow the Identify, Protect, Detect, Respond, Recover lifecycle.

As such, the platform delivers comprehensive OT security controls that support all components of this lifecycle.

> "[ATT&CK for ICS] can play several key roles for defenders, including helping establish a standard language for security practitioners to use as they report incidents. With expertise in this domain in short supply, it can also help with the development of incident response playbooks, prioritizing defenses as well as finding gaps, reporting threat intelligence, analyst training and development, and emulating adversaries during exercises."
>
> —The MITRE Corporation

OVERVIEW OF CLAROTY DETECTION CAPABILITIES

Claroty can detect all MITRE ATT&CK for ICS techniques. Most of these techniques can be detected directly, while some can be detected indirectly via collateral effects. The matrix below illustrates these capabilities for each technique and corresponding tactic.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command & Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Ports	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Later Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organizational Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity & Revenue
Replication Through Removeable Media	Project File Injection		Utilize/ Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/ Change Operating Mode		

Key*

	Claroty can detect technique directly
	Claroty can detect technique indirectly

*This key also applies to all subsequent charts in this report.

ANALYSIS OF CLAROTY DETECTION CAPABILITIES

This section of the paper provides a detailed analysis of The Claroty Platform's detection capabilities for each technique that corresponds with each of the 11 ICS adversary tactics in the MITRE ATT&CK for ICS framework.

Tactic 1: Initial Access

As the first MITRE ATT&CK for ICS tactic, Initial Access comprises ten different techniques adversaries may use as entry vectors in order to gain an initial foothold within an ICS network.

ID	Initial Access Technique	Claroty Detection Capability
T810	Data Historian Compromise	Claroty utilizes several different methods to detect the compromise of a data historian. These include passive detection of anomalies, remote access connections, and configuration changes.
T817	Drive-by Compromise	Claroty can detect network anomalies, as well as Snort and Yara rules, in order to help detect a machine compromised by a remote website.
T818	Engineering Workstation Compromise	Claroty utilizes several different methods to detect the compromise of an engineering workstation. These include passive detection of anomalies, remote access connections, and configuration changes.
T819	Exploit Public-Facing Application	Claroty utilizes several different methods to detect the compromise of a public-facing application. These include passive detection of anomalies, remote access connections, and configuration changes.
T822	External Remote Services	Claroty can alert on specific communications between subnets or by defining a specific policy for passive monitoring on which to alert.
T882	Internet Access Device	Claroty can alert on specific communications between subnets or by defining a specific policy for passive monitoring on which to alert.
T847	Replication Through Removeable Media	Claroty utilizes active detection to detect external removable media insertions.
T865	Spearphishing Attachment	Claroty can detect malicious files on a network by leveraging Claroty threat intelligence and Yara signatures.
T862	Supply Chain Compromise	Claroty utilizes its DPI capabilities and resulting baselines to detect network anomalies. Data from the Claroty Cloud also enables the detection of anomalies via comparison to that which has been observed on similar networks and devices.
T860	Wireless Compromise	Claroty can detect anomalies by passively monitoring network ports, as well as leveraging active detection capabilities when necessary.

Tactic 2: Execution

Execution, the second MITRE ATT&CK for ICS tactic, encompasses nine techniques that can result in adversary-controlled code running on a local or remote system, device, or other asset.

ID	Execution Technique	Claroty Detection Capability
T875	Change Program State	Claroty can detect changes in the state of an OT device by issuing "Monitor Debug", "Mode Change", "Firmware Download", and "Configuration Download" alert types.
T807	Command-Line Interface	Claroty can detect and issue alerts on remote connections to various services. Users can set baseline rules to alert on specific protocols.
T871	Execution through API	Claroty can detect and issue alerts on remote connections to various services. Users can set baseline rules to alert on specific protocols.
T823	Graphical User Interface	Claroty can detect and issue alerts on remote connections to various services. Users can set baseline rules to alert on specific protocols.
T830	Man in the Middle	Claroty utilizes a dedicated alert logic in order to detect man-in-the-middle attacks.
T844	Program Organization Units	Claroty can detect changes to the logic of an OT asset by identifying software updates and configuration downloads to OT assets.
T873	Project File Infection	Claroty can digest project files via its AppDB scanning capabilities. In the event of a conflict between the data available from project files and the data available from passive monitoring, Claroty issues an alert.
T853	Scripting	If an adversary uses a scripting engine to compromise a network, Claroty can detect any anomalies that appear in the network traffic or asset attributes.
T863	User Execution	If an adversary uses a scripting engine to compromise a network, Claroty can detect any anomalies that appear in the network traffic or asset attributes.

Tactic 3: Persistence

Persistence is how an adversary maintains their foothold in an ICS environment despite restarts, credential changes, and other interruptions. This tactic consists of six techniques.

ID	Persistence Technique	Claroty Detection Capability
T874	Hooking	Claroty can identify configuration changes in ICS devices. Extracting these changes and highlighting the code diffs between versions enables Claroty to detect hooking.
T839	Module Firmware	Claroty can detect changes to the logic of an OT asset by identifying software updates and configuration downloads to OT assets.
T843	Program Download	Claroty can detect changes to the logic of an OT asset by identifying software updates and configuration downloads to OT assets.
T873	Project File Infection	Claroty can digest project files via its AppDB scanning capabilities. In the event of a conflict between the data available from project files and the data available from passive monitoring, Claroty issues an alert.
T857	System Firmware	Claroty can detect changes to the logic of an OT asset by identifying software updates and configuration downloads to OT assets, as well as by inspecting program diffs.
T859	Valid Accounts	Claroty can detect failed login attempts, which can be an indicator of the misuse of valid accounts. Claroty can also detect the use of dangerous and/or dated protocols that do not encrypt credentials.

Tactic 4: Evasion

Evasion, the fourth MITRE ATT&CK for ICS tactic, consists of seven techniques adversaries may use to attempt to avoid detection by human operators and technical defenses.

ID	Evasion Technique	Claroty Detection Capability
T820	Exploitation for Evasion	Claroty can detect full-match CVEs based on its real-time updated threat intelligence, as well as by identifying and matching the specific software version of an asset to all corresponding vulnerabilities. Since these capabilities enable the proactive remediation of vulnerabilities, they also greatly minimize the risk of exploitation.
T872	Indicator Removal on Host	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T849	Masquerading	Claroty can detect anomalies, including masquerading, based on the baselines it creates and continually updates for ICS environments. Claroty does this by dissecting all protocols, extracting the relevant data, and alerting on significant deviations.
T848	Rogue Master Device	Claroty's policies and anomaly detection engines enable alerting on any abnormal communications between assets, including unauthorized rogue master devices.
T851	Rootkit	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T856	Spoof Reporting Message	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T858	Utilize/Change Operating Mode	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.

Tactic 5: Discovery

Discovery includes seven techniques adversaries may use to survey an ICS environment's internal network, devices, and processes to inform targeting and subsequent tactics.

ID	Discovery Technique	Claroty Detection Capability
T808	Control Device Identification	Claroty utilizes specialized logic to detect and alert on host and network scans. Claroty also uses passive monitoring to detect and alert on any type of anomaly, including the querying of a control device.
T824	I/O Module Discovery	Claroty uses passive monitoring to detect and alert on any type of anomaly, including the querying of a control device for I/O module discovery.
T840	Network Connection Enumeration	Claroty uses passive monitoring to detect and alert on any type of anomaly, including the querying of a control device for asset discovery.
T841	Network Service Scanning	Claroty utilizes specialized logic to detect and alert on host and network scans. Claroty also uses passive monitoring to detect and alert on any type of anomaly, including the querying of a control device.
T842	Network Sniffing	Claroty can detect anomalies caused by network sniffing, such as the transit of data.
T846	Remote System Discovery	Claroty uses passive monitoring to detect and alert on any type of anomaly, including the querying of a control device for asset discovery.
T854	Serial Connection Enumeration	Claroty can detect network anomalies, including the presence of an asset requesting serial enumeration over other devices.

Tactic 6: Lateral Movement

Lateral Movement is how an adversary moves through an ICS environment. This tactic consists of six techniques adversaries may use to enter and control remote systems on a network.

ID	Lateral Movement Technique	Claroty Detection Capability
T812	Default Credentials	Claroty can detect failed login attempts, which can be an indicator of the misuse of valid accounts. Claroty can also detect the use of dangerous and/or dated protocols that do not encrypt credentials.
T866	Exploitation of Remote Services	Claroty utilizes its anomaly detection engine to detect any abnormal behavior exhibited by a network service. Claroty also provides comprehensive vulnerability management controls based on the latest OT threat intelligence, as well as the latest common vulnerabilities and exposures (CVE) data from the National Vulnerabilities Database (NVD).
T822	Eternal Remote Services	Claroty can detect and alert on any abnormal traffic within the network. Additionally, Claroty's approach to micro-segmentation via its Virtual Zones feature enables it to issue alerts on abnormal communications between subnets, with external zones, or with specific protocols.
T844	Program Organization Units	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets.
T867	Remote File Copy	Claroty utilizes its anomaly detection engine to detect and alert on any abnormal communications in the network, including that which may be an indicator associated with the Remote File Copy technique. Claroty users can also set custom baseline rules for such alerts.
T859	Valid Accounts	Claroty can detect failed login attempts, which can be an indicator of the misuse of valid accounts. Claroty can also detect the use of dangerous and/or dated protocols that do not encrypt credentials.

Tactic 7: Collection

Collection, the seventh MITRE ATT&CK for ICS tactic, consists of 11 techniques adversaries may use to gather data and knowledge on an ICS environment to inform their objectives.

ID	Collection Technique	Claroty Detection Capability
T802	Automated Collection	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T811	Data from Information Repositories	Claroty's anomaly detection engine can detect any abnormal behavior on a network, including the transit of data from information repositories.
T868	Detect Operating Mode	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T870	Detect Program State	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T877	I/O Image	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T825	Location Identification	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T801	Monitor Process State	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T861	Point & Tag Identification	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T845	Program Upload	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T850	Role Identification	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries. Additionally, Claroty users can also set custom baseline rules for alerts on specific communication from other key assets.
T852	Screen Capture	Claroty's detection engines can detect abnormal traffic and issue alerts on baseline rules or policies in a manner such that successfully transmitting screen captures becomes difficult for adversaries.

Tactic 8: Command & Control

The Command & Control tactic includes three techniques that adversaries may use to communicate with and control compromised ICS systems, controllers, and platforms.

ID	Command & Control Technique	Claroty Detection Capability
T885	Commonly Used Port	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.
T884	Connection Proxy	Claroty's anomaly detection engine can detect any abnormal behavior on a network, including the transit of data from information repositories.
T869	Standard Application Layer Protocol	Claroty's OT DPI and anomaly detection capabilities enable the detection of any abnormal OT device queries.

Tactic 9: Inhibit Response Function

Inhibit Response Function encompasses 15 techniques that adversaries may use in order to hinder safeguards implemented for ICS processes and products.

ID	Inhibit Response Function Technique	Claroty Detection Capability
T800	Activate Firmware Update Mode	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T878	Alarm Suppression	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T803	Block Command Message	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T804	Block Reporting Message	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T805	Block Serial COM	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T809	Data Destruction	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T814	Denial of Service	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T816	Device Restart/Shutdown	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T835	Manipulate I/O Image	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.

Tactic 9: Inhibit Response Function [Continued]

Inhibit Response Function encompasses 15 techniques that adversaries may use in order to hinder safeguards implemented for ICS processes and products.

ID	Inhibit Response Function Technique	Claroty Detection Capability
T838	Modify Alarm Settings	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T833	Modify Control Logic	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T843	Program Download	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T851	Rootkit	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T857	System Firmware	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T858	Utilize/Change Operating Mode	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.

Tactic 10: Impair Process Control

As the tenth tactic, Impair Process Control includes 11 techniques adversaries may use to manipulate, disable, or damage physical control processes in compromised ICS environments.

ID	Impair Process Control Technique	Claroty Detection Capability
T806	Brute Force I/O	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T875	Change Program State	Claroty can detect changes in the state of an OT device by issuing "Monitor Debug", "Mode Change", "Firmware Download", and "Configuration Download" alert types.
T849	Masquerading	Claroty can detect anomalies, including masquerading, based on the baselines it creates and continually updates for ICS environments. Claroty does this by dissecting all protocols, extracting the relevant data, and alerting on significant deviations.
T833	Modify Control Logic	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T836	Modify Parameter	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T839	Module Firmware	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T843	Program Download	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T848	Rogue Master Device	Claroty's policies and anomaly detection engines enable alerting on any abnormal communications between assets, including unauthorized rogue master devices.
T881	Service Stop	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.

Tactic 10: Impair Process Control [Continued]

As the tenth tactic, Impair Process Control includes 11 techniques adversaries may use to manipulate, disable, or damage physical control processes in compromised ICS environments.

ID	Impair Process Control Technique	Claroty Detection Capability
T856	Spoof Reporting Message	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.
T855	Unauthorized Command Message	Claroty can detect changes to the logic of an OT asset by detecting software updates and configuration downloads to OT assets. Additionally, Claroty can detect status changes and process value changes, which can also be indicators of this technique.

Tactic 11: Impact

Impact, the framework's final tactic, consists of 11 techniques adversaries use to disrupt, manipulate, or destroy the integrity or availability of ICS systems, data, and their environment.

ID	Impact Technique	Claroty Detection Capability
T879	Damage to Property	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T813	Denial of Control	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T815	Denial of View	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T826	Loss of Availability	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T827	Loss of Control	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T828	Loss of Productivity & Revenue	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T880	Loss of Safety	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T829	Loss of View	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T831	Manipulation of Control	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T832	Manipulation of View	Claroty allows the reading of process values in a manner that enables users to verify their standard operating environment and identify Impact techniques used within it.
T882	Theft of Operational Information	Claroty can detect any unauthorized transmission or acquisition of data by defining policies and/or baseline rules within its anomaly detection engine and then monitoring for policy violations and/or baseline deviations.

CONCLUSION

About Claroty CTD

As the foundation of the Claroty platform, Claroty Continuous Threat Detection (CTD) delivers unmatched asset discovery, risk and vulnerability management, and threat detection coverage for industrial networks. These capabilities will empower you to reveal and protect your OT, IoT, and IIoT assets, as well as identify and respond to the earliest indicators of known and emerging threats to those assets and the critical processes they underpin.

CTD is powered by the industry's largest library of industrial protocols, three unique asset discovery methods, five distinct detection engines, proprietary virtual segmentation technology, and the multi award-winning Claroty research team.

About Claroty SRA

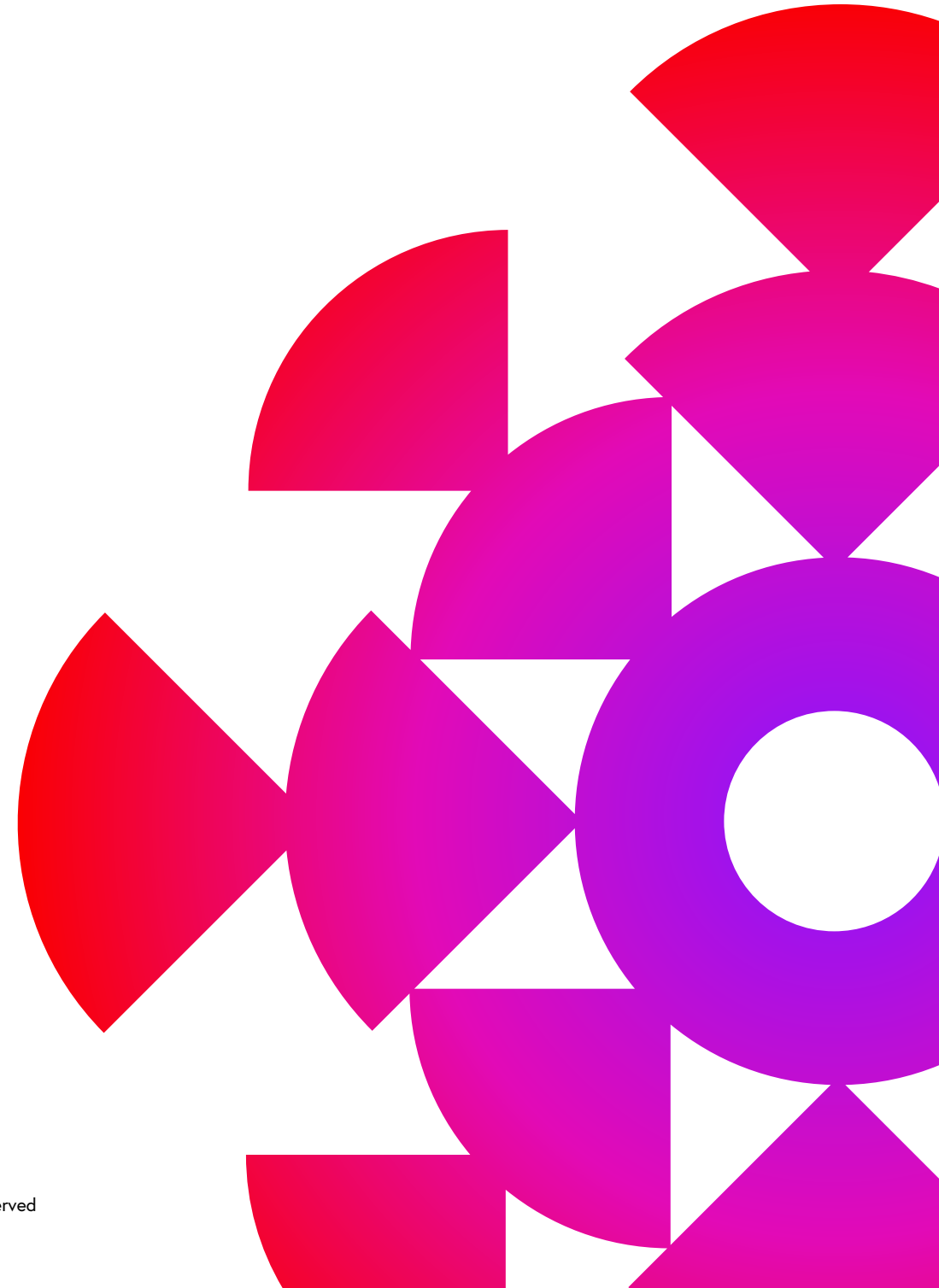
Claroty Secure Remote Access (SRA) delivers frictionless, reliable, and highly secure remote access to OT environments for internal and third-party users. Unlike traditional remote access solutions—most of which are designed solely for IT networks—Claroty SRA is purpose-built for the specific operational, administrative, and security needs of industrial networks.

The result is a unique solution that reduces your mean-time-to-repair (MTTR), minimizes the cost and complexity of configuring and administering access for your OT remote users, and diminishes your OT environment's exposure to the risks posed by unmanaged, uncontrolled, and unsecured access.

About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia- Pacific, and Latin America, and deployments on all seven continents.

For more information, visit www.claroty.com.



CLAROTY