DOME™ Technical Overview

DOME is a cybersecurity platform that secures connected devices such as operational technology (OT), IoT, industrial controls and building controls. DOME software can be embedded into OEM devices or implemented externally with security appliances that provide overlay security that is transparent to the existing unsecure devices.

DOME provides the following primary applications:

- Device-level security
- Secure firmware upgrades
- Secure supply chain

Device-Level Security

DOME establishes a "secure enclave" using a Zero Trust architecture where all devices and equipment inside are trusted and safe, and makes the establishment and on-going management of the secure enclave simple enough to be implemented by existing technicians without the need for cyber or extensive IT skills.

The key components of DOME include:

DOME Server™	The DOME Server maintains the blockchain pedigree of devices and is a system for installation set-up and device management. It also has a user Dashboard for system information, analytics, and alerts.
DOME Interface Appliance™ (DIA)	Local management device at an installation being protected. The DIA authenticates new devices (e.g. DOME Sentry), distributes security certificates, and collects logs to be pushed to the DOME Server
DOME Sentry™	Security appliance that protects unsecure edge devices and equipment. The DOME Sentry only accepts communications from trusted devices and encrypts data being sent to other devices.
DOME Client™	Security software that can be embedded into OEM devices and provides the same level of security as a DOME Sentry.

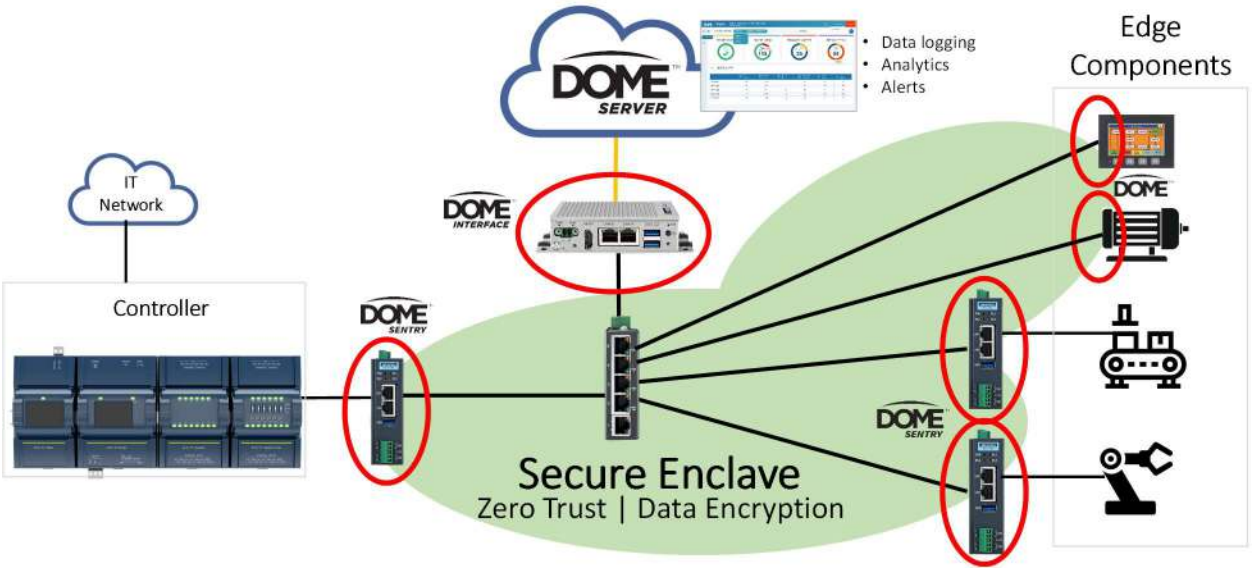

Figure 1 – DOME Architecture

Zero-Touch Provisioning

The DOME platform validates device ownership pedigrees before installation. During installation, devices are authenticated, receive in-field provisioning by a DOME Interface Appliance (DIA) and then handed off to a system controller to securely perform their intended day to day function. Devices that do not have embedded DOME security can be placed behind a DOME Sentry security appliance. Management of the security certificates is automated during installation and renewal, and certificates can be renewed at any desired interval.

Zero Trust Framework and Deployed Secure Enclave

A DIA maintains the identification, authentication, and encrypted connectivity to every device it has enrolled within the facility's ecosystem as well as the controllers that interact with those devices. The DIA monitors device status and can deliver secure firmware update packages and additional provisioning such as site-specific configuration changes. The DIA also communicates with the DOME Server to report on device inventory, device status, cyberattack attempts in the form of forged or unauthenticated commands, and users.

A Zero Trust framework assumes that all devices are untrustworthy unless authenticated. When trusted devices are authenticated, a secure enclave is created so that only trusted devices can communicate safely with each other. DOME uses a Zero Trust framework and all devices in the secure enclave must be mutually authenticated to each other in order to communicate. Any communications from non-authenticated devices is blocked and an alert is issued. This also applies to devices being protected by a DOME Sentry – if a device behind a DOME Sentry is replaced without proper authorization, any communications from the new device are blocked and an alert is generated.

Attackers that gain physical access to the automation network or exploit an entry point into the network by way of an unsecured device will launch attacks on the components that make up the secured building network. Through this they may attempt to conduct malicious activity such as eavesdropping on the network traffic in an attempt to obtain useful data, or capturing, modifying and playing back data in an effort to tamper with sensor readings or issue commands to actuators, etc. In addition, they may attempt to control connected devices to launch DDOS attacks or attempt to access the facility owner's IT

infrastructure. The attacks could also emanate from a rogue device that was introduced into the network in an unsecured way. With the network secured by DOME, unauthenticated devices and unauthorized access attempts are detected and blocked.

Data Encryption and Crypto-Agility for Lifetime Security

DOME encrypts data between devices to prevent potential eavesdropping devices from learning anything about the network traffic or devices.

Crypto-agility is an important consideration when making a long-term commitment to a security platform. This is a capability to support different and improved security methods that may develop in the future. With OT network infrastructure devices having potential lifespans of decades, crypto-agility enables those devices to stay secure.

This may require the ability to support quantum-resistant algorithms in the future, while supporting existing standard methods today. DOME supports Quantum-Resistant protocols, and 'Next Generation' cryptographic primitives that may emerge in the coming years to ensure the right security method is deployed today and does not become a barrier, or worse, a vulnerability as the cyber landscape evolves.

Network Protocols

DOME has been tested for compatibility with the following protocols:

- BACnet/IP
- EtherNet/IP
- Modbus TCP
- DNP3
- OPC UA
- SNMP

Devices that use a serial communication protocol (e.g. Modbus RTU, BACnet MS/TP) can be protected in a 1:N manner with a DOME Sentry located in front of an IP-to-Serial gateway, or with DOME Client software embedded into a gateway.

Secure Firmware Updates

DOME supports secure firmware updates for DOME-enabled devices. When a DOME-enabled device gets deployed, it gets registered with the DOME Server and the device owner automatically gets registered for firmware updates from the manufacturer. When a manufacturer has a firmware update for their products, they register the update with DOME. DOME then informs the product owners that an update is available, and gives the owners the chance to schedule the update on a device-by-device basis (selecting one, several, or all devices) for testing and deployment.

The firmware update process is as follows:

1. Devices are registered with DOME automatically when they are deployed and provisioned
2. Manufacturer builds an update and publishes it to the DOME Server
3. The device owner is notified about the update
4. The device owner schedules the deployment via the DOME Server
5. The DOME Server inventory list shows the current device firmware version for each device
6. Once the firmware update is approved by the owner (or the approval period times out), the DOME Server pushes the update to the DIA, which will push the update to the affected devices

Secure Supply Chain

DOME's secure supply chain functionality ensures that devices to be installed are authentic and the embedded software has not been compromised. This starts by providing a lifetime blockchain pedigree for each device beginning prior to its installation and ending with a device's decommissioning and removal from the building.

The process begins when a device is provisioned with the DOME Client software plus public key credentials that are shared with its original owner (for example – the Manufacturer). This step will allow a device to participate in its ownership management and authentication processes in the field without the need to connect to a cloud or central server. The manufacturer also provides a credential to the device so identification and mutual authentication can be performed with the device anywhere. The credential for each device is signed into a 'block,' giving every device its own pedigree embedded in a blockchain which is stored on the DOME Server. This framework allows owners to establish proof of ownership without the need for a pervasive cloud or network connection and enables device-level security management.

The credentials are signed into the device's blockchain to support each transfer of ownership and follow the physical movement of the devices through the supply chain and each transfer of ownership.

Summary

DOME establishes a secure enclave for automation devices and requires mutual authentication for communication between devices. Security certificates are automatically managed by DOME which simplifies deployment and reduces or eliminates the need for highly-trained IT or cyber staff.

Data traffic between authenticated devices is encrypted, and communication from unauthorized devices is logged and an alert is generated. DOME provides crypto-agility and quantum-resistant protocols to provide long-term security. DOME supports secure firmware updates for protected devices and ownership of DOME-enabled devices is managed in a block chain and that can track ownership and authenticity end-to-end through the supply-chain.