BlackBear
Cyber Security

BlackBear Cybersecurity Solutions

Table of Contents

Corporate Strengths

IEC 62443 certified consultants

IEC 62443-4-1 Industrial cyber security certified manufactured products

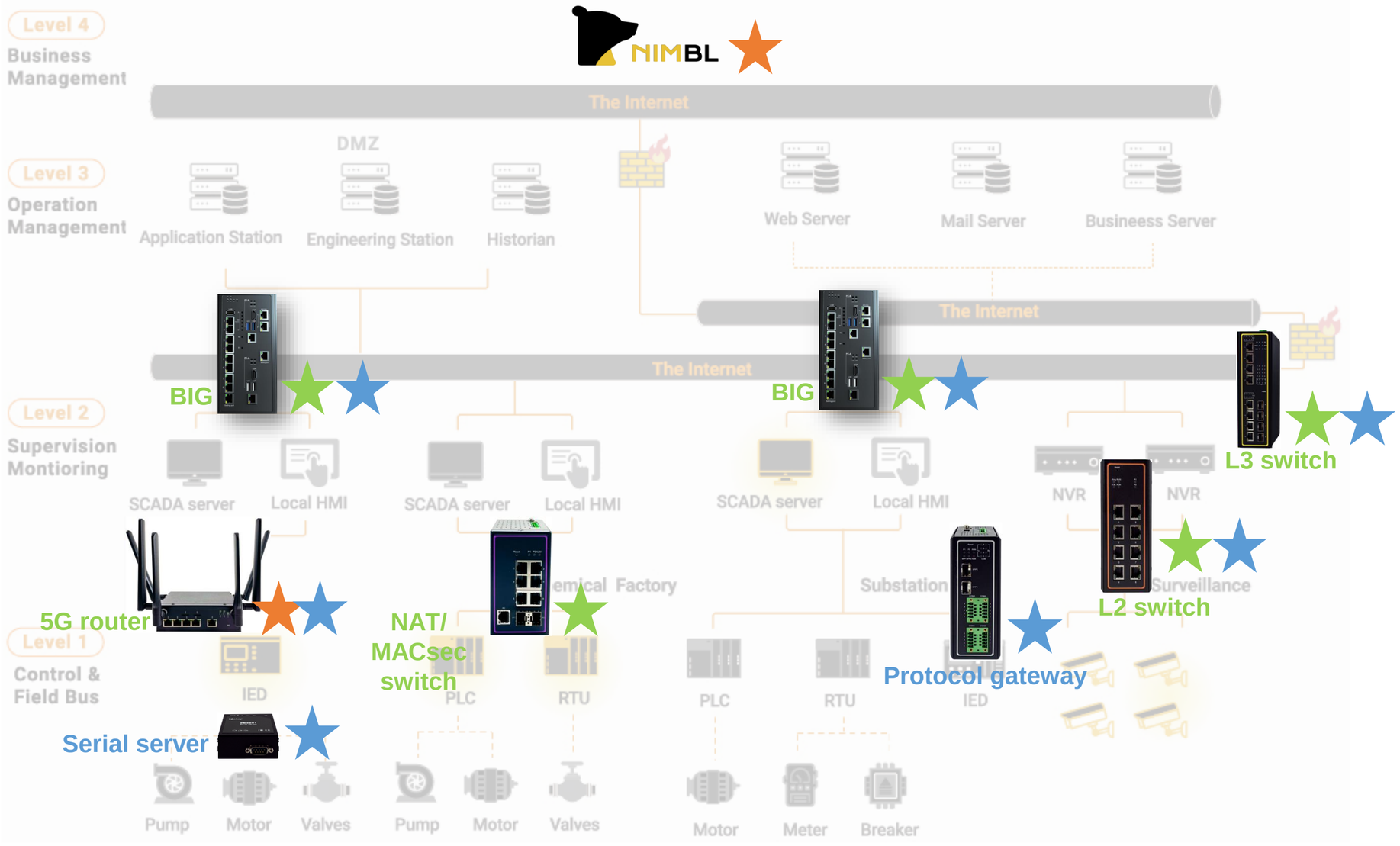
30+ years of experience in the critical infrastructure market

Solid case studies in LATAM, ASIA, MEA, renowned customers in various vertical markets

Tailored product for various use cases to address different engineering challenges

Prompt and on-time project support

BlackBear TechHive Cybersecurity Propositions



Protect Your Network

- Network Segmentation
- Air-gap protection

Network Status

- Secured Management
- Secured remote access

Secured Devices

- IEC/ISA 62443
- IEC 62351
- TAICS

OT vs IT Security

BlackBear
Cyber Security

Cybersecurity Gap Between OT and IT

Operational Technology	VS	Information Technology
Availability	Business Priority	Confidentiality
Cannot tolerate downtime	Major focus	Data integrity
Specified protocols	Protocols used	Tons of protocols
PLC, HMI, Meter	Protection targets	Computers, Servers
No	Patch or AV software installed	Yes

OT Threat Assessments

Assets From Closed Network Are Exposed

Access to assets from outside are inevitable due to **IIoT 4.0**

01

02

Absence of Secured SW Protection

Legacy devices with outdated SW

Easily Compromised System

Legacy system with known vulnerabilities and exposure

03

04

Horizontal Propagation

Compromised hosts could destroy the production line

Vertical Propagation

Hidden malicious code in **existing devices** could attack the IT

05

06

Demand for 24/7 Operation

Continuous operation creates endless attack time window for culprits

OT Cybersecurity Approaches

01

White List Approach

Specific Protocols Only

02

External Secure Appliances

Firewall, Diode, IPS/IDS

03

Seamless Operation

No efforts from OT operator(s)

Expert’s Perceptions

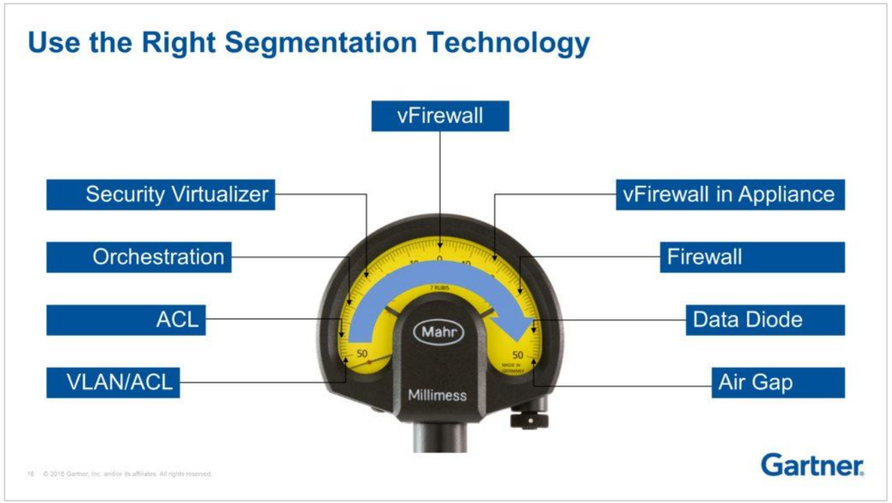
Seven Steps to Effectively Defend Industrial Control Systems

1. Application Whitelisting
2. Configuration/Patch Management
3. Reduce Attack Surface
4. Defendable Environment
5. Manage Authentication
6. Implement Secure Remote Access
7. Monitor & Respond

By U.S. Department of Homeland Security; National Cybersecurity and Communications Integration Center

https://www.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

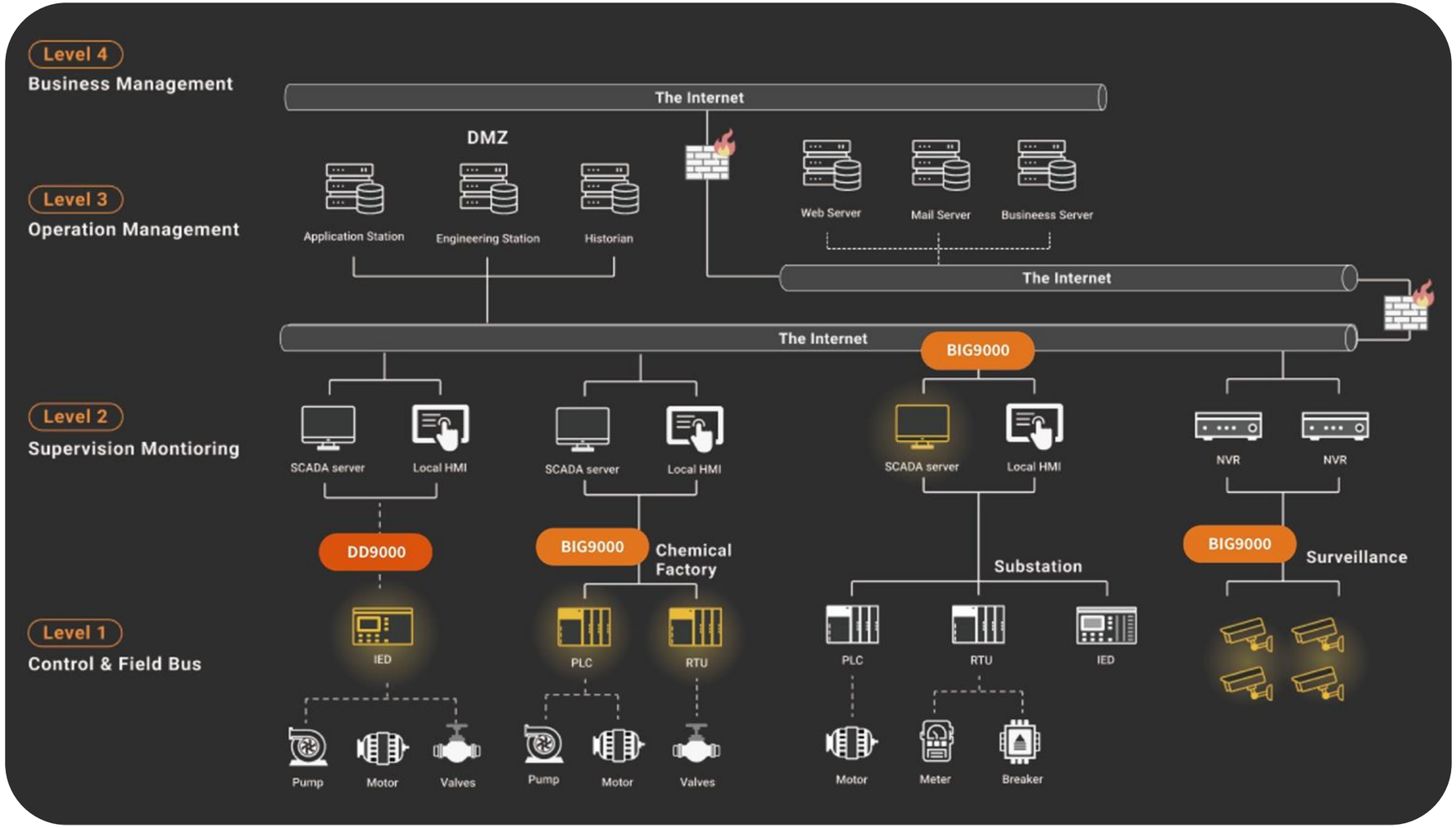
- 98% out of the 295 cyber security incidents reported by ICS-CERT in FY2014-2015 could be prevented with this technique.
- Data diode supports these techniques.



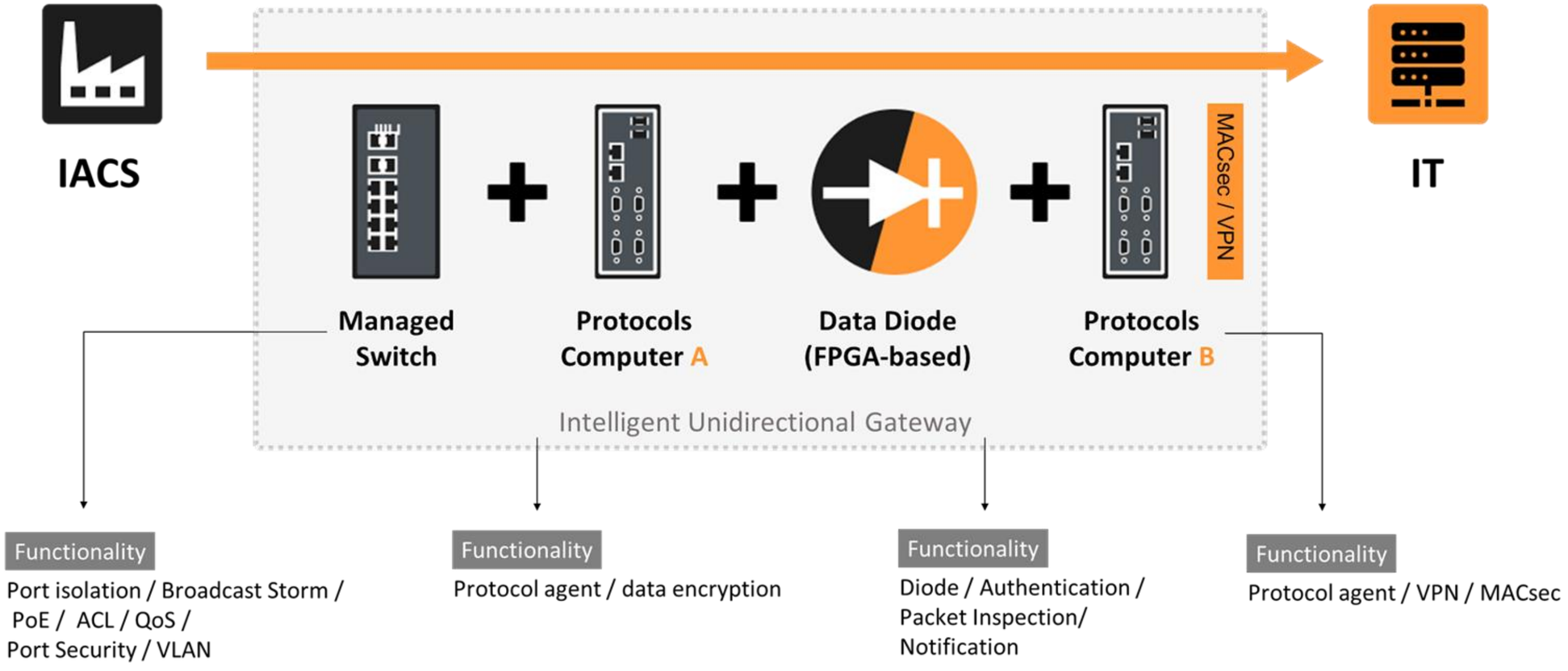
BlackBear Intelligent Gateway

BlackBear
Cyber Security

Where is BIG being USED?



BIG9000 System Diagram



Product Features

One-way data transfer: Impenetrable defense
Virus & malware prevention due to law of physics

Physical isolation
Network segmentation at physical layer

Patented horizontal & vertical protection
Deep packet inspection and port isolation

Data filtering & validation
Rule-based and packet inspection

Built-in packet sniffing
Works well with poor networking environments for technical support

Built-in proxy servers
DNP3/OPC-UA/MQTT/Modbus/ONVIF…

Hardware based real time data transfer & low latency
Operate at 1Gbps line speed

Connect up to 8 OT devices
For simpler topologies and installation

Seamless operation
Plug and run upon configuration

Reduced human error
No or little maintenance required

Add-value functions
ACL/Port isolation/broadcast storm/ data encryption & many more

Product Values

All in one—no hidden costs
No need to buy proxy server/ software licenses
No subscription

Industrial grade with long life cycle
Long MBTF

Compliance with various industrial certifications
NIST
NERC-CIP
HPAA
IEC62443-3

Plug and play installation
No changes needed in original OT environment
Zero impact during installation

Prevent misconfigurations
99% of firewall breaches are due to misconfigurations

Saves maintenance work
Less policy & procedure updates on network

Saves maintenance cost
No regular reconfiguration necessary
No need to hire advanced personnel

BIG9000 Case Studies

BlackBear
Cyber Security

Case 1: Secure Network Tapping (Practical use)

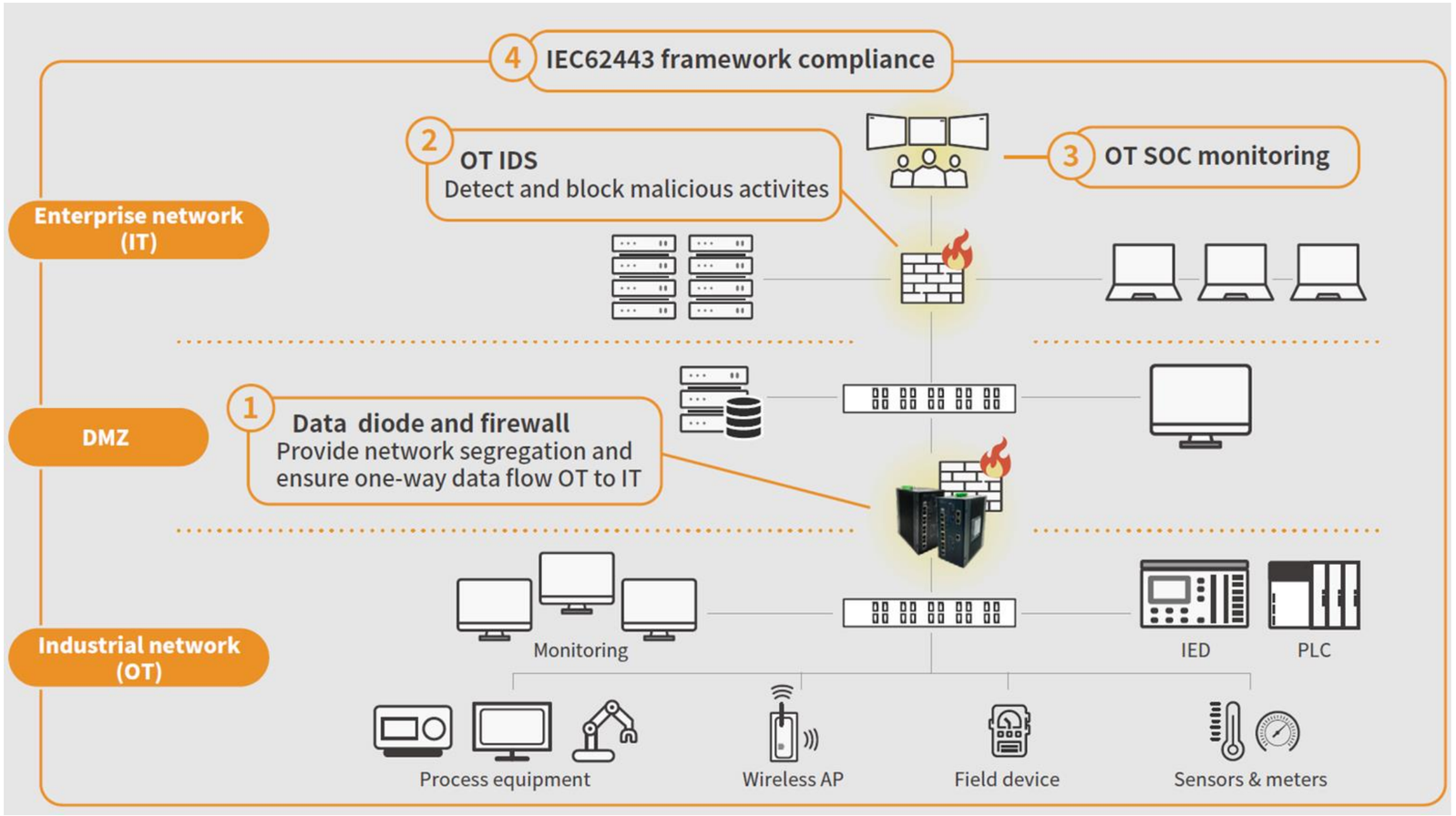
Substation

Use Case

- All the data packet from SCADA/HMI/Server are mirrored via mirror port in BIG, send to SOC IDS.

BIG is used as

- Secured network tapping
- Built-in switch will filter the data packet based on switch rules.
- Data from BIG > SOC is protected with MACSec
- Pure data diode



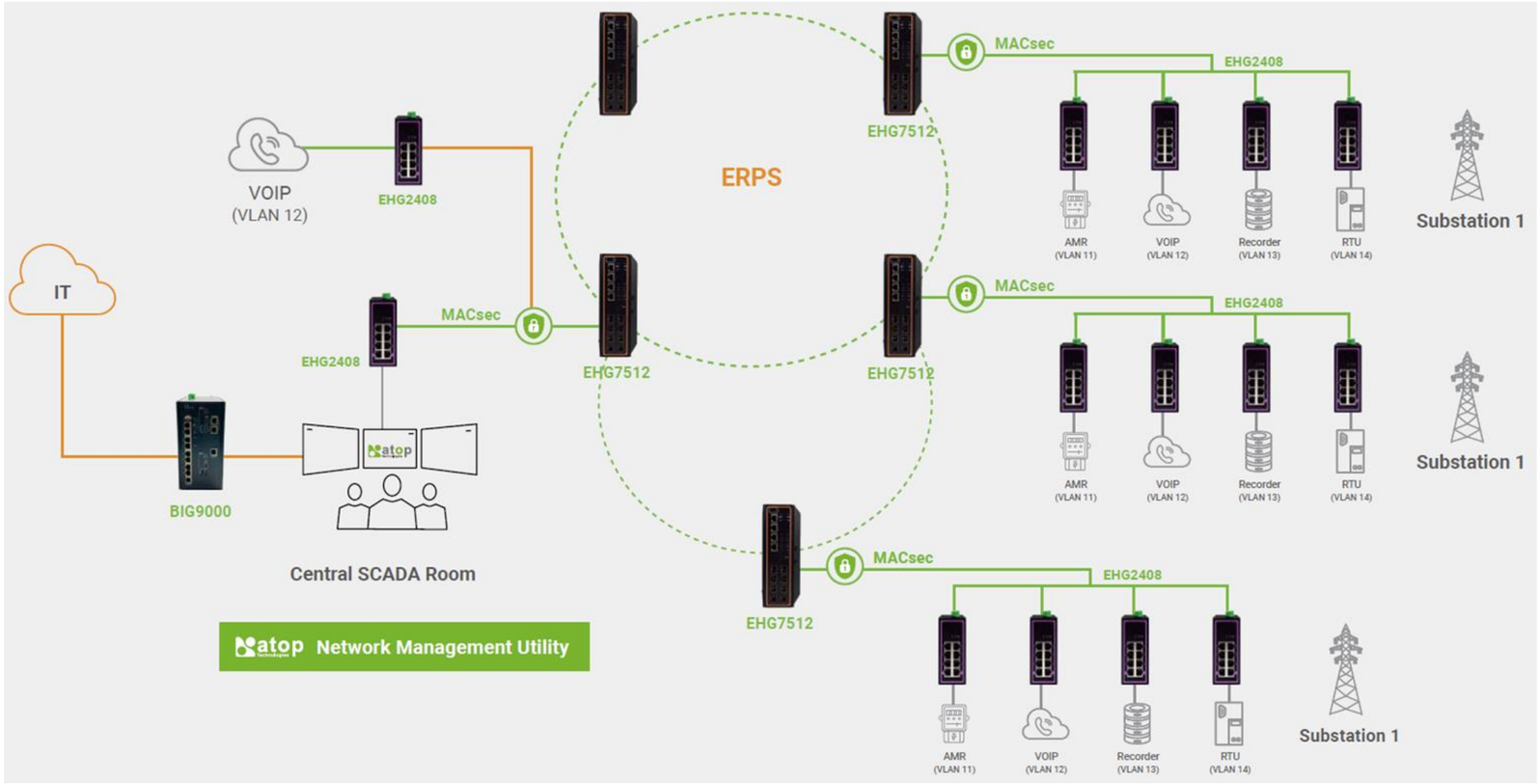
Case 2: Robust and Secure Networking (Practical use)

Substation

Use Case
- Robust networking redundancy
- Secured data transmission

BIG is used as
- Secured file transmission via FTP/sFTP
- Pure data diode

ATOP switches are used as
- Robust Networking redundancy
- MACsec data transmission
- Unifi networking management tool



Case 3: Secured Syslog Transmission (PoC)

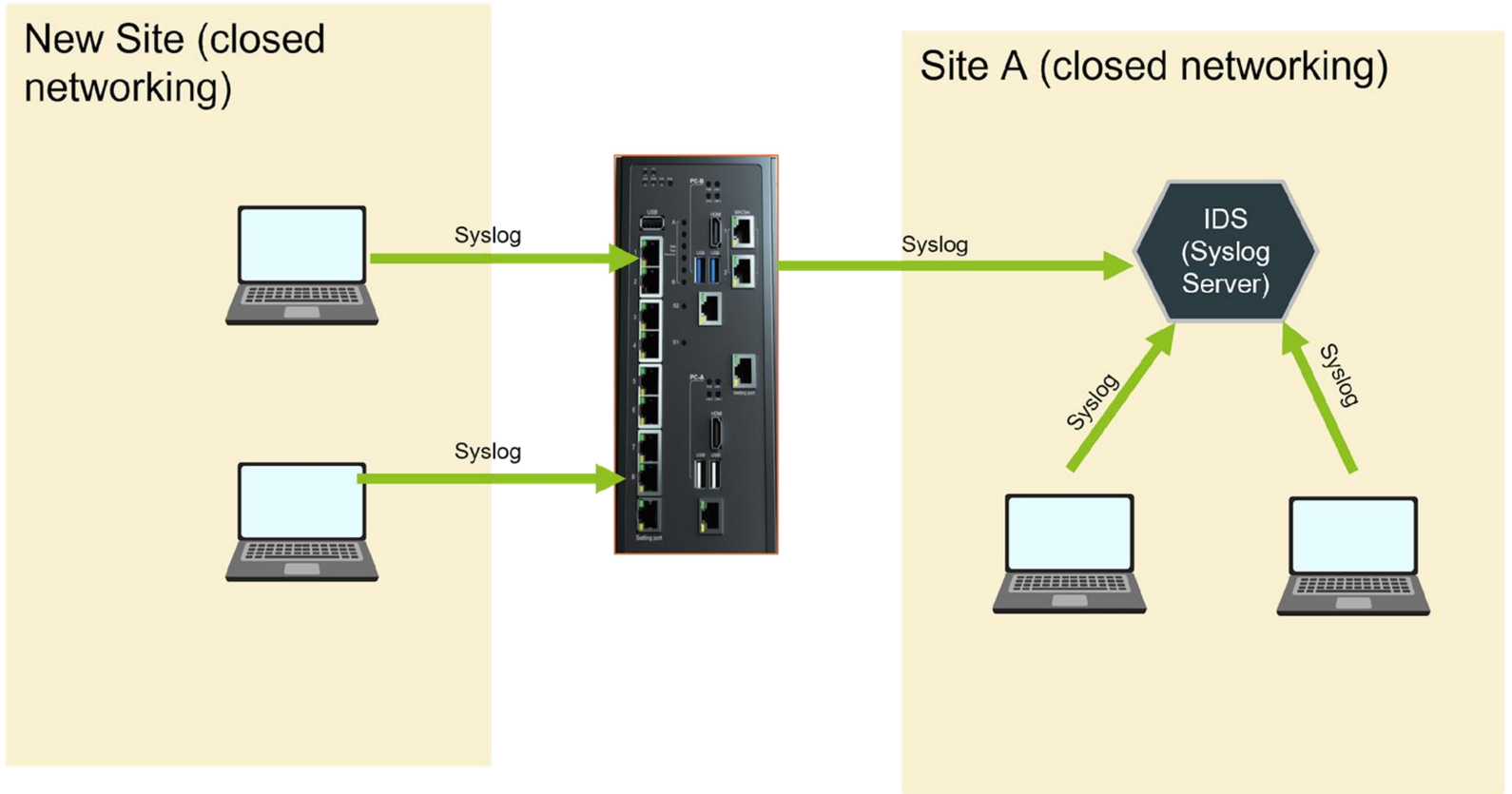
Central Bank

Use Case

- Mirror syslog message from one secure site to another secure site

BIG is used as

- Secured syslog transmission
- Data from BIG to IDS is protected with MACsec
- Pure data diode

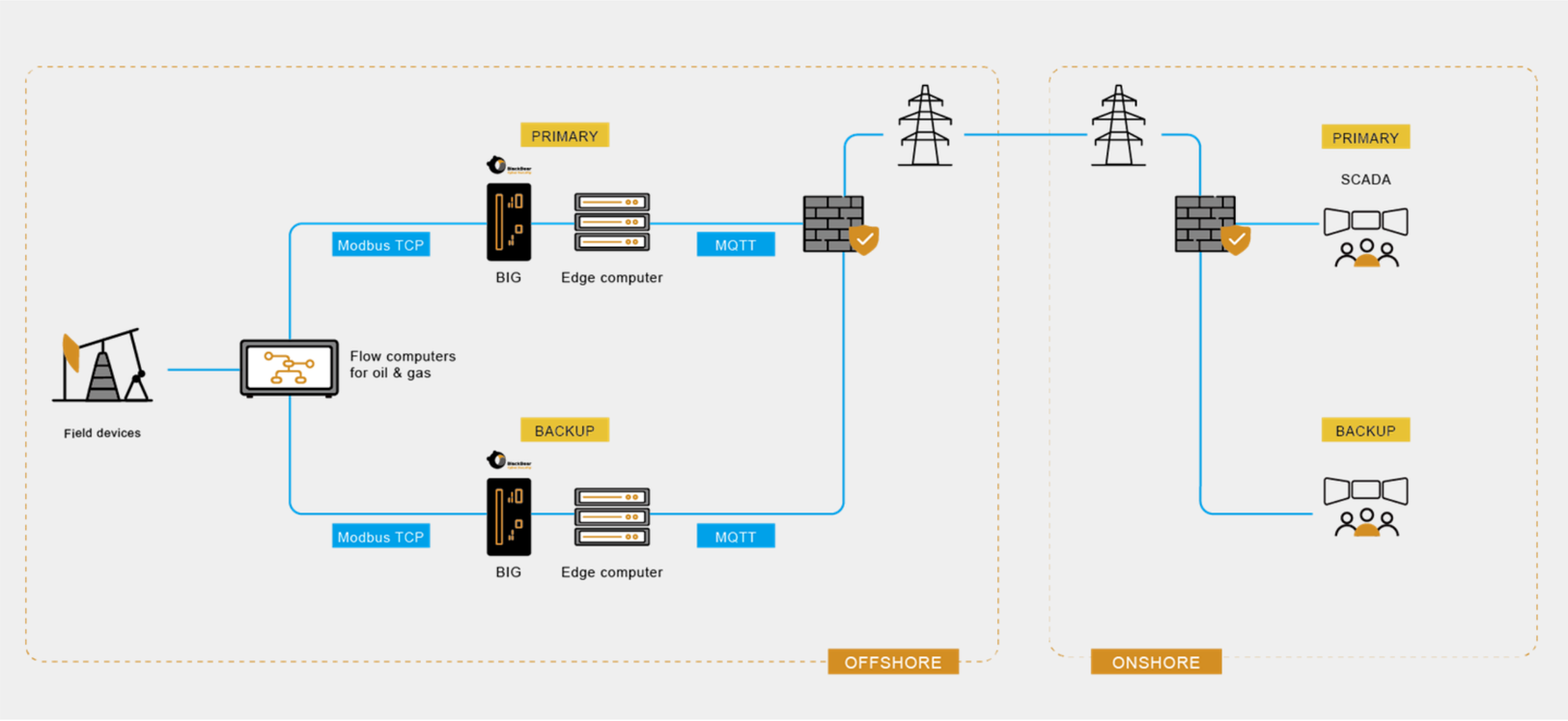


Case 4: Secured Modbus/OPCUA Data Collection (Practical use)

Offshore Mining

Use Case
- Offshore Modbus and OPCUA data collection

BIG is used as
- Secured Modbus and OPCUA data transmission
- Pure data diode



Case 5: Secured Big Data Transmission (Practical use)

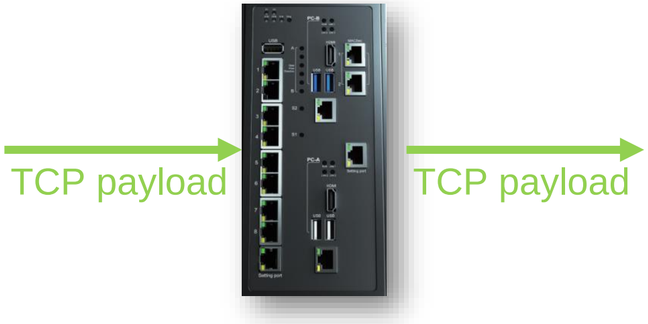
Manufacturer

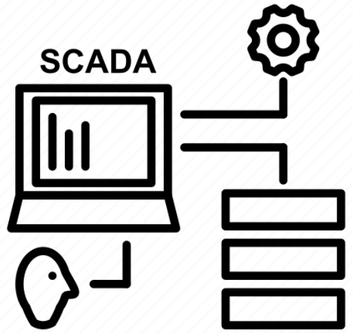
Use Case

- 10GB data transmission without packet loss.
- Using TCP payload only

BIG is used as

- Efficient and secured big data transmission without packet loss.
- Pure data diode





Case 6: Secured Commands Transmission (PoC)

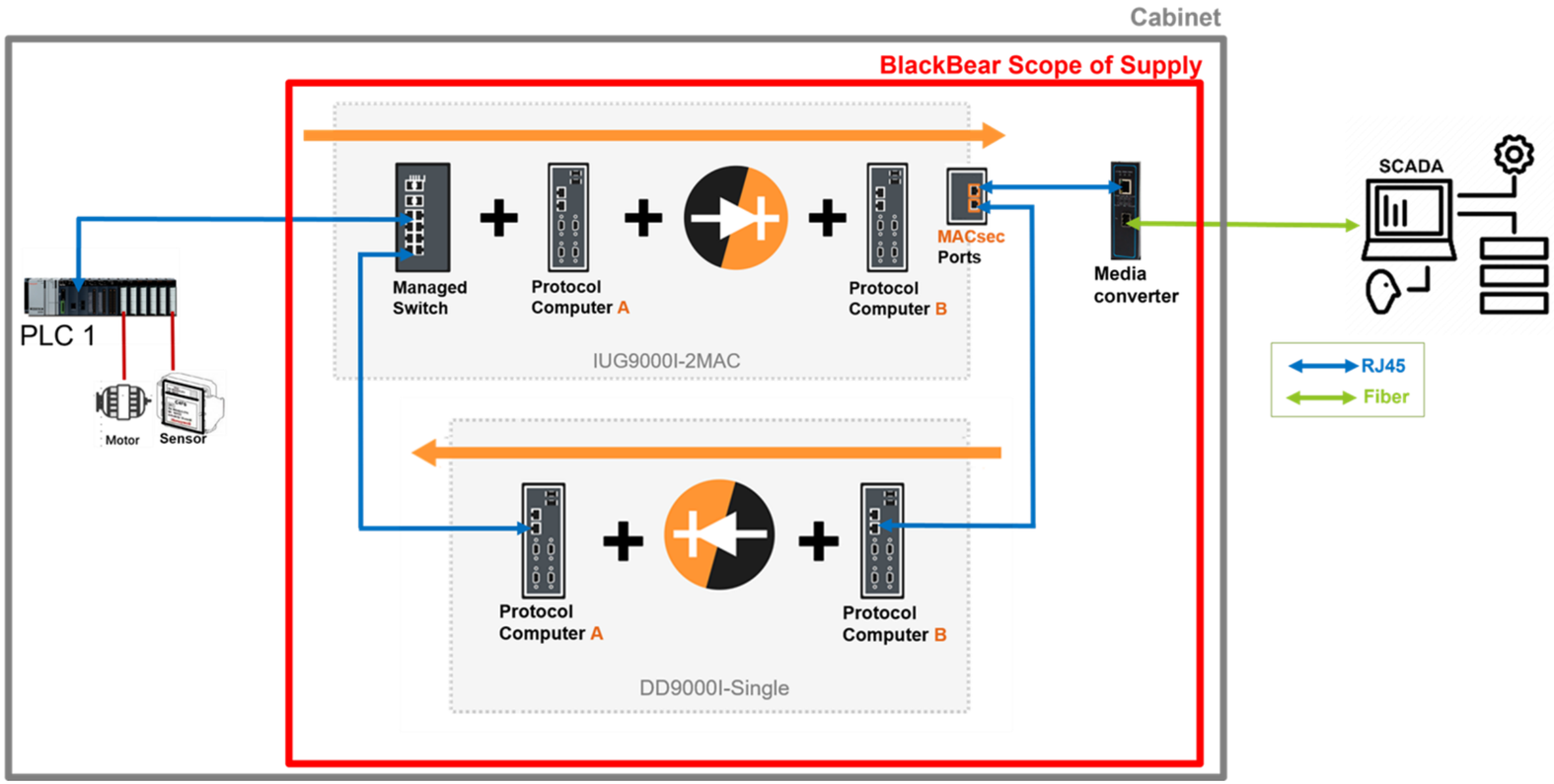
Offshore Mining

Use Case

- Offshore Modbus collections and command transmission

BIG is used as

- Secured Modbus data collection
- Secured Modbus command transmission
- Reversed diode



Case 7: Floating Solar Power Field Monitoring (Practical use)

Solar Farm

Use Case
- OPCUA data collection

BIG is used as
- OPCUA data transmission
- Pure data diode

OPCUA

OPCUA

Cloud

Competitor Analysis

BlackBear
Cyber Security

Competitor Analysis – Hardware Aspect

	Waterfall WF500	OWL OPDS1000	BlackBear BIG9000
Mechanism	Rack mount (1U) & DIN-Rail	Rack mount (1U)	Din-rail
Operating temperature	0°C to 43.33°C	0°C to +43.33°C	-40°C to +70°C
Diode technologies	Optical fiber	Optical fiber	FPGA
Cooling	Fans	Conductive/Fans	Thermal pad
Network connectivity	1000Mbps x 6 (OT:3, IT:3)	1000Mbps x 2 (OT:1, IT:1)	1000Mbps x 10 (OT:8, IT:2)
Approvals	Security: EAL 4+, ANSSI CSPN, KC, NITES, NISA	Security: EAL 4+ Others: CE/FCC, UL, VCCI	Security: IEC62443 Others: CE/FCC, UL
PoE PSE	N/A	N/A	802.3 af/at x 8
MACsec data encryption	N/A	N/A	MACsec x 2
Hardware	Commercial grade	Commercial grade	Industrial grade

Data source: Waterfall and OWL websites, 20231214.
Table by BlackBear Cyber Security.

Competitor Analysis – Software Aspect

	Waterfall WF500	OWL OPDS1000	BlackBear BIG9000
Substation protocols	IEC104, DNP3.0	IEC104 (add-on)	IEC104, DNP3.0, IEC61850
Building protocols	N/A	N/A	BACnet
Video	RTP, RTSP	N/A	ONVIF, RTSP
Historians & DB	Yes	Yes	N/A
File transfers	SFTP, FTPs, FTP, SMB, HTTPFS, NFS, TFTP (add-on)	FTP, RFTS SFTP (add-on)	SFTP, FTP, SMB
Automation protocols	Modbus, S7 historian, OPC DA/UA, Emerson(EDS), GE(iFix),OPC DA, A&E, OPC UA, MQTT	OPC DA, A&E, OPC UA, MQTT (add-on)	Modbus, OPC UA, S7(TBD), MQTT
Enterprise monitoring	SNMP, Syslog, SMTP ……	SNMP, Syslog	Syslog

Data source: Waterfall and OWL websites, 20231214.
Table by BlackBear Cyber Security.

Competitor Analysis – Use Case

	Waterfall WF500	OWL OPDS1000	BlackBear BIG9000
Location	SCADA, ERP, WMS…	SCADA, ERP, WMS…	PLC, SCADA…
OT assets protection	Yes	Yes	Yes
OT assets isolation	N/A	N/A	Yes
Protection for malicious OT traffic propagated to IT	N/A	N/A	Yes
Reverse channel	Yes	Yes	Yes
MBTF	10-20 years	11 years	25 years

Data source: Waterfall and OWL websites, 20231214.
Table by BlackBear Cyber Security.

Unidirectional Media Converter (UMC24)

BlackBear
Cyber Security

Unidirectional Media Converter – UMC24

UDP packets with reliable output

DIN rail / Wall mount

Industrial grade and **long MBTF**

Optical fiber for high speed up to **1Gbps**
Long distance transmission up to **40km**

LED to indicate data transfer

Dual power input

Cost effective

For **critical infrastructure**:
Nuclear, water treatment plant, transportation, enterprise, finance

UMC24 – Preliminary Specs

Different connectors: SC/ST/LX fiber connectors
Different speed: 100/1000
Different distance: 550m – 40km

Environmental Limits

Operating Temperature: 10°C to +75°C (-40°F to +167°F)
Storage Temperature: 40°C to +85°C (-40°F to +185°F)
Ambient Relative Humidity: 5% to 95% (Non-condensing test)

Physical Characteristics:

Housing: IP30 protection, metal house
Weight: 300g (TBD)
Dimension: 110 x 90 x 35 mm (TBD)
Installation: DIN-Rail. Mounting & Wall mount kit (optional)

Coming up—
Product Roadmap

BlackBear
Cyber Security

Roadmap

Data Diode - Software

Support more protocols: MQTT, etc
Built-in NTP server
Features on demand

Data Diode - Hardware

Rackmount form factor
10Gbps transmission speed

New Product

Firewall

Frequently Asked Questions

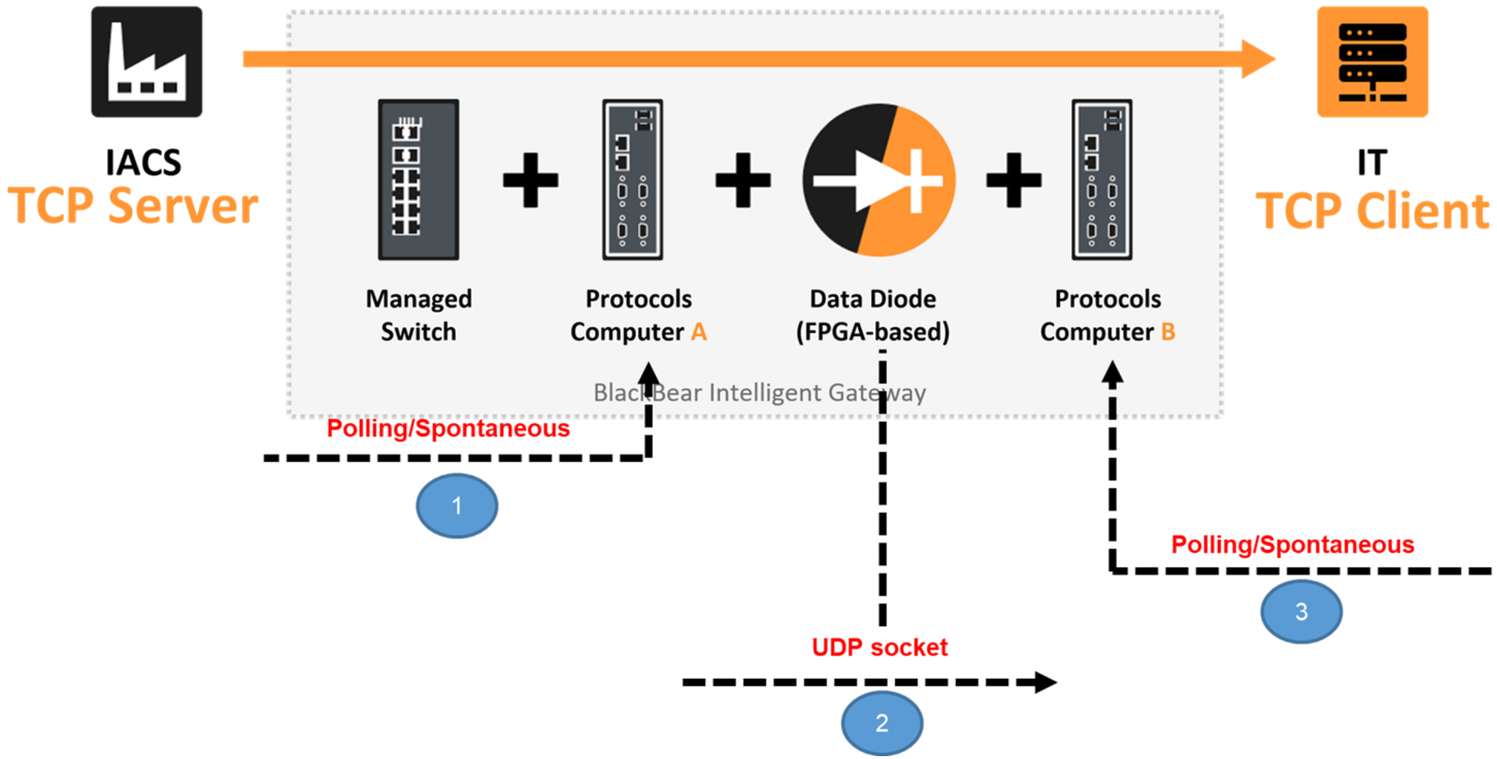
BlackBear
Cyber Security

BIG Performance and Latency

TCP-based Industrial Protocols (Modbus/DNP3/IEC104/IEC61850/OPCUA…)

Time Spent

1. Polling/Spontaneous (<10ms)
2. <10ms
3. Polling/Spontaneous (<10ms)

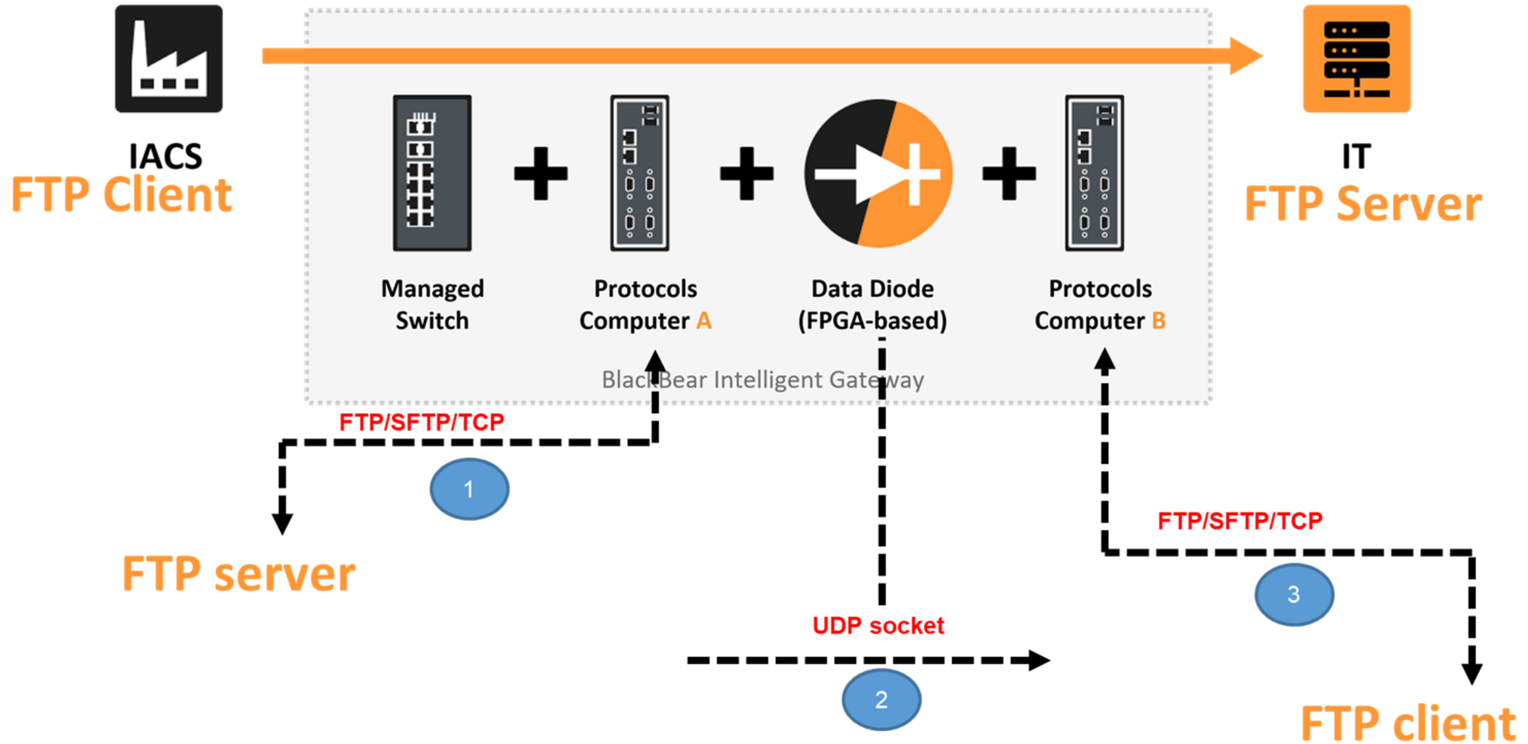


BIG Performance and Latency

File transfer (TCP payload/FTP/SFTP…)

Time Spent

1. 10GB file size in 30mins.
2. Consequent 10 times testing without packet loss.



Cyber Security Level Recognition

Penetration Test Labs	Country	Status	Test Coverage and Results; Notes
CSTI 資安科技研究所 CyberSecurity Technology Institute / 財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY	Taiwan	Completed	OWASP IoT Top 10, OWASP Top 10, CWE/SANS Top 47 – No vulnerability after revisiting
STH SIAM THANAT HACK	Thailand	Completed	Add PCI Penetration, IEEE Top 10 Software Security Design Flaw - No vulnerability after revisiting
strategic partner / 中華資安國際 CHT Security	Taiwan	Completed	Add reverse channel communication Include Security for industrial and control systems, Part 62443-4-2
exida	Singapore	Completed	Achilles Certification Services Lv2 Pentest
NECTEC a member of NSTDA	Thailand	Completed	Pentest include reverse horizontal channel communication + BreakingPoint vulnerability scan
Flatt SECURITY	Japan	Completed	Pentest Include reverse + horizontal channel communication + USB two-factor authentication
BUREAU VERITAS	France	IEC 62443-4-1 Completed IEC 62443-4-2 Processing	IEC 62443-4 certification assessment services

THANK YOU
FOR YOUR ATTENTION.

BlackBear Industrial Networking Security Ltd. | by BlackBear TechHive

Address: No. 146, Sec. 1, Dongxing Rd., Zhubei City, Hsinchu County , Taiwan

Phone: +886 3 5501898

Email: sales@blackbear-ics.com