SOLUTION OVERVIEW

Claroty and Frenos

Transforming OT Security from Passive Monitoring to Active Validation

Industrial organizations struggle with a fundamental disconnect between security visibility and actionable risk reduction. Too many alerts, not enough context of their Cyber-Physical Systems (CPS), and no idea how to prioritize remediation actions leave these critical environments and processes at risk of downtime.

Security teams face pressure to prove their programs are effective beyond checkbox compliance, yet defenses for are infrequently tested. Claroty and Frenos address these challenges for joint customers across critical infrastructure industries.

The Joint Solution

Claroty xDome and CTD provide comprehensive visibility into what exists in CPS environments, while Frenos adds testing capabilities for the critical question: "Can an attacker actually exploit these conditions to cause damage?"

This integration enables security teams to continuously validate their defensive posture against real-world attacker behavior, measure actual exploitability of detected vulnerabilities, and prioritize remediation based on demonstrated risk rather than theoretical scores. Organizations gain confidence that their security investments in people, processes, and technology are effectively reducing attack surface.

Key Features & Benefits

- **Validated Source of Operational Truth:** Claroty provides the foundational visibility and trusted asset inventory required for meaningful risk reduction.
- **Automated Exploitability Assessment:** Frenos ingests Claroty's asset and vulnerability intelligence to model how attackers could weaponize environmental conditions and identify potential attack paths.
- **Safe Red Team Validation:** Frenos leverages Claroty's asset understanding for automated penetration testing without touching production systems.

Threat-Informed Vulnerability Prioritization

The joint solution informs security users which exposures could impact critical systems. Frenos ingests Claroty's deep asset understanding to build environment-specific digital twins. The Frenos AI adversary agent, SAIRA, analyzes which vulnerabilities are actually exploitable and then provides specific remediation options.

Continuous Validation of Segmentation and Firewall Policy Effectiveness

Validating that network segmentation prevents unauthorized lateral movement typically requires risky live testing. Claroty provides the necessary visibility into network communications and device connections, which Frenos uses to model and simulate attacks. This allows security teams to validate that segmentation designs successfully protect high-value OT targets.

Threat Actor Emulation and Exposure Assessment

When new threat intelligence emerges, organizations must rapidly assess their exposure. This integration allows security teams to immediately emulate specific threat actor TTPs within the digital twin. Claroty provides the detection layer and environmental context, while Frenos replicates the attack sequence to determine if a threat can lead to production disruption, transforming abstract warnings into concrete defensive assessments.

About Claroty xDome

Claroty xDome is a modular, SaaS-powered industrial cybersecurity platform that scales to protect your environment and fulfill your goals as they evolve. xDome extends core industrial cybersecurity controls across multiple use cases on your industrial cybersecurity journey and is designed for flexibility and ease of use, seamlessly integrating with your existing tech stack.

The foundational module of this platform is xDome Essentials. Starting with comprehensive, accurate, and in-depth network discovery capabilities, xDome Essentials offers core features across an array of use cases including vulnerability & risk management, network protection, threat detection, and asset & change management. In addition to the core value provided by xDome essentials, the platform's capabilities can be enhanced through the advanced modules for Vulnerability & Risk Management, Network Security Management, and Threat Detection.

About Claroty Continuous Threat Detection (CTD)

CTD was created to help both IT and OT teams overcome challenges associated with digital transformation and a converged IT/OT network environment. As the foundation of The Claroty Platform's comprehensive industrial cybersecurity capabilities, CTD is backed by an unmatched library of industrial protocols, three unique asset discovery methods, proprietary DPI and virtual segmentation technology, and the renowned Claroty research group, Team82. This solution empowers customers to reveal and protect their XIoT assets, detect and respond to the earliest indicators of threats, and seamlessly extend their existing enterprise security and risk infrastructure and programs to harden their industrial networks. CTD extends the same controls IT security teams use to minimize risk in IT environments to OT environments.

About Frenos

Frenos is the industry's first fully simulated AI penetration testing platform, combining digital twin technology with an AI reasoning agent that thinks like an adversary to reveal every attack path in your OT environment, risk-free. Frenos transforms how operational technology (OT) cybersecurity teams assess the cybersecurity posture of mission-critical sites and environments, reducing assessment time from months to minutes with zero impact on operations. Discover more at frenos.io. Follow our blog and connect with us on LinkedIn.

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.