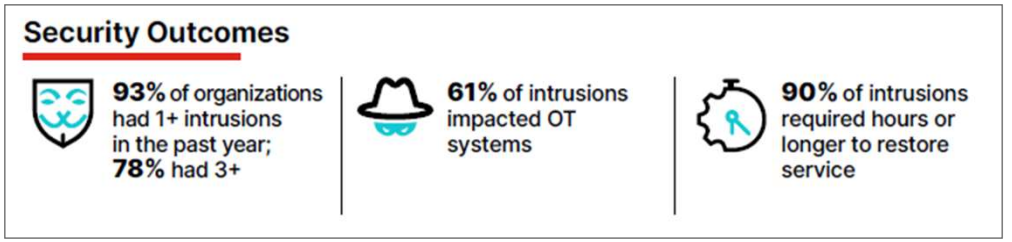
Zero Trust Security

Stopping Cyberattacks on Industrial Control Systems (ICS / OT / SCADA)

Veridify Security

Cyber Attacks on Industrial/OT Networks are Growing

The State of Industrial Cybersecurity, May 2022 | Trend Micro



2022 State of Operational Technology and Cybersecurity Report | Fortinet

Today's OT Cybersecurity Solutions are Re-Active

Dwell times are still measured in the range of days, weeks, and months

Device Visibility	Monitoring	Remediation
Identify Devices	**Watch for Intrusion**	***"Identified"* Intrusions**
Asset Database Classification	Risk Assessment Anomaly detection Analytics	Actionable Data Network segmentation IT Staff intervention

Useful capability…but does not stop attacks

Multiple Standards / Guidelines / Frameworks

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-207 Zero Trust Architecture

ISA/IEC 62443 Security for Industrial Automation and Control Systems

ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements

ISO/IEC 27001 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ATT&CK® for ICS

Applying Standards / Guidelines / Frameworks

All of the these are standard / guidelines / frameworks are useful

The multitude and scope leads to complexity and significant effort to implement

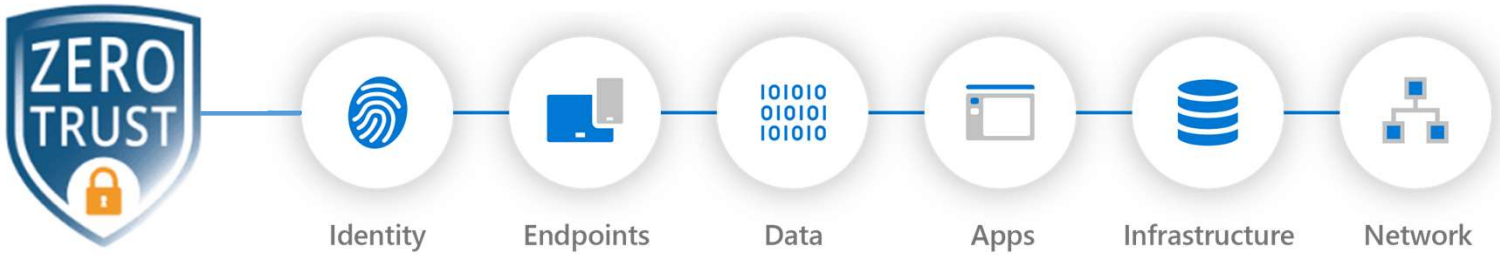
Compliance & Certification

- How do you really know if there is compliance?
- Certification is not available for all items.

Gap in real-time protection for individual devices

Why Zero Trust?

Zero Trust - a security framework requiring all users/devices to be authenticated, authorized, and continuously validated for before being granted or keeping access to applications/data/devices



Zero Trust is PRO-ACTIVE security framework than can prevent/stop damage from attempted cyber attacks

DOME™ BY Veridify Security

- Cybersecurity for devices at the edge
- Commercial, Public Sector, and DoD
- Solutions for OT networks, buildings and critical infrastructure that STOPS attacks
- 18+ years of delivering security solutions

ISO 26262
ASIL D Certified

2019 WINNER
exida Safety and Cyber Award
2019

cybernews
2022 TOP PICK
Best IoT Security Solutions

Developed in partnership with

ADVANTECH

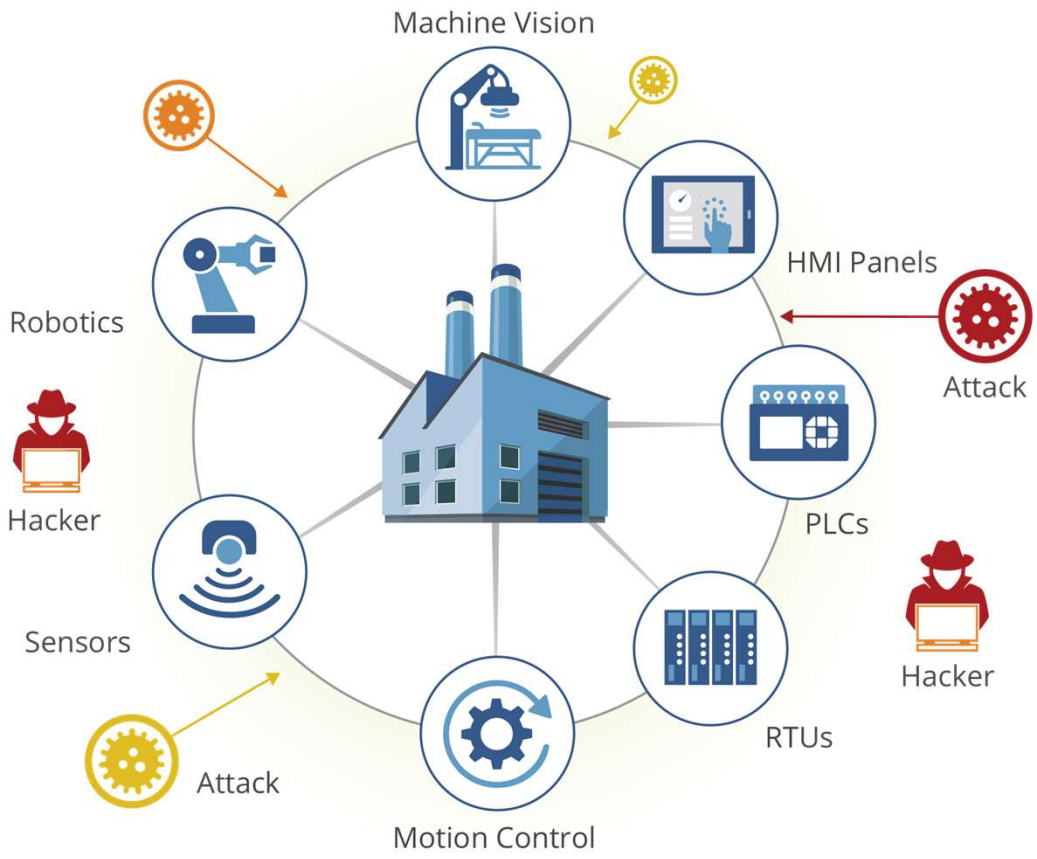
intel

aws

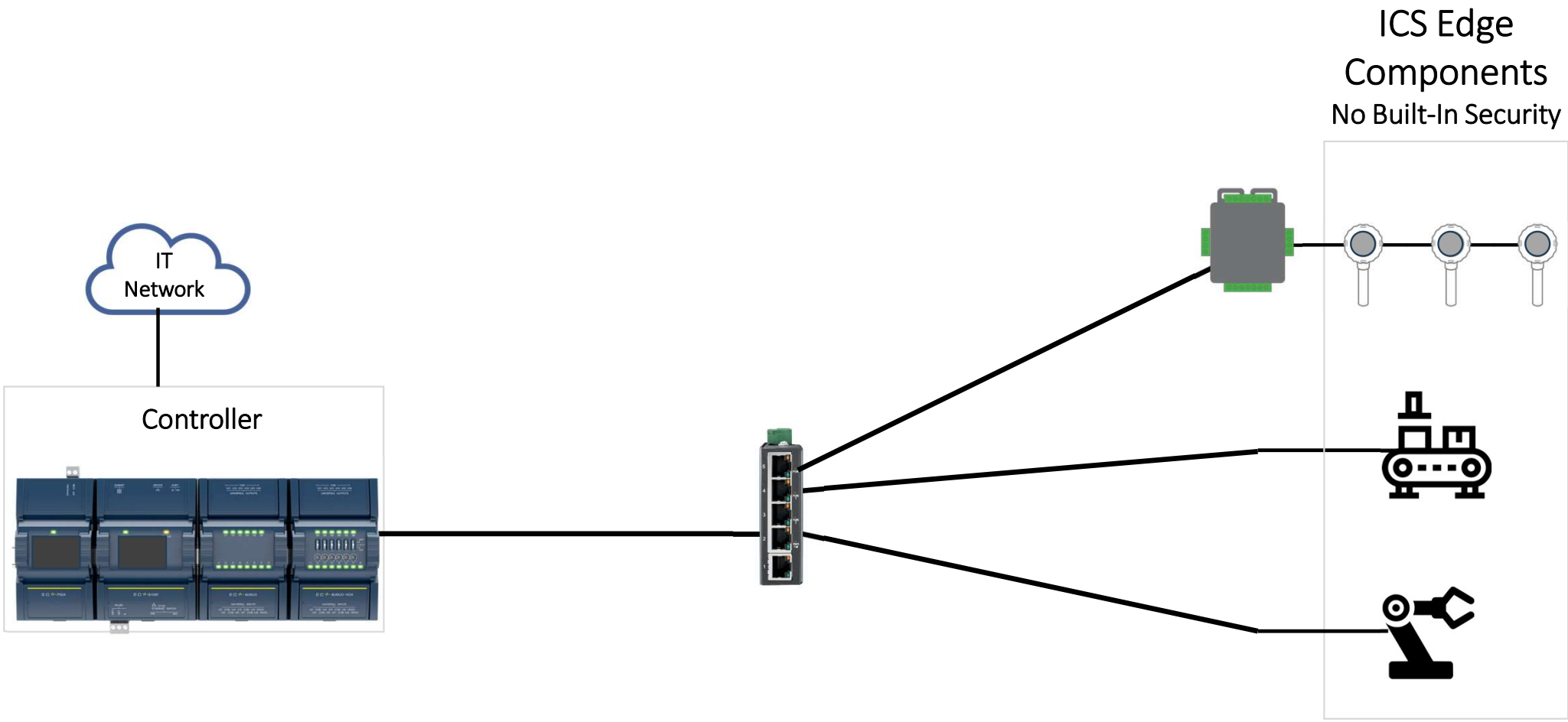
DOME™ Provides Device-Level Protection

- NIST-compliant
- Authenticates all edge devices
- Protects Data and Commands
- Manages Connections
- Automates Certificate Mgmt
- Monitors and Alerts

Easy-to-Implement Solution that STOPS Cyber Attacks

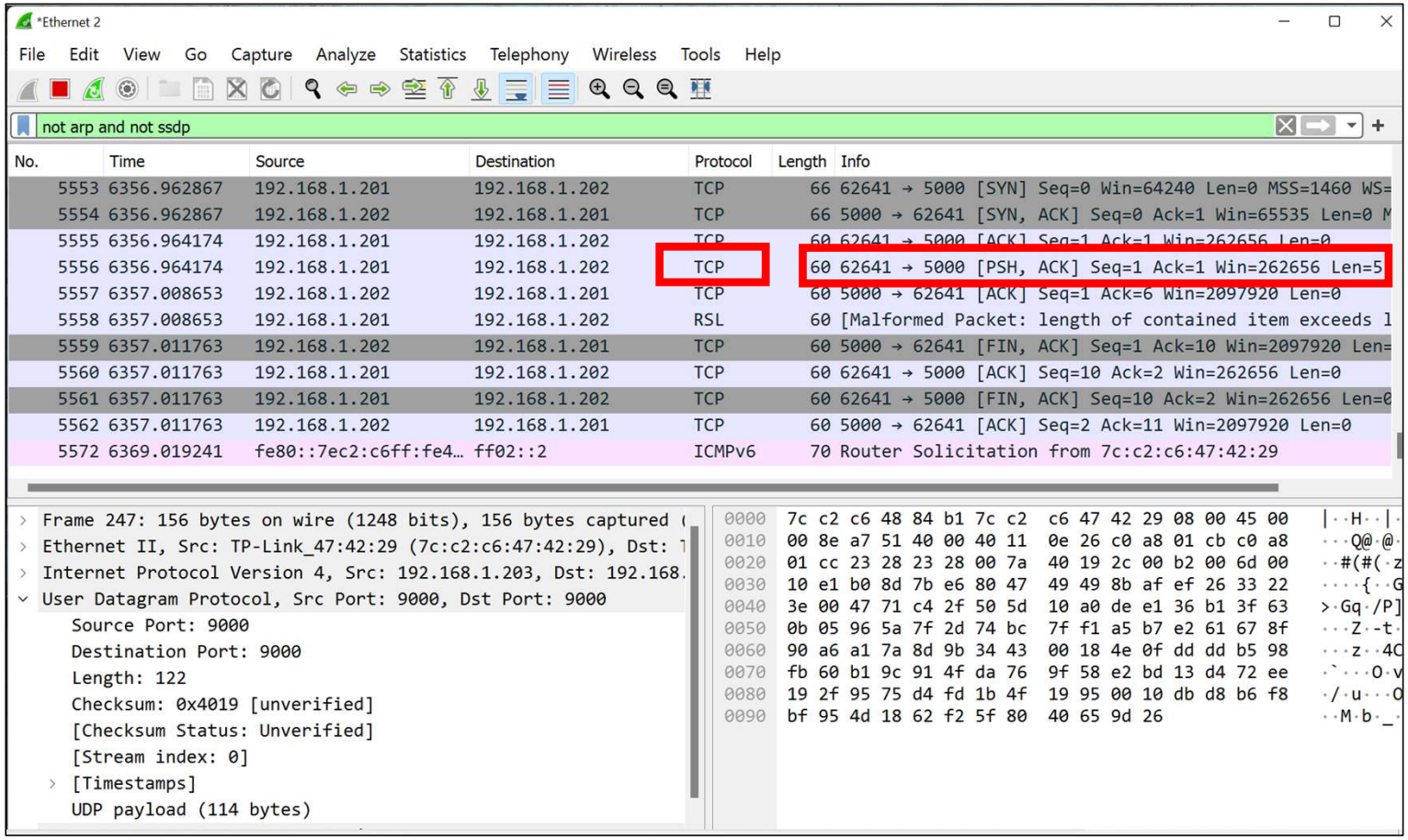


Unprotected Industrial Network

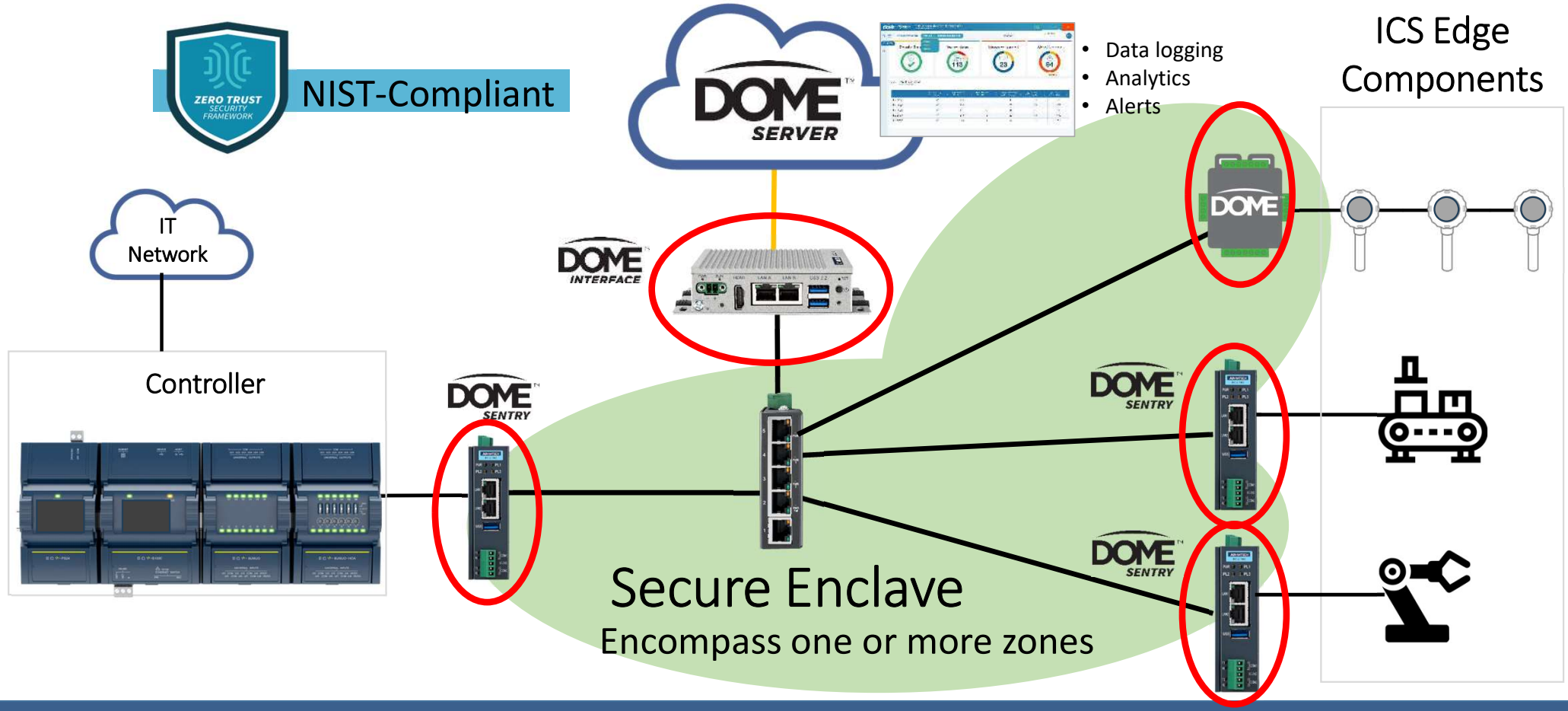


Unprotected Network

Message Info and Data are Visible



DOME™ Protects New & Existing Industrial Networks



DOME™ Sentry – Protection for Existing Devices

NIST Zero Trust framework

- all data packets authenticated and encrypted between devices
- blocks all attacks

Auto Configuration

- Network parameters
- Security parameters (keys, certs, etc.)
- Auto discovery of devices for some protocols

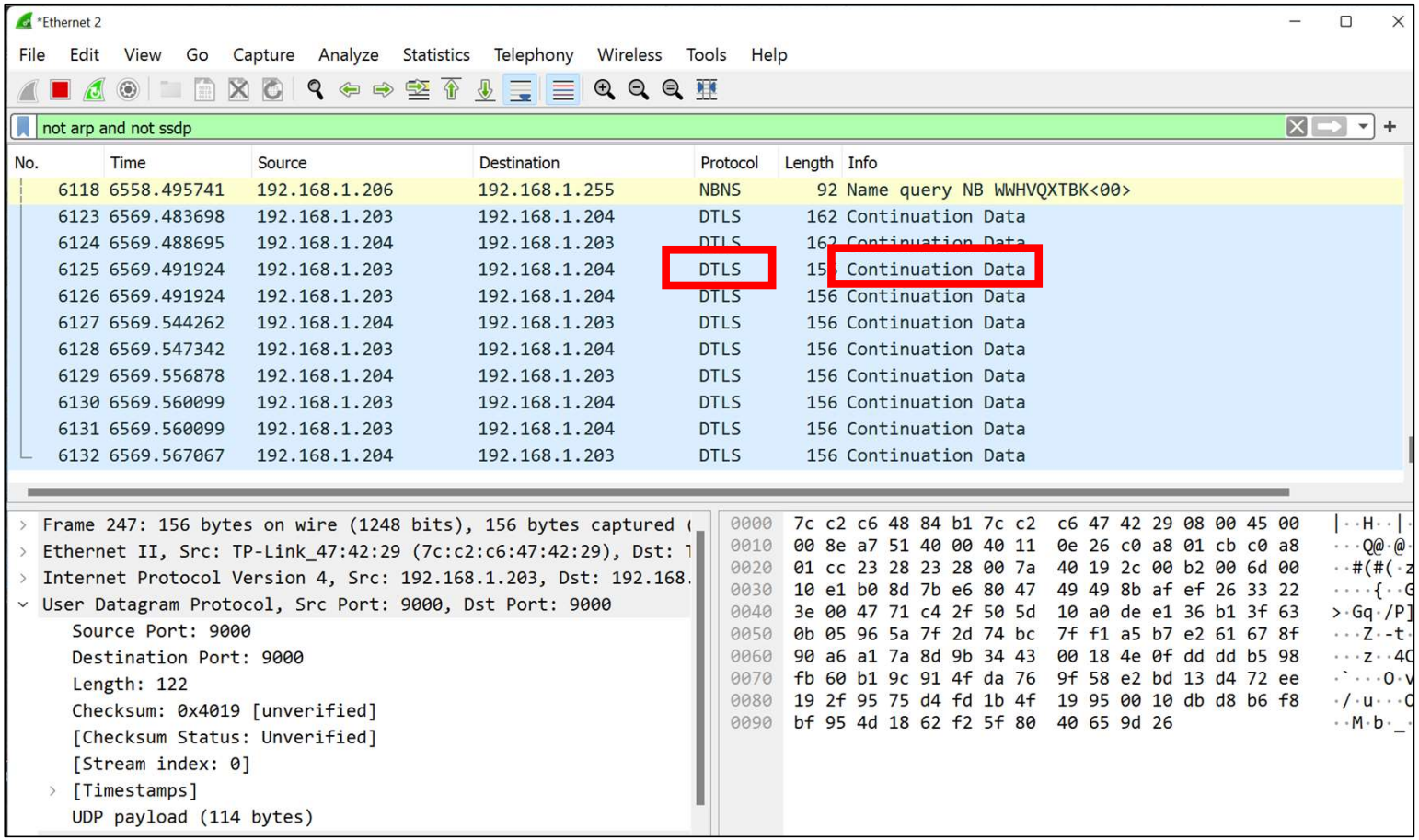
Centralized Control

- Local firewall (port/service block)
- Allowed/denied peers (whitelisting)

Detailed Logging

- Traffic analytics
- blocked attacks/other anomalies

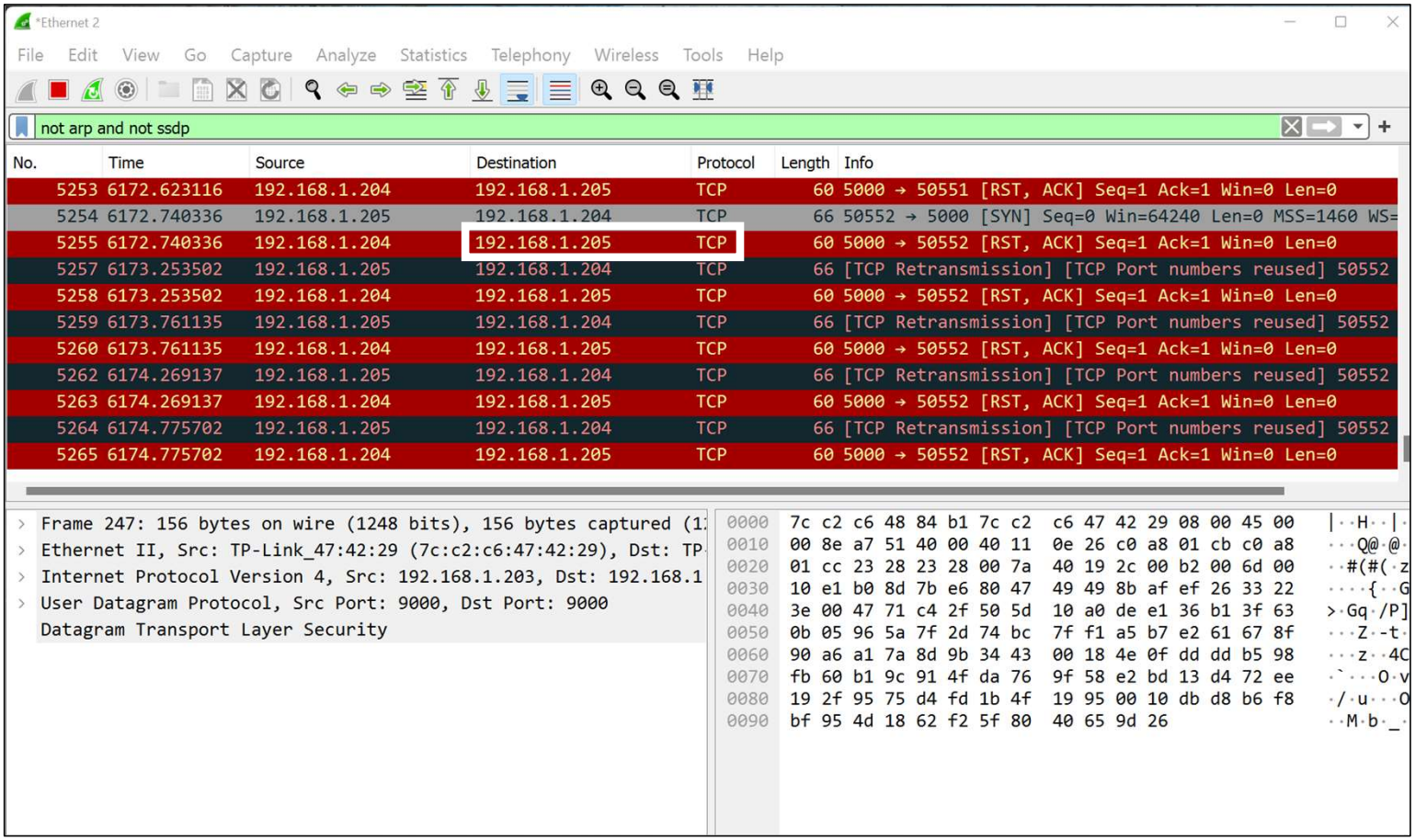
All Traffic Protected



DOME™ Stops Attacks and Unauthorized Traffic

Request from Un-Authenticated Device & Retries

Messages Blocked



“Cybersecurity In a Box”

Easy Installation and Immediate Protection

DOME SaaS/Dashboard

- Analytics
- Security Alerts
- Daily Status Email

DOME Interface Appliance (DIA)

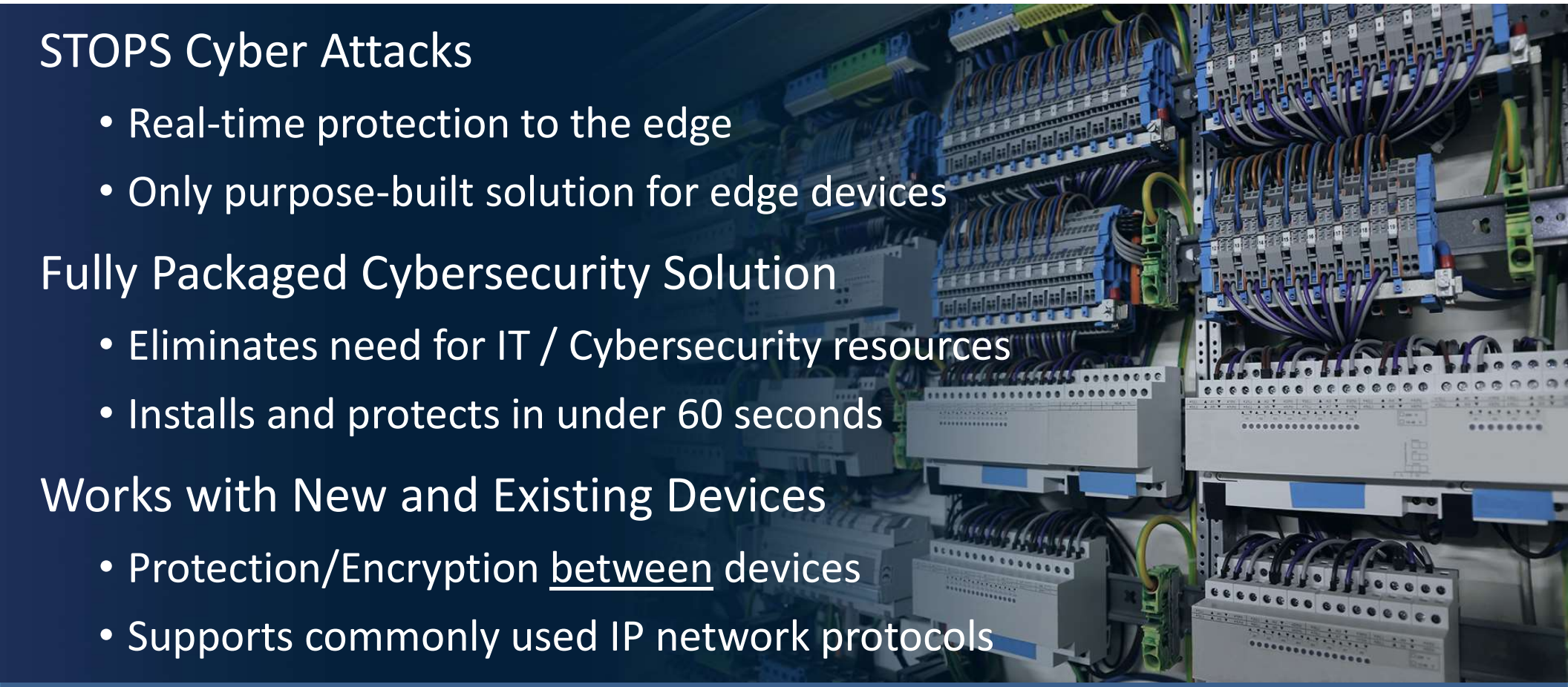
- Manages Cloud Connection
- Device Management
- Credential Management
- Data Logging Capture

DOME Sentry

- STOPS Cyber Attacks
- Works with Installed Devices
- 100% NIST Zero Trust Framework
- Zero Touch Onboarding
- Installs in Under 60 seconds
- No IT or Cyber Skills Needed
- Protects 1:1 and 1:Many Devices

DOME supports “No Cloud Connectivity” option

DOME™ Cybersecurity Made Easy



STOPS Cyber Attacks

- Real-time protection to the edge
- Only purpose-built solution for edge devices

Fully Packaged Cybersecurity Solution

- Eliminates need for IT / Cybersecurity resources
- Installs and protects in under 60 seconds

Works with New and Existing Devices

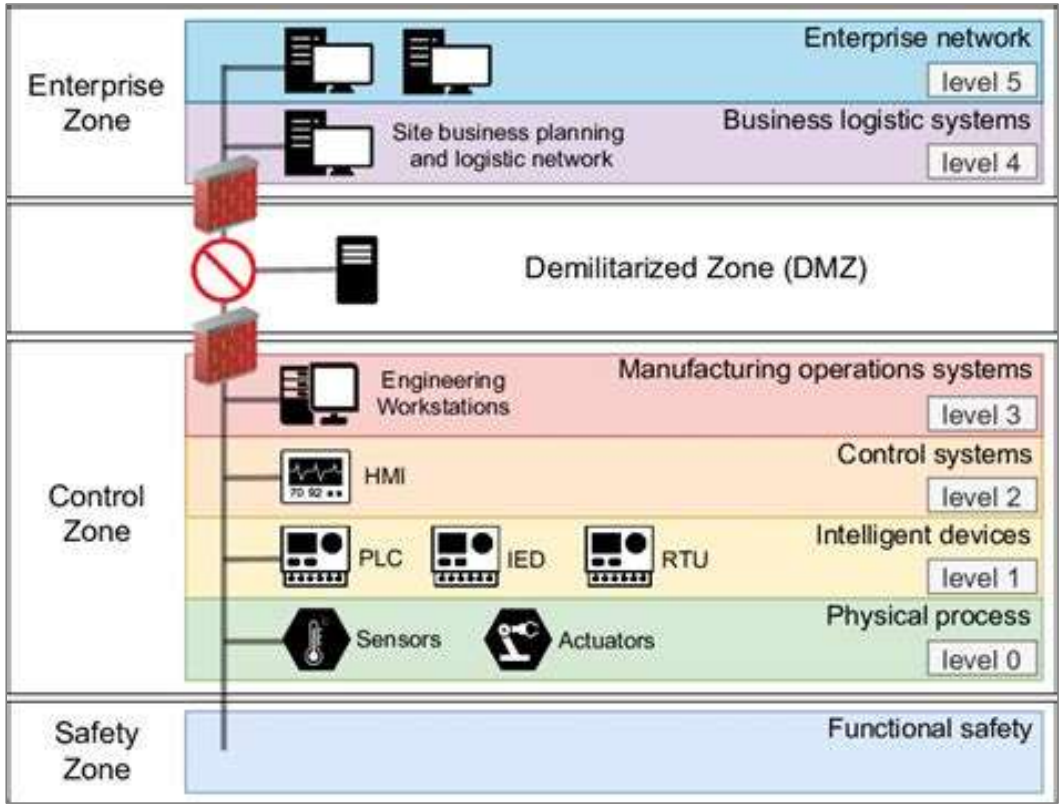
- Protection/Encryption between devices
- Supports commonly used IP network protocols

Risk Management Framework: DOME Compliance

NIST 800-53

Category	Control
Device Authentication & Proof-of-Ownership (Mutual Authentication)	AC-3, IA-{3,9}, MA-7, PM-30, SC-{12,13,17,43}, SR-{4,11,12}
Zero-Touch Provisioning	AC-{7,24}, CM-{6,7,8}, IA-3, MA-{6,7}, SC-{2,3,12,13,16,17,43}
Firmware Updates	CM-11, SC-{8,9,34}, SI-{2,7}
Device Management	AC-21, CA-9, CM-{10,11}, IA-{3,10,11}, IR-5, MA-{2,6,7}, PL-9, SC-{2,3,16,43,45}, SI-{6,10}
Key/Certificate Updates (Re-Provisioning)	CA-9, CM-{6,7}, IA-{3,9,10,11}, MA-{6,7}, SC-{12,13,16,17}
Network Authentication	AC-{3,4,7,17,24}, CA-9, IA-{3,9,10,11}, SC-{7,11,13,24,32,50}
Device-to-Device Authentication	AC-{3,4,7,17,24}, CA-9, IA-{3,10,11}, SC-{3,4,7,11,12,13,32,50}
Communication Encryption	AC-{3,4,17,24}, SC-{3,4,7,8,9,10,11,12,13,23,24,32,48,50}
Auto-Configuration (DOME Sentry)	AC-{3,24}, CM-8, MA-{6,7}, PM-5, SC-{3,41,45}
Integrations (DOME Sentry)	RA-5, SC-{4,28,34,41,45,49}, SI-{4,6,7}
Logging:	AU-{2,3,4,8,9,11,12,13}, CA-7, CM-8, IR-5, PM-{5,31},SC-{12,13}, SI-{4,6,11,12}
Cloud Server Components	CP-{6,7,9,10}, IA-{9,10,11}, IR-5, MA-{2,6,7}, PL-9, PM-{5,31}, PT-{2,4,5}, RA-5, SC-{2,3,4,10,11,12,13,23,28,43,45,48,50}, SI-{4,7,10,12}
Overall System	SC-{38,42}

Applying DOME in the Purdue Model



DOME™

Can be implemented from Levels 0-3 in the Purdue Model

Summary

Existing ICS/OT solutions are network-based

- Many solutions coming from the IT space
- Asset Inventory, Monitoring, Remediation are Re-Active
- Not stopping cyber attacks

Standards/Guidelines/Frameworks are helpful

- Multiple options add complexity

Zero Trust at the Device-Level (i.e. DOME)

- Pro-actively protects devices in real-time
- Stops cyber attacks from impacting edge devices

For More Information

veridify.com

+1.888.272.1977