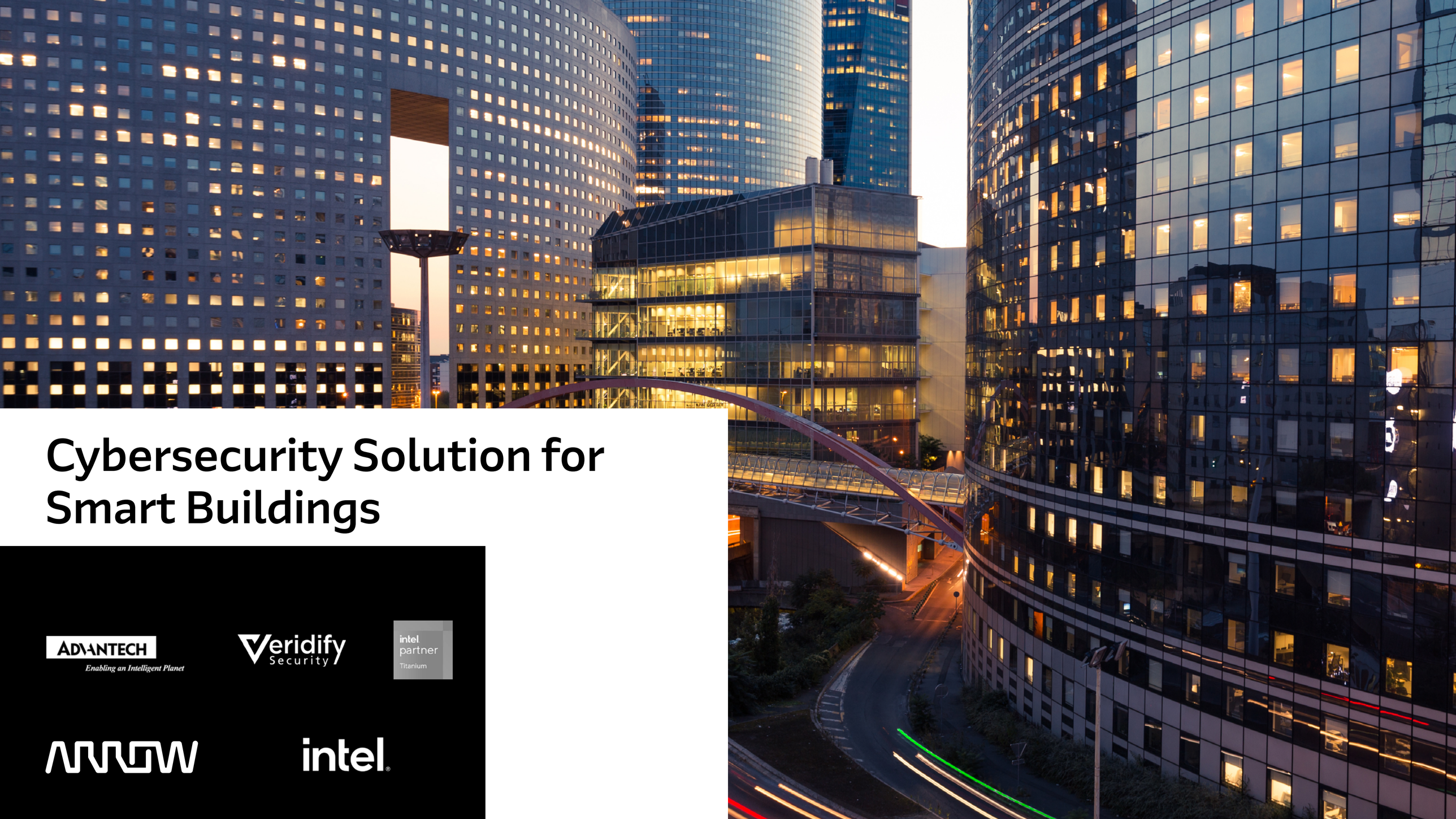


Cybersecurity Solution for Smart Buildings

ADVANTECH
Enabling an Intelligent Planet

Veridify Security

intel partner Titanium

ARROW

intel

Enable Cybersecurity at the Edge for Smart Building Automation

Cloud connectivity, smarter control devices, and high-performance networks are making buildings smarter and more efficient. From climate and lighting control, sensors and building access to operational elements like elevators, all components of buildings are now interconnected. Additionally, these systems can be accessed remotely and interact with a complex web of internal and external systems. All this connectivity while enhancing convenience and affording greater user control can be a source of vulnerability exposing buildings and enterprises in commercial settings to security threats. Cyber attacks can disrupt a building's HVAC system or disable elevators and endanger the health and safety of occupants and lead to a complete shutdown of building operations resulting in financial and productivity loss. To keep buildings safe and secure, it is critical to provide cybersecurity protection to building management systems (BMS).

Arrow in partnership with industry leaders Intel, Veridify, and Advantech, brings to market a cybersecurity platform for Smart Building Automation. The cybersecurity platform constitutes an end-to-end technology stack that includes hardware and software to deliver cutting-edge security solutions for smart buildings. Powered by Advantech's embedded automation computer, and Veridify's DOME™ (Device Ownership Management and Enrollment) Sentry at the network edge, the holistic solution provides stakeholders a comprehensive security offering that protects not just the network but also the devices in the building from threats.

Veridify's DOME™ SaaS (Software as a Service) solution provides device-level security for new and existing building automation systems and is protocol-agnostic for added adaptability to various building protocols. At the heart of DOME™ are Veridify's cybersecurity software tools that provide device-to-device authentication, management, and data protection to secure even the smallest connected devices at the edge of OT networks. While many cybersecurity systems only provide protection to the BMS or the controller level, DOME™ provides end-to-end security to the edge of the network. A key element of Veridify's cybersecurity offering is its DOME™ Sentry, a standalone hardware device placed at the edge of a building to protect an installed device or system. It can be installed in an existing building network and immediately provide authentication and data protection. In addition to the Sentry device, Veridify's DOME™ Interface Appliance (DIA) manages all onboarding, security credentials, and data logging within a building or campus.

In addition to the DOME™ Sentry hardware and DIA, DOME™ Software Development Kits are available for a wide range of processors, which allows OEMs to add robust security quickly and easily to devices running at the edge of a building system OT network. The solution enables rapid deployment of a cost-effective, end-to-end security solution on an easy-to-use SaaS platform.

Value Outcomes

- Reduce the risk of cyberattacks and protect critical devices and systems
- Enhance the lease and aspirational value of a building by promoting cyber safety environment
- Lower building insurance costs
- Help building occupants and end-users feel safe and secure
- Easy installation reduces costs and complexity for systems integrators
- Real-time, 24/7 security protection and monitoring for every building device

Solution Stack:

Veridify

- DOME™ Sentry (based on Intel® MAX® 10 FPGA)

Intel®

- Intel® MAX® 10 FPGA
- Intel Atom® processors

Advantech

- UNO-2271GV2 Edge IoT Gateway

Arrow Intelligent Solutions

- **Products:** IIoT/OT technology solutions
- **Product services:** Design, support, and professional services
- **Manufacturing services:** Supply chain, integration, and logistics

Solution Overview

DOME™ Platform Features and Benefits

- **Hardware Flexibility:** Security tools are hardware and platform agnostic and work with the smallest IoT devices
- **Protocol Flexibility:** Compatible with industry protocols such as BACnet, Modbus, and KNX, and multiple data link protocols such as MS/TP, IP, etc.
- **Crypto Agility**: Secure in-field updates devices for both keys and firmware with both legacy and future-ready quantum-resistant algorithms
- **Scalability**: On-boarding and chain-of-custody operations easily scale to millions of devices
- **Zero-Touch Provisioning:** Enables the secure installation of devices, even for buildings with no user interface
- **Block-Chain Supply Chain:** Lifetime block-chain pedigree for any building device

UNO-2271GV2 Edge IoT Gateway

- Intel® Celeron® Dual-core N6210/Pentium® Quad core N6415/Atom® Quad core x6413E processor with 4GB/8GB DDR4 onboard memory
- Compact, robust, fanless, and cable-free system with high stability
- Modular design offers an optimized basic unit with 2 x GbE,2 x USB 3.2 Gen1, 1 x HDMI 1.4
- Optional second stack for increased functionality including PoE, COM, wireless connectivity, or iDoor expansion
- Built-in TPM2.0 for hardware-based security
- Supports Win10, Ubuntu Classic, and Ubuntu Core 20

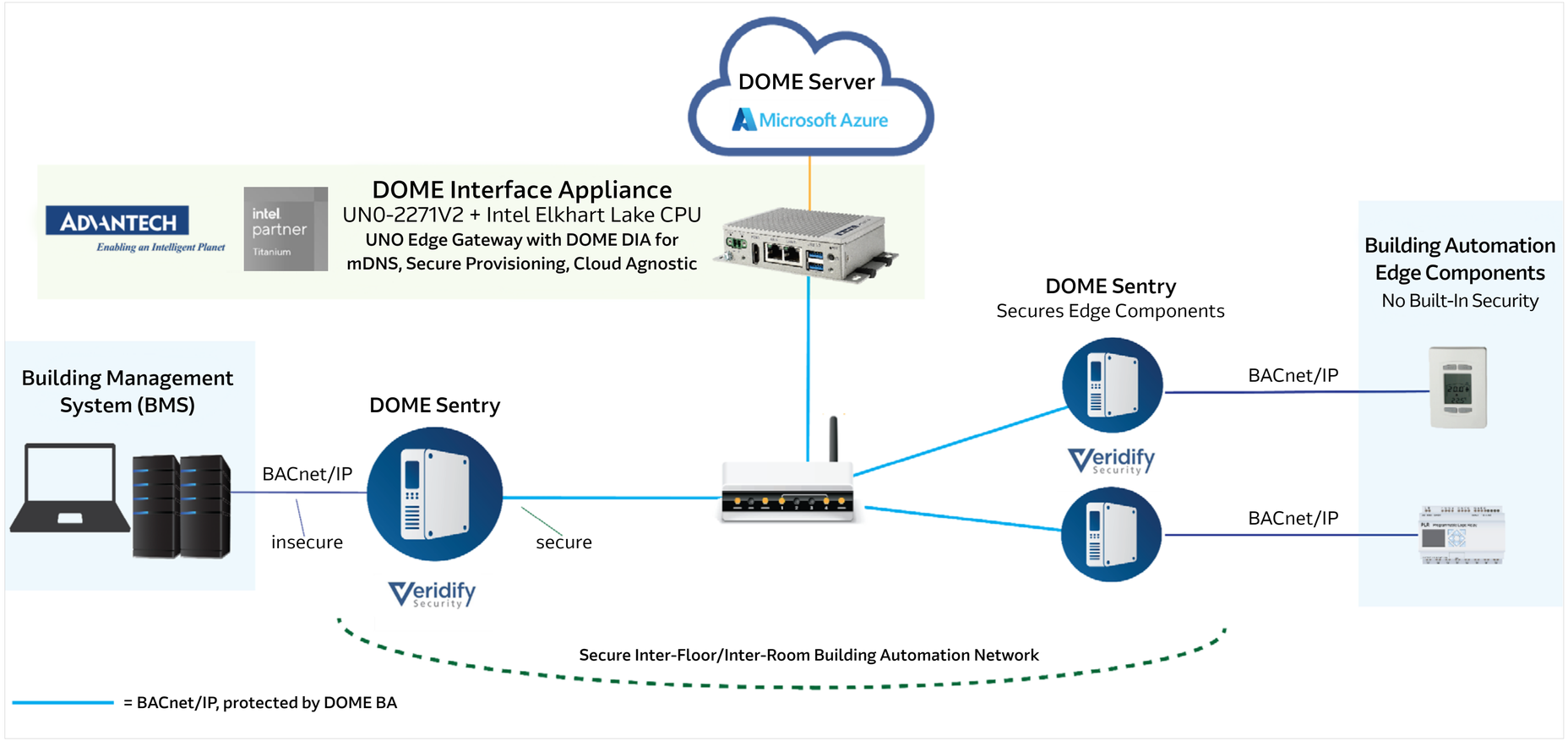
UNO-2271GV2

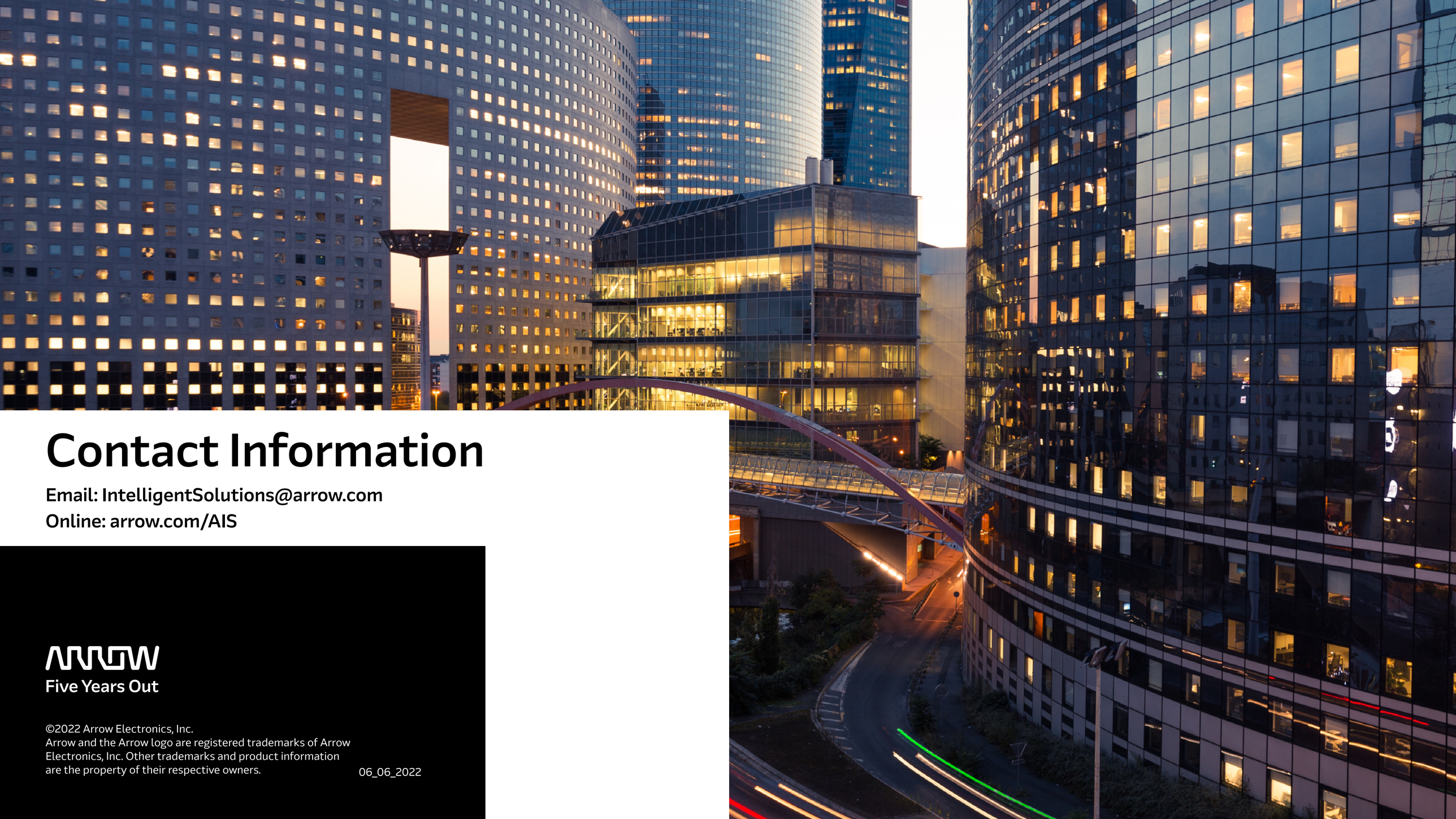
Key Industries

- Manufacturing Facilities
- Commercial Buildings
- Retail Spaces
- Utilities and Smart Grid
- Educational Institutions
- Hospitals

Solution Architecture

The platform enables zero-touch onboarding reducing the time and complexity associated with manual provisioning. The solution for Smart Buildings creates a zero-trust network over existing infrastructure to safeguard a building's management system all the way to the edge through current network protocols like BACnet. A blockchain pedigree is deployed to ensure only authorized controllers and devices are authenticated at the edge and allowed to issue commands. In addition, the solution offers Security Dashboard to monitor building systems round the clock. All deployed DOME™ devices' event logs are gathered and analyzed locally for threats and anomalies. The internal IT system triggers notifications instantaneously to on-site personnel in the event of such threats. The log files are also transferred to the DOME™ server for further processing, archiving, and inclusion in the Security Dashboard for historical analysis. Stakeholders can opt for additional notifications via SMS or other methods.





Contact Information

Email: IntelligentSolutions@arrow.com
Online: arrow.com/AIS

Five Years Out

06_06_2022