Claroty Announces Major Enhancements to Market-Leading Industrial Cybersecurity Platform

*Groundbreaking multispectral data acquisition and network segmentation capabilities provide deeper OT network visibility and reduce risk for industrial enterprises and critical infrastructure providers*

**NEW YORK, December 11, 2018** – Claroty, the leader in operational technology (OT) network protection, today announced several significant enhancements to its award-winning Continuous Threat Detection product and technology integrations with several leading industrial automation, network infrastructure and cybersecurity providers. Already the industry’s most complete industrial control systems (ICS) cybersecurity platform, this release incorporates new functionality to provide even more “extreme” visibility into ICS networks and help industrial enterprises decrease the risk of a cyberattack.

The latest release of Claroty Continuous Threat Detection provides a large number of significant enhancements including:

- **Virtual Zones and OT Network Segmentation** – an innovative approach to creating both virtual and policy-based segmentation for your OT network without the typical time, expense and disruption. Read [here](#) for more detail.

- **Multispectral Data Acquisition** – a groundbreaking new approach to data collection that provides nearly 100% visibility into all the assets in the OT network environment, what they are, what function they perform, configuration information, how the assets are communicating in the network and specific details about the application-level (Layer 7) process automation “conversations.” Read [here](#) for more detail.

- **Technology Ecosystem Integrations** – Claroty has expanded its technology integration ecosystem to include partnerships with several additional market-leading industrial automation and cybersecurity technology providers. These integrations enable enterprises to better leverage their current OT investments in technology, processes and training. A complete list of integrations is available [here](#).
“From the beginning, Claroty’s focus has been to provide our customers with the deepest possible visibility into all the assets in their OT environment, including granular configuration information for each asset, how the assets are communicating on the network and specific details about process automation conversations,” said Dr. Benny Porat, CTO and co-founder of Claroty. “Our new multispectral data acquisition raises the bar on the insights we can deliver and provides the foundation for our industry-leading threat detection and unique network segmentation capabilities.”

The enhancements to Continuous Threat Detection are part of the Claroty Platform and built on Claroty’s advanced CoreX engine. This fully integrated platform is unparalleled in its depth, coverage and scalability. It provides:

- **Real-time Threat Detection** including advanced anomaly and signature-based detection for complete coverage of known and unknown threats and analysis tools for ICS threat hunting.

- **Continuous Vulnerability Monitoring** enabling customers to uncover and remedy network configuration “hygiene” issues and identify assets with known vulnerabilities (CVEs).

- **Secure Remote Access** with policy- and workflow-based access control and session monitoring.

- **Enterprise Scalability** including a consolidated “single pane of glass” management console for multiplant environments and integration with existing security systems (e.g., SIEM, log management, security analytics, etc.).

- **Cost-effective Deployments** in remote, bandwidth- or compute-constrained environments, leveraging an advanced sensor-based architecture suitable for use cases such as electric transmission or oil/gas pipelines.

These enhancements to the Claroty Platform fill critical gaps in the industrial cybersecurity market, where industrial enterprises and critical infrastructure providers have been increasingly impacted by cyberattacks targeting OT networks and broad-based attacks which “spillover” from IT networks into the operational environment. The release of this latest version of the platform is generally available to all existing clients as of the time of this announcement.

**About Claroty**

Headquartered in New York and launched as the second startup from the famed Team8 foundry, Claroty combines elite management and research teams with deep technical expertise from both IT and OT disciplines. The company is backed by an unrivaled syndicate of investors and partners, including some of the most important industrial control automation companies and asset owners on earth. With an unmatched understanding of ICS, SCADA and other essential OT/IoT systems, Claroty built a fully integrated cybersecurity platform. Our award-winning suite of products provides extreme visibility into industrial networks – enabling unparalleled cyberthreat protection, detection and response. For more information, visit [www.claroty.com](http://www.claroty.com).

###

*All product and company names herein may be trademarks of their respective owners.*