SOLUTION OVERVIEW

Claroty and Rapid7

Enterprise Attack Surface Management for All Assets

The Industrial Cybersecurity Challenge

Digital transformation is introducing increasingly connected Cyber-Physical Systems (CPS) into industrial, critical infrastructure, building automation, and other complex environments to deliver a wide array of benefits, including accelerated productivity, cost savings, and innovation. While this connectivity has spurred some of the most rapid growth trajectories in recent history, it has far outpaced industrial organizations' abilities to properly secure their networks–resulting in an expanded attack surface in extremely valuable and mission-critical operational environments.

With each additional unmanaged device, organizations expand their exposure to risk. It can be easy to fall into the trap of chasing greater efficiencies and control over processes without pausing to consider the impact these devices may have on the enterprise's overall security posture.

Key Features & Benefits

- **Eradicate blind spots** – Eliminate shadow IT and enhance security by monitoring your OT and IT asset inventory to identify and address coverage gaps.
- **Unified View of Attack Surface** – 360° view of your attack surface that teams can trust to detect and prioritize security issues from cyber-physical to cloud.
- **Accelerate response** – With relevant context around assets and exposures, teams can respond faster and triage the full blast radius of an attack across IT and OT environments.

Streamlined Risk Management: Prioritize, Comply, and Anticipate Threats

Prioritize Remediation – Providing exposure context for both IT and OT CPS devices gives teams a comprehensive view to manage critical business risks. This approach offers clear internal and external perspectives, enriches assets with first and third-party data, and delivers a customizable risk score to swiftly prioritize remediation based on toxic combinations.

Enforce Compliance – Gain control of your compliance posture across your dynamic, hybrid environment. Discover assets that are missing required controls or permissions as well as enforce organizational policies by leveraging automation that sends out alerts the moment drift occurs.

Anticipate threats – Eliminate systems integration headaches and drive greater efficiency with native, no-code automation that drives remediation and faster time-to-response. Plus, with automated notification and ticketing, developers get real-time feedback to minimize greater risk before production even begins.

Comprehensive Asset Visibility with Rapid7 Surface Command and Claroty xDome Integration

Rapid7 Surface Command ingests CPS data from Claroty xDome, platforms via a tested and certified integration. Rapid7 then aggregates and correlates this information and other relevant findings with security data collected from numerous third-party security tools to provide organizations with a complete and comprehensive inventory of SaaS, Cloud, IT, OT, and other CPS assets.

> **"Only 17% of organizations can clearly identify and inventory a majority (95% or more) of thier assets."**
>
> 2024 Gartner Innovation Insight: Attack Surface Management

About Claroty xDome

Claroty xDome is a SaaS-powered CPS 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 exposure 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 Exposure Management, Network Protection, and Threat Detection.

About Rapid7 Surface Command

Rapid7's Surface Command is a comprehensive exposure management solution that provides full visibility into your attack surface, from endpoints to the cloud. It combines high-fidelity risk context with detailed environmental insights to help teams identify and prioritize vulnerabilities effectively. The platform integrates data from both native and third-party sources, offering enriched asset information and automated risk scoring. This enables organizations to manage compliance, anticipate threats, and remediate risks efficiently.

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.

About Rapid7

Rapid7 is a leading cybersecurity company founded in 2000, dedicated to simplifying and enhancing digital security for organizations worldwide. The company offers a comprehensive suite of products and services, including vulnerability management, incident detection and response, application security, cloud security, threat intelligence, and security orchestration and automation. Rapid7's solutions, such as InsightVM, InsightIDR, and InsightCloudSec, empower security professionals to manage and mitigate risks effectively, providing full visibility into their attack surface and enabling swift, informed decision-making.