

Utilities must constantly ensure their assets are operating as designed, configured, and calibrated, in spite of the evolving cyberthreat landscape. However, assets without device-level security are inherently vulnerable and will be eventually breached, compromising service integrity, revenue, and safety.

NanoLock ensures connected devices work as intended

NanoLock Device Defender protects smart meters, EV chargers, RTUs & other connected devices against outsiders, insiders, 3rd party cyber events, and even technician mistakes. With NanoLock protection, all modifications of critical code, configuration and calibration data must be authenticated and signed before becoming operational, including those utilizing access privileges.

Mitigate tampering, fraud and theft by insiders, 3rd party, human errors, as well as outsiders cyber events

Device-level prevention for battery-operated and electric devices

Applicable to both legacy and new devices, the Device Defender's has a small footprint and minimal energy requirements with no impact on performance or functionality. It's ideal for devices with limited resources, such as battery-operated or low-end devices.

THE NANOLOCK ADVANTAGE



Security of Supply

Blocks outsider, insider and supply chain cyber events as well as human errors



Improved Safety

Prevents unauthorized tampering



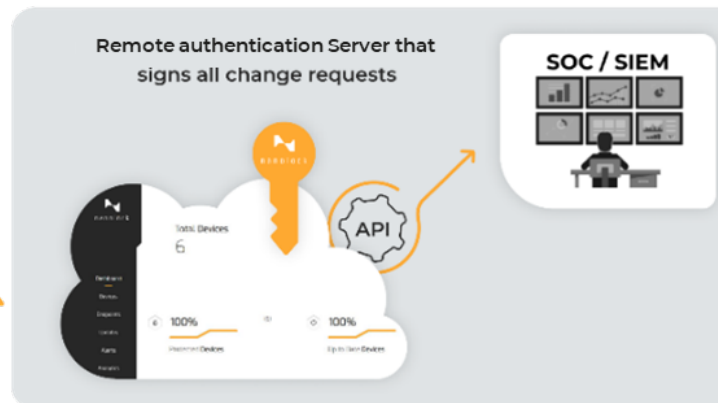
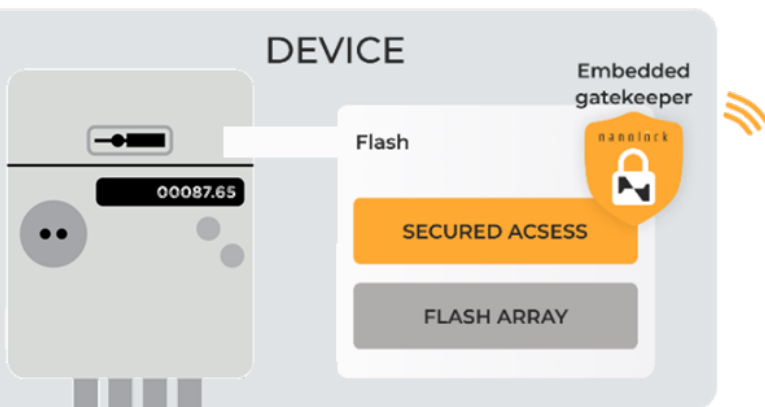
Business Continuity

Protects revenue, assets value, and brand.



Integration with SOC & 3rd Party Platforms

No impact on performance or functionality
Applicable to legacy and new devices



Reliable, multi-vendor device visibility

- Authenticated & managed OTA updates
- Device-level monitoring & posture, attack alerts, unique forensic insights,

TAP INTO ONGOING OPERATIONAL INTEGRITY AND REVENUE PROTECTION

NanoLock Security protects power generation and energy management, water and wastewater plants as well as food & beverage manufacturing.



THE CHALLENGE

Securing the operational integrity of EV chargers

- Protect EV chargers from cyber events & human errors
- Provide the highest level of protection & prevent cyber events that others cannot
- Provide secured remote and local upgrades
- Zero impact on the EV charger performance
- Works on new and legacy devices

THE SOLUTION

NanoLock's Device Defender is embedded in EV chargers to provide zero-trust, device-level protection

- Blocking cyber events from trusted sources (insiders, human errors & customers) as well as outsider adversaries
- Providing secured and validated remote and local updates
- Reliable visibility and management
- Lightweight, passive prevention with small footprint and no performance hit or functionality impact
- Works on legacy and new machines

VALUE PROPOSITION

- Competitive advantage
- Business reputation protection
- Operational integrity protection
- Reduced liability
- Regulatory compliance

VALUE FOR UTILITIES & CPO

- Security of supply
- Improved safety
- Protecting investment, revenue, assets value, and brand
- Saving remediation time and costs



THE CHALLENGE

Securing the operational integrity of smart meters

- Protect smart meters from cyber events & human errors
- Provide the highest level of asset protection & prevent cyber events that others cannot
- Comply with regulatory requirements
- No impact on performance and functionality
- Applicable to legacy & new smart meters

THE SOLUTION

NanoLock's Device Defender is embedded in smart meters to provide zero trust, device-level protection

- Protecting against outsider, insider and supply chain cyber events and even human errors
- Providing secured and validated remote and local updates
- Reliable visibility and management
- Small footprint, no performance or functionality impact, applicable even to battery operated devices
- Works on legacy and new smart meters

VALUE PROPOSITION

- Competitive advantage
- Business reputation protection
- Operational integrity protection
- Reduced liability
- Regulatory compliance

VALUE FOR UTILITIES

- Security of supply
- Improved safety
- Protecting revenue, assets value, and brand
- Saving remediation time and costs

Renesas Electronics Corporation is a Japanese semiconductor manufacturer and a global leader in microcontrollers, analog, power, and SoC products.

THE CHALLENGE

Securing the operational integrity of smart meters

- Protect the operational integrity of smart meters from cyber events & human errors
- Provide the highest level of asset protection & prevent cyber events that others cannot
- Comply with regulatory requirements
- No impact on performance and functionality
- Applicable to legacy & new devices

THE SOLUTION

NanoLock's Device Defender – a zero trust, device-level protection - was implemented in Renesas smart meters

- Protecting against insider threats
- Providing secured and validated remote and local updates
- Reliable monitoring and alerts as well as detailed forensic data
- Small footprint, no performance or functionality impact
- Works on legacy and new devices

THE VALUE



Competitive
advantage



New & recurring
revenue streams



Regulatory
compliance



Business
reputation protection



Operational integrity
protection



Improved safety



Reduced liability

CONTACT US

 info@nanolocksecurity.com

 www.nanolocksecurity.com

About NanoLock

NanoLock Security revolutionizes the IoT/IOT and connected device protection with a zero-trust, device-level prevention against outsiders, insiders, supply chain cyber events, and even technician mistakes. The winner of multiple prestigious industry awards, NanoLock is headquartered in Israel with offices in the US, Europe, and Japan.



20 Winner 2020

