

# Zero Trust Security

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

The logo for Veridify Security, featuring a stylized 'V' icon followed by the text 'Veridify' and 'Security' below it.

**Veridify**  
Security

# Cyber Attacks on Industrial/OT Networks are Growing

FACTORY | CYBERSECURITY

## New Industrial Control System Security Threat

The U.S. government's Cybersecurity and Infrastructure Agency issues new alert about attacks targeting ICS/SCADA devices.

AutomationWorld

## Cyber-Attacks on Industrial Assets Cost Firms Millions

June 02, 2022



### CYBERATTACK IMPACT

What consequences did cyberattacks make in the organizations in the last 12 months?

**Supply Affected**  
89%



**Disruption 4 days or more**  
56%



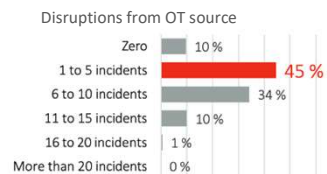
**Average amount of damage**  
\$2.8 million



### LIKELIHOOD AND RECOGNIZED CAUSES

How many times did the organizations face disruptions in the last 12 months?

**6-10 times disrupted**  
in the last 12 month  
**44%**



The State of Industrial Cybersecurity, May 2022 | Trend Micro

### Security Outcomes



**93%** of organizations had 1+ intrusions in the past year;  
**78%** had 3+



**61%** of intrusions impacted OT systems



**90%** of intrusions required hours or longer to restore service

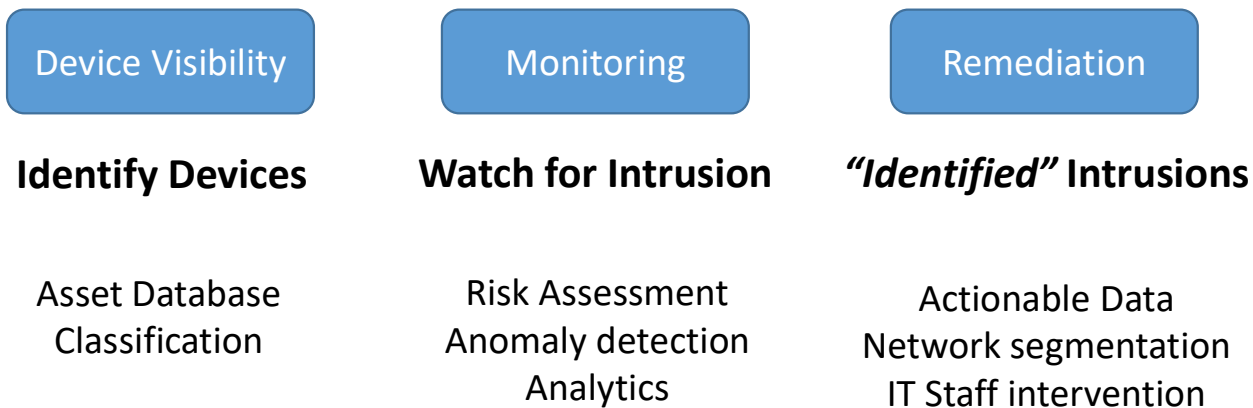
2022 State of Operational Technology and Cybersecurity Report | Fortinet

## A Third of Industrial Control Systems Attacked in H1 2021

infosecurity  
GROUP

# Today's OT Cybersecurity Solutions are Re-Active

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



Useful capability...but does not stop attacks



# Applying Standards / Guidelines / Frameworks

All of 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.

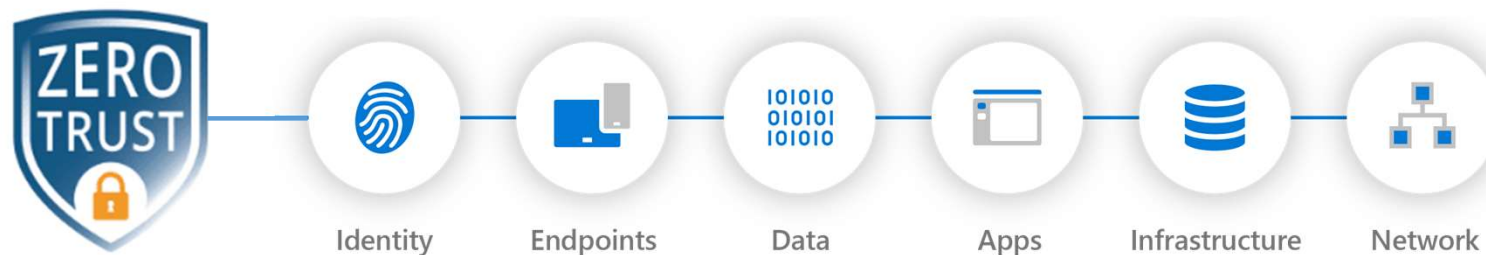
Gap in real-time protection for individual devices

The logo for the National Institute of Standards and Technology (NIST), consisting of the letters "NIST" in a bold, black, sans-serif font.The logo for MITRE, consisting of the letters "MITRE" in a bold, blue, sans-serif font.



# 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**



- 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



Developed in partnership with

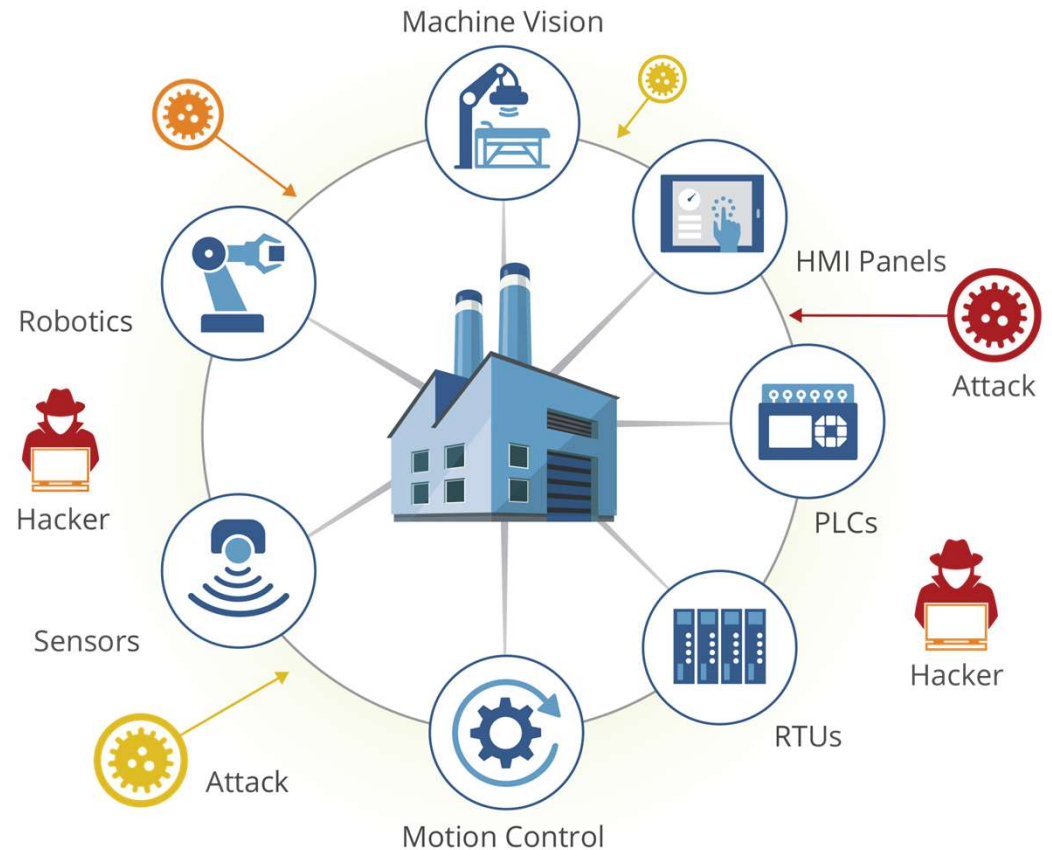




# Provides Device-Level Protection

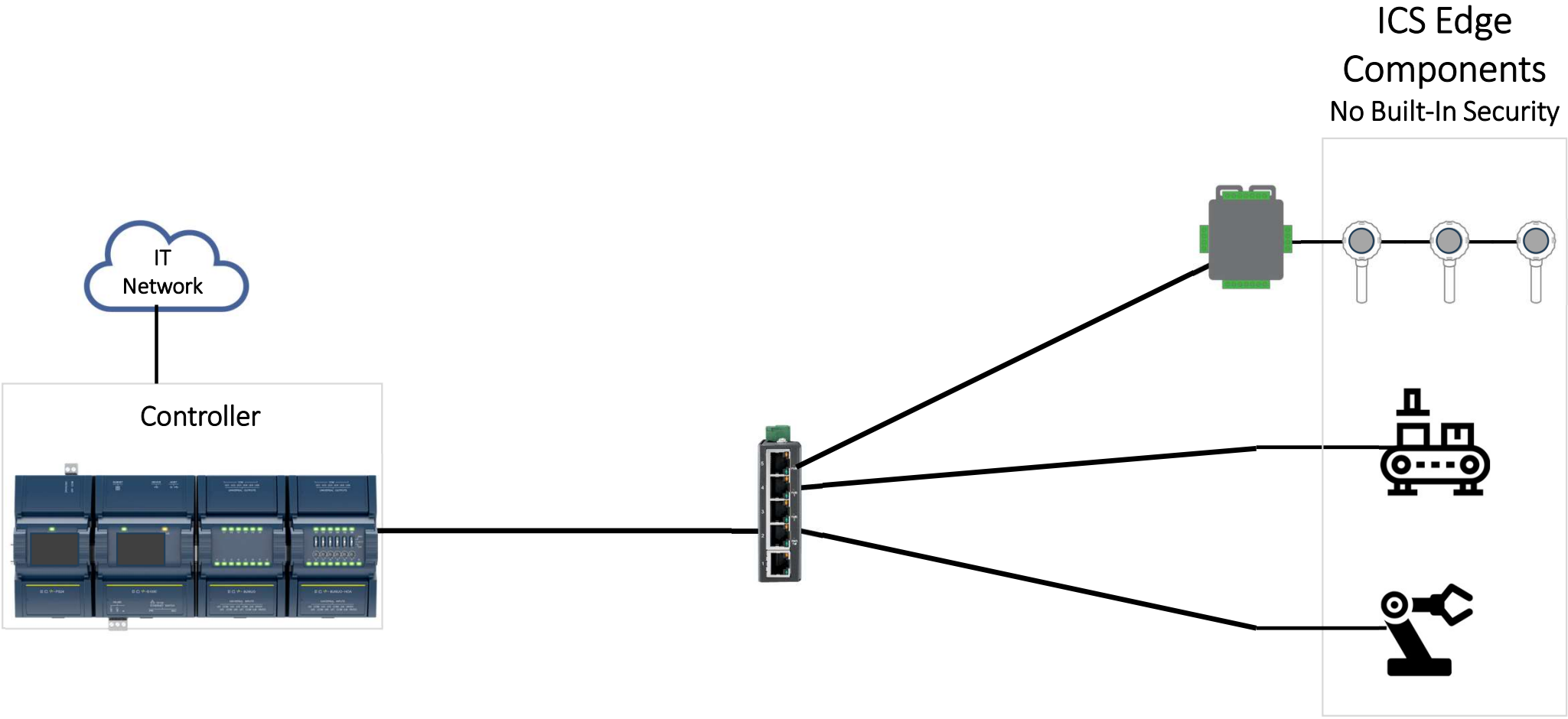
- NIST-compliant
- Authenticates all edge devices
- Protects Data and Commands
- Manages Connections
- Automates Certificate Mgmt
- Monitors and Alerts

Easy-to-Implement  
Solution that  
STOPS Cyber Attacks





# Unprotected Industrial Network



# Unprotected Network

## Message Info and Data are Visible

The image shows a Wireshark network traffic capture window titled '\*Ethernet 2'. The main pane displays a list of captured packets. The 5556th packet is highlighted in blue and has a red box around the 'TCP' protocol column and another red box around the packet details: '60 62641 → 5000 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=5'. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
5553	6356.962867	192.168.1.201	192.168.1.202	TCP	66	62641 → 5000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
5554	6356.962867	192.168.1.202	192.168.1.201	TCP	66	5000 → 62641 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
5555	6356.964174	192.168.1.201	192.168.1.202	TCP	60	62641 → 5000 [ACK] Seq=1 Ack=1 Win=262656 Len=0
5556	6356.964174	192.168.1.201	192.168.1.202	TCP	60	62641 → 5000 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=5
5557	6357.008653	192.168.1.202	192.168.1.201	TCP	60	5000 → 62641 [ACK] Seq=1 Ack=6 Win=2097920 Len=0
5558	6357.008653	192.168.1.201	192.168.1.202	RSL	60	[Malformed Packet: length of contained item exceeds 1
5559	6357.011763	192.168.1.202	192.168.1.201	TCP	60	5000 → 62641 [FIN, ACK] Seq=1 Ack=10 Win=2097920 Len=
5560	6357.011763	192.168.1.201	192.168.1.202	TCP	60	62641 → 5000 [ACK] Seq=10 Ack=2 Win=262656 Len=0
5561	6357.011763	192.168.1.201	192.168.1.202	TCP	60	62641 → 5000 [FIN, ACK] Seq=10 Ack=2 Win=262656 Len=0
5562	6357.011763	192.168.1.202	192.168.1.201	TCP	60	5000 → 62641 [ACK] Seq=2 Ack=11 Win=2097920 Len=0
5572	6369.019241	fe80::7ec2:c6ff:fe4...	ff02::2	ICMPv6	70	Router Solicitation from 7c:c2:c6:47:42:29

The bottom pane shows the details of the selected packet (No. 5556):

- > Frame 247: 156 bytes on wire (1248 bits), 156 bytes captured (1000000 bits on interface)
- > Ethernet II, Src: TP-Link\_47:42:29 (7c:c2:c6:47:42:29), Dst: 192.168.1.202 (08:00:27:00:00:02)
- > Internet Protocol Version 4, Src: 192.168.1.203, Dst: 192.168.1.202
- > User Datagram Protocol, Src Port: 9000, Dst Port: 9000
  - Source Port: 9000
  - Destination Port: 9000
  - Length: 122
  - Checksum: 0x4019 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 0]
- > [Timestamps]
- UDP payload (114 bytes)

The hex dump shows the raw data of the packet, with ASCII characters visible on the right side.

# DOME™ Protects New & Existing Industrial Networks



NIST-Compliant

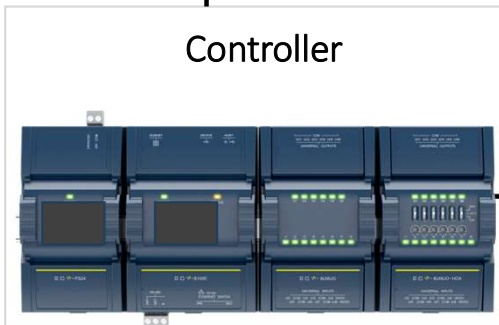


- Data logging
- Analytics
- Alerts

ICS Edge Components



Controller



DOME  
INTERFACE



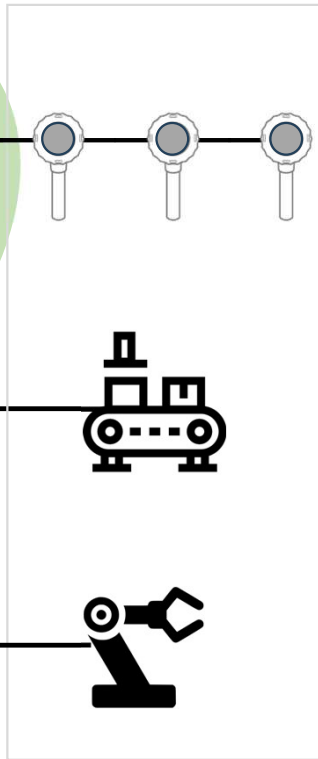
DOME  
SENTRY



DOME  
SENTRY



DOME  
SENTRY



Secure Enclave  
Encompass one or more zones

# DOME<sup>™</sup> 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

The image shows a Wireshark network traffic capture window titled '\*Ethernet 2'. The filter bar contains 'not arp and not ssdp'. The packet list pane shows a series of packets, with packet 247 (No. 6125) highlighted. This packet is a DTLS Continuation Data packet (Length: 156) from source 192.168.1.203 to destination 192.168.1.204. The 'DTLS' and 'Continuation Data' text in this row are highlighted with red boxes. The packet details pane for packet 247 shows it is a User Datagram Protocol (UDP) packet with source port 9000 and destination port 9000. The UDP payload is 114 bytes. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6118	6558.495741	192.168.1.206	192.168.1.255	NBNS	92	Name query NB WWHVQXTBK<00>
6123	6569.483698	192.168.1.203	192.168.1.204	DTLS	162	Continuation Data
6124	6569.488695	192.168.1.204	192.168.1.203	DTLS	162	Continuation Data
6125	6569.491924	192.168.1.203	192.168.1.204	DTLS	156	Continuation Data
6126	6569.491924	192.168.1.203	192.168.1.204	DTLS	156	Continuation Data
6127	6569.544262	192.168.1.204	192.168.1.203	DTLS	156	Continuation Data
6128	6569.547342	192.168.1.203	192.168.1.204	DTLS	156	Continuation Data
6129	6569.556878	192.168.1.204	192.168.1.203	DTLS	156	Continuation Data
6130	6569.560099	192.168.1.203	192.168.1.204	DTLS	156	Continuation Data
6131	6569.560099	192.168.1.203	192.168.1.204	DTLS	156	Continuation Data
6132	6569.567067	192.168.1.204	192.168.1.203	DTLS	156	Continuation Data

Frame 247: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface 0  
Ethernet II, Src: TP-Link\_47:42:29 (7c:c2:c6:47:42:29), Dst: 192.168.1.204 (08:00:27:00:00:02)  
Internet Protocol Version 4, Src: 192.168.1.203, Dst: 192.168.1.204  
User Datagram Protocol, Src Port: 9000, Dst Port: 9000

- Source Port: 9000
- Destination Port: 9000
- Length: 122
- Checksum: 0x4019 [unverified]  
[Checksum Status: Unverified]
- [Stream index: 0]
- [Timestamps]
- UDP payload (114 bytes)

```
0000 7c c2 c6 48 84 b1 7c c2 c6 47 42 29 08 00 45 00 |..H..|..
0010 00 8e a7 51 40 00 40 11 0e 26 c0 a8 01 cb c0 a8 |...Q@.@..
0020 01 cc 23 28 23 28 00 7a 40 19 2c 00 b2 00 6d 00 |..#(#{..z
0030 10 e1 b0 8d 7b e6 80 47 49 49 8b af ef 26 33 22 |...{..G
0040 3e 00 47 71 c4 2f 50 5d 10 a0 de e1 36 b1 3f 63 |>.Gq./P]
0050 0b 05 96 5a 7f 2d 74 bc 7f f1 a5 b7 e2 61 67 8f |...Z--t..
0060 90 a6 a1 7a 8d 9b 34 43 00 18 4e 0f dd dd b5 98 |...z..4C
0070 fb 60 b1 9c 91 4f da 76 9f 58 e2 bd 13 d4 72 ee |...0.V
0080 19 2f 95 75 d4 fd 1b 4f 19 95 00 10 db d8 b6 f8 |./u...C
0090 bf 95 4d 18 62 f2 5f 80 40 65 9d 26 |..M.b_..
```





# Stops Attacks and Unauthorized Traffic

Request from  
Un-Authenticated  
Device & Retries



Messages Blocked

The screenshot shows a network traffic capture in Wireshark. The packet list pane displays several TCP packets. Packet 5254 is a SYN packet from 192.168.1.205 to 192.168.1.204. Packet 5255 is an RST, ACK packet from 192.168.1.204 to 192.168.1.205, which is highlighted with a red box. Subsequent packets (5257-5265) show retransmissions and further RST, ACK packets. The packet details pane shows the structure of a blocked message: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (port 9000).

No.	Time	Source	Destination	Protocol	Length	Info
5253	6172.623116	192.168.1.204	192.168.1.205	TCP	60	5000 → 50551 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5254	6172.740336	192.168.1.205	192.168.1.204	TCP	66	50552 → 5000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
5255	6172.740336	192.168.1.204	192.168.1.205	TCP	60	5000 → 50552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5257	6173.253502	192.168.1.205	192.168.1.204	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50552
5258	6173.253502	192.168.1.204	192.168.1.205	TCP	60	5000 → 50552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5259	6173.761135	192.168.1.205	192.168.1.204	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50552
5260	6173.761135	192.168.1.204	192.168.1.205	TCP	60	5000 → 50552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5262	6174.269137	192.168.1.205	192.168.1.204	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50552
5263	6174.269137	192.168.1.204	192.168.1.205	TCP	60	5000 → 50552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5264	6174.775702	192.168.1.205	192.168.1.204	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 50552
5265	6174.775702	192.168.1.204	192.168.1.205	TCP	60	5000 → 50552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 247: 156 bytes on wire (1248 bits), 156 bytes captured (1...  
> Ethernet II, Src: TP-Link\_47:42:29 (7c:c2:c6:47:42:29), Dst: TP...  
> Internet Protocol Version 4, Src: 192.168.1.203, Dst: 192.168.1...  
> User Datagram Protocol, Src Port: 9000, Dst Port: 9000  
Datagram Transport Layer Security

```
0000 7c c2 c6 48 84 b1 7c c2 c6 47 42 29 08 00 45 00 |..H...|
0010 00 8e a7 51 40 00 40 11 0e 26 c0 a8 01 cb c0 a8 |...Q@.@.
0020 01 cc 23 28 23 28 00 7a 40 19 2c 00 b2 00 6d 00 |..#(#{.z
0030 10 e1 b0 8d 7b e6 80 47 49 49 8b af ef 26 33 22 |...{.G
0040 3e 00 47 71 c4 2f 50 5d 10 a0 de e1 36 b1 3f 63 |>.Gq./P]
0050 0b 05 96 5a 7f 2d 74 bc 7f f1 a5 b7 e2 61 67 8f |...Z.-t.
0060 90 a6 a1 7a 8d 9b 34 43 00 18 4e 0f dd dd b5 98 |...z..4C
0070 fb 60 b1 9c 91 4f da 76 9f 58 e2 bd 13 d4 72 ee |`...O.v
0080 19 2f 95 75 d4 fd 1b 4f 19 95 00 10 db d8 b6 f8 |./u...O
0090 bf 95 4d 18 62 f2 5f 80 40 65 9d 26 |..M.b._
```





# “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

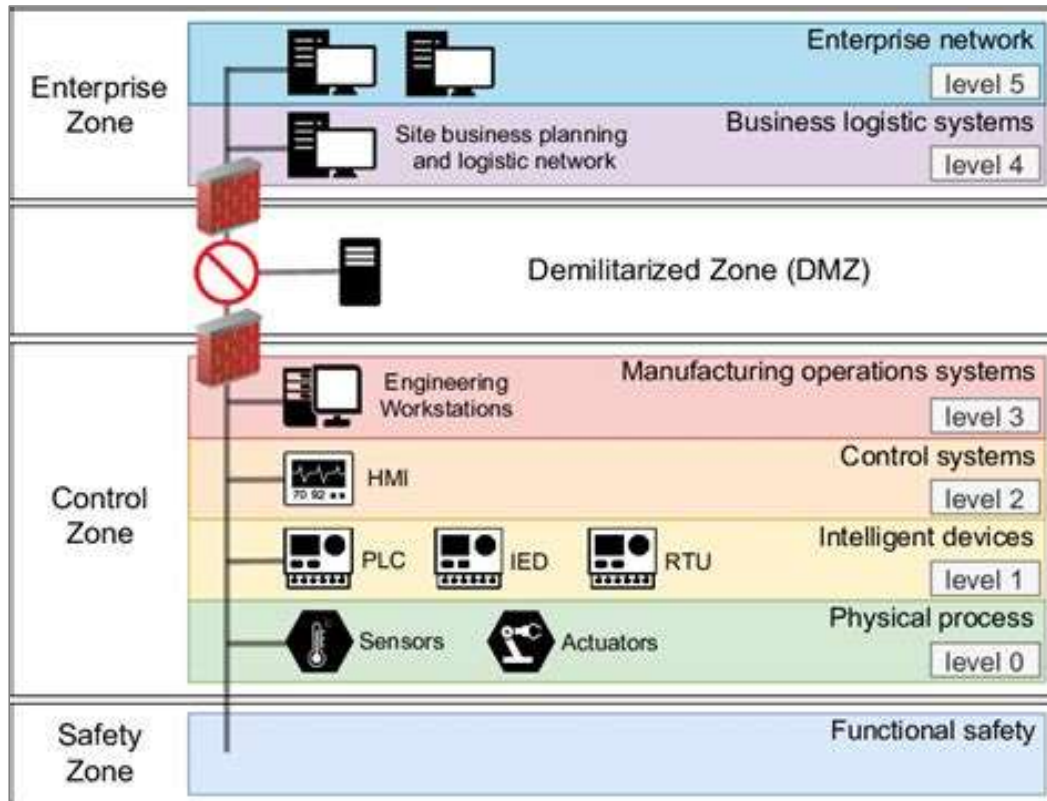
- Protection/Encryption between devices
- Supports commonly used IP network protocols

# Risk Management Framework: DOME Compliance

## NIST 800-53

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

# Applying DOME in the Purdue Model



**DOME**<sup>TM</sup>

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](https://veridify.com)

+1.888.272.1977