****

**Claroty Delivers Octuple Revenue Growth for the Asia Pacific Region in 1H 2020**

*Company achieves remarkable growth in the region as critical infrastructure operators recognize the need for comprehensive, in-depth OT security*

**SINGAPORE – August 25, 2020 –** [Claroty](https://www.claroty.com/), the global leader in operational technology (OT) security, recorded octuple annual recurring revenue growth and more than tripled total contract value year-over-year for the Asia Pacific region including Japan (APJ), from the first half (1H) of 2019 to 1H 2020, fueled by growing demand for critical infrastructure security in the region.

The growth is attributed to demand arising from the introduction of regulatory frameworks in key markets, along with surging demand for secure remote access solutions, especially in the manufacturing and energy sectors. Another growth driver is Claroty’s [partnership with Deloitte](https://claroty.com/resource/claroty-and-deloitte-partner-to-boost-cybersecurity-across-apacs-industrial-technology-systems/), combining Claroty’s software with Deloitte’s expertise to boost cybersecurity in industrial technology systems across Australia, China, Hong Kong SAR, and Singapore.

Claroty’s business grew in most APJ markets, notably in Australia, Korea, Taiwan, and the ASEAN region where spending on cyber security is rising exponentially, expected to triple over the next five years to some [$5 billion by 2025](https://www.smartcompany.com.au/partner-content/articles/cyber-security-opportunity/).

**Growing Regulatory Requirements and Mounting Risk**

A contributing factor to Claroty’s growth is that operators with critical infrastructure are now obligated to meet OT security standards. Singapore’s Cyber Security Agency (CSA) revealed its [OT Cybersecurity Master Plan](https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan) in 2019, after the Monetary Authority of Singapore (MAS) had established a set of [Technology Risk Management](https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines) guidelines for financial institutions to secure their critical systems. In 2019 Thailand passed a [Cybersecurity Act](https://www.bakermckenzie.com/en/insight/publications/2019/03/thailand-cybersecurity-act-has-been-passed) and in Taiwan the [Cybersecurity Management Act](https://www.loc.gov/law/foreign-news/article/taiwan-new-cybersecurity-law-takes-effect/) was put in place. In August 2020 the Australian Government released its [2020 Cyber Security Strategy](https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf), proposing to develop legislation that would impose cyber standards on operators of critical infrastructure and systems of national significance. And the Korean Internet and Security Agency (KISA) is finalising its guidelines for [Industrial Control Systems](https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=259&dno=117&fseq=2) (ICS), which are expected to be introduced in late 2020.

**Impact of COVID-19**

Since the onset of the COVID-19 pandemic, exploitation of ICS vulnerabilities is on the rise as reliance on remote access has increased.

The Claroty Research Team’s [Biannual ICS Risk & Vulnerability Report: 1H 2020](https://info.claroty.com/biannual-ics-risk-vulnerability-report-1h-2020?utm_campaign=Biannual%20ICS%20Risk%20%26%20Vulnerability%20Report%20-%20H1%202020&utm_source=pressrelease) revealed that more than 70% of ICS vulnerabilities disclosed in 1H 2020 can be exploited remotely, noting that energy, critical manufacturing, and water & wastewater infrastructure were the most impacted sectors. Claroty researchers also recently disclosed [vulnerabilities in VPN products](https://www.claroty.com/2020/07/28/vpn-security-flaws/) commonly used in field-based industries, such as oil & gas and utilities, which could lead to a complete security breach of industrial control networks. These discoveries underscore the importance of protecting internet-facing ICS devices and remote access connections.

Thus demand has surged for Claroty’s [Secure Remote Access](https://claroty.com/secure-remote-access/) (SRA) solution, which provides a single, secure and clientless interface through which all external users can connect to perform software upgrades, periodic maintenance, and other support activities on assets within OT networks, minimising risk from remote users and third party vendors.

**Sales cycles are collapsing, positively impacting revenue**

Eddie Stefanescu, Regional Vice President, Business, APJ at Claroty, says that this year, the company’s sales cycle has halved from one year to six months, and that installations originally planned for 2021 are now expected to materialize this year.

“Overall, we’re seeing remarkable growth because our customers are prioritizing the protection of remote access to their critical infrastructure,” said Stefanescu. “They see value in Claroty’s solutions because not only can we rapidly deploy, but our solutions seamlessly integrate with existing IT security tools as well. That means that we can help protect their OT without entailing a steep learning curve.”

Claroty’s investors include Temasek, Schneider, Rockwell, and Siemens.

To learn more about The Claroty Platform, including SRA, [request a demo](https://www.claroty.com/request-a-demo/).

**--**

**About Claroty**

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty’s converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

For more information, visit[www.claroty.com](http://www.claroty.com).

MEDIA CONTACTS

ILLKA GOBIUS

Managing Director

PINPOINT PR Pte. Ltd.

illka@pinpointpr.sg | pinpointpr.sg

Singapore: +65 9769 8370

KELLY FERGUSON

Director of Communications, Claroty

kelly.f@claroty.com | +1 (862) 223 9346

claroty.com