AutomationWorld®

EXECUTIVE SUMMARY

Mitigating Cyber Risks in Operational Technology, Buildings, and Critical Infrastructure

KEY TAKEAWAYS

- Despite known vulnerabilities, OT systems still lack security.
- Attacks on operational technology networks are increasing.
- DOME secures OT devices at the edge.
- DOME stops cyberattacks before they can happen.

in partnership with

ADVANTECH

Enabling an Intelligent Planet

Mitigating Cyber Risks in Operational Technology, Buildings, and Critical Infrastructure

Operational technology (OT), buildings, and critical infrastructure are becoming smarter and more efficient with connected systems, controls, sensors, and more. However, cybersecurity risks to OT infrastructure are increasing as OT devices become more integrated with IT environments and capabilities. Cyberattacks take advantage of more exposed vulnerabilities in a connected OT environment, bringing with them financial, operational, and intellectual property risks that can have a significant negative impact on enterprises.

Veridify Security and Advantech have partnered to develop the Intel-based DOME™ solution to provide real-time protection and device-level cybersecurity for the OT space. Using a zero-trust security framework, DOME secures OT devices at the edge.

Despite known vulnerabilities, OT systems still lack security.

Both OT and IT technologies have existed for decades, but only in recent years have the two been brought together to drive efficiencies and controls in new areas. The combination of the two has increased the cyberattack surface.

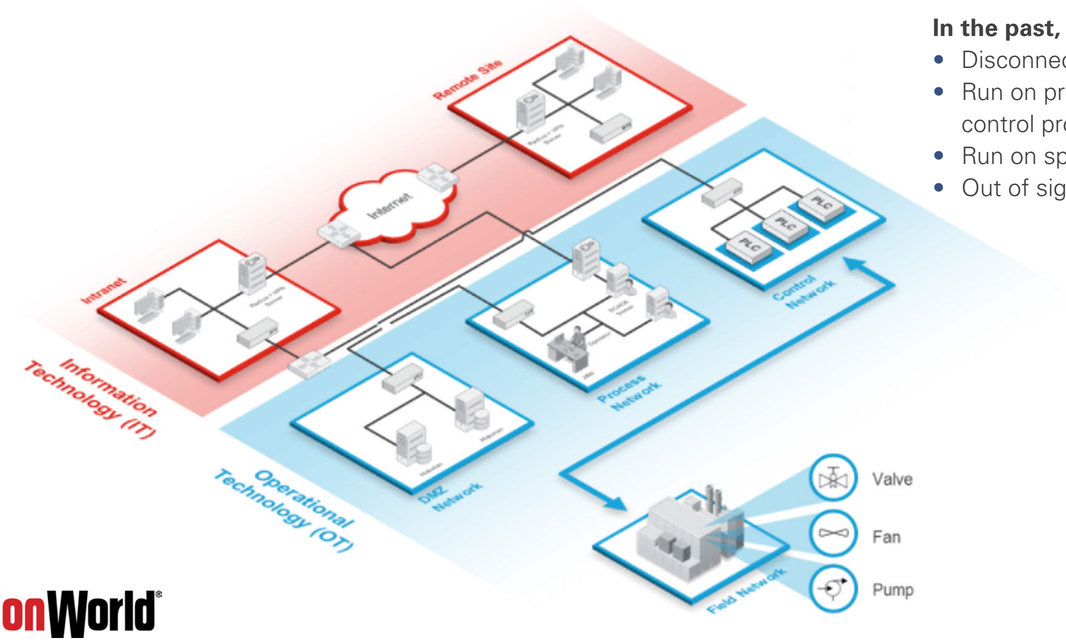
In the IT world, threats such as ransomware can lead to significant financial loss. In the OT world, the effects of an attack can be much more substantial, impacting the safety and function of an operation, industrial plant, or building. But with cybersecurity focus historically placed on IT systems, many of the existing and mature solutions for cybersecurity are IT-centric, including network and asset visibility, patching and updates, network segmentation, firewalls, antivirus software scans and alerts, monitoring, and zero trust security. Although having solutions that address these areas is important, their emphasis on IT security means there is a still a large gap in OT security.

Attacks on operational technology networks are increasing.

Cybersecurity and cyberattacks result in significant operational and financial costs and are a growing concern in the industrial OT network space, which presents unique challenges due to:

- **Legacy infrastructure.** In the industrial world and sectors such as building automation, systems may be years or even decades old.

Figure 1: OT and IT security have historically been siloed



In the past, OT was . . .

- Disconnected from IT
- Run on proprietary bridged control protocols
- Run on specialized hardware
- Out of sight, out of mind

- **Proprietary systems.** Many of the systems and solutions in the industrial and building space use proprietary protocols.
- **Multiple protocols/vendors.** As each solution often uses its own proprietary protocol, using solutions from multiple vendors requires interfacing with multiple protocols.
- **Screenless.** No physical UI means it is not possible to key in two-factor authentication or use a clickable interface.
- **Limited device security at the edge.** The devices used in industrial and building solutions are typically engineered and designed very specifically for their functions, leaving little or no memory, storage, and/or computing power to implement new security technologies.
- **System/device location.** In the OT world, long-distance device management presents challenges when remote devices come under attack.
- **Siloed engineering and IT management.** Facilities and industrial engineers might be responsible for system operations, but cybersecurity of the system, whether HVAC, access controls, or even the PLC, might not fall under the responsibility of IT staff, resulting in a lack of protection.

DOME secures OT devices at the edge.

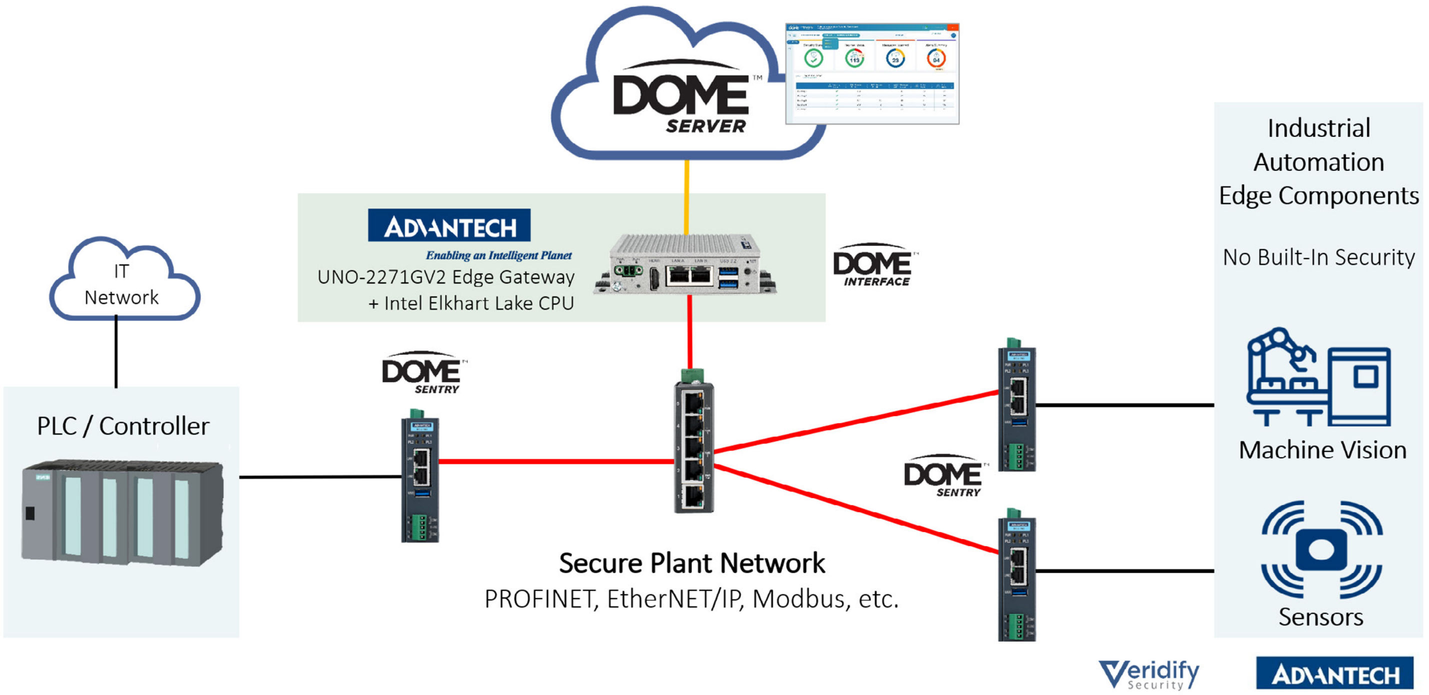
In partnership with Advantech, Veridify has developed the Intel-based DOME cybersecurity solution for the OT network cybersecurity space. DOME is the only solution that provides device-level security at the edge to stop cyberattacks on OT networks, buildings, and critical infrastructure.

Cybersecurity is a broad topic and IT resources are tight and often shorthanded. Veridify's technologies are all developed with zero-touch onboarding. Simply connect the DOME Sentry in front of the device, add power, and the system begins protecting the network and devices in under 60 seconds. DOME supports in-field firmware updates and mutual authentication, and all data and commands are encrypted.

The DOME solution offers functionality for the OT security space that is mature and even taken for granted in the IT security space, including:

DOME Functionality	Description
Zero-trust framework	A framework in which everything is considered untrustworthy unless authenticated.
Mutual authentication of all devices	Authenticated devices are trusted devices, and only trusted devices can communicate on the DOME platform, with no device replacement required in the current environment.
Secure tunnels between devices	DOME establishes a secure tunnel between each DOME Sentry for end devices that communicate to each other.
Encryption of data and commands	Data and commands are encrypted between DOME Sentry devices.
Real-time alerting	Any activity that is not authentic is stopped by DOME and alerted immediately.
Retrofit and embedded options to protect legacy and new devices	Together with Advantech, Veridify has put its DOME solution on a hardware device, so it can be retrofitted to an existing system without the need to replace anything. Software tools to embed DOME in new devices are also included.

Figure 2: DOME creates a secure plant network



> “DOME is specifically designed and built to address each individual device at the very edge of a network.”
>
> *- Louis Parks, CEO, Veridify Security*

DOME stops cyberattacks before they can happen.

DOME was purpose-built for ease of use, with no cyber/IT skills or resources required. Upon receipt of the DOME solution, simply unbox it and turn on the DOME interface gateway to enable Intel technology to immediately begin protecting the OT system. DOME provides protection from automation controllers to IP-enabled edge devices, securing devices and communication.

The DOME solution includes:

- **DOME Dashboard.** The easy-to-use interface includes edge data analytics, real-time security alerts, and a daily status email for review and retrospection. The DOME Dashboard receives data logs and alerts from the DOME interface appliance.
- **DOME Interface.** The DOME Interface appliance uses the Intel Elkhart Lake CPU Edge Gateway on the Advantech UNO-2271GV2, a powerful fan-less industrial computer with built-in I/O. The DOME Interface handles device management, cloud connectivity, credential management, and data logging capture for the DOME solution.
- **DOME Sentry.** The DOME Sentry stands watch. The number of DOME Sentry devices depends on the environment, but whether there are 2 or 200, the Sentry is the protector that stops cyberattacks. The zero-touch onboarding makes DOME Sentry easy to deploy, installing in under 60 seconds, and it works with already-installed devices.

The simplicity and efficiency of deployment, combined with the ability to stop attacks instead of only alerting on them, differentiates DOME from other solutions in the marketplace.

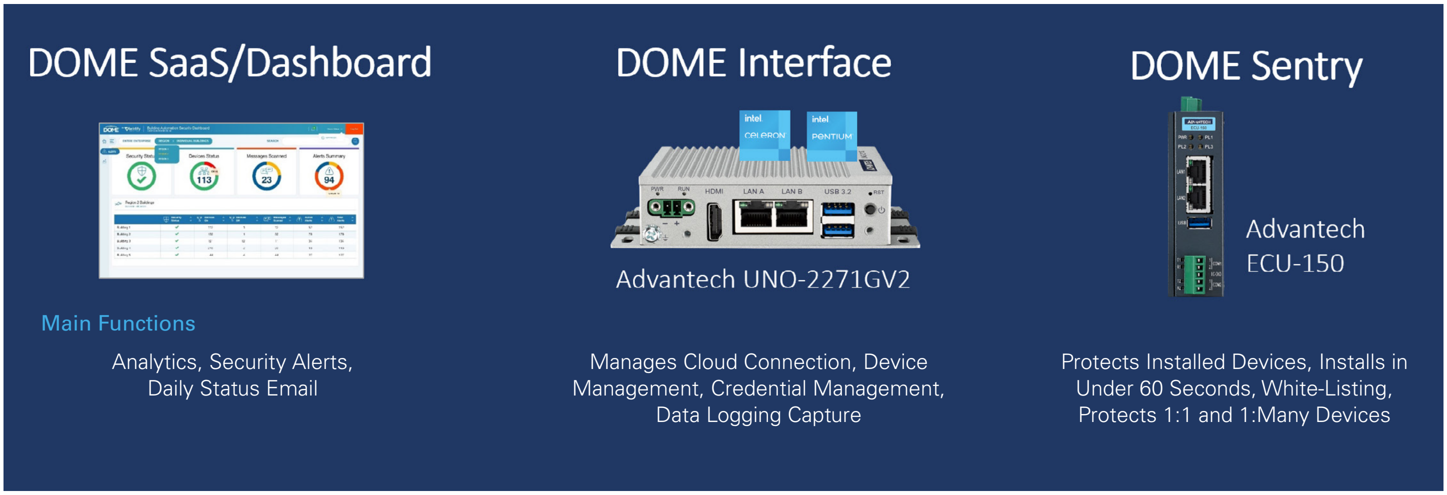
> "DOME is not a monitoring solution. It actually stops attacks. With DOME installed, the shields are up and real-time active protection is in place the moment it is installed. It's a complete cybersecurity solution in a box."
>
> *- Carolyn Swan, Director, Partnerships, Advantech IIoT Group*

As quantum computers have gone from theoretical to actual existence, shifts in security technology will follow in short order. Although quantum computers have yet to gain widespread use, Veridify's emphasis on "future-proofing" has already led to the development of a range of tools and applications for authenticating and protecting data in a post-quantum world.

Veridify has applied its solutions to some of the platforms and devices developed in partnership with Advantech, including DOME. As a result, DOME is developed using applicable standards for the industry as a guide, primarily focusing on NIST and ISO standards to ensure that DOME either is certified or can be certified as needed.

The complete DOME solution is available from Advantech partner and Intel IoT Aggregator, Arrow Electronics.

Figure 3: The complete DOME solution



DOME SaaS/Dashboard

Main Functions

Analytics, Security Alerts, Daily Status Email

DOME Interface

Advantech UNO-2271GV2

Manages Cloud Connection, Device Management, Credential Management, Data Logging Capture

DOME Sentry

Advantech ECU-150

Protects Installed Devices, Installs in Under 60 Seconds, White-Listing, Protects 1:1 and 1:Many Devices

To learn more, you can reach the Advantech team at ANA.SmartSpaces@Advantech.com. You can also visit: https://go.advantech.com/DOME.