

INTEGRATION BRIEF

Claroty and Check Point IoT

Protection, Virtual Patching, Unified Threat Exposure Management

The Modern Industrial Cyber Security Challenge

With billions of smart devices in use today, there are 10 times more connected devices than ever before. As a result, the expansion of the attack surface has made traditional security measures insufficient. As industries embrace digital transformation, the rapid surge of connected devices, especially in critical infrastructure sectors, introduces new vulnerabilities that must be managed. Organizations are tasked with protecting sensitive data and ensuring the continuous operation of mission-critical systems, all while facing an increasing volume of sophisticated threats. This growing complexity calls for an integrated response, combining deep visibility, advanced threat detection, and robust security controls.

The partnership between Claroty xDome and Check Point IoT protection directly addresses these challenges, offering a unified solution that enhances asset visibility, strengthens risk management, and accelerates device protection via segmentation, virtual patching, and expedited incident response across complex and interconnected networks.

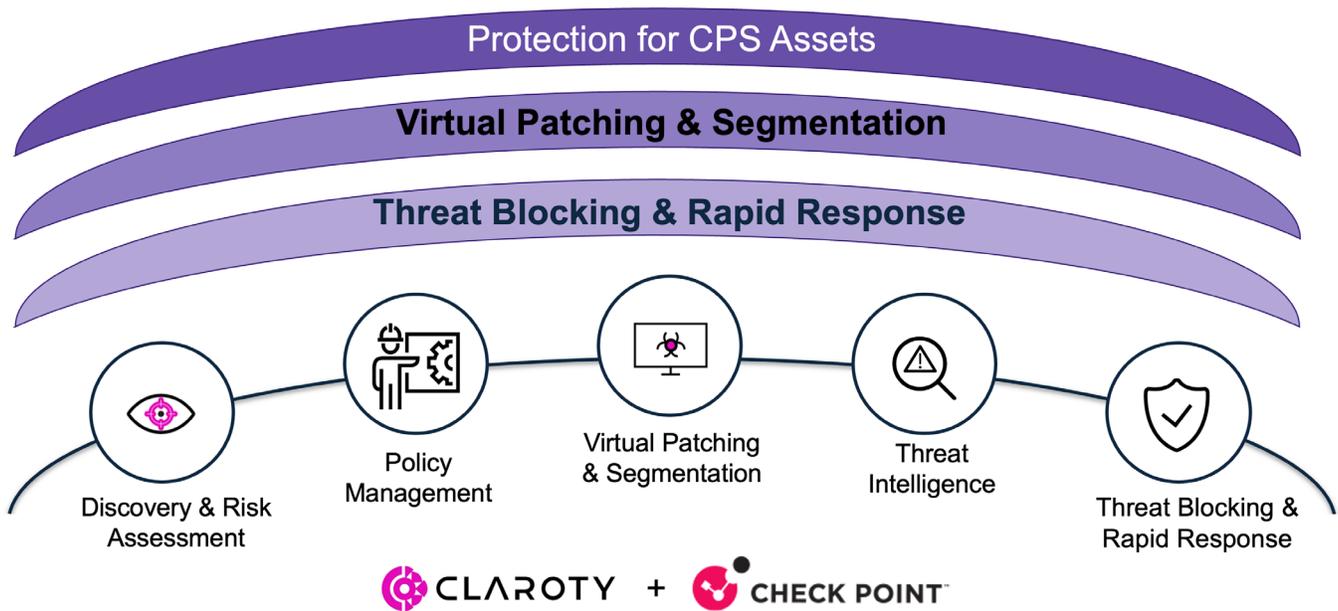
Protection for OT, IoT, and other Cyber Physical Systems (CPS)

The collaboration between Claroty xDome and Check Point IoT protection offers a unified security solution that addresses the unique challenges of securing OT, IoMT, IoT and other CPS environments. By combining Claroty's deep asset visibility and threat detection capabilities with Check Point's advanced security measures, organizations benefit from a comprehensive approach to cybersecurity. This integration streamlines security operations, reduces complexity, and enhances the organization's ability to protect critical assets from evolving threats.

Key Features & Benefits

- Discover and assess risk for IoT, OT, and IoMT devices.
- Managed security policies dynamically with intelligence exchange for real-time threat responses.
- Virtually patch and segment devices to protect vulnerable assets from threats.
- Expedite response and block malicious intents with a centralized risk view.

Better Approach To CPS Protection Security Response



The collaboration between Claroty xDome and Check Point IoT protection provides a robust, unified approach to securing cyber-physical systems. This integration enhances asset visibility, strengthens security measures, and streamlines incident response, delivering significant value to organizations seeking to protect their critical infrastructure.

Impacts	Benefits
Maximize Technology Investments	Leverage the combined strengths of Claroty xDome and Check Point IoT optimizes existing security infrastructure, providing enhanced protection without the need for additional standalone solutions.
Discovery & Risk Assessment	Comprehensive asset discovery and centralized risk posture view ensures that all devices, including unmanaged and IoT devices, are identified and continuously monitored.
Virtual Patching & Segmentation	Protect devices and device groups by creating assets zones and applying policies to segment, virtually patch, and protect devices from external threats and exploits.

Threat Intelligence for CPS

Enrich device intelligence by combining Claroty's detailed asset profiles with Check Point's threat intelligence, providing a more comprehensive understanding of each device's risk profile.

Block Malicious Intent

Accelerate incident response times, enabling organizations to swiftly contain and remediate threats to CPS with enhanced visibility and real-time threat detection, minimizing potential damage.

Contact us to learn more about how Claroty xDome and Check Point IoT delivers OT and other CPS assets protection needed for industrial, healthcare, and commercial operational resiliency.

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

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.