ADVANTECH

Enabling an Intelligent Planet

Advantech eBook

intel partner Titanium IoT Solutions

Cybersecurity for Building Automation and Smart Facilities

As the number of connected devices in buildings increases, so do the opportunities for cyber criminals to exploit vulnerabilities. Discover how building automation trends may be increasing your cyber attack surface and how to safeguard connected assets.

The Impact of Connected Facilities

As networks, controls, and sensors for building management integrate with IT and the Internet of Things (IoT), structures are becoming smarter and more efficient. Rising energy costs and environmental factors, along with increased security and building requirements, are driving the need for secure, cost-effective and easy-to-implement connected building solutions.

The merging of Operational Technology (OT) and Information Technology (IT) in building networks, however, can create cybersecurity risks. Cyberattacks can lead to financial, professional, and intellectual property issues, as well as jeopardize the safety of building occupants.

Historically, cybersecurity efforts focused solely on IT systems, leading to established IT-centric solutions such as network segmentation, patch management, firewalls and antivirus software. While having these measures in place is critical, the emphasis on IT security results in a significant void regarding OT security.

Building Automation and Connected Facilities

Building automation is the centralized control of a facility's main functions through a building management system (BMS) or a building automation system (BAS): heating, ventilation, air conditioning, lighting, access control, elevators, life safety systems and more. The goal of BMS or BAS implementation is multi-faceted—to increase occupant comfort and safety, improve building efficiency, reduce energy consumption and operating costs and gain a holistic view of resource usage trends.

Educational facilities may use a BMS for maintaining a safe learning environment or air quality (various state/federal requirements mandate safe CO2 levels). Hospitals or medical offices can utilize automation for reducing energy consumption while also ensuring patient safety and comfort. Offices may require a BMS to monitor building conditions and security. The usage options and associated benefits are limitless.

Smart building technology revolutionizes building management by enhancing control and efficiency over critical systems. In turn, building managers see improvements in operations and working environments, and a reduction in energy consumption and related costs. To achieve these benefits, however, connected devices for real-time data collection and controls are necessary.

In one example, a recent Advantech smart building project focused on data-driven energy management. Nanjing Nengkong, established in 2017, aims to be a top innovation service provider in China's construction engineering sector. With a primary focus on green buildings, they are dedicated to offering intelligent energy management solutions for structures utilizing advanced IoT technologies.

Use Case Example: Energy Management in Public Buildings

Nanjing Nengkong's business largely involves the smart transformation of public building projects. Emphasizing sustainability, energy conservation and emission reductions, the government established clear policies and guidelines. Local authorities also mandate central or state-owned enterprises to promote smart building construction for new commercial spaces.

Advantech collaborated with Nanjing Nengkong to develop a tailored, cloud-based smart monitoring solution for efficiency improvements in a 26-story court building. The solution covers facility functions like energy consumption analysis, fire control, equipment asset management, HVAC systems and IT room management.

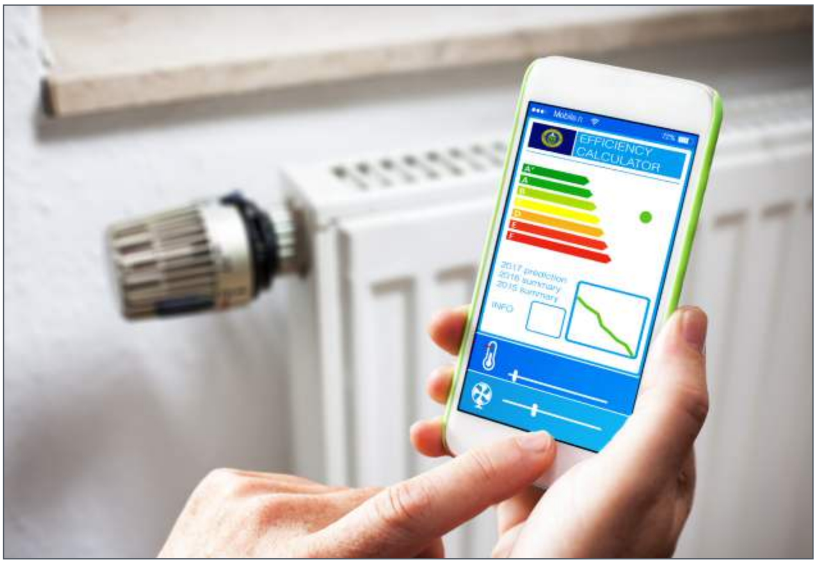
In this specific solution, the Advantech ECU-1051 IoT gateway and WISE-Edgelink edge software gather data from a PLC via the Modbus/TCP protocol. The data is then securely transmitted to the cloud platform using the MQTT protocol in 4G mode with an Advantech HPC-7282 lightweight server facilitating privatization for added safety and reliability.

The equipment lifecycle management, building energy management and smart security management systems are integrated through Advantech's smart building platform. The result is a system for real-time monitoring and management.

What Can be Achieved with Cyber-Secure Building Automation?

- Access to real-time, 24/7 security protection
- Visibility of facility resource trends for efficiency improvements
- Overall cost savings with energy usage enhancements
- Ability to lower building insurance costs
- Maintain reputation with building occupants and end-users, and maintain occupant comfort
- Reduce risk of future cyberattacks and associated costs
- Enhanced lease potential with a 'cyber-safe' building
- Maintain overall safe building operations through cybersecurity

OT/IT Networks & Cyber Attack Surface



As building automation systems increase in popularity, it is crucial to protect IoT-connected devices from external cyber threats. Breaches in connected building systems can lead to manipulation of various settings, equipment damage, compromised data, disrupted business operations and/or significant financial losses.

IT and OT networks are converging within the IoT to the network edge at a rapid rate across varying industries and infrastructure. Previously, engineering teams utilizing OT networks and IT management were in two differing siloes. The growing network convergence offers significant benefits for business intelligence, but also creates new avenues for cyber-attacks.

The digital attack surface of an organization encompasses all possible routes that may be vulnerable to unauthorized access. Addressing these cybersecurity challenges can be a daunting task for IT departments. Utilizing traditional IT cybersecurity methods may not be viable in OT systems, especially those containing legacy equipment or infrastructure.

Combined with growing hacker sophistication and an increase of connected, remote devices, additional pathways to sensitive data are at risk. Additionally, many organizations utilize numerous proprietary systems with multiple protocols from multiple vendors.

With varying levels of control over cybersecurity of complicated IT systems and connected devices, remote support from 3rd-party vendors may look like a solid solution. However, remote support from external vendors may increase the risk of compromised connections, in addition to potentially unsecure systems or data corruptions.

5 Ways to Protect Your Building Devices

Transferring IT security methods to OT devices leave commercial and industrial facilities open to cyber-attacks. To mitigate these risks, it is essential to secure networks and IoT-connected devices with a combined approach. This involves implementing strong security measures, such as:

1. **Network Security**: solutions like firewalls help prevent unauthorized access to a network, and network segmentation helps limit exposure if a breach occurs.

2. **Software Updates**: regular software updates and patches are necessary to address system vulnerabilities.

3. **Physical Security Measures**: smart building devices should be physically secured with access restricted to authorized personnel only. This helps prevent unauthorized physical access and tampering, which can compromise overall security or allow for device spoofing.

4. Security Processes: document security processes and implement regular audits to ensure processes are followed and teams know how to respond in a cybersecurity event. Smart building devices should integrate into the overall security architecture of the facility. Safeguard devices with a comprehensive security plan that includes incident response procedures, regular security audits and security awareness training.

5. Device-Level Security: authenticate devices to each other using a zero trust framework so only authorized device-to-device communications are permitted with encrypted communications.

Why You Need Device-Level Endpoint Protection

With device-level protection in place, every building, manufacturing, or process control OT device becomes its own security powerhouse. By implementing device-level identification and mutual authentication, a zero-trust security environment is ensured, keeping systems safe and secure.

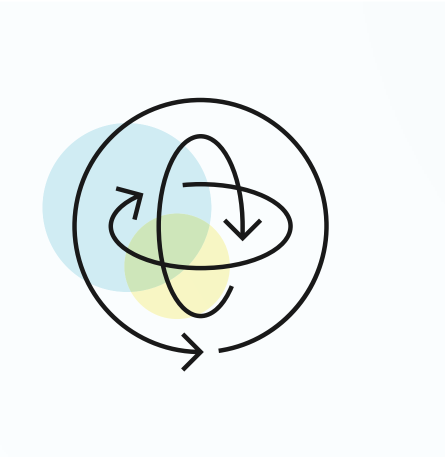
By empowering each OT device with self-defense through mutual authentication, device-level protection offers security for connected devices that firewalls and micro-segmentation alone cannot match.

Device-level endpoint protection benefits include the following:

- Prevents attackers and attack traffic from connecting or communicating with protected building, manufacturing and process control OT devices
- Prevents attack propagation through protected endpoints
- Surrounds device communications with future-proof advanced encryption tunnels

With device-level endpoint protection safeguarding OT devices, attackers cannot establish a foothold. Only identified, authenticated OT endpoints can connect to and communicate with each other, preventing communication from unauthorized users or devices.

Device-level security also ensures connections from the Internet or connections from the Cloud are off-limits. Any unidentified and unauthorized device connections are automatically rejected.



Case Study Briefs

Secure Building Management in Action

Access Control Measures for 24/7 Fitness Centers

An Advantech customer who supplies advanced security solutions, including door access and video surveillance systems, to a global chain of fitness centers needed to provide top-notch security. This specific fitness center chain operates unmanned gyms, providing 24/7 accessibility via key-cards.

The client sought a comprehensive solution encompassing surveillance cameras, video recording, IPTV, Wi-Fi, VoIP and more. Each facility was also equipped with its own dedicated WAN access through Ethernet switches, routers and other necessary components. These networks and devices required cyber protection.

To help design an ideal system, Advantech offered a USB RS-422 converter interface for the building control system. All public areas in the gyms are equipped with cameras and client data is stored in the Cloud. Maintaining security to these connected devices and networks was top priority.

With the isolated Advantech USB to RS-422/485 converter, the BB-USOPTL4, the host PC links to the door circuit or RFID access relay device. By connecting the PC through Ethernet to a location-wide LAN there is seamless integration. The door entry system's serial connection was a key aspect in selecting Advantech's equipment.

Prior to implementing Advantech's USB converter solution, the client relied on a PCI serial expansion card. By transitioning to the USB to serial converter, they were able to enhance PC performance and boost reliability and security.

The client opted for a customized private label version of Advantech's standard BB-USOPTL4 for several reasons. First, it allowed them to streamline support by directing all inquiries to their team. Secondly, the tailored label design facilitated standard installation guidelines for a seamless experience. This way, installers can effortlessly follow the label and match colors without needing prior knowledge of RS-485.

Campus Energy Management with a LoRaWAN Network

In Northern Taiwan, a county government sought to enhance the learning experience for elementary and junior high school students by implementing air conditioning and solar panels to buildings. This initiative not only aimed to create a comfortable learning atmosphere, but also aimed to alleviate the financial strain of energy expenses by utilizing data-driven decision-making and monitoring.

To enhance efficiency and minimize labor expenses, the energy management system required remote monitoring and control, allowing for streamlined management across several district facilities. Furthermore, the new system needed to deliver features like electricity consumption management, automated demand response, real-time monitoring, in-depth statistical reporting, robust system management and device-level security.

Advantech offers a seamless LoRaWAN wireless network solution specifically designed to enhance facility energy management. It tackles challenges faced by rural building networks, such as weak signals, sluggish connection speeds and insufficient telecommunications infrastructure. Utilizing the Advantech WISE-2200-M and WISE-6610, networks can be easily set up to send data to the Cloud.

By utilizing the long-range and high penetration capabilities of LoRaWAN, alongside the simple installation and flexible configuration of the WISE series, users can effortlessly implement a cost-effective management solution. The WISE-6610 boasts an array of features tailored for edge intelligence systems, exhibiting both hardware and software adaptability. Furthermore, its compatibility with various VPN tunneling protocols guarantees secure communication channels.

The sleek, compact design of the WISE-2200-M (measuring 7.1 x 5.2 x 3 cm) incorporates a specialized connector for industrial control, ensuring the device remains securely in place and minimizes the chances of dislodgement. This offers enhanced reliability and protection in outdoor settings. Additionally, the WISE-2200-M eliminates the need for a separate power cable by allowing direct connection to a device's USB port, simplifying installation and adding convenience.

A Smart System for Monitoring & Control in School District Buildings

Faced with multiple building monitoring challenges, the Chicago Public Schools (CPS) district sought an integrated system for district buildings to integrate IT and OT networks. Additional requirements included monitoring indoor air quality, temperature and humidity control, lighting control, occupancy tracking, management of safety measures for building accessibility and more.

Ultimately, the objective was to enhance energy efficiency, reduce operational and maintenance expenses, ensure the well-being and safety of the building's occupants (employees, staff and students) and facilitate access to resource data for more analytics-driven monitoring and management.

Watch the Chicago Public Schools Case Study Video at

https://go.advantech.com/CPS

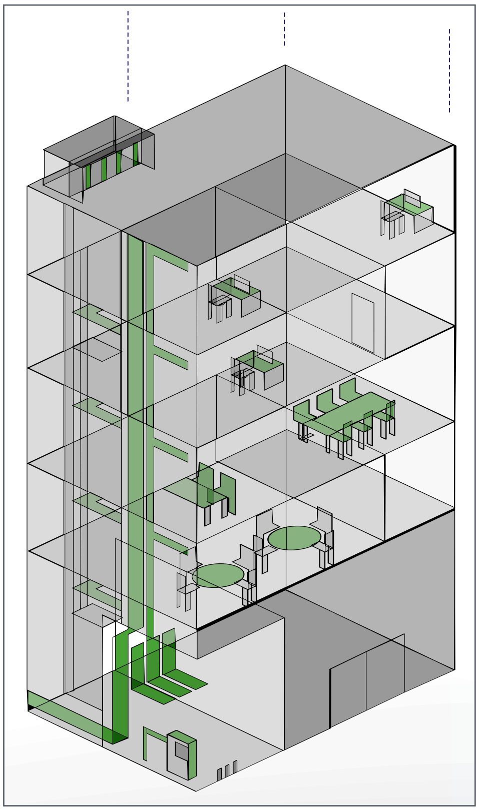
This finalized solution includes Advantech’s Intel-based UNO-420 Power over Ethernet (PoE) sensing gateway and KMC Commander®, an IoT and Automation Platform from KMC Controls, a strategic partner of Advantech. The UNO-420 supports an Ethernet cable for both data and power delivery. The gateway collects data from sensors, devices, controllers and other building systems, which feed into KMC Commander.

The KMC Commander platform is a secure platform that tracks data and trends based on the preferences set by CPS. Users can also use KMC Commander to set up alarms and notifications, create schedules and configure internal and external user-profiles segmented by authorization with custom dashboards. Additional features of KMC Commander include a responsive user interface, cellular capability and cloud service powered by Amazon Web Services (AWS).

The UNO-420 device includes built-in support for Trusted Platform Module (TPM) 2.0 for cybersecurity. TPM is essentially a small, powerful microcontroller designed to safeguard vital information on platforms, such as a PC or laptop. By securely storing essential authentication data like passwords, certificates and encryption keys, TPM support helps keep digital assets safeguarded.

Additionally, the UNO-420 gateway is pre-certified and pre-loaded with Ubuntu 20.04 LTS. By certifying Advantech's UNO-420 for Ubuntu 20.04, Canonical—publisher of Ubuntu—guarantees five years of maintenance updates and five years of extended security maintenance (ESM) software support to deliver enterprises a stable and secure IoT platform for connected devices.

With Ubuntu 20.04 the UNO-420 offers enhanced security and stability, including constant security patching processes and features like kernel self-protection, stack-clash protection, control flow integrity and more.



Eliminating Cyber Vulnerabilities in Existing Building Networks with DOME

A client and building owner needed to address cyber vulnerabilities threatening an entire building network and its associated systems. The OT networks and devices running the building's daily operations lacked cyber protection. Without proper security measures, connections to OT networks through IT or IoT networks pose a vital threat to internal systems.

The customer recognized their BMS—and unsecured devices on every floor—presented easy entry points for a cyberattack. Any attack could disrupt building operations, impact revenue streams and even allow outside access to valuable data stored on connected servers. The customer also had the challenge of retrofitting the solution into existing infrastructure—all without replacing the current system network or wiring.

The customer's existing BMS system was relatively new and not scheduled for replacement in the near future. Due to cost and current occupants who would remain in the building during the upgrades, an entirely new BMS system was not a viable option. New system installations or upgrades could not interrupt building operations for occupants.

The customer implemented the DOME™ system from Veridify Security, which creates a 'VPN-like' connection between all connected devices and controllers. DOME creates a secure tunnel over existing networks, authenticates devices and encrypts data and commands to create a trusted environment for building devices.

Operational and engineering teams do not typically focus on cybersecurity measures, and IT resources don't easily transfer to OT devices. To help, Veridify offers cybersecurity "in a box" to make it easy for non-experts to secure OT devices. Veridify and Advantech, collaborating with Arrow and Intel, designed and deployed a full solution to secure the existing BMS without interfering with existing infrastructure.

Stop Cyber Attacks Before They Happen with DOME™ Device-Level Cybersecurity

Engineers and network technicians can install device-level endpoint protection for OT security without IT staff or cybersecurity experience.

Veridify's DOME™ SaaS (Software as a Service) solution provides device-level security for industrial IoT and OT networks, and new or existing building networks. DOME™ is a complete SaaS platform delivering Zero Trust, real-time cybersecurity protection. It is protocol-agnostic for added adaptability, supporting IP networks and non-IP devices through a gateway device that converts serial to IP networks.

At the foundation of DOME are Veridify's cybersecurity software tools that provide device-to-device authentication, management and data protection. While most cybersecurity systems only provide protection to the BMS controller due to processing requirements, DOME delivers security to even the smallest processors at the edge of the network.

Veridify's DOME Interface Appliance (DIA) manages on-boarding, security credentials and data logging within a building or campus. The DOME DIA includes an Advantech industrial controller, the UNO-2271G-V2, which leverages Intel's Elkhart Lake dual-core CPU. The Advantech UNO-2000 series of embedded automation computers are rugged with a fanless and modular design, optimized I/O and various stack expansion module options. The UNO-2271G-V2 means flexible and swift time-to-market for smart building networks.

A DOME Sentry, the Advantech ECU-150 gateway, is a standalone hardware device placed at the edge of a building to protect connected devices or systems. DOME Sentries feature zero-touch on-boarding for fast and easy installation in front of a building device, and immediately provide authentication and data protection. The ECU-150 is an i.MX8M-based, high-performance IoT gateway with an open platform design and Quad Core processor.

DOME INTERFACE

UNO-2271G-V2

Pocket-Size Edge IoT Gateway with Intel® Celeron®N6210/Pentium® N6415

- Power Consumption: 12W (typical), 30W (max.)
- Operating Temperature: -20 ~ 60 °C with 0.7m/s airflow
- Software Compatibility: WISE-Edge365, Azure IoT Edge, AWS IoT Greengrass, VMware, RedHat
- Fanless, cable-free system with various I/O ports and expansion options to support wired/ wireless communication

Veridify's DOME™ solution protects a building's management system right to the edge over existing network protocols, such as BACnet. The system provides zero-touch on-boarding to reduce time and errors from manual provisioning; a block chain pedigree for device ownership and authentication; and a low-cost security gateway used to retrofit security for existing, deployed devices. It is also crypto-agile, supporting legacy and quantum-resistant security and safeguarding customers' investments with long life cycle protection.

DOME incorporates the Veridify Security Dashboard for monitoring building systems 24/7. Event logs are collected from deployed DOME devices with data processed locally for potential threats and anomalies. Notifications for such events are sent via the DOME Dashboard and can be customized per user. Additionally, the log files are uploaded to the DOME server for additional processing, archiving and use in the Security Dashboard.

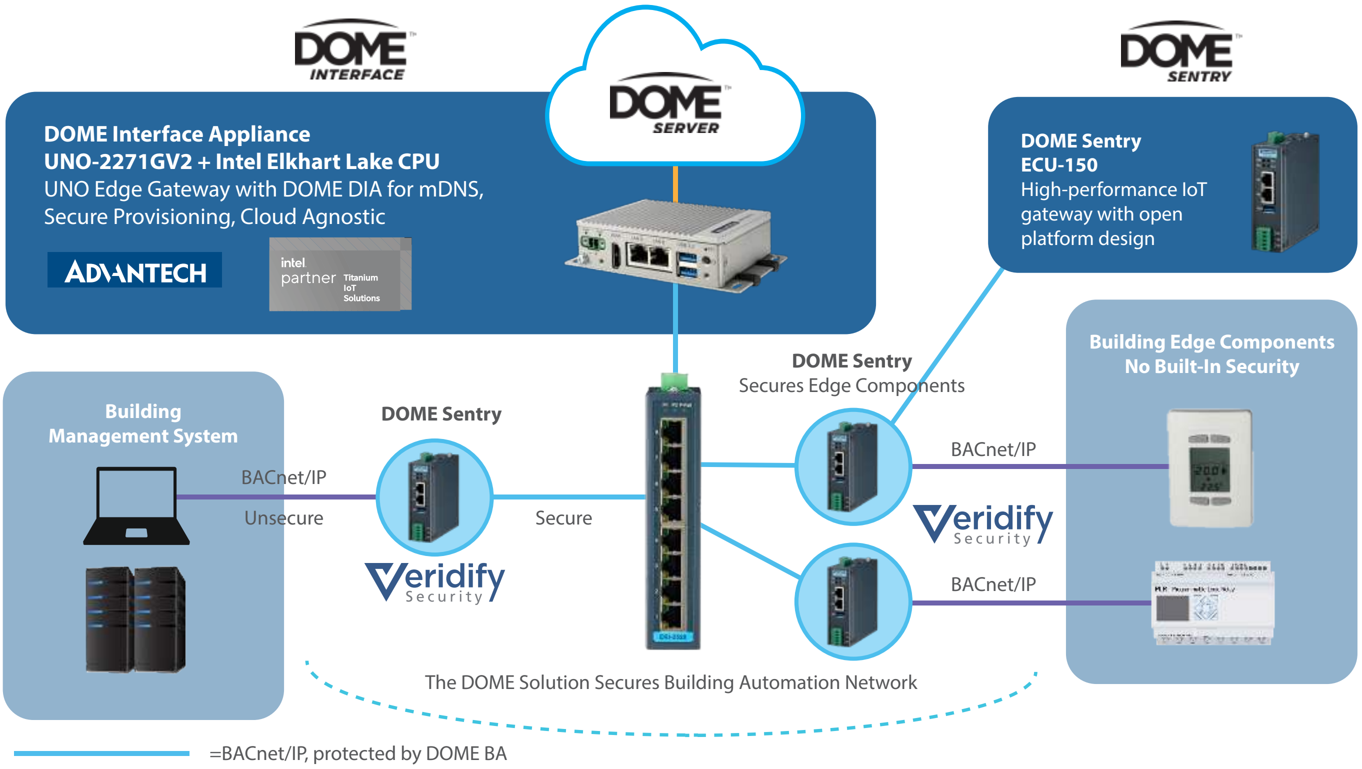
The DOME solution from Veridify Security and Advantech is an approved Intel® IoT RFP Ready Kit. Visit the Intel Solutions Marketplace to learn more about the kit.

ECU-150

High-Performance IoT Gateway

- NXP i.MX8M Quad Core Cortex A53 1.3G CPU
- Operation Temperature: -40 ~ 70°C
- Power Requirements: 10 ~ 30 VDC
- Supports SD card, online firmware updates, and auto-configuration
- Supports BACNet protocol, Modbus, IEC-60870-5, DNP3.0, OPC-UA

Solution Architecture


DOME INTERFACE
DOME SERVER
DOME SENTRY
DOME Interface Appliance
UNO-2271GV2 + Intel Elkhart Lake CPU
UNO Edge Gateway with DOME DIA for mDNS, Secure Provisioning, Cloud Agnostic
ADVANTECH
intel partner Titanium IoT Solutions
DOME Sentry
ECU-150
High-performance IoT gateway with open platform design
Building Management System
BACnet/IP
Unsecure
DOME Sentry
Secure
Veridify Security
DOME Sentry
Secures Edge Components
Building Edge Components
No Built-In Security
BACnet/IP
BACnet/IP
Veridify Security
The DOME Solution Secures Building Automation Network
=BACnet/IP, protected by DOME BA

In any connected system or network, security teams must constantly be aware of the cyber-attack surface and implement processes and technology to help mitigate risks. Technologies developed to address these challenges must unify various aspects of attack surface management to help reduce detection time *and* improve response time.

Protecting connected devices in any facility is crucial to maintain the confidentiality and integrity of critical information, and to ensure the overall safety and security of the building and its occupants. By implementing strong security measures and regularly reviewing and updating them, organizations can reduce the risk of security breaches, minimize costs and maintain the reliability and functionality of smart building systems.

Learn More about DOME. Schedule a Demo!

Is DOME™ Device-Level Cybersecurity right for your connected facility, application or system? Contact us at **ANA.smartspaces@advantech.com** with any questions or to schedule a demo. **Click here** to email the team.

Additional Learning Resources

- Intel Solutions Marketplace: DOME Device-Level Cybersecurity | *https://go.advantech.com/Intel-Marketplace*
- Mitigating Cyber Risks in OT Networks, Buildings & Critical Infrastructure | *https://go.advantech.com/AW-Brief*
- Veridify: Cybersecurity for Building Automation Systems | *https://go.advantech.com/Veridify*
- Arrow: Cybersecurity Solution for Smart Buildings | *https://go.advantech.com/Arrow*

ADVANTECH

Enabling an Intelligent Planet

Regional Contact Information: https://www.advantech.com/contact

Technical Support: https://www.advantech.com/support

Advantech Global Headquarters

Address: No. 1, Alley 20, Lane 26, Rueiguang Rd.,
Neihu Dist., Taipei 114, Taiwan
Tel : 0800-777-111

Advantech USA

Tel : 1-888-576-9668
Contact:
https://www.advantech.com/contact/inquiryrequestform

www.advantech.com | Please verify specifications before quoting. This guide is intended for reference purposes only. All product specifications are subject to change without notice. No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission of the publisher. All brand and product names are trademarks or registered trademarks of their respective companies.