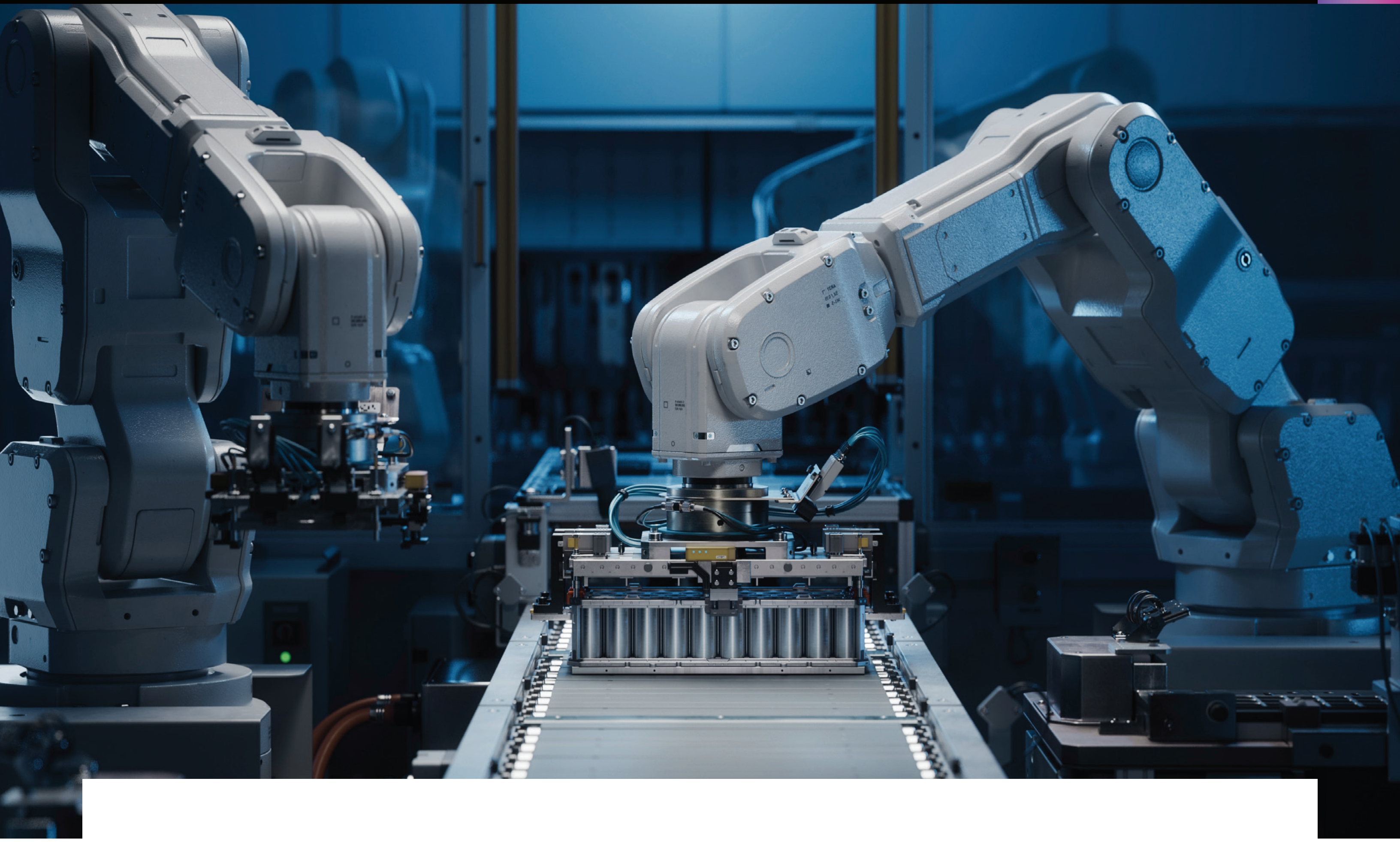


WHITE PAPER

5 Steps for Network Segmentation in Cyber-Physical Systems

TABLE OF CONTENTS

Protecting the backbone of society

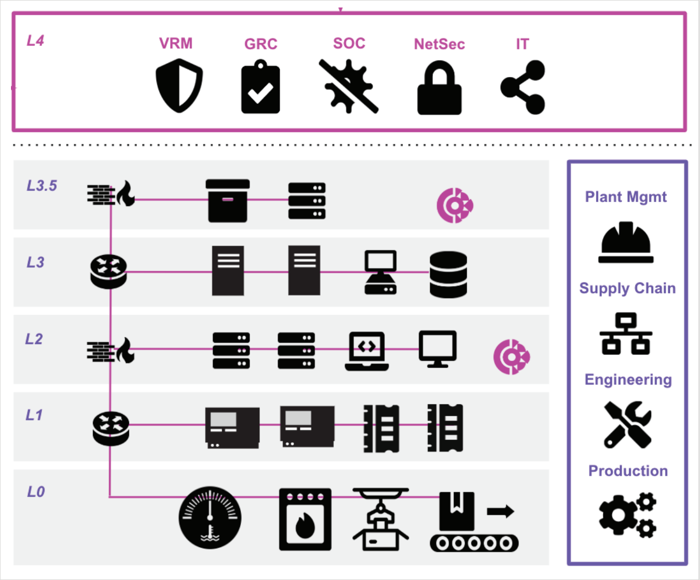
Segmentation braces CPS networks against evolving attacks

Manufacturing and other critical infrastructure sectors are abuzz with automation and connectivity. Organizations are chasing digital transformation initiatives to improve velocity, but they face a formidable opponent: how to secure newly connected systems that were designed to remain disconnected.

As an IT or OT security team member responsible for protecting cyber-physical systems (CPS) amidst expanding and targeted threat activity, one thing has become explicitly clear: existing IT solutions fall short in this arena. The unique architectures, proprietary protocols used, and environmental and operational constraints make traditional IT tools ill-equipped and ineffective.

Security analysts and engineers experience this technology mismatch every day as they try to reverse engineer IT tools to fit in air-gapped environments, or across high-latency and geographically dispersed networks.

Why do CPS networks need a different approach?



1. Legacy systems

Unlike IT environments, in which systems are updated every few years, industrial CPS environments are full of legacy devices and systems that have decades-long lifecycles. The legacy industrial control systems (ICS) located in these environments were largely built without any security concepts, as connectivity was not yet conceived. These systems may lack the necessary features to support network segmentation or accept new security controls.

2. Integration with IT systems

IT and OT networks today may need to exchange data and information. Allowing specific communications between segmented OT networks and IT infrastructure requires collaboration between historically siloed parts of a business. Just like the technology gap between IT and OT, the people and process gap can lead to oversights, added complexity, duplicated work, an increase in operational costs, or security exposures.

3. Segmentation policies are error prone

Implementing effective network segmentation policies in industrial environments is hard. Asset visibility gaps, complex architectures, and countless proprietary protocols make it an error-prone, expensive process.
It's also typically manually-intensive, which is not only costly and time consuming for architects and engineers, but also leaves room for oversights, misunderstandings, and mistakes caused by innocent human error.

4. Compliance is inconsistently enforced

Critical infrastructure organizations are subject to many complex industry and regional-specific regulations and standards. Monitoring and ensuring compliance with these regulations often requires granular, properly tuned policies that many organizations lack. This can lead to suboptimal segmentation that is inconsistently enforced but meets compliance minimums, while not actually improving the network security posture.

5. Unsecured Remote Access is Widespread

All industrial environments rely on remote access to enable both internal and third-party personnel to maintain assets, but common IT practices are risky and inefficient. If not managed properly, remote access has the potential to bypass network segmentation measures–and makes a lack of segmentation far riskier.

What this means for security teams

While many network security professionals can create policies for IT networks in their sleep, as if they've developed a sixth sense, this learned prowess doesn't necessarily apply in CPS environments.

IT security analysts and OT security engineers use the information available to them to make the best segmentation strategy possible. Teams make it work, every day, to protect their business's critical infrastructure. And they do it with a metaphorical hand tied behind their back because they:

- Lack the depth of asset information to know what existing communications are normal and necessary;
- Design and implement policies that may or may not protect the network, and could cause outages due to incorrectly blocked communications;
- Face complex recovery steps if a device goes down, as device dependencies are unknown.

How CPS-specific network protection help security teams

IT and OT security analysts and engineers are set free when they have a complete picture of the assets in their network and how they communicate internally and externally. Closing the gap in visibility makes a significant difference, creating informed and understood network segmentation decisions, rather than gut feelings or educated guesses.

Beyond visibility, a policy-based approach from a CPS protection platform provides informed recommendations for allowed and disallowed communication, can adapt to contextual changes, and understands the nuance of CPS networks to provide a higher level of efficacy. A policy-based approach includes policy decision points (PDPs) and policy enforcement points (PEPs).

Let's break down how you can leverage a CPS protection platform to make informed network protection decisions and ultimately reduce organizational risk.

1. Start with Visibility

The first step towards network protection is to gain complete visibility into all devices on the network.

This simple statement veils immense complexity. In fact, if you're reading this and are responsible for securing a CPS environment, I bet you chuckled.

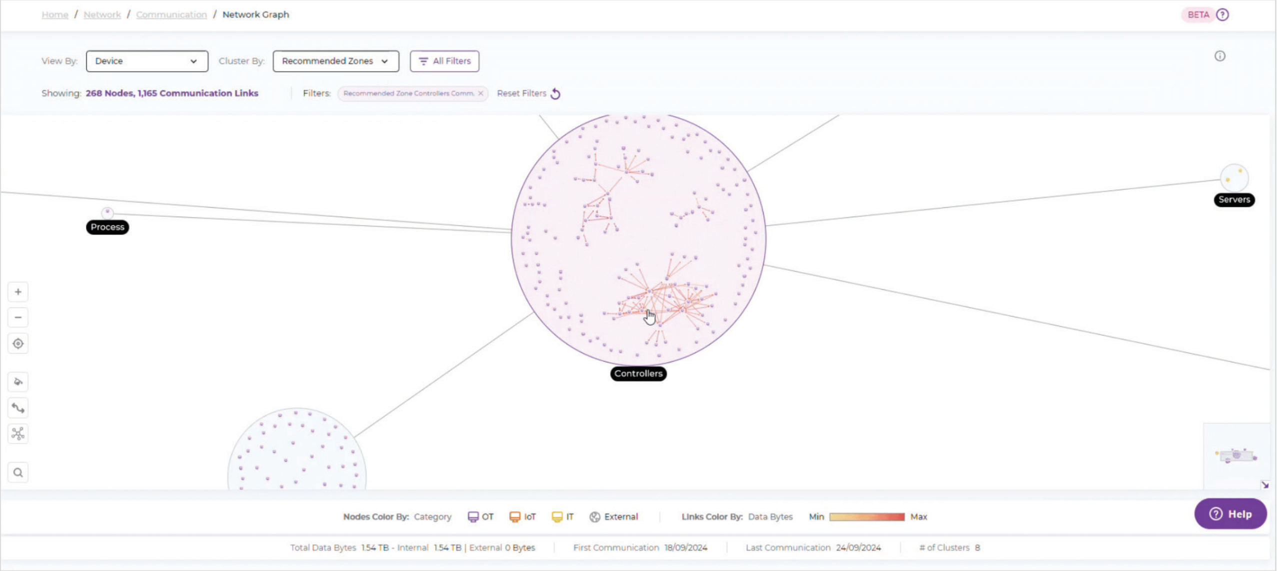
Visibility in CPS has become synonymous with passive discovery techniques. For a long time, it was the only choice, and although it's still necessary for visibility into network traffic and communication patterns, this hardware-based, packet sniffing approach comes with resource challenges, requiring both time and money.

Despite the need for passive discovery to meet network protection goals, there is value in beginning with non-passive techniques. Deploying a Safe Query executable or leveraging existing integrations to gain detailed information about assets in the environment provides a visibility foundation in hours instead of months, with no hardware deployments or downtime.

A Claroty Food & Bev customer operates data centers across the globe. Their segmentation journey started by using a combination of discovery methods, including non-passive and passive techniques. Dynamic Discovery gave them detailed information of their assets and identified the appropriate central switches where passive monitoring could enrich data to create the greatest impact in risk reduction.

For the purposes of network protection, this quick visibility helps organizations know exactly where passive deep packet inspection (DPI) technology needs to be physically deployed. Tailoring visibility to your specific needs and architecture speeds time to value, even while deploying passive discovery hardware.

DPI combined with the industry's broadest portfolio of CPS protocol coverage provides the necessary details to profile device communications and provide users a visualized look into network communication patterns.



Home / Network / Communication / Network Graph

View By: Device

Cluster By: Recommended Zones

Showing: 268 Nodes, 1,165 Communication Links

Filters: Recommended Zone Controllers Comm.

Nodes Color By: Category

Links Color By: Data Bytes

Total Data Bytes 1.54 TB - Internal 1.54 TB | External 0 Bytes | First Communication 18/09/2024 | Last Communication 24/09/2024 | # of Clusters 8

DPI AND ACTIVE QUERIES ADD CONTEXT OF DEVICE LOCATIONS, RELATIONSHIPS, AND COMMUNICATIONS, WHICH ARE USED TO CREATE A NETWORK GRAPH

2. Establish Security Zones

Define zones for assets within the system that need to be segmented

Once you know what assets exist and where they're physically located, the next step is to establish security zones. The goal of security zones is to limit lateral movement, reduce the attack surface, and layer protection of critical assets by zoning off, or segmenting, the network.

There are many ways assets can be classified to define segmentation zones. Some common ways Claroty customers approach this task include:

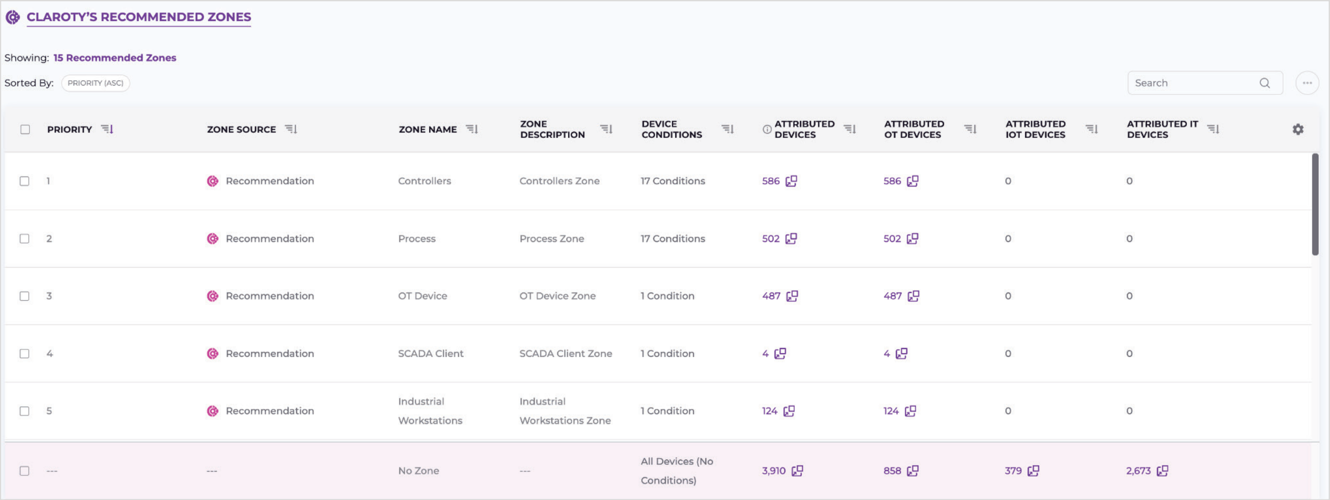
- By network architecture
- By geographic location
- By security sensitivity or risk tolerance
- By access sensitivity

Claroty will provide recommended zones based on your network topology as well.

Segmentation can also be implemented using technology within your existing infrastructure, including:

1. **Firewalls:** ideal for precise control over network traffic between network segments and with external communications. They focus on traffic flow and are designed to prevent lateral movement.
2. **VLANs:** chosen for logical segmentation based on roles, functionality, or security levels. They are typically easier to deploy when parts of the environment are physically separated.
3. **NACs:** provide dynamic and automated control over which devices can connect to the network. They are ideal for continuous device compliance, and are designed for environments with mixed device types.

After gaining visibility of devices and their network communications, our Claroty Food & Bev customer found that zones based on asset type would be the most appropriate approach to segmentation. They used Claroty's recommended zones to establish device conditions that best defined each group of assets.



CLAROTY'S RECOMMENDED ZONES

Showing: 15 Recommended Zones

Sorted By: PRIORITY (ASC)

	PRIORITY	ZONE SOURCE	ZONE NAME	ZONE DESCRIPTION	DEVICE CONDITIONS	ATTRIBUTED DEVICES	ATTRIBUTED OT DEVICES	ATTRIBUTED IOT DEVICES	ATTRIBUTED IT DEVICES
□	1	Recommendation	Controllers	Controllers Zone	17 Conditions	586	586	0	0
□	2	Recommendation	Process	Process Zone	17 Conditions	502	502	0	0
□	3	Recommendation	OT Device	OT Device Zone	1 Condition	487	487	0	0
□	4	Recommendation	SCADA Client	SCADA Client Zone	1 Condition	4	4	0	0
□	5	Recommendation	Industrial Workstations	Industrial Workstations Zone	1 Condition	124	124	0	0
□	---	---	No Zone	---	All Devices (No Conditions)	3,910	858	379	2,673

CLAROTY RECOMMENDED ZONES PROVIDE INFORMED OPTIONS FOR GROUPING ASSETS, ADDING INSIGHT AS TEAMS PROGRESS THEIR CPS SECURITY JOURNEY

3. Simulate Communication to Monitor Behavior

Create communication policies between zones and monitor device behavior

Once zones are established, a security team can observe normal communication behavior between zones and subsequently create a baseline from which policies can be derived.

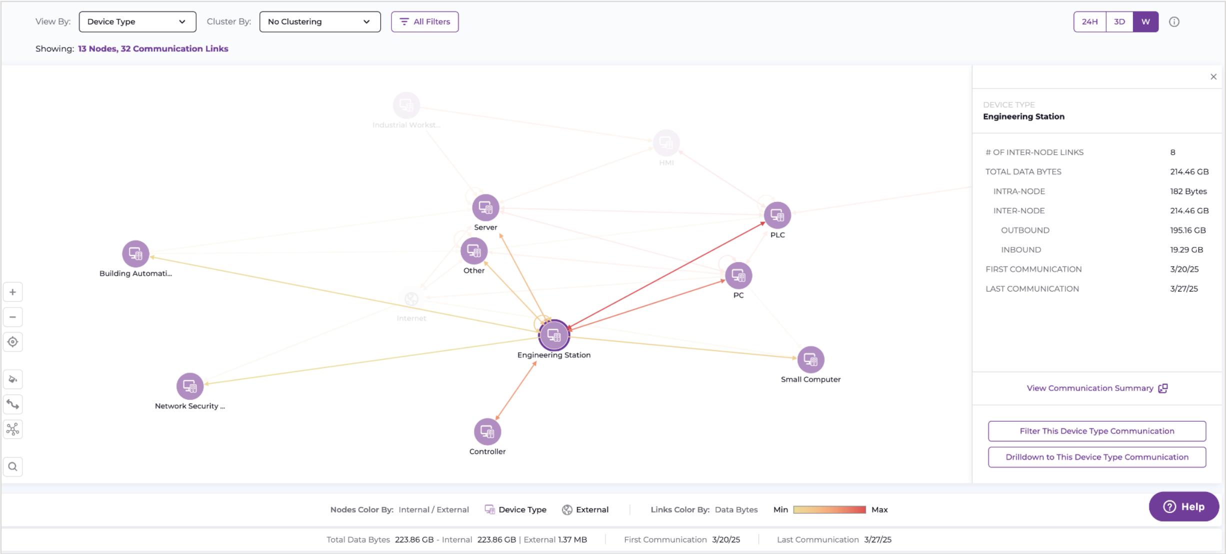
Creating a unique policy for each device is impractical, but creating policies for device types or groups of devices makes segmentation both effective and scalable.

Types of communication mapping that may be helpful to understand how devices interact with each other include:

- **Graph Device Communications:** Visualize how all the sites, device types, zones and devices in your network are connected and communicate with each other.
- **Visualize Device Communications:** See how devices communicate, as a list or a matrix, including protocols and communication type.

This granular mapping enables administrators to clearly identify communication flows, assess risks, and design effective segmentation strategies tailored to their network topology. Maybe you find a device allowing external communication that shouldn't, or see an engineering workstation is communicating heavily with a building management system (BMS), or a PLC with a SCADA server that isn't considered normal.

Once their zones were created, our Food & Bev customer began monitoring communication between zones to design policies. This is where it got exciting for our customer team, as all the intelligence and understanding they had gained was put into action. Using Claroty's recommended policies took a lot of manual labor and guesswork out of the process, setting how robotic arms could communicate with PLCs, whether any EWS could communicate with the internet, and over which ports controllers could receive inputs.



View By: Device Type　Cluster By: No Clustering

Showing: 13 Nodes, 32 Communication Links

DEVICE TYPE
Engineering Station

# OF INTER-NODE LINKS	8
TOTAL DATA BYTES	214.46 GB
INTRA-NODE	182 Bytes
INTER-NODE	214.46 GB
OUTBOUND	195.16 GB
INBOUND	19.29 GB
FIRST COMMUNICATION	3/20/25
LAST COMMUNICATION	3/27/25

Nodes Color By: Internal / External　Device Type　External　Links Color By: Data Bytes　Min　Max

Total Data Bytes 223.86 GB - Internal 223.86 GB | External 1.37 MB　First Communication 3/20/25　Last Communication 3/27/25

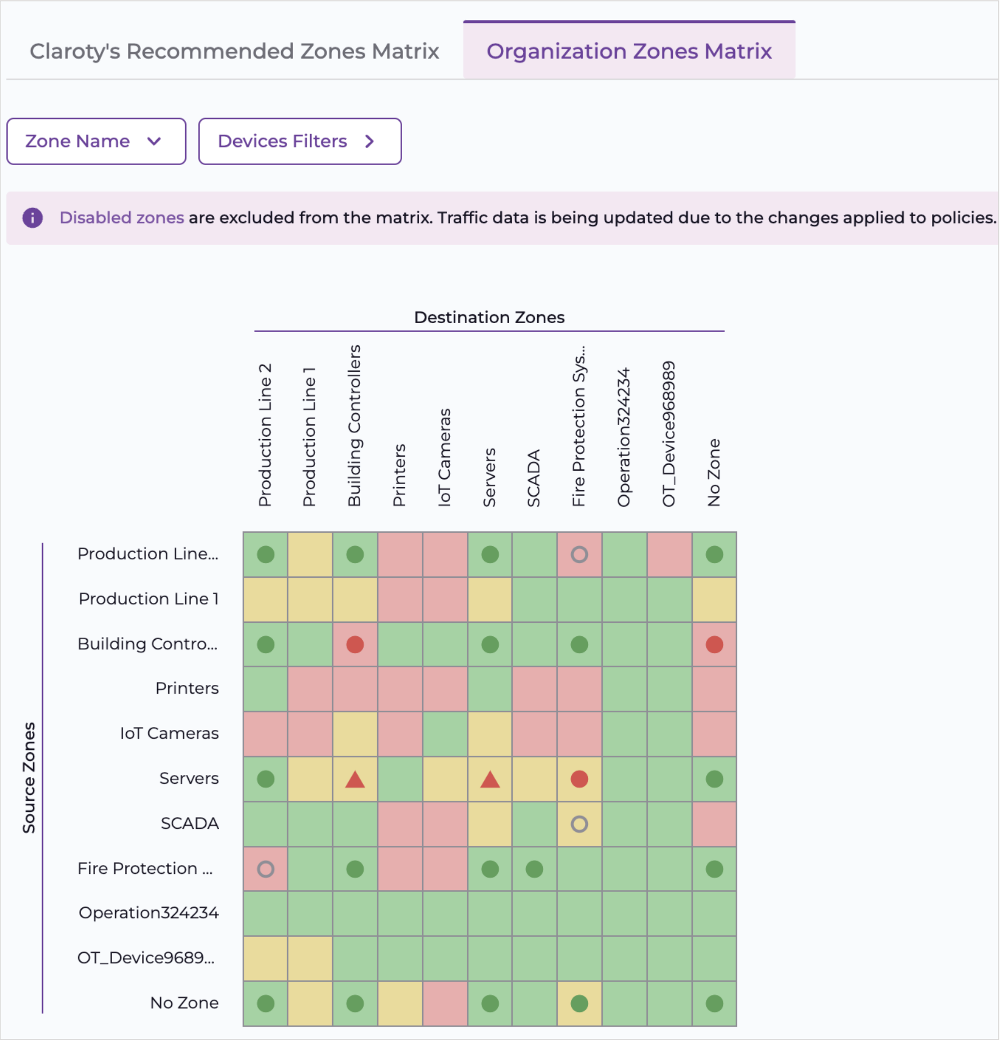
DETAILED COMMUNICATION INFORMATION IN THE NETWORK GRAPH HELPS SECURITY TEAMS UNDERSTAND IDENTIFY ANOMALIES AND UNDERSTAND WHAT'S NORMAL IN THEIR CPS ENVIRONMENT

The trick with communication policies

You are not only responsible for preventing malicious activity from taking down critical systems – you also have to ensure security policies don't break those systems.

Network policies must be designed without introducing negative impacts to system functionality. Be sure to test policies outside of production to determine any unforeseen consequences before they're enforced.

Claroty minimizes this uncertainty by automatically recommending expert-defined policies for each asset group according to their communication baselines. You can then test, monitor, and further refine those policies before enforcement. As a result, you can be sure that your OT network policies fully account for the unique requirements and potential limitations of your environment — allowing you to confidently implement segmentation without introducing additional risk.



Disabled zones are excluded from the matrix. Traffic data is being updated due to the changes applied to policies.

Destination Zones

Source Zones	Production Line 2	Production Line 1	Building Controllers	Printers	IoT Cameras	Servers	SCADA	Fire Protection Sys...	Operation324234	OT_Device968989	No Zone
Production Line...	🟩●	🟨	🟩●	🟥	🟥	🟩●	🟩	🟥○	🟩	🟥	🟩●
Production Line 1	🟨	🟨	🟨	🟥	🟥	🟨	🟩	🟩	🟩	🟩	🟨
Building Contro...	🟩●	🟩	🟥🔴	🟩	🟩	🟩●	🟩	🟩●	🟩	🟩	🟥🔴
Printers	🟩	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟩	🟩	🟥
IoT Cameras	🟥	🟥	🟨	🟥	🟩	🟨	🟥	🟥	🟩	🟩	🟥
Servers	🟩●	🟨	🟨🔺	🟩	🟨	🟨🔺	🟨	🟨🔴	🟩	🟩	🟩●
SCADA	🟩	🟩	🟩	🟥	🟥	🟨	🟩	🟨○	🟩	🟩	🟥
Fire Protection ...	🟥○	🟩	🟩●	🟥	🟥	🟩●	🟩●	🟩	🟩	🟩	🟩●
Operation324234	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
OT_Device9689...	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
No Zone	🟩●	🟨	🟩●	🟨	🟥	🟩●	🟩	🟨●	🟩	🟩	🟩●

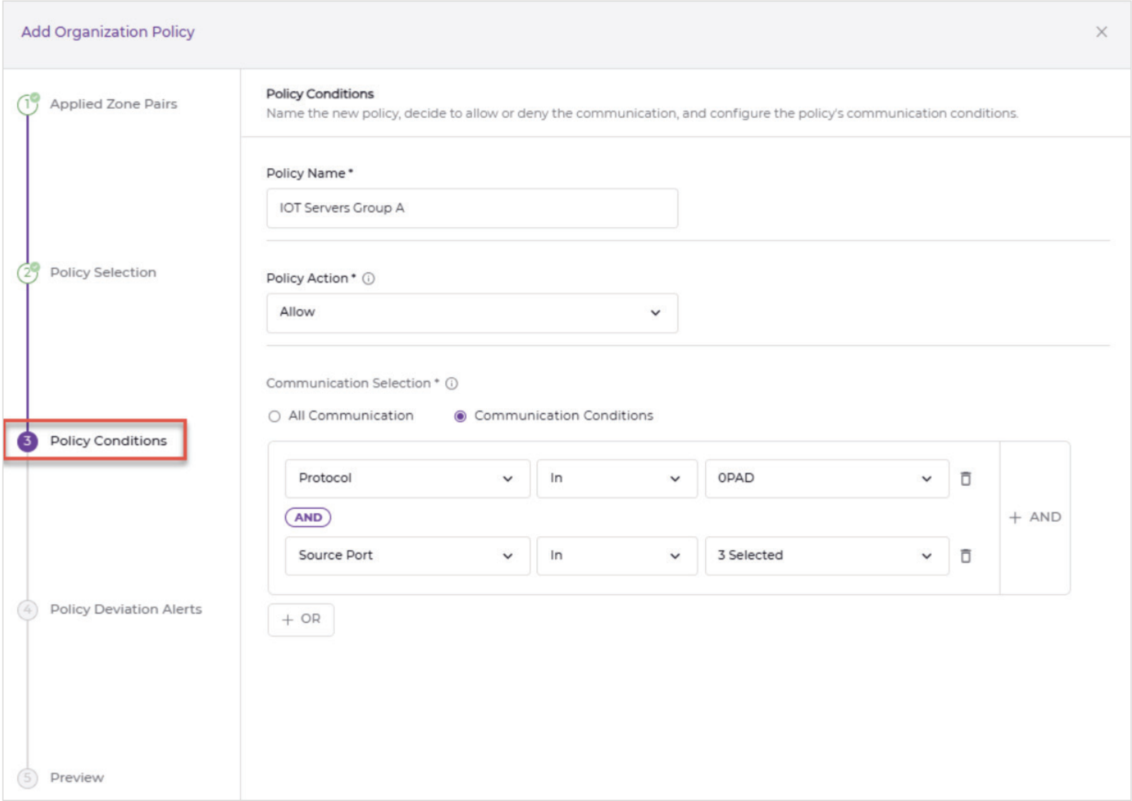
THE ZONE MATRIX SUPPORTS TEAMS EVALUATING THE EFFICACY OF APPLIED POLICIES, ALLOWING FOR DIRECT MODIFICATION TO POLICIES APPLIED TO ZONE PAIRS

4. Alert on Deviations

Alert on deviations from expected behavior and tune policies over time

Once policies are in place they must be monitored to ensure behavior continues as expected. Maybe there's a monthly traffic occurrence that didn't take place during testing, but must be allowed – that nuance may require a policy to be tuned for system performance to continue as expected.

While you're observing and investigating alerts for deviated communication behavior, you may come across times when complex policies are required. These are network policies that use communication conditions, such as protocols or ports, to create "if, then" style decisions. For example, you could allow communication between internet of things (IoT) servers and a building management system (BMS) if the communicating device uses OPAD over port 37020.



Add Organization Policy

Policy Conditions

Name the new policy, decide to allow or deny the communication, and configure the policy's communication conditions.

Policy Name *

IOT Servers Group A

Policy Action *

Allow

Communication Selection *

○ All Communication ● Communication Conditions

Protocol In 0PAD

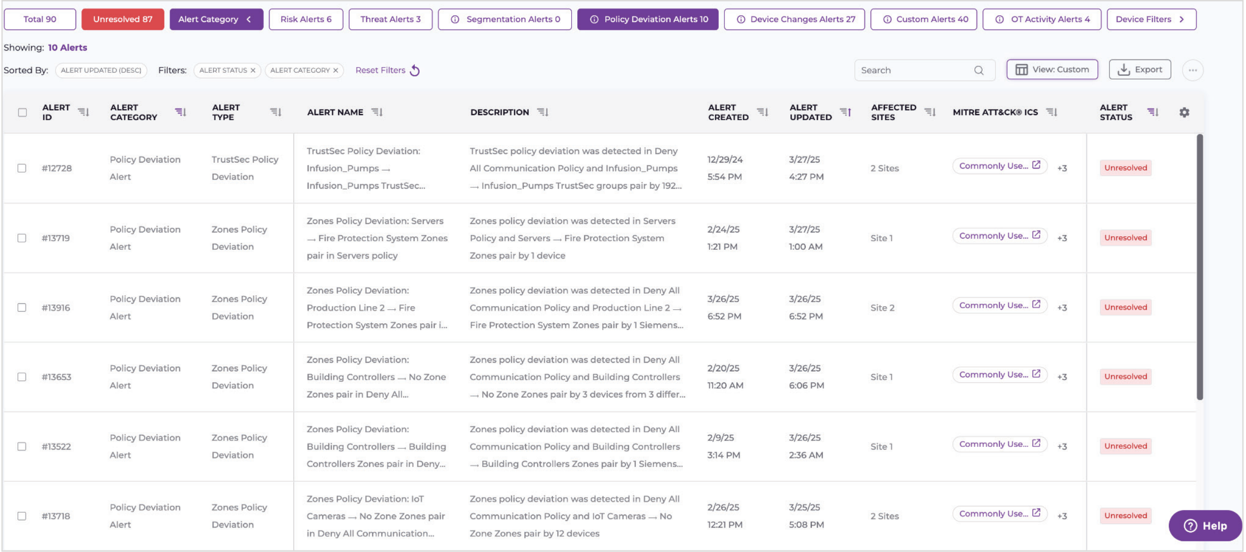
AND

Source Port In 3 Selected

CUSTOM POLICIES HELP MEET THE UNIQUE NEEDS OF EVERY ORGANIZATION AND ENVIRONMENT TO APPROPRIATELY REDUCE RISK WITHOUT COMPROMISING PRODUCTION

Receiving real-time alerts allows security teams to test enforcement during this early phase of implementation. It also allows for investigations and remediation of any indicators of compromise or attack.

These alerts are part of what makes a policy decision point so critical in a network-centric risk reduction plan – they're the warning signal when something or someone has changed an expected device communication behavior. Many threat vectors, including lateral movement, malware, man-in-the-middle (MitM) attacks, and vulnerability exploit chains, can cause changes in device communications.



Showing: 10 Alerts

Sorted By: ALERT UPDATED (DESC) Filters: ALERT STATUS × ALERT CATEGORY × Reset Filters

☐	ALERT ID	ALERT CATEGORY	ALERT TYPE	ALERT NAME	DESCRIPTION	ALERT CREATED	ALERT UPDATED	AFFECTED SITES	MITRE ATT&CK® ICS	ALERT STATUS
☐	#12728	Policy Deviation Alert	TrustSec Policy Deviation	TrustSec Policy Deviation: Infusion_Pumps → Infusion_Pumps TrustSec...	TrustSec policy deviation was detected in Deny All Communication Policy and Infusion_Pumps → Infusion_Pumps TrustSec groups pair by 192...	12/29/24 5:54 PM	3/27/25 4:27 PM	2 Sites	Commonly Use... +3	Unresolved
☐	#13719	Policy Deviation Alert	Zones Policy Deviation	Zones Policy Deviation: Servers → Fire Protection System Zones pair in Servers policy	Zones policy deviation was detected in Servers Policy and Servers → Fire Protection System Zones pair by 1 device	2/24/25 1:21 PM	3/27/25 1:00 AM	Site 1	Commonly Use... +3	Unresolved
☐	#13916	Policy Deviation Alert	Zones Policy Deviation	Zones Policy Deviation: Production Line 2 → Fire Protection System Zones pair i...	Zones policy deviation was detected in Deny All Communication Policy and Production Line 2 → Fire Protection System Zones pair by 1 Siemens...	3/26/25 6:52 PM	3/26/25 6:52 PM	Site 2	Commonly Use... +3	Unresolved
☐	#13653	Policy Deviation Alert	Zones Policy Deviation	Zones Policy Deviation: Building Controllers → No Zone Zones pair in Deny All...	Zones policy deviation was detected in Deny All Communication Policy and Building Controllers → No Zone Zones pair by 3 devices from 3 differ...	2/20/25 11:20 AM	3/26/25 6:06 PM	Site 1	Commonly Use... +3	Unresolved
☐	#13522	Policy Deviation Alert	Zones Policy Deviation	Zones Policy Deviation: Building Controllers → Building Controllers Zones pair in Deny...	Zones policy deviation was detected in Deny All Communication Policy and Building Controllers → Building Controllers Zones pair by 1 Siemens...	2/9/25 3:14 PM	3/26/25 2:36 AM	Site 1	Commonly Use... +3	Unresolved
☐	#13718	Policy Deviation Alert	Zones Policy Deviation	Zones Policy Deviation: IoT Cameras → No Zone Zones pair in Deny All Communication...	Zones policy deviation was detected in Deny All Communication Policy and IoT Cameras → No Zone Zones pair by 12 devices	2/26/25 12:21 PM	3/25/25 5:08 PM	2 Sites	Commonly Use... +3	Unresolved

ALERTS ALLOW TEAMS TO TEST POLICIES BEFORE THEY'RE ENFORCED, FINE TUNING FOR THE BEST BALANCE OF RESTRICTIONS WHILE PRODUCTION KEEPS FLOWING

In testing their established policies, our Food & Bev customer learned two important things. First, they had a class of switches that were internet exposed, which significantly added to their attack surface and overall risk score. Second, traffic to a Rockwell HMI in their most business-critical production line was being received on port 3389. Communication to this port was denied in their initial policy, but this HMI needed to receive data from this particular server, so the policy was customized to better suit their environment.

5. Enforce Policies

Integrate with a NAC or Firewall to enforce network communication policies

As we know, a policy-based approach to network protection requires both a PDP and a PEP. Now that we have tested the alerts to initially refine policies, it's finally time for policy enforcement.

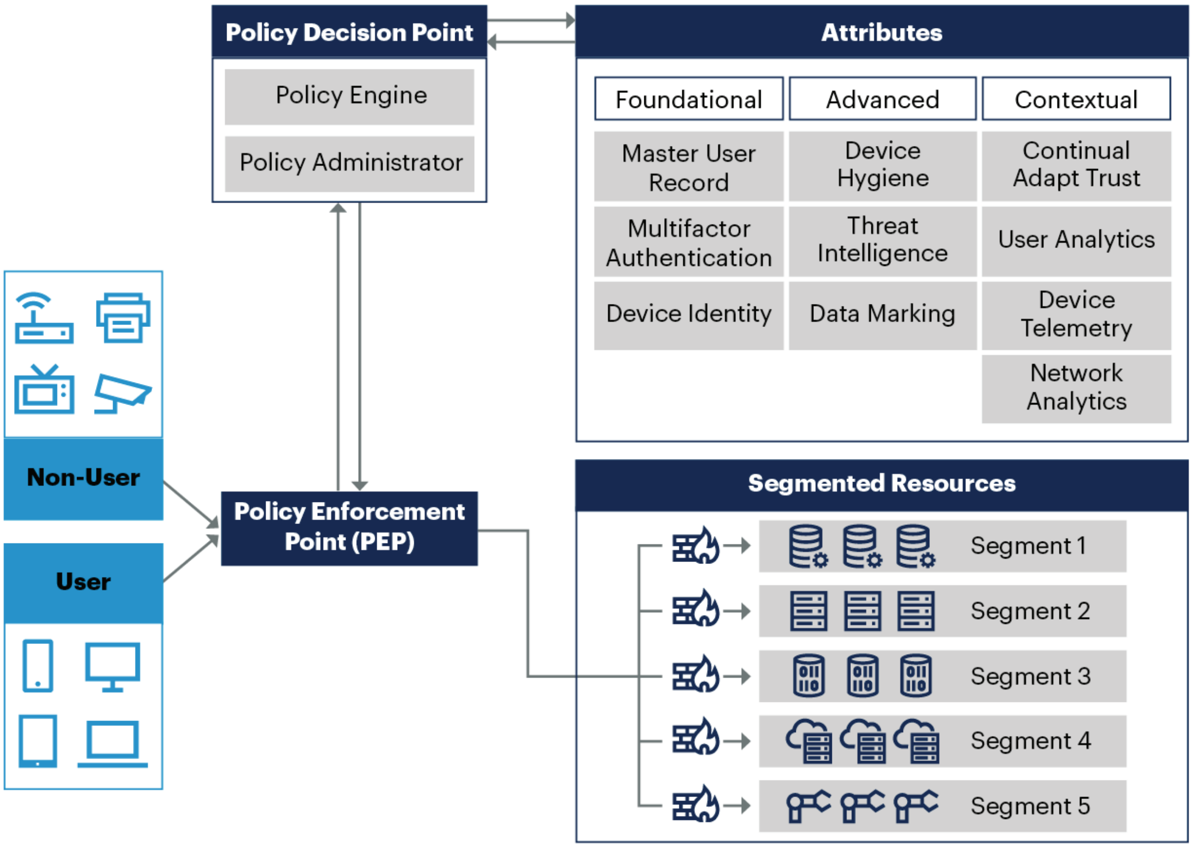
A PEP takes the decisions from the PDP and, well, enforces them. These are the NACs, firewalls, and VLANs that allow or block device communications according to the policies you've created.

Integrating your PDP and PEP helps streamline this process, allowing policies to be applied in your NAC or firewall. This integration also enables policies to be dynamically refined based on feedback from the enforcement point.

Gartner considers, "Both a PDP and a PEP are foundational to build a basic zero trust architecture." PDPs are responsible for evaluating access requests against defined policies and making authorization decisions based on contextual information, making them the brains of the operation, directing PEP actions.

The Food & Bev customer team was now ready to add tested policies to their Palo Alto Firewall to begin controlling the flow of traffic across their segmented network. Once enforced, they continue to monitor deviation alerts in xDome as their early warning system for threats, and to identify unintended consequences of device changes. Since then, they successfully stopped the early signs of a targeted ransomware attack by identifying attempted lateral movement, saving the organization significant financial and reputational losses.

Zero Trust Functional Overview



Source: Gartner
805852_C

Gartner

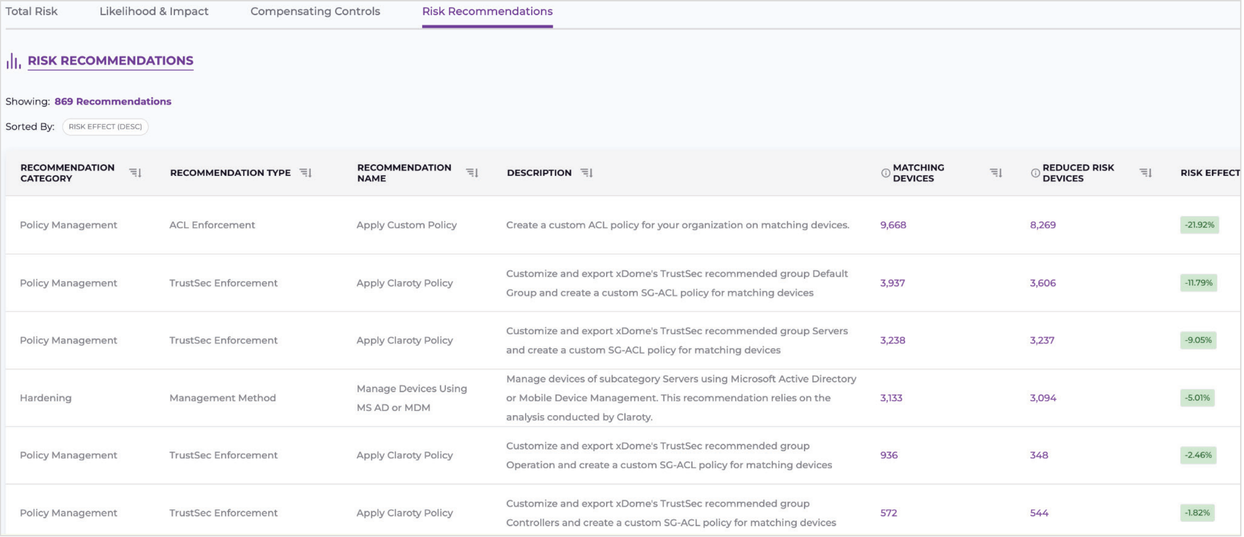
GARTNER, PREDICTS 2024: ZERO TRUST JOURNEY TO MATURITY, DECEMBER 15, 2023

At Claroty, we understand the importance of PDPs and further simplify this workflow by providing policies pre-written according to your NAC or firewall, alongside zones that can be pushed directly to your firewall.

Conclusion

Network protection takes entire classes of risk off the table.

But, this is not an easy process. It takes time and effort to get it done and get it right. But the impact to risk is significant. At Claroty, we've seen segmentation have the greatest risk reduction of any remediation efforts – a whopping 12x greater than remediating a CVE across hundreds of your devices.



RISK RECOMMENDATIONS

Showing: 869 Recommendations

Sorted By: RISK EFFECT (DESC)

RECOMMENDATION CATEGORY	RECOMMENDATION TYPE	RECOMMENDATION NAME	DESCRIPTION	MATCHING DEVICES	REDUCED RISK DEVICES	RISK EFFECT
Policy Management	ACL Enforcement	Apply Custom Policy	Create a custom ACL policy for your organization on matching devices.	9,668	8,269	-21.92%
Policy Management	TrustSec Enforcement	Apply Claroty Policy	Customize and export xDome's TrustSec recommended group Default Group and create a custom SG-ACL policy for matching devices	3,937	3,606	-11.79%
Policy Management	TrustSec Enforcement	Apply Claroty Policy	Customize and export xDome's TrustSec recommended group Servers and create a custom SG-ACL policy for matching devices	3,238	3,237	-9.05%
Hardening	Management Method	Manage Devices Using MS AD or MDM	Manage devices of subcategory Servers using Microsoft Active Directory or Mobile Device Management. This recommendation relies on the analysis conducted by Claroty.	3,133	3,094	-5.01%
Policy Management	TrustSec Enforcement	Apply Claroty Policy	Customize and export xDome's TrustSec recommended group Operation and create a custom SG-ACL policy for matching devices	936	348	-2.46%
Policy Management	TrustSec Enforcement	Apply Claroty Policy	Customize and export xDome's TrustSec recommended group Controllers and create a custom SG-ACL policy for matching devices	572	544	-1.82%

NETWORK PROTECTION CONTROLS CREATE SIGNIFICANT RISK REDUCTION FOR ORGANIZATIONS WITH CYBER-PHYSICAL SYSTEMS

Partnering with a cyber-physical systems protection platform that gives you visibility, context, and understanding of your network and device communication is the key to successfully implementing a network-centric risk reduction strategy.

If a PDP is the brains behind effective Zero Trust architectures, why not trust the platform with two PDPs that ranked highest and furthest to the right in the 2025 Gartner® Magic Quadrant™ for CPS Protection Platforms.

Ready to win at network protection? Reach out for a demo today.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection — whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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. To learn more, visit claroty.com.