Cyber Security for Building Management Systems Operation Technology (OT) Networks

BMS Security Blind Spot

Heating , ventilation, air-conditioning and other critical functions, are administered by Building Management Systems (BMS). These systems rely on Operational Networks (OT), for which operational continuity is paramount. However, facility administrators have limited visibility and no modern security solutions for the critical OT network making them vulnerable to operational disruptions, stemming from either cyber threats, or system malfunctions.

Your BMS OT Network is Vulnerable

Smart, sophisticated & highly connected, Modern OT networks share many features with IT networks. However, when it comes to security, OT networks lag way behind the IT industry standards leaving them extremely vulnerable and fairly easy to exploit.

A vulnerable OT network holds a double risk to your building:

1. Disruption of critical building processes.
2. A potential single point of failure (SPOF) to the entire BMS.

Buildings' energy and HVAC infrastructures are a soft target and have extensive damage potential.

The Cyber Threat

Your building management systems are vulnerable, and the threat to your buildings' critical functions due to OT risks is real.

"FBI: Hackers Breached New Jersey Industrial HVAC System"
"Hackers Penetrate Google's Building Management System"

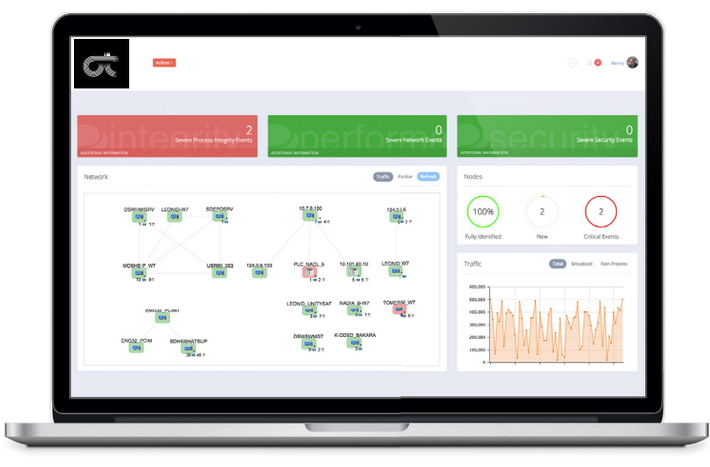
The OT network can be penetrated in a number of ways; via the IT network (Internet connection), through other remote access solutions, through the supply chain of patches and updates or via an internal threat. Shutting-down energy or HVAC systems for ransom or sabotage purposes is a threat that organizations can and should prepare for.

Claroty's Solution Provides a Comprehensive Cyber-Security Solution for BMS OT Networks

Claroty is a comprehensive cyber-security solution for data centers' OT networks, unleashing the power of modern networks to the OT world. Claroty's solution provides actionable security and visibility to OT threats, designed for the use of data center operations and information security personnel. Claroty will alert to any anomalies in communication patterns within the OT network, in addition to firmware manipulations, configuration changes, detection of new devices, attempts of spoofing, poisoning and man-in-the-middle attacks, changes in network trac load and more – all including the relevant information in order to identify attack patterns and compromised devices for actionable response.

Respond to Incidents with Maximum Visibility

Claroty's solution provides visibility to the OT network and its devices to allow optimal response to cyber incidents. Our dashboard visualizes the network components and communication channels, allowing for quick understanding of any changes or malicious activity and compromised devices. For each alert, the solution also provides a detailed forensics trail, highlighting relevant historical changes as well as allowing a full investigation of past and current network behavior.



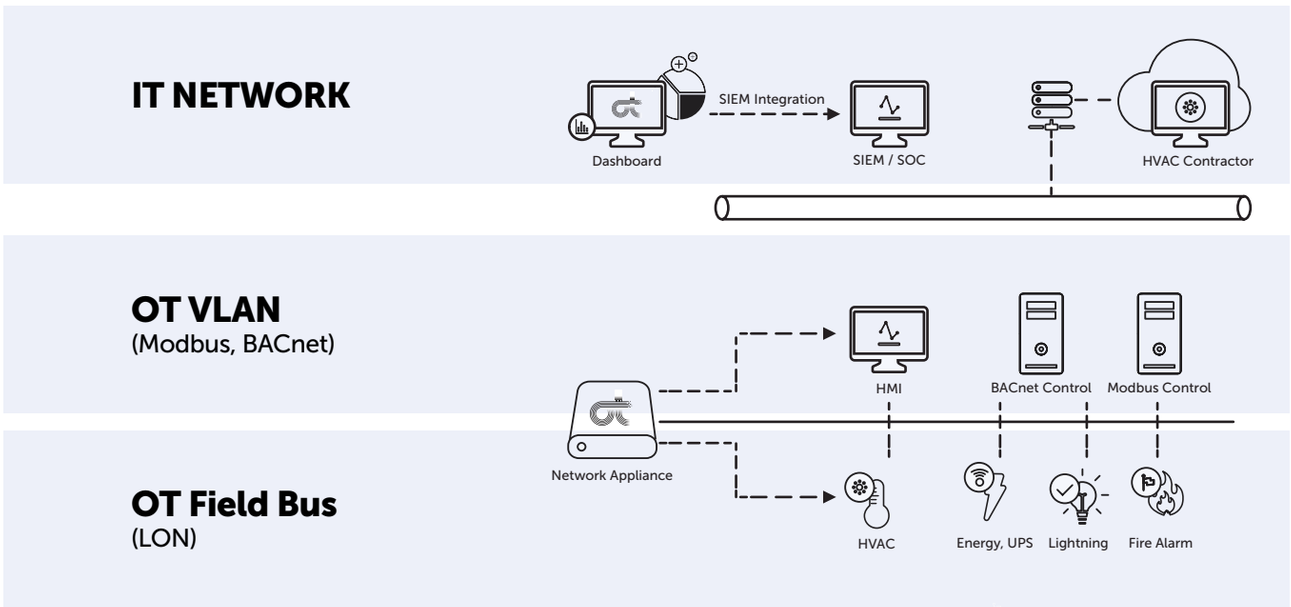
Cyber Security for Building Management Systems Operation Technology (OT) Networks

How It Works?

Claroty is a network appliance, easily deployed on Ethernet networks by connecting to a mirror/span port of existing network equipment, and on Field Bus networks by connecting the appliance as a new device to the network. Claroty2's solution passively monitors all network trac, applying deep packet inspection (DPI) capabilities, built specifically for the relevant SCADA protocols (Modbus, Lon, BACnet etc). Using advanced machine-learning algorithms, behavioral and predictive, the solution automatically whitelists a legitimate base line of activities and alerts to any suspicious anomalies. The solution is agent-less and passive, eliminating any impact or potential damage to the OT network.

Benefits

- Comprehensive cyber-security and visibility solution for your OT network
- Bridging the gap between OT and IT: visibility and alerts in the information security language
- Identify known and unknown threats (signature-less)
- Passive, no potential damage to your network
- Easy deployment, span/mirror port, agent-less
- Vendor-agnostic, no ICS vendors integration
- Supports all devices, controls and protocols



About Us

Claroty was conceived to secure and optimize OT networks that run the world's most critical infrastructures.

Claroty empowers the people who run and protect industrial systems to make the most of their OT networks. By discovering the most granular elements, extracting the critical data, and formulating actionable insights, Claroty provides extreme visibility and brings unparalleled clarity to OT networks.

Claroty was launched by the world-renowned Team8 Platform. Team8 established the world's strongest cyber security syndicate with global partners and investors including Cisco, Microsoft, Qualcomm, AT&T, Accenture, Nokia, Bessemer Venture Partners, Marker LLC, and Innovation Endeavors.

BESSEMER VENTURE PARTNERS · MARKER LLC · REDDOT CAPITAL PARTNERS · MITSUI & CO. · INNOVATION ENDEAVORS