



Contact:

Jenna Finn
Shift PR for Claroty
jfinn@shiftcomm.com
617.779.1875

Claroty Awarded with SAFETY Act Approval by U.S. Department of Homeland Security

Company is the first OT security provider to receive DHS certification, adding an extra layer of liability protection for its customers

New York, New York - November 12, 2019 - [Claroty](#), the global leader in industrial cybersecurity, today announced that the U.S. Department of Homeland Security (DHS) has awarded its best-in-class OT network monitoring solution SAFETY Act approval, making it the first OT security provider to receive this designation. As a result, Claroty's customers now have added protection from lawsuits or claims following an act of cyber terrorism.

The U.S. Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) to encourage the development and deployment of technologies that counter terrorist threats. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter firms from developing, commercializing and deploying technologies that significantly reduce the risks or effects of terrorist attacks, including acts of cyber terrorism. The SAFETY Act creates a system of "risk management" and "litigation management" that protects both providers and users of approved technologies from potential liability.

"Claroty is proud to be the first OT security provider to receive SAFETY Act approval, which means we are now offering our customers even greater confidence that they are getting unmatched OT security as well as important liability protection," said Dave Weinstein, Claroty Chief Security Officer. "Claroty was conceived to secure the safety and reliability of industrial control networks that run the world from cyber-attacks. As it follows an extensive review by DHS, this SAFETY Act designation not only substantiates the value of Claroty's solution, but validates our position as a leader in the OT security space."

Claroty's OT network monitoring solution provides visibility into OT networks and assets through passive and active monitoring. The platform further secures industrial network operations by establishing operational network baselines and facilitating anomaly detection, network visualization and data collection on OT networks, with security alerts forwarded to a graphical dashboard for operator review. Claroty's platform is comprised of three primary components: [Continuous Threat Detection](#), [Secure Remote Access](#) and [Enterprise Management Console](#).

For additional information about the SAFETY Act, please visit the DHS Safety Act [website](#). For additional info about Claroty's OT networks monitoring solution, please visit www.claroty.com.



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 many of the world's leading industrial control automation companies and asset owners. With an unmatched understanding of ICS, SCADA and other essential OT/IloT systems, Claroty provides a complete, 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.