NanoLock Security

Field: Cybersecurity, Device-Level, Zero-Trust

NanoLock's MoT (Management of Things)

Year of founding	2017
Web	https://www.nanolocksecurity.com/
Location	Hod Hasharon, Israel
Funding	USD 18.2M
Experience in global market	Major utilities, industrial companies and large ecosystem partners in Japan, Italy, Spain, Switzerland, Netherlands, India, Singapore, US and Israel.
Availability in Japanese	Yes

HackOsaka 2022
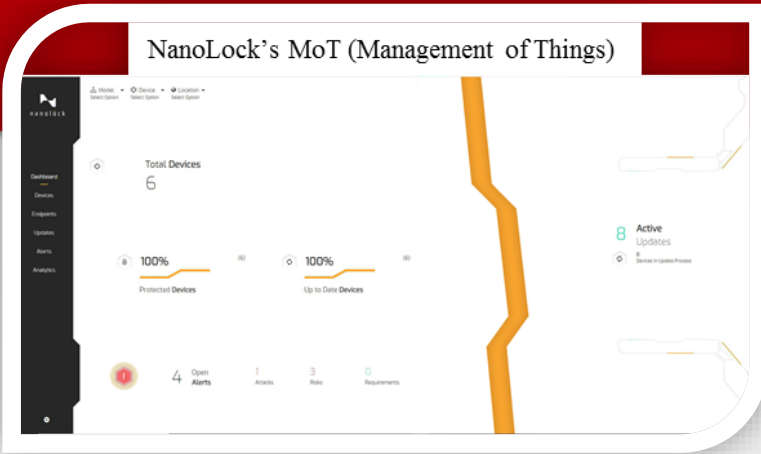
NanoLock's zero-trust, device-level protection safeguards the operational integrity of connected devices and industrial machines to secure revenue streams and support business continuity.

- NanoLock prevents unauthorized tampering of critical code and data, before it becomes operational, regardless if it is a cyber event or a human errors..

- NanoLock protects smart meters, industrial machines, sensors, EV chargers, RTUs, and other connected devices against outsiders, insiders, supply chain cyber events, and even technician mistakes.

NanoLock is working with major utilities, industrial companies and large ecosystem partners in Japan, Italy, Spain, Switzerland, Netherlands, India, Singapore, US and Israel.

Problems in society and proposed solutions

As the cyberthreat landscape of utilities & industrial manufacturing continues to evolve in terms of sophistication, complexity, and impact, connected devices and machines are eventually breached.
- Breached devices and machines compromise service integrity and revenue and jeopardize the safety of customers, employees, and the public.
- As a result, utilities and industrial companies must constantly ensure their devices and machines are operating as designed, configured, and calibrated.

NanoLock makes sure devices & machines work as intended. NanoLock's zero-trust, device-level protection secures the operational integrity of connected devices and machines against multiple attack vectors, including outsiders, insiders, supply chain and even human mistakes.

Strength of your company/ products

- Preventing all unauthorized tampering of critical code and data at the device/machine level
- Blocking insiders and supply chain tampering and even human errors
- No performance or functionality impact. Near zero power requirements.
- Applicable to all devices - legacy and new, electric or battery-operated

Business model

Annual subscription model per protected device is based on two license types:
- STANDARD license for lifetime protection as well as authenticated and managed local and remote updates
- ADVANCED license with features that yield significant operational cost savings, such as detailed alerts and unique forensic data, analytics etc.

Objectives participating in Hack Osaka Business Meeting

- Collaboration with Japanese corporations
- Finding investors