

E.S. EMBEDDED SOLUTIONS 3000
(E.S.)

Brief Company Introduction

June 2023

“In Zero Trust we Trust”

Cyber Security World



- Founded in 2002, privately held
- Led by CEO,CTO Dr. Larisa Tsirinsky
- HQ: Ramat Gan Israel
- Employees: ~40 engineers
- Pioneering in:
 - Cyber security invisible to attackers
 - Zero-trust, Quantum-Ready OT cybersecurity, White Box Cryptography
 - Secure IT/OT convergence
- Helping our global customers to secure networks and become compliant to latest standards
- Patented technology
- Certified Israel Defense Exporter



From defense to civilian applications

- ▶ Our group got over 18 years of experience with solutions originally designed for the Israeli Armed Forces and adapted to other defense and civilian customers.
- ▶ E.S. Embedded solutions 3000 (ES), founded in 2021, is a spin-off focusing entirely on civilian applications offering network security appliance product portfolio to Government, Manufacturing, Critical Facilities, Telecom and other industries



Meet Embedded Solutions 3000 leadership



Dr. Larisa Tsirinsky

Founder, CEO, CTO

- ▶ Holds Ph.D. degree in Technical Cybernetics and Computer Science
- ▶ Holds several registered patents in the fields of time/mission-critical communication and network security
- ▶ A committee member of the "ISO Global Directory" for Industrial and IT security standards
- ▶ Prior to founding E.S., Dr. Tsirinsky led a team at Israel Aircraft Industry, MLM division



Yaron Mintzker

VP Business Development and Sales

- ▶ Holds a master's degree in innovation and entrepreneurship
- ▶ Engineering background in computer science
- ▶ 15 years experience in global sales, marketing, business development, and channel management positions both in private and public high-tech companies, as well as forming successful collaborations



Ilya Feigin

Chief Customer Officer

- ▶ Holds an MBA from the Wharton School at the University of Pennsylvania and a BA in Computer Science from the Open University of Israel.
- ▶ Prior to joining Embedded Solutions 3000, he held roles in cyber security strategy and global business development at Samsung in Korea.
- ▶ Before Samsung, Ilya led a team of ethical hackers at EY in Israel and served as an information security team leader in the elite MAMRAM unit of the Israeli Defense Forces (IDF).

Customers

After 20 years of experience with Israeli defense customers, we are quickly expanding globally with over 100 civilian installations since 2021

Government

Defense Contractors

Industry / Critical Infrastructure

Enterprises

- Israel Defense Force
- Israel Air Force
- Israel Ministry of Defense
- Israel Ministry of Finance
- Office of Israel Prime Ministry
- EU Member Government
- APAC Country Government
- Southern Africa Country Government
- APAC Country Smart City Project



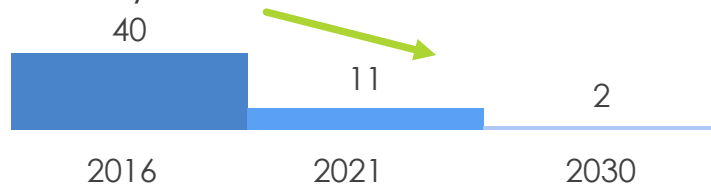
: Most of our international customers' names could not be disclosed due to NDA requirements, reference calls might be arranged on request

Managing Cyber-risk is no longer optional

Cyber Attacks Impact is substantial



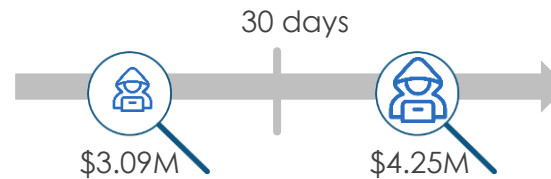
- Impact include:
 - Financial losses
 - Loss of productivity
 - Reputation damage
 - Legal liability
 - Business continuity problems
- Ransomware is on the rise** (from once every 40 seconds in 2016 to 11s in 2021) :



Breaches take time to be discovered



- 197** days to discover a breach
- 69** days more to contain it
- The longer it takes the more expensive the breach is :

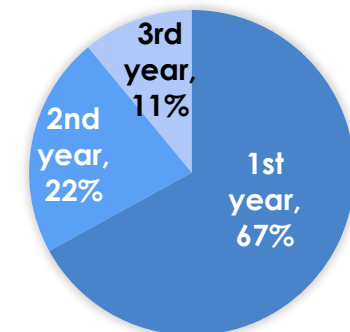


Cyber Crime costs are rising



- Long tail implications of a breach may take years: **lost data, business disruption, revenue losses from system downtime, notification costs, or even damage to a brand's reputation**

Long tail costs post-breach:



Advancements in attacks drive cyber security technology modernization

Some Cyber Tech becoming fast obsolete..



Legacy Firewalls



- ▶ **Firewalls are not bulletproof:** "October 2022 Fortinet Firewall Vulnerability may allow an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP/HTTPS requests".

Data Diodes



- ▶ "Data Diodes: Super Security or Super **Pain?** Issues with TCP and bypasses."

Password Encryption



- ▶ **60%** of large companies and 90 percent of midsize companies will implement passwordless methods for more than half of their operations over the next few years (2020).



- ▶ "At least **70%** of new remote access deployments will be served mainly by ZTNA instead of VPN services by 2025—up from less than 10% at the end of 2021. "

But new tech help fend of modern attacks



Zero Trust



- ▶ The ZTNA market has continued to mature and grow at a rapid pace of **60%** YoY 2019-2025.

IT/OT convergence



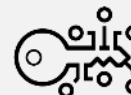
- ▶ "By 2025, **70%** of asset-intensive organizations will have converged their security functions across both enterprise and operational environments."

Invisible Security



- ▶ "Cybersecurity teams need to **cloak all assets** by providing no public IP addresses or open ports willing to accept connections. "

White Box Cryptography



- ▶ "Cryptographic key discovery is one of today's most prevalent threats in industrial networks. White box cryptography is an important aspect to the strategy of the cryptographic key protection"

Firewalls too are vulnerable and need to be protected

Hackers Exploited Zero-Day RCE Vulnerability in Sophos Firewall – Patch Released

Sep 24, 2022 Ravie Lakshmanan

Security software company Sophos has released a patch update for its firewall product after it was discovered that attackers were exploiting a new critical zero-day vulnerability to attack its customers' network.

Zero-day vulnerability found in Palo Alto VPN

Steve Zurier November 11, 2021

Researchers on Wednesday discovered a zero-day buffer overflow vulnerability that causes an unauthenticated remote code execution on Palo Alto Networks (PAN) firewalls using the vendor's GlobalProtect Portal VPN.

SonicWall warns customers to patch 3 zero-days exploited in the wild

By Sergiu Gatlan

April 20, 2021 02:23 PM 0

Security hardware manufacturer SonicWall is urging customers to patch a set of three zero-day vulnerabilities affecting both its on-premises and hosted Email Security products.

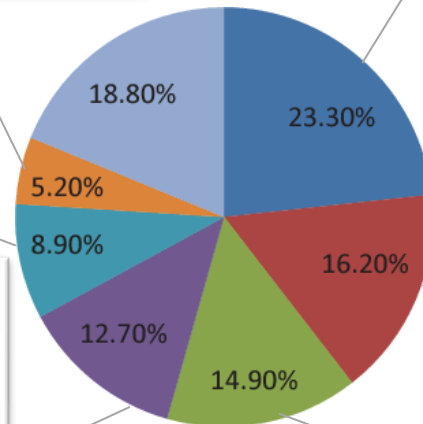
"In at least one known case, these vulnerabilities have been observed to be exploited 'in the wild,'" SonicWall said in a security advisory published earlier today.

- Palo Alto
- Fortinet
- Checkpoint
- Juniper Networks
- Dell
- Sophos
- Others

Multiple Vulnerabilities in Juniper Products Could Allow for Remote Code Execution

July 23, 2020 Security Advisory

Multiple vulnerabilities have been discovered in Juniper products, the most severe of which could allow for remote code execution. Juniper is a vendor for IT, networking and cybersecurity solutions. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.



home Virus & Threats



Fortinet Admits Many Devices Still Unprotected Against Exploited Vulnerability

By Eduard Kovacs on October 17, 2022

[Share](#) [Tweet](#) [Recommend 0](#) [RSS](#)

Fortinet is concerned that many of its customers' devices are still unprotected against attacks exploiting the recently disclosed zero-day vulnerability and the company has urged them to take action.

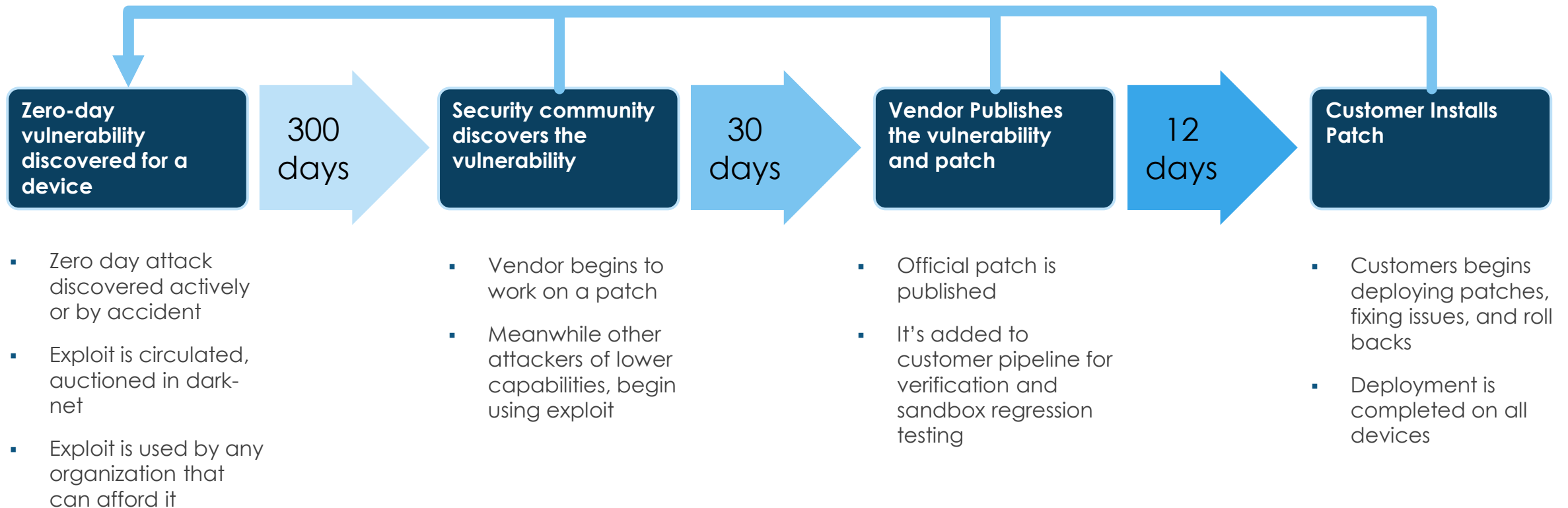
CodeGreen Discovers Check Point SSL VPN Zero Day Vulnerability (CVE-2021-30358)

Friday, October 22, 2021

In Check Point SSL VPN, when environment variables are used in configuration before build 800007042, 'Mobile Access Portal Agent' arbitrary applications from a specially crafted location instead of the predefined Native Application. 'Mobile Access Portal Agent' runs predefined Native Applications. If an administrator configured such an application with environment variables in the path, Portal Agent may run an arbitrary

Firewalls could be leaving our networks vulnerable

Additional vulnerability found by a different vendor



Throughout the whole cycle the network is exposed*

* Depending of firewall vendor mix, the network could be exposed continuously

Regulations and Cyber risks drive OT Security Adoption and Zero Trust Network Access

Vulnerabilities are becoming more complex

- ❑ Multiple OEMs
- ❑ **A range of vulnerabilities**, from hard-coded credentials to nonexistent or weak passwords
- ❑ **A range of exploitation options**, from remote code execution to file/firmware/configuration manipulation
- ❑ Systems impacted including safety-instrumented systems that are designed to protect **human life**

Current Security Tools are insufficient

- ❑ Careful planning that needs to take place so as not to introduce more **risk to production uptime in operations**.
- ❑ OEMs that play a key role in the operational phase of the life cycle of their products and have the burden to develop, test and roll out patches in **tightly controlled physical process environments**.
- ❑ End users having an even heavier **burden to know where these vulnerabilities are**, and then determine whether patching, isolation, upgrades or a combination of these things make sense to their own custom-made operations.
- ❑ Having to **schedule deployment of patches** and updates to coincide with scheduled downtime of the production process.
- ❑ **Unavailability of patches** to OT systems for out-of-support OS.

Governments respond with new regulations (in addition to existing ones like IEC 62443)

- ❑ The CISA “Shields Up” Campaign in the U.S., and similar efforts in other countries
- ❑ Various directives from the U.S. Transportation Security Administration for pipeline and surface transportation operators:
 - ❑ Enhancing Pipeline Cybersecurity — SD-Pipeline-2021-01B
 - ❑ Enhancing Rail Cybersecurity — SD 1580-21-01
 - ❑ Enhancing Public Transportation and Passenger Railroad Cybersecurity — SD 1582-21-01
 - ❑ Enhancing Surface Transportation Cybersecurity — IC 2021-01 Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing - SD-Pipeline-2021-02B
 - ❑ Pipeline — Table of Implementation Timeframes — Attachment 1 to SD Pipeline- 2021-02B
 - ❑ Information Circular (IC) to Enhance Pipeline Cyber Security (IC Pipeline-2022-02)
- ❑ A new U.S. Cyber Incident Reporting law for operators of critical infrastructure
- ❑ In the European Union, the upcoming NIS2 directive will increase security controls and incident reporting mandates across all EU countries. 4

ES portfolio provides best in-class mitigation of IT¹ and OT² cyber threats



Bit Net Sentry (BNS)

Our flagship six-in-one network security appliance for OT/IT environments



ZTMFW

Zero Trust – Micro-segmentation Firewall for segregating OT devices from one another



Hardware Diode

Pure Hardware Data Diode for unidirectional IT/OT separation

ES Portfolio covers 100% MITRE ATT&CK® for Enterprise/Network

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application ✓	Command and Scripting Interpreter ✓	Modify Authentication Process ✓	Valid Accounts ✓	Impair Defenses ✓	Adversary-in-the-Middle ✓	File and Directory Discovery ✓	Adversary-in-the-Middle ✓	Non-Application Layer Protocol ✓	Automated Exfiltration ✓	Firmware Corruption ✓
Valid Accounts ✓		Pre-OS Boot ✓		Indicator Removal ✓	Brute Force ✓	Network Service Discovery ✓	Data from Configuration Repository ✓	Proxy ✓		System Shutdown/Reboot ✓
		Server Software Component ✓		Modify Authentication Process ✓	Input Capture ✓	Network Sniffing ✓	Data from Local System ✓	Traffic Signaling ✓		
		Traffic Signaling ✓		Modify System Image ✓	Modify Authentication Process ✓	Password Policy Discovery ✓	Input Capture ✓			
		Valid Accounts ✓		Network Boundary Bridging ✓	Network Sniffing ✓	Remote System Discovery ✓				
				Pre-OS Boot ✓		System Information Discovery ✓				
				Traffic Signaling ✓		System Network Configuration Discovery ✓				
				Valid Accounts ✓		System Network Connections Discovery ✓				
				Weaken Encryption ✓						

BNS+ZTMFW cover 100% of MITRE ATT&CK® for Enterprise Network! ✓

ES Portfolio covers 100% MITRE ATT&CK® for ICS

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise ✓	Change Operating Mode ✓	Modify Program ✓	Exploitation for Privilege Escalation ✓	Change Operating Mode ✓	Network Connection Enumeration ✓	Default Credentials ✓	Automated Collection ✓	Commonly Used Port ✓	Activate Firmware Update Mode ✓	Brute Force I/O ✓	Damage to Property ✓
Exploit Public-Facing Application ✓	Command-Line Interface ✓	Module Firmware ✓	Hooking ✓	Exploitation for Evasion ✓	Network Sniffing ✓	Exploitation of Remote Services ✓	Data from Information Repositories ✓	Connection Proxy ✓	Alarm Suppression ✓	Modify Parameter ✓	Denial of Control ✓
Exploitation of Remote Services ✓	Execution through API ✓	Project File Infection ✓		Indicator Removal on Host ✓	Remote System Discovery ✓	Lateral Tool Transfer ✓	Detect Operating Mode ✓	Standard Application Layer Protocol ✓	Block Command Message ✓	Module Firmware ✓	Denial of View ✓
External Remote Services ✓	Graphical User Interface ✓	System Firmware ✓		Masquerading ✓	Remote System Information Discovery ✓	Program Download ✓	I/O Image ✓		Block Reporting Message ✓	Spoof Reporting Message ✓	Loss of Availability ✓
Internet Accessible Device ✓	Hooking ✓	Valid Accounts ✓		Rootkit ✓	Wireless Sniffing ✓	Remote Services ✓	Man in the Middle ✓		Block Serial COM ✓	Unauthorized Command Message ✓	Loss of Control ✓
Remote Services ✓	Modify Controller Tasking ✓			Spoof Reporting Message ✓		Valid Accounts ✓	Monitor Process State ✓		Data Destruction ✓		Loss of Productivity and Revenue ✓
Replication Through Removable Media ✓	Native API ✓						Point & Tag Identification ✓		Denial of Service ✓		Loss of Protection ✓
Rogue Master ✓	Scripting ✓						Program Upload ✓		Device Restart/Shutdown ✓		Loss of Safety ✓
Spearphishing Attachment ✓	User Execution ✓						Screen Capture ✓		Manipulate I/O Image ✓		Loss of View ✓
Supply Chain Compromise ✓							Wireless Sniffing ✓		Modify Alarm Settings ✓		Manipulation of Control ✓
Transient Cyber Asset ✓									Rootkit ✓		Manipulation of View ✓
Wireless Compromise ✓									Service Stop ✓		Theft of Operational Information ✓
								System Firmware ✓			

BNS+ZTMFW cover 100% of MITRE ATT&CK® for ICS! ✓

Bit Net Sentry (BNS) is a six-in-one network security appliance

Industrial Firewall

- ▶ Bidirectional Separation of networks on OSI level 2
- ▶ Zero Trust Microsegmentation
- ▶ Enables secure, convenient access to OT environments



IDS/IPS*

- ▶ AI-enabled anomaly detection
- ▶ Zero Day attack prevention
- ▶ SIEM integration



NG Firewall*

- ▶ Deep Packet inspection
- ▶ Packet adjustment/redirection
- ▶ White/Black list filtering
- ▶ Data / Headers filtering on OSI Level 2
- ▶ Just-In-Time Administrative access



Invisible to attackers 6-in-1 protection



VPN

- ▶ ZTNA Secure Tunneling
- ▶ White Box Cryptography
- ▶ Insider-attacker-proof
- ▶ Quantum-ready
- ▶ Patented/Standard encryption
- ▶ Passwordless

Logical Data Diode

- ▶ Unidirectional Separation of networks on OSI level 2
- ▶ Protocol agnostic (tested on 40+ protocols)
- ▶ Secure remote operation
- ▶ Bidirectional communication compliant with IEC 62443



Tactical/Airborne Firewall

- ▶ Airborne Certification (DO 178, DO 254), SOF
- ▶ MIL-STD 810G, MIL-STD 704, MIL-STD 461
- ▶ Ruggedized for extreme temperatures, vibration, dust, humidity

BNS

Invisible Network Security Appliances enabling ultra-secure Bidirectional Network Separation

Invisible to Cyber Attackers

- No IP or Mac addresses
- No latency
- Just-In-Time administrative access

Bidirectional Separation of networks

- White/Black list filtering
- Deep Packet inspection/control/redirection
- Data / Headers filtering on OSI Level 2
- Zero Trust Microsegmentation
- Secure, convenient access to OT environments

Threat Detection / Prevention

- AI-enabled anomaly, Zero Day detection / prevention
- Insider threat prevention
- Ransomware prevention

Encryption without Keys

- White Box Cryptography
- Passwordless/Credential Theft Prevention

Compliance

- NERC CIP, IEC 62443, NRC 5.71, NIST 800-82r2, CFATS, ISO 19790 levels 1-4, ISO/IEC 15408 EALs 1-7, others

- ✓ Ultra low latency
- ✓ 1Gbit/sec to 100Gbit/sec throughput
- ✓ Ruggedized options (Airborne, Tactical certified)
- ✓ Supports most protocols (incl. proprietary)
- ✓ Quantum ready encryption



Seamless Deployment

Pre-configuration

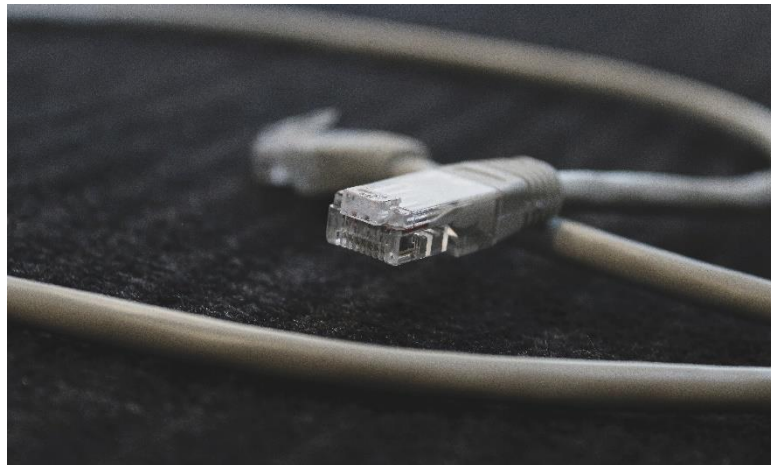
- ▶ Order finalized
- ▶ Customer fills short questionnaire
- ▶ BNS preconfigured
- ▶ BNS shipped



Deployment

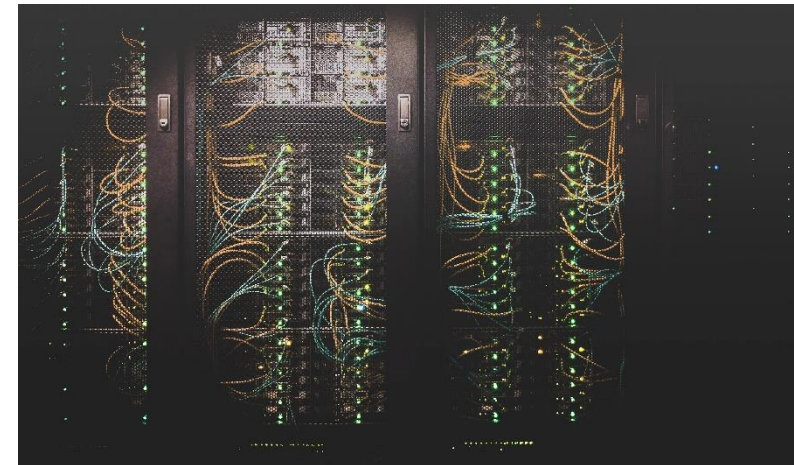


- ▶ BNS Deployed in-line in the network
- ▶ ES Supports remotely or on-site
- ▶ No architecture change or down time required



Operation

- ▶ Network is protected and compliant seamlessly
- ▶ Traffic redirected as needed
- ▶ No maintenance required
- ▶ SLA available



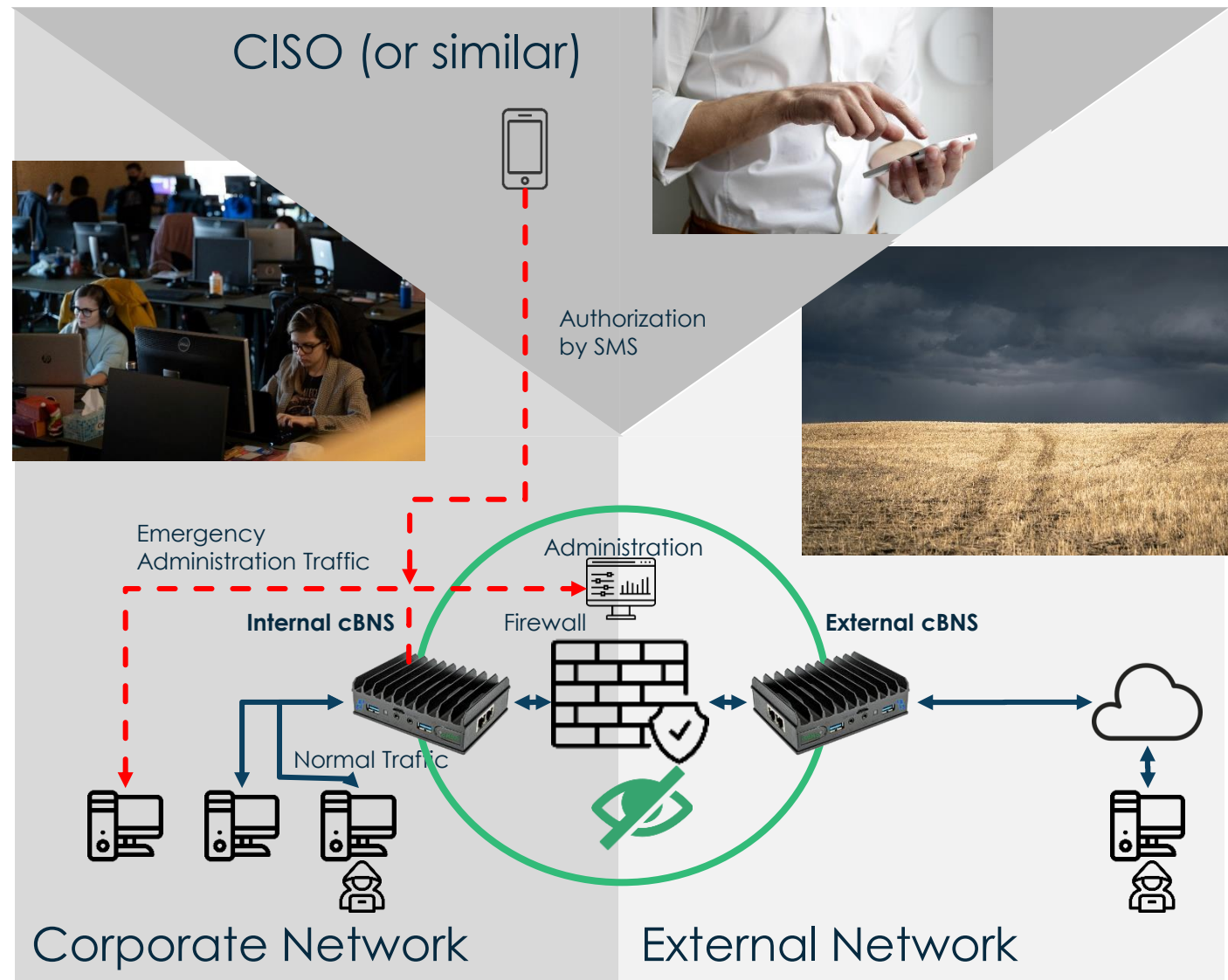
1 a

BNS Use Case for Firewalled Corporate Networks

Defend Corporate network from zero day firewall attacks:

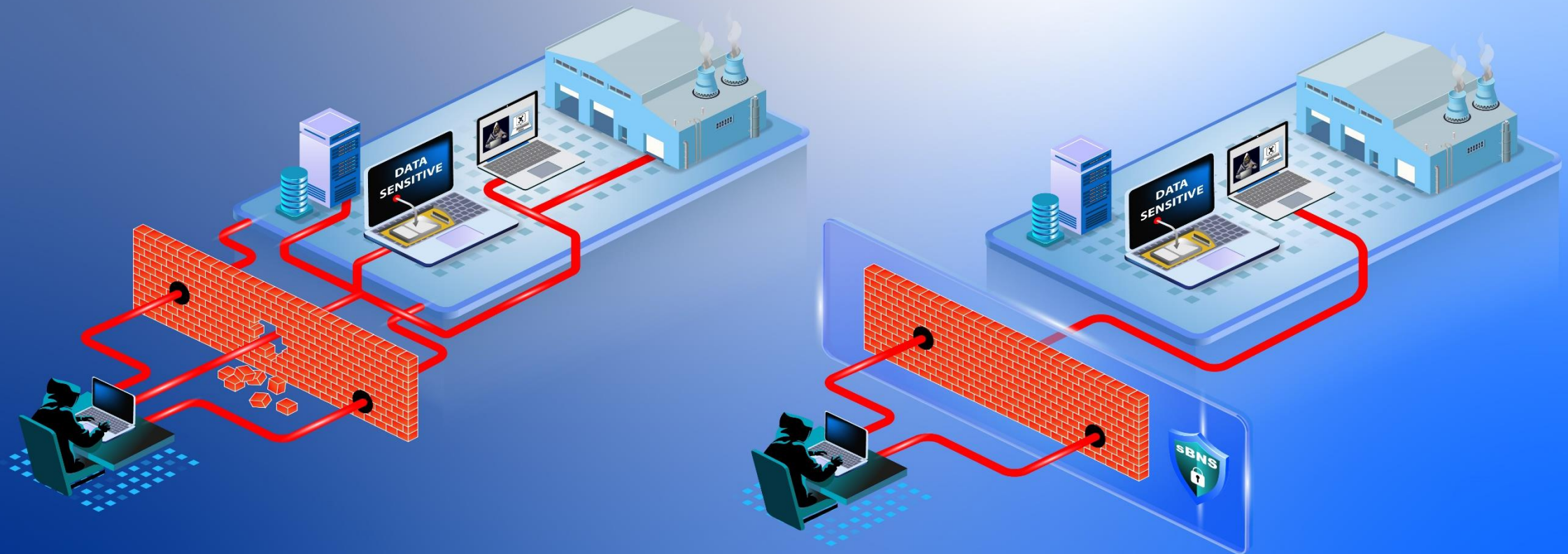
- ▶ Two BNS appliances are located at the inside and outside legs of the firewall.
- ▶ Firewall performs normal filtering work yet is not accessible on any port for anything else incl. administration
- ▶ When Firewall administration is required person in charge enables access:
 - ▶ Using a text message from a designated mobile device
 - ▶ For a short period of time (e.g. 20min)
 - ▶ Only to specific IP/MAC
- ▶ Firewall is completely shielded from both inside and outside attackers

Customer Example:
European Chemical Processing Plant



1 a

BNS Use Case for Firewalled Corporate Networks - cont



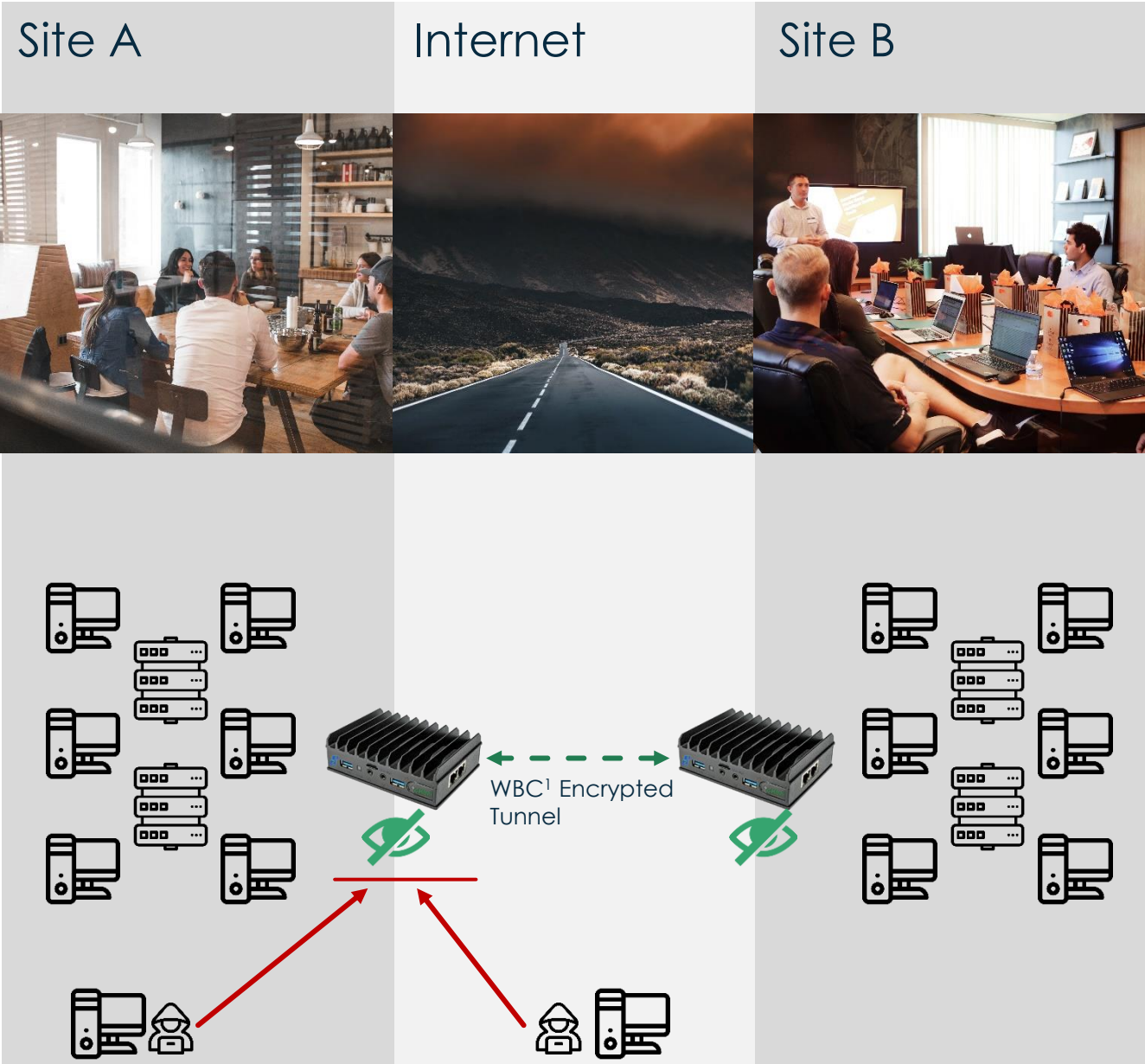
1 b

BNS Use Case for Multi Site Networks

Enable ultra secure zero trust site-to-site tunneling:

- ▶ ZTNA Secure Tunneling
 - ▶ No Passwords / Keys handled by humans
 - ▶ Insider-attacker-proof
 - ▶ Keys automatically update every several seconds
- ▶ BNS itself is invisible so cannot be attacked
- ▶ White Box Cryptography
- ▶ Quantum-ready
- ▶ ES Patented or Standard encryption

Customer Example:
Israeli Government Agency with multiple branches



1: White Box Cryptography – Passwordless, Quantum ready encryption approved by IEC 62443

1c

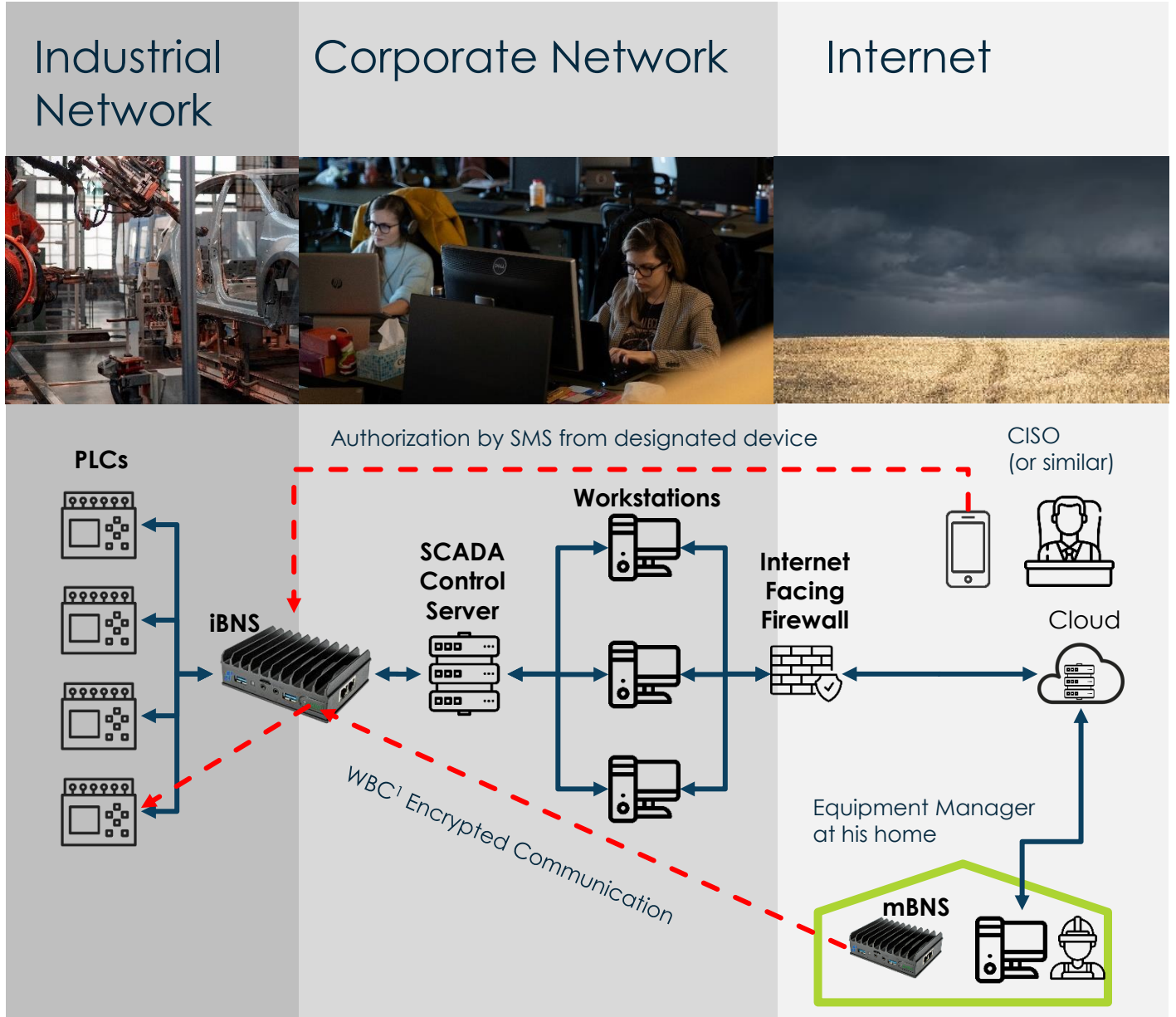
BNS Use Case for ICS Networks

Bidirectional ultra secure, communication compliant with IEC62443

- ▶ SCADA server has secure bidirectional access to managed devices in the ICS network
- ▶ Operation manager controls sensitive ICS equipment from the convenience of his home using a separate mBNS and an approval from CISO. Other rules can be set:
 - ▶ Time of day
 - ▶ Bandwidth
 - ▶ MAC/ IP address
 - ▶ Custom rules
 - ▶ Multi Factor authentication (SMS from a designated device)
- ▶ Honeypot (optional) can collect all requests that didn't go through mBNS-iBNS channel

Customer Example:

Israeli Water Treatment Facility

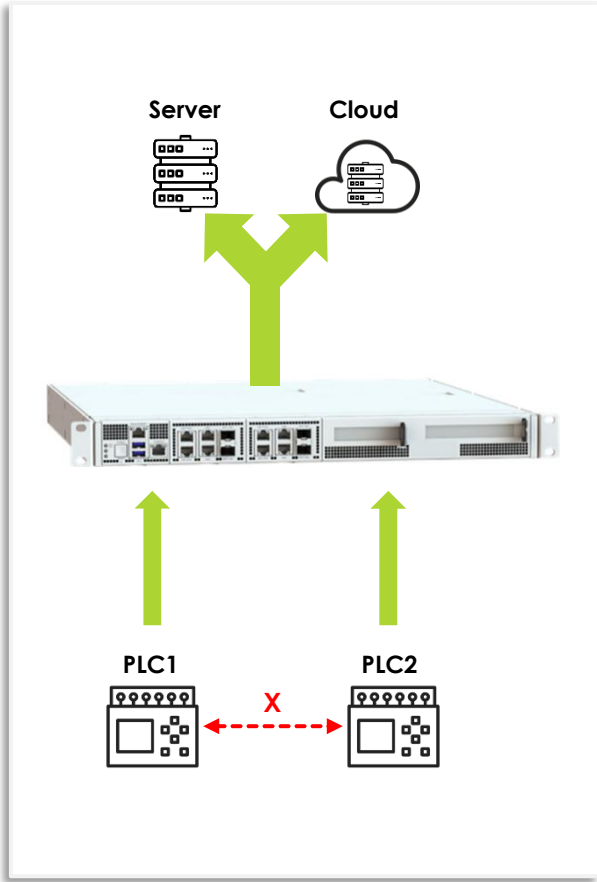


1: White Box Cryptography – Passwordless, Quantum ready encryption approved by IEC 62443

Zero Trust - Microsegmentation Firewall (ZTMFW) 1/2

Zero Trust Microsegmentation	<ul style="list-style-type: none"> Preconfigured to only allow specific devices in the OT environment – lateral movement blocked. Preconfigured to only allow communication with specific server/s on the IT side or cloud Protocol specific control (e.g. Modbus, OPC,PROFINET)
Deep packet inspection	<ul style="list-style-type: none"> Filtration by protocol (including proprietary) Support of 40 ICS Protocols AI-enabled anomaly, Zero Day prevention
Easy to deploy	<ul style="list-style-type: none"> Seamless Integration Military grade Security Intuitive Control
Compliance	<ul style="list-style-type: none"> Enables compliance with NERC CIP, IEC 62443, NRC 5.71, NIST 800-82r2, CFATS, ISO 19790 levels 1-4, ISO/IEC 15408 EALs 1-7, others

- ✓ Ultra low latency
- ✓ 1Gbit ,10Gbit or 40Gbit throughput
- ✓ Ruggedized options (Airborne, Tactical certified)



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

ISO/IEC 15408 EAL 7+

IEC IEC 62443

RTCA

PATENTED

MISSION CRITICAL

CERTIFIED AS9100

COMPLIANT AIRCRAFT MIL-STD-704

COMPLIANT DO-178 DO-254

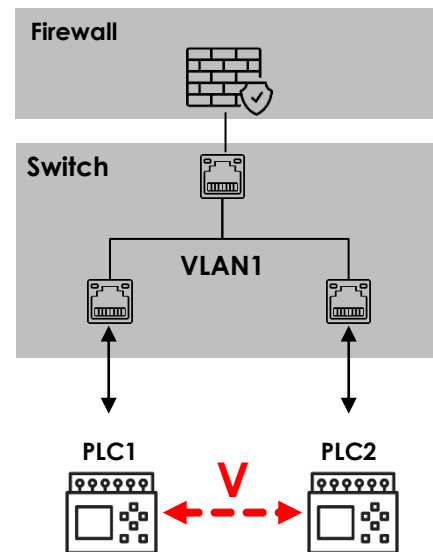
COMPLIANT ELECTROMAGNETIC MIL-STD-461

COMPLIANT ENVIRONMENTAL MIL-STD-810

Zero Trust - Microsegmentation Firewall (ZTMFW) 2/2

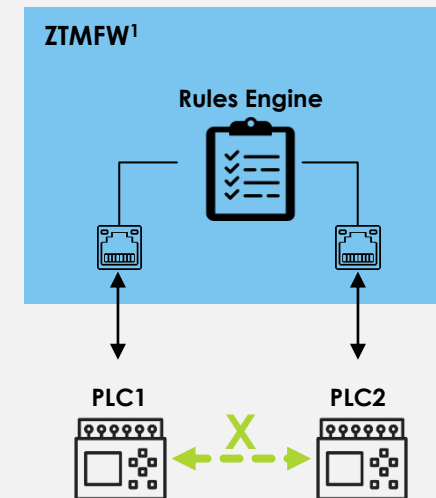
Naïve Architecture

- ❑ **Two** network appliances: Switch and North-South Firewall
- ❑ **No Isolation** between OT devices
- ❑ **VLANs** freely forward network packets to devices that are part of the same broadcast domain.
- ❑ **VLAN Hopping², Double tagging²** attacks are possible
- ❑ **Only packets that need to travel beyond the broadcast domain undergo control**
- ❑ **Insufficient security** for OT environment



Zero Trust Architecture

- ❑ **One** OT firewall for both North-South and East-West communication
- ❑ **No PLC-PLC access**
- ❑ PLCs can only access **specified server** or cloud service
- ❑ **Deep packet inspection** looks for communication anomalies in key protocols
- ❑ Network is zero-trust and **compliant** with key standards (e.g. IEC62443)



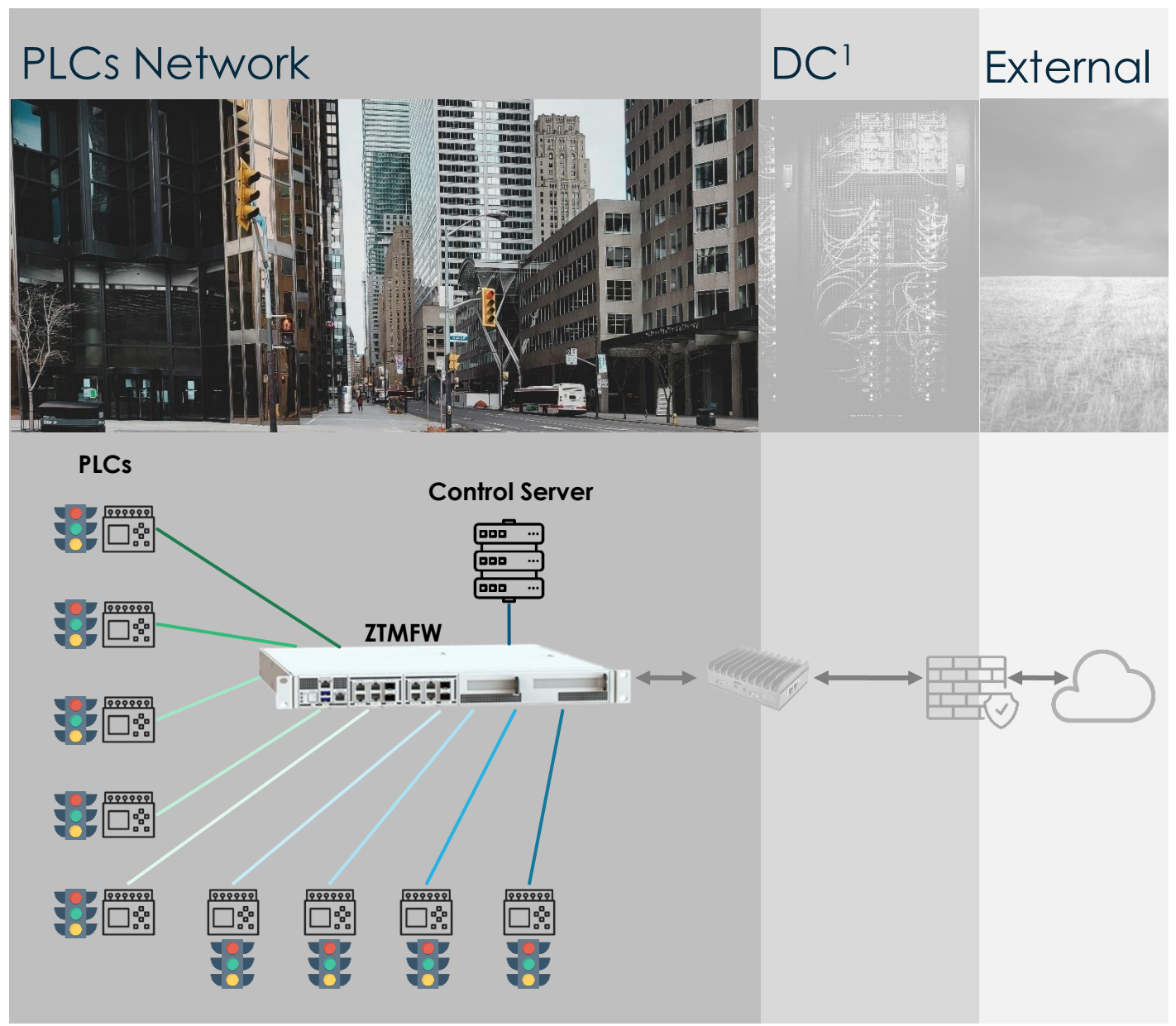
2

ZTMFW Use Case for ICS Networks

For a smart traffic light network a major risk is that adversaries would compromise one traffic light system and access others from it. Customer wanted to make sure there is no way to access other PLCs from a compromised device. Using ZTMFW:

- ▶ Communication to PLCs is isolated
- ▶ Lateral movement blocked
- ▶ Each device can only communicate with the designated server
- ▶ Each request is analyzed for anomalies
- ▶ Protocol specific rules can be enabled

Customer Example:
APAC Smart Traffic Lights Operator



1: Data Center

Pure Hardware Data Diode

Unidirectional Network Separation

- ▶ Unidirectional Separation of networks on OSI level 2
- ▶ Impassable physical barrier through galvanic or electrical separation
- ▶ Hardware only – no possibility of human error
- ▶ Any unidirectional protocols available: UDP support (Syslog, NTP, SNMP traps)

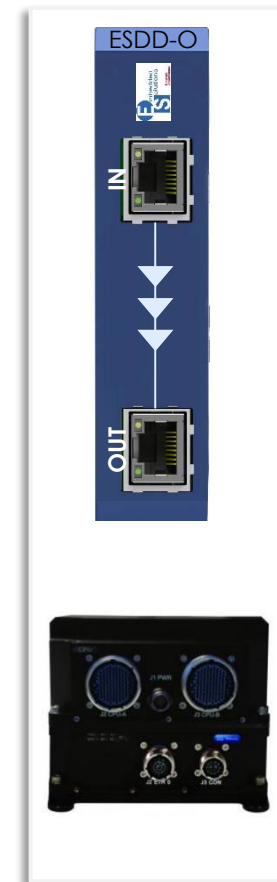
Multiple Uses

- ▶ Media streaming or CCTV monitoring.
- ▶ Data transfer from ICS/SCADA networks to IT networks.
- ▶ File transfer for data storage replication or software updates
- ▶ Secure log collection to administrative or audit network
- ▶ Sensor data transfer from lower classified network to higher classified network

Compliance

- ▶ Enables compliance with NERC CIP, IEC 62443, NRC 5.71, NIST 800-82r2, CFATS, ISO 19790 levels 1-4, ISO/IEC 15408 EALs 1-7, others

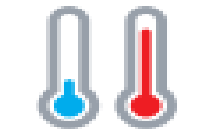
- ✓ Two separate power supplies (to mitigate against side-channel attacks)
- ✓ Ultra low latency
- ✓ High Availability (Optional redundancy)
- ✓ 1Gbit ,10Gbit or 100Gbit throughput
- ✓ Ruggedized options (Airborne, Tactical certified)
- ✓ Fiber optical or Copper interface



ISO/IEC 15408
EAL 7+



RTCA



3

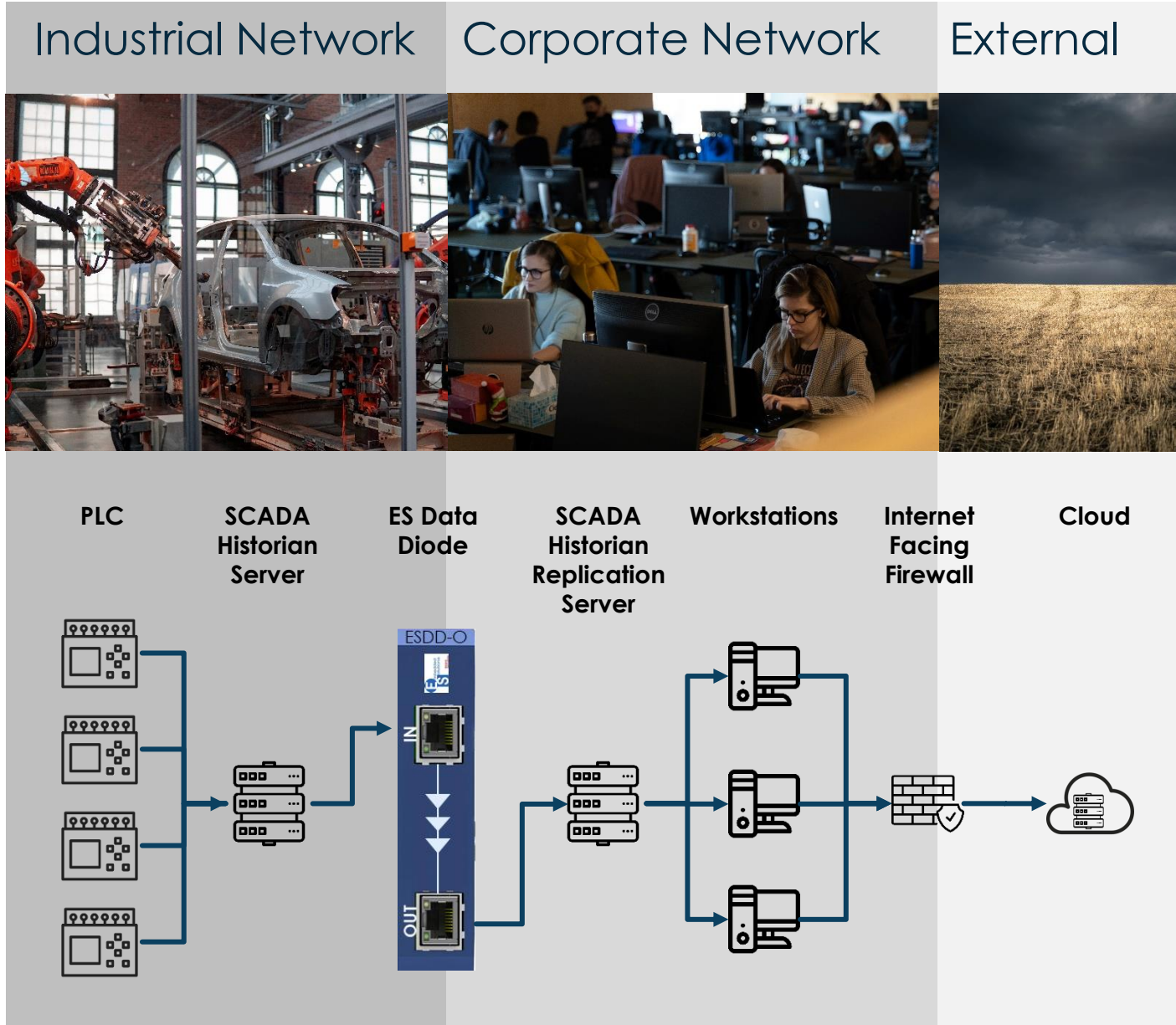
ES Data Diode Use Case

Our customer had powerplant-level cyber security compliance requirements, yet wanted to securely access the OT environment remotely to leverage big data advantages:




- ▶ Scada Historian Server is located in the operational network
- ▶ Historian server collects all telemetry from PLCs
- ▶ The SCADA telemetry data is transported in real time using one-way protocols (e.g. Syslog over UDP) via ES Data Diode to the replication Server
- ▶ Telemetry from safety-critical networks captured in real-time and sent across the globe for monitoring and analysis

Customer Example:

European Chemical Processing Plant



Embedded Solutions 3000 Portfolio Summary

Feature	1		2		3	
	BNS		Microsegmentation Firewall		Data Diode	
White Box Cryptography	✓					
Bi-directional secure communication	✓		✓			
Hardware Enforced Uni-directional communication					✓	
Deep packet inspection including bit-level filtering	✓		✓			
Communication redirection	✓					
Zero Day attack protection	✓					
Microsegmentation (via network)			✓			
Microsegmentation (via endpoint)	✓					
AI-enabled anomaly prevention	✓		✓			
Compliance with key standards ¹	✓		✓		✓	
Invisible to network (no IP, Mac)	✓		✓		✓	
Misconfiguration protected	✓		✓		✓	
Zero-trust approach – insider threat not possible	✓		✓		✓	
Fast deployment (<1H)	✓		✓		✓	



Time for your questions

Thank you

ES White Box Cryptography (WBC) – How it works?

WBC Frame composition:

- ▶ BNS SN#
- ▶ MAC
- ▶ Production Time (date and time of the device firmware packaging)
- ▶ Other Parameters that update the algorithm every frame



Latency Options for frame 800-1500 bytes:

- ❑ ES WBC – 4 Nano Seconds
- ❑ AES 256 (SW) + ES WBC – 1 Micro Second (1000 Nano Seconds)
- ❑ AES 256 (HW) + ES WBC – 4 Nano Seconds



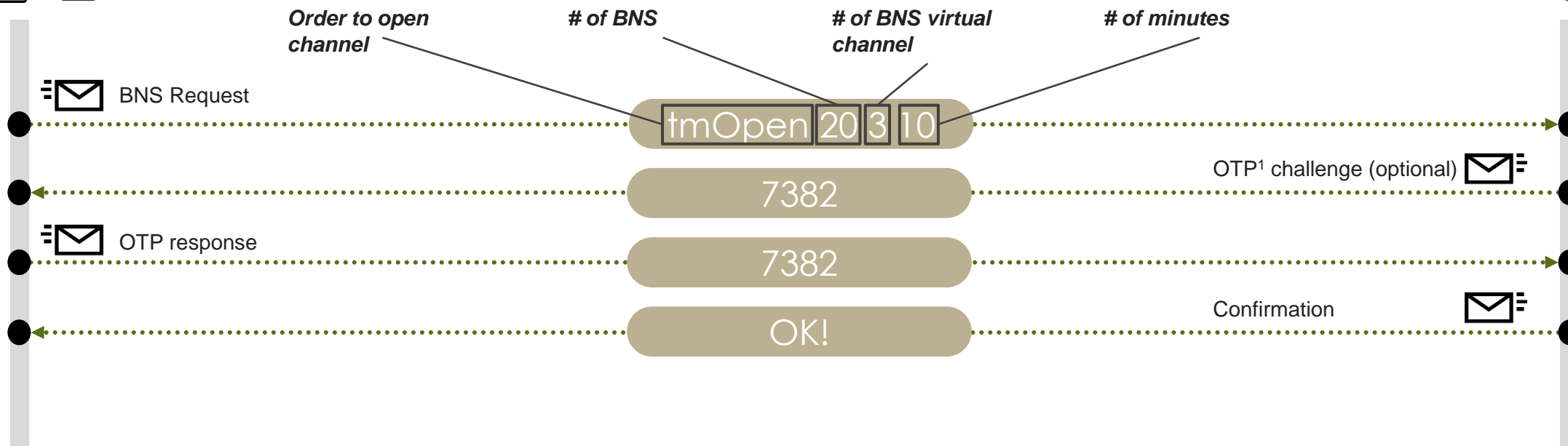
1: Group = A logical list of BNS devices that need to communicate between them. Other BNSs will not be able to communicate with the group

SMS Authorization – How it works?

CISO
(or similar)



Target BNS



Making the existing firewall invisible to attackers

As is – Firewall is accessible to adversaries



Risks:

- ❑ Firewall is vulnerable to **zero day attacks**
- ❑ Firewall could be **misconfigured**:
 - ▶ Exposed **admin** interfaces
 - ▶ **Default passwords**
 - ▶ Not **patched**

With BNS deployed – Firewall is invisible to attackers



Pros:

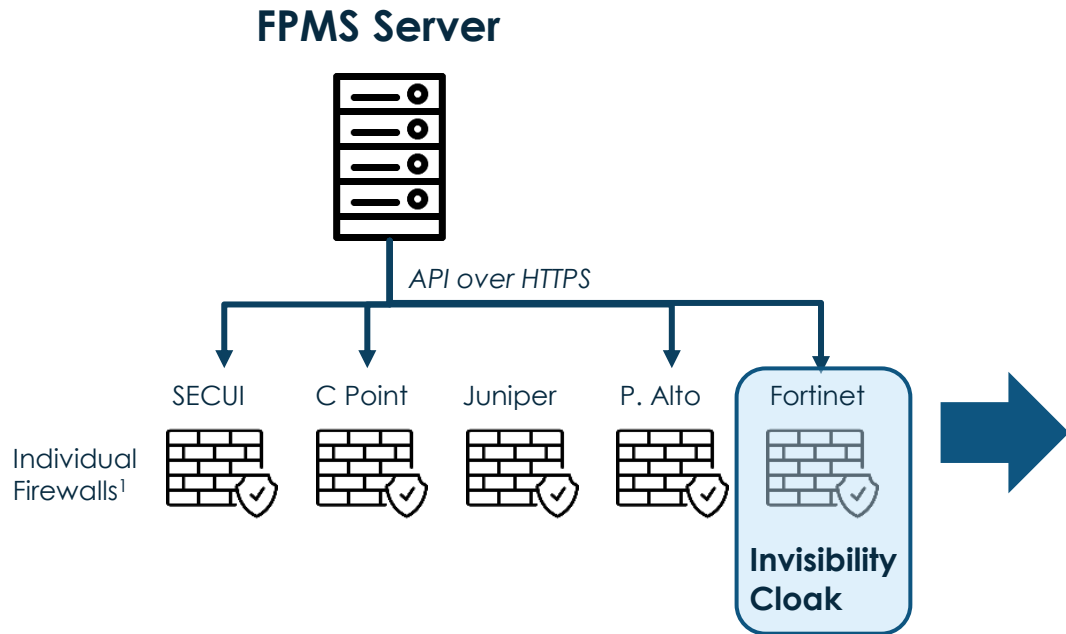
- ❑ Firewall is now **invisible** inside and out while **operating normally**
- ❑ Zero day attacks, and other vulnerabilities **risks** all but **eliminated**

Cons:

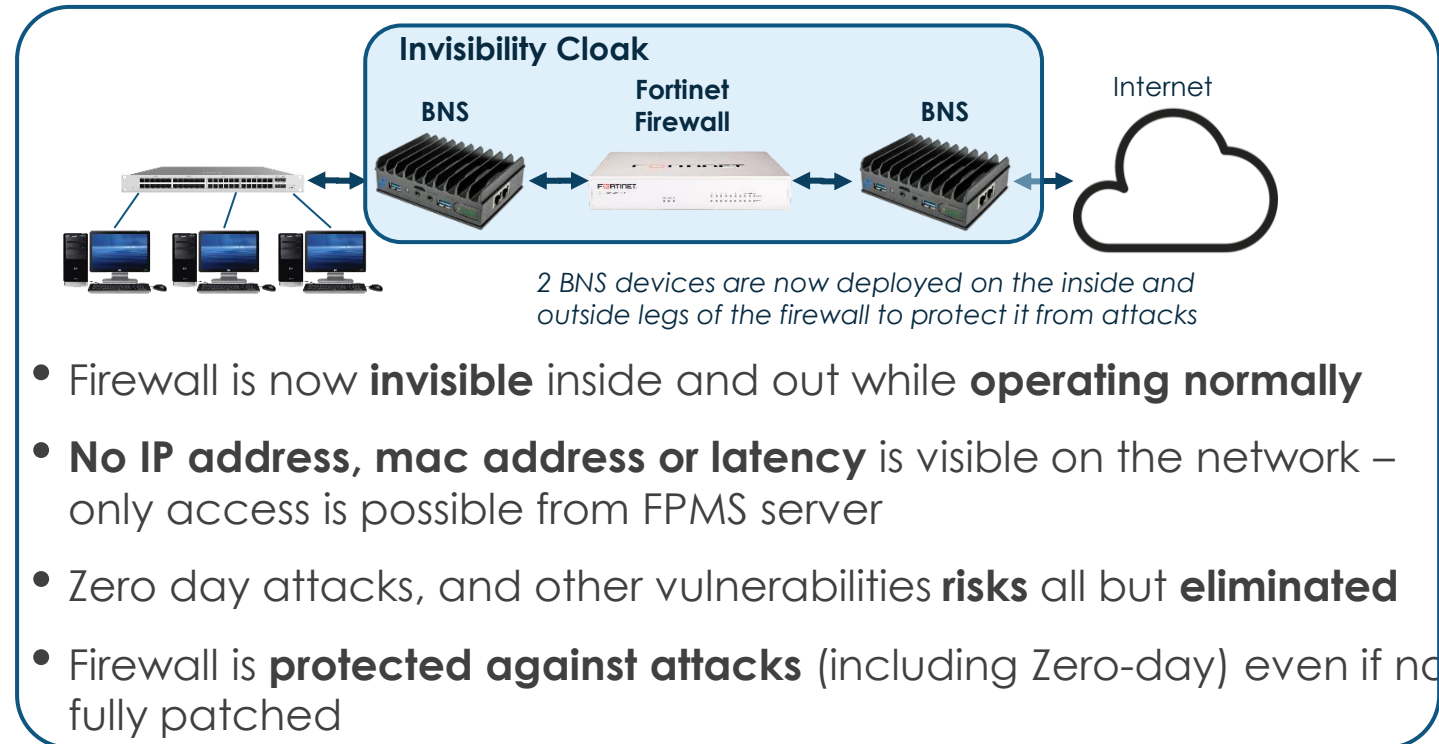
- ❑ Changing firewall rules would require an additional authentication step using SMS to BNS

(Optional) Protect individual firewall from zero-day attacks

FPMS automates firewall management



Using BNS, an individual firewall is hidden from attackers



Key firewalls in the organization can get additional protection and become **invisible to anyone** inside and outside of the network **except the FPMS Server**

Key Network Cyber Security Risks For a Polar Research Ship

Risk		Impact	Suggested Mitigation
Remote access	Ships can be remotely accessed and controlled by attackers, potentially compromising navigation and control systems	<p>Since the ship will often be at unforgiving, extreme polar environment, the impact could be severe:</p> <ul style="list-style-type: none"> • Loss of life/Injury • Damage to vessel or research equipment • Damage to vessel • Financial loss • Loss of scientific data • Loss of scientific artifacts • Environmental harm 	<ul style="list-style-type: none"> • Protect the firewall from zero day attacks • Monitor network anomalies on board and external inbound and outbound communication • Ensure IT/OT separation by using deep packet inspection, only allowing particular protocols with set limitations • Microsegment Shipboard Control, Instrument, dedicated connector networks by using deep packet inspection, allowing only known protocols for specific values • Encrypt all the traffic with other vessels, autonomous equipment without the use of passwords • Enable Quality of Service, ensuring that critical communication is prioritized when bandwidth is limited
Network congestion	Network congestion can lead to delays in communication and control, potentially causing safety issues		
Interference	Ships' communications can be jammed or interfered with, disrupting navigation and control systems		
Man-in-the-middle	Attackers can intercept and manipulate communications between ships and other vessels or shore-based systems, potentially compromising navigation and control systems		
Unauthorized connections	Unauthorized devices and connections can be used to gain access to ship networks, potentially compromising navigation and control systems		
Lack of encryption	Without proper encryption or in case of compromised keys, communications can be intercepted and compromised		
Lack of network segmentation	Lack of proper network segmentation can allow an attacker or a worm to move laterally and compromise other systems once they have access to one		
Dependence on third-party providers	Ship operators rely on multiple third-party providers, having weak cyber security measures in one of them can compromise overall security of the vessel		
Outdated protocol or equipment	Use of outdated network protocol or equipment can be vulnerable to known exploits and attacks		

Key Network Cyber Security Risks For Ships

Risk		Impact	Suggested Mitigation
Remote access	Ships can be remotely accessed and controlled by attackers, potentially compromising navigation and control systems	<p>Since ships are often be in unforgiving, extreme weather environments, the impact could be severe:</p> <ul style="list-style-type: none"> • Loss of life/Injury • Damage to vessel or research equipment • Damage to vessel • Financial loss • Loss of scientific data • Loss of scientific artifacts • Environmental harm 	<ul style="list-style-type: none"> • Protect the firewall from zero day attacks • Monitor network anomalies on board and external inbound and outbound communication • Ensure IT/OT separation by using deep packet inspection, only allowing particular protocols with set limitations • Microsegment Shipboard Control, Instrument, dedicated connector networks by using deep packet inspection, allowing only known protocols for specific values • Encrypt all the traffic with other vessels, autonomous equipment without the use of passwords • Enable Quality of Service, ensuring that critical communication is prioritized when bandwidth is limited
Network congestion	Network congestion can lead to delays in communication and control, potentially causing safety issues		
Interference	Ships' communications can be jammed or interfered with, disrupting navigation and control systems		
Man-in-the-middle	Attackers can intercept and manipulate communications between ships and other vessels or shore-based systems, potentially compromising navigation and control systems		
Unauthorized connections	Unauthorized devices and connections can be used to gain access to ship networks, potentially compromising navigation and control systems		
Lack of encryption	Without proper encryption or in case of compromised keys, communications can be intercepted and compromised		
Lack of network segmentation	Lack of proper network segmentation can allow an attacker or a worm to move laterally and compromise other systems once they have access to one		
Dependence on third-party providers	Ship operators rely on multiple third-party providers, having weak cyber security measures in one of them can compromise overall security of the vessel		
Outdated protocol or equipment	Use of outdated network protocol or equipment can be vulnerable to known exploits and attacks		

Network security adoption is driven by maritime regulations and high profile security incidents

Maritime regulations become more robust

BIMCO and MSC.428 (98):

- **Secure network architecture** - Ensure the confidentiality, integrity, and availability of information and communication systems.
- **Access control measures** - Restrict access to sensitive information and systems to authorized personnel only.
- **Firewalls and intrusion detection/prevention systems** - Prevent unauthorized access to networks and detect cyber threats in real-time.
- **Encryption of sensitive information** - Protect information while it is transmitted over networks and ensure privacy.
- **Secure remote access solutions** - Allow authorized personnel to access information and systems from remote locations.
- **Network segmentation** - Minimize the risk of cyberattacks and isolate critical systems from less secure systems.

High Profile Maritime Security incidents emphasize risk

Recent attack examples:

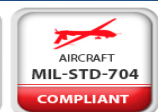
- **Malware / Ransomware attacks** - Encryption of data and ransom demands, such as the Ransomware attack on 1000 DMV Ships using malware in ShipManager software in January 2023.
- **Phishing attacks** - Unauthorized access to information via tricking employees, such as the attack on Hapag-Lloyd in March 2022.
- **Data breaches** - Theft of sensitive information due to insufficient security measures, such as the attack on SPO in November 2021.
- **Network intrusion** - Unauthorized access to networks and disruption of operations, such as the attack on the Port of San Diego in 2018.

BNS Use Case for Coast Guard

- ▶ Rugged BNS (**rBNS**) is deployed to **each vessel, aircraft** – can handle 80 virtual channels and is connected to existing communication equipment (e.g. VHF, LTE, 5G, Satellite, etc)
- ▶ **cBNS** is deployed **on land installation** – can handle 320 virtual channels
- ▶ BNSs can be put into **logical groups** so they are only able to communicate within the group. Further separation can be enabled within each group.
- ▶ All communication is **encrypted** with **AES 256** (or other, standard encryption) and **White Box Cryptography** with encryption algorithm and key changing every frame for each virtual channel
- ▶ In case of a device compromise, e.g. vessel falls into enemy hands, rBNS can activate **emergency erase** of its configuration as well as be **removed from the group**, and no longer have access to network communication
- ▶ BNS can manage **bandwidth allowance** policies and **priorities** for different kinds of traffic (virtual channels) for optimal work in both high bandwidth and low bandwidth situations
- ▶ Optimized for work in **high** bandwidth, **low** bandwidth and **varied/intermittent** bandwidth environments

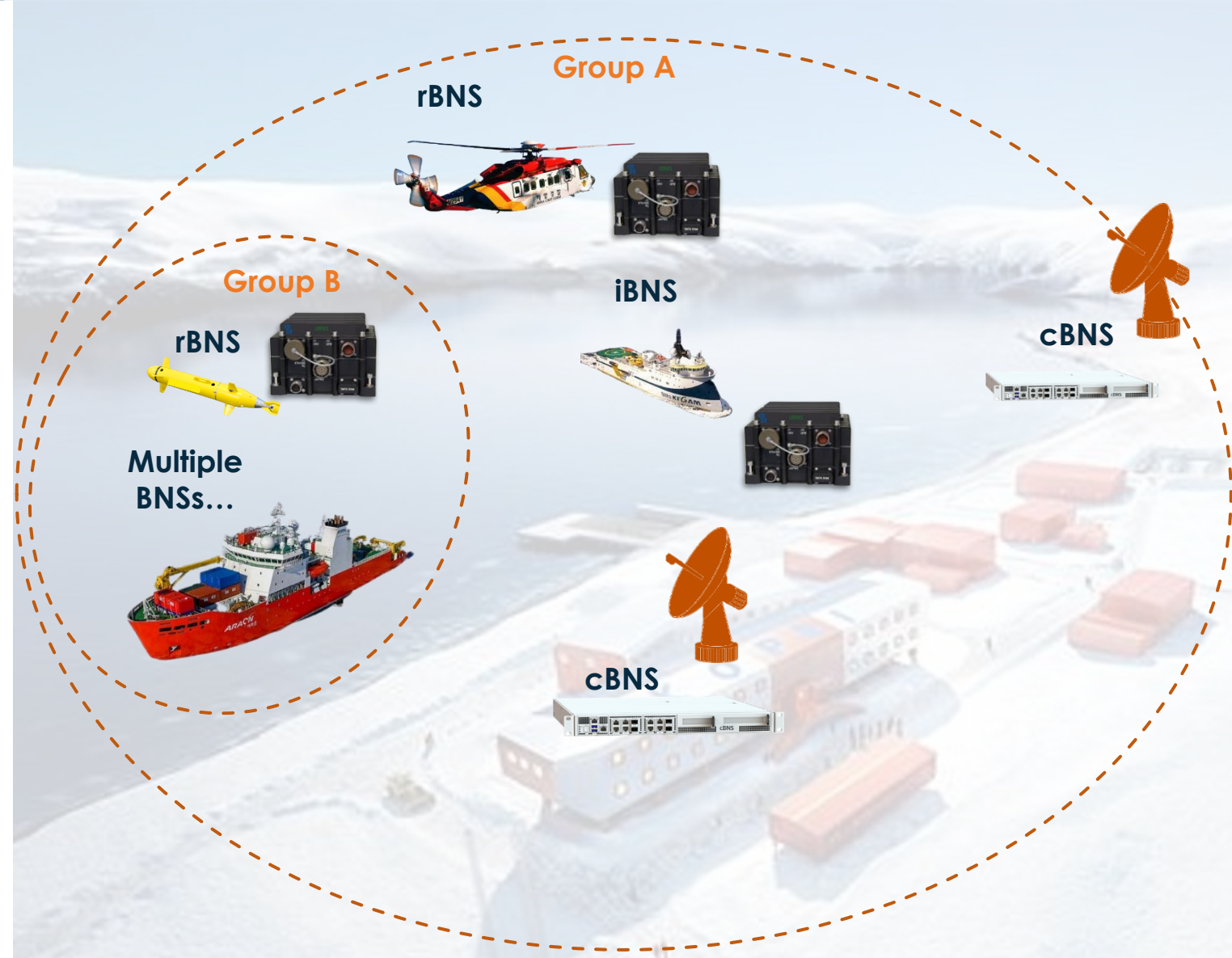


Enable secure communication for maritime communication

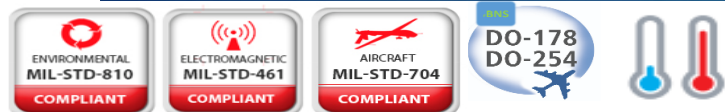


BNS around the ship

- ▶ Rugged BNS (**rBNS**) is deployed to **each vessel**, aircraft – can handle up to 80 virtual channels and is connected to existing communication equipment (e.g. VHF, LTE, 5G, Satellite, etc)
- ▶ **cBNS** is deployed **on land installation** – can handle 480 virtual channels
- ▶ BNSs can be put into **logical groups** so they are only able communicate within the group. Further separation can be enabled within each group.
- ▶ All communication is **encrypted** with **AES 256** (or other, standard encryption) and **White Box Cryptography** with encryption algorithm and key changing every frame for each virtual channel
- ▶ In case of a device compromise, rBNS can activate **emergency erase** of its configuration as well as be **removed from the group**, and no longer have access to network communication
- ▶ BNS can manage **bandwidth allowance** policies and **priorities** for different kinds of traffic (virtual channels) for optimal work in both high bandwidth and low bandwidth situations
- ▶ Optimized for work in **high** bandwidth, **low** bandwidth and **varied/intermittent** bandwidth environments

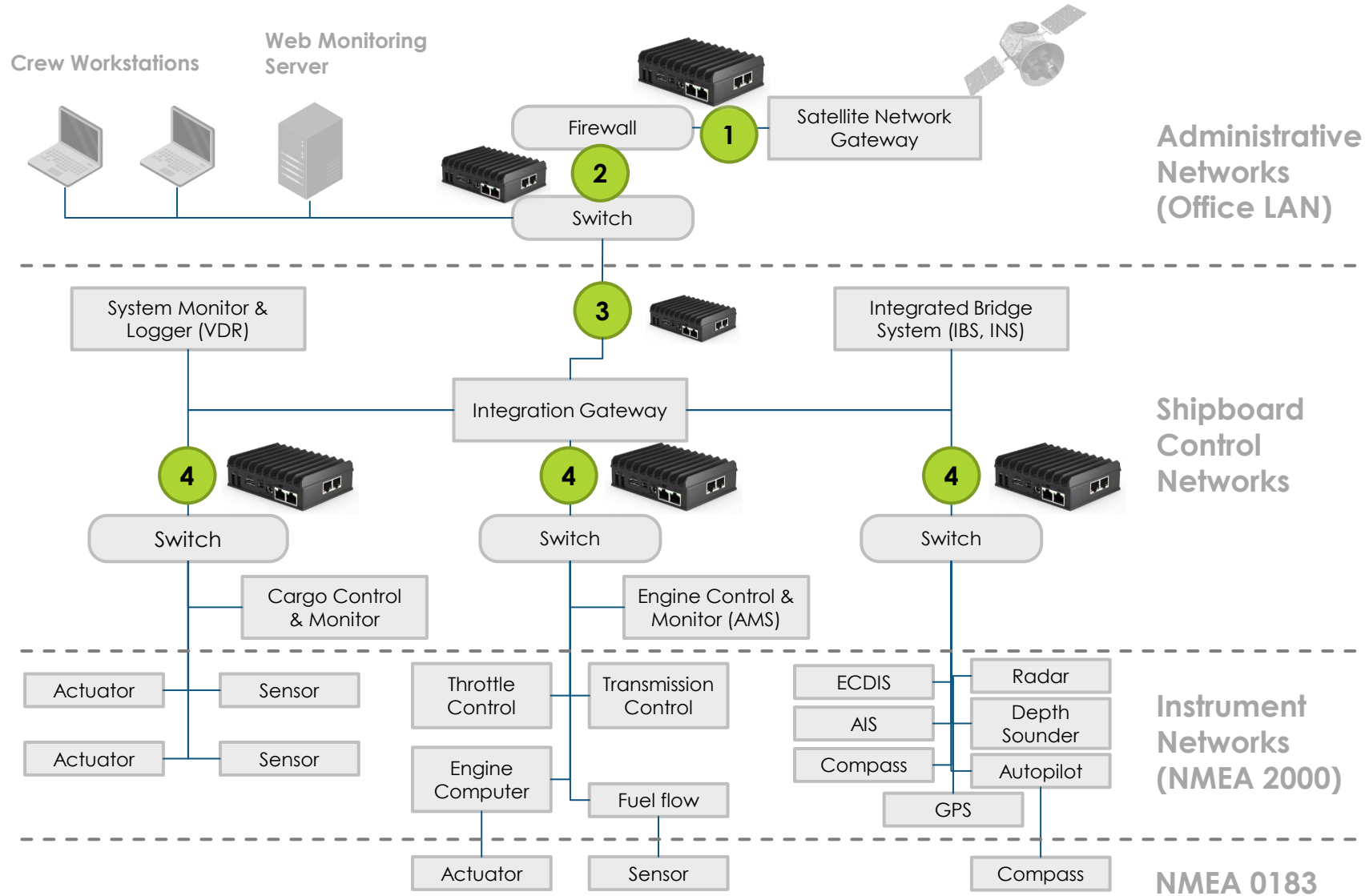


Protect the communication of the ship with external parties



Protect network on board

BNS application on the vessel



Purpose

- 1**

 - ▶ Make firewall invisible from outside
 - ▶ Bandwidth Control
 - ▶ Prioritization according type of traffic
 - ▶ QoS Control – Enable stable communication with AUV, others
 - ▶ Establish secure tunnels using WBC+AES 256 with AUV (e.g. Other ships, AUV)
- 2**

 - ▶ Make firewall invisible from inside
 - ▶ Regular FW Administration only from specific MAC addresses
- 3**

 - ▶ Separate IT/OT networks
 - ▶ Lock to allow only protocols, patterns needed to communicate with the integration gateway
 - ▶ AI anomaly detection
- 4**

 - ▶ Separate Admin network from Shipboard Control network
 - ▶ Lock to allow only particular protocols, patterns
 - ▶ AI anomaly detection
 - ▶ Microsegmentation

1 d

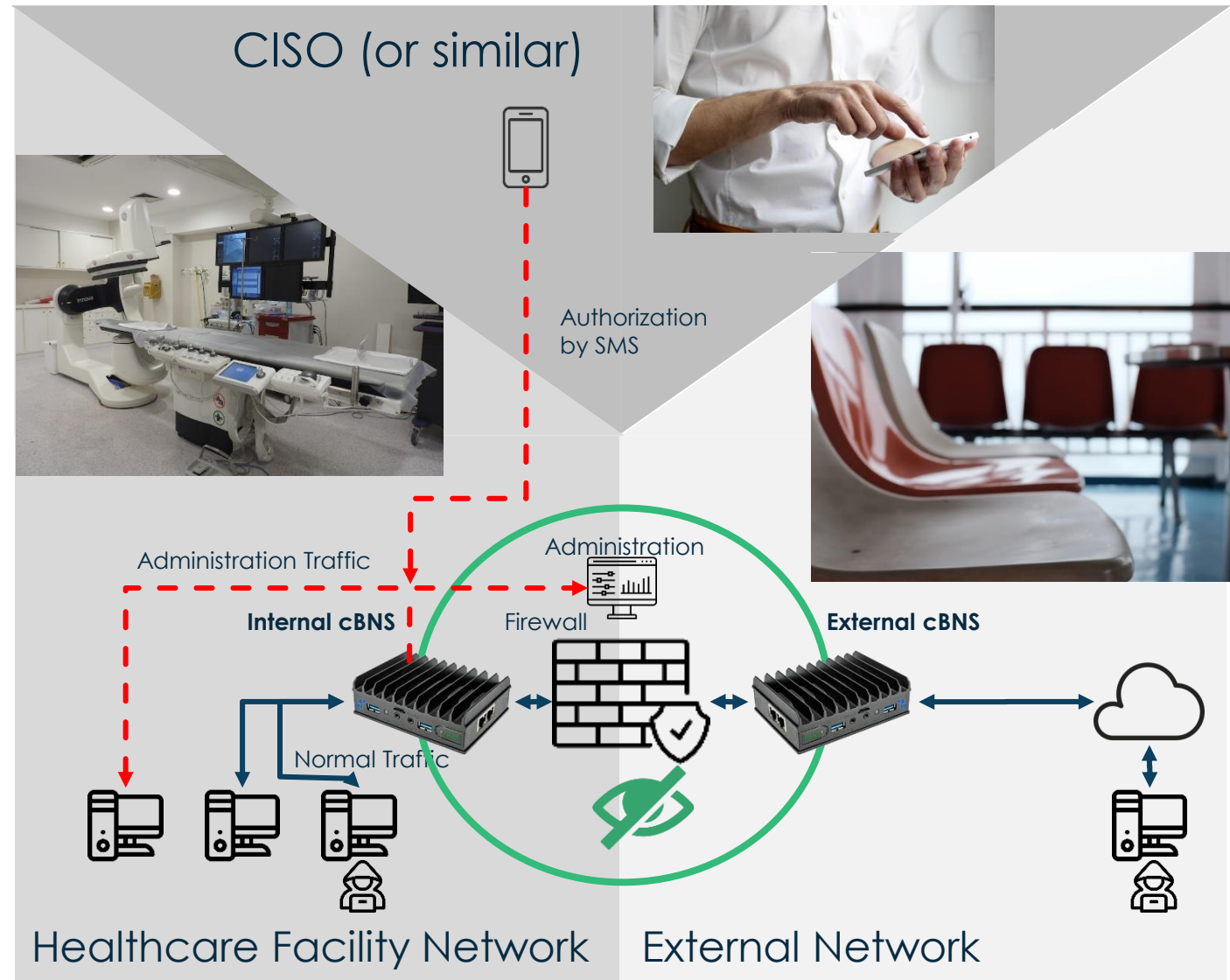
BNS Use Case for Firewalled HealthCare Facility Networks

Defend Healthcare Facility network from **ransomware** and **zero day** firewall attacks:

- ▶ Two BNS appliances are located at the inside and outside legs of the firewall.
- ▶ Firewall performs normal filtering work yet is not accessible on any port for anything else incl. administration
- ▶ When Firewall administration is required Hospital CISO enables access:
 - ▶ Using a text message from a designated mobile device
 - ▶ For a short period of time (e.g. 20min)
 - ▶ Only to specific IP/MAC
- ▶ Firewall is completely shielded from both inside and outside attackers

43%¹ of healthcare organizations experienced ransomware attacks in the last 24 months

Each data breach total cost: \$1M - \$13M¹



1: Source: Cynerio – Insecurity of Connected Devices in Healthcare 2022

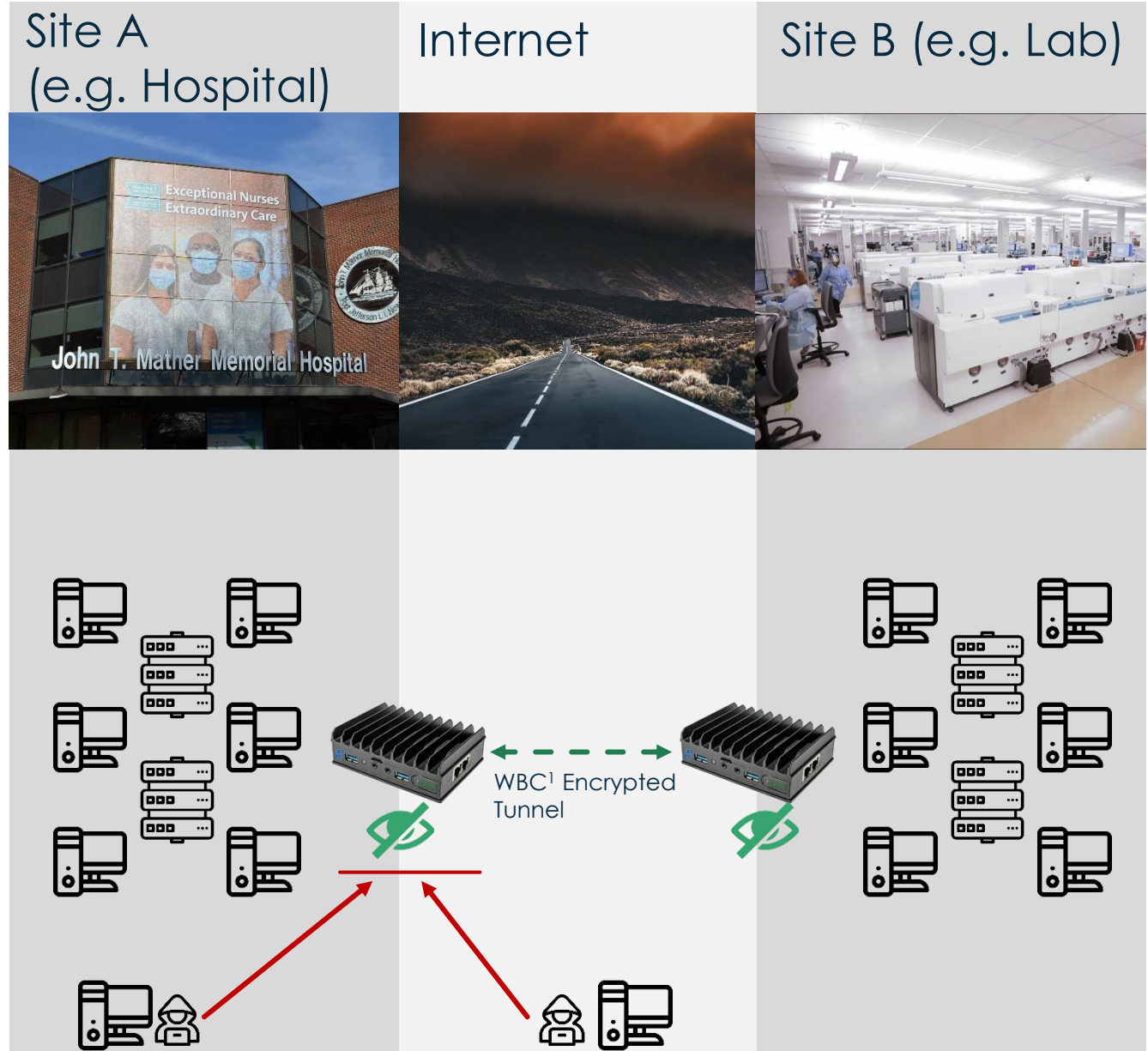
1 e

BNS Use Case for Multi Site Networks

Enable ultra secure zero trust site-to-site tunneling:

- ▶ ZTNA Secure Tunneling
 - ▶ No Passwords / Keys handled by humans
 - ▶ Insider/Visitor-attacker-proof
 - ▶ Keys automatically update every several seconds
- ▶ BNS itself is invisible so cannot be attacked
- ▶ White Box Cryptography
- ▶ Quantum-ready
- ▶ ES Patented or Standard encryption

43%² experienced data breach of PHI
54%² of these experienced increased mortality rate



2 b

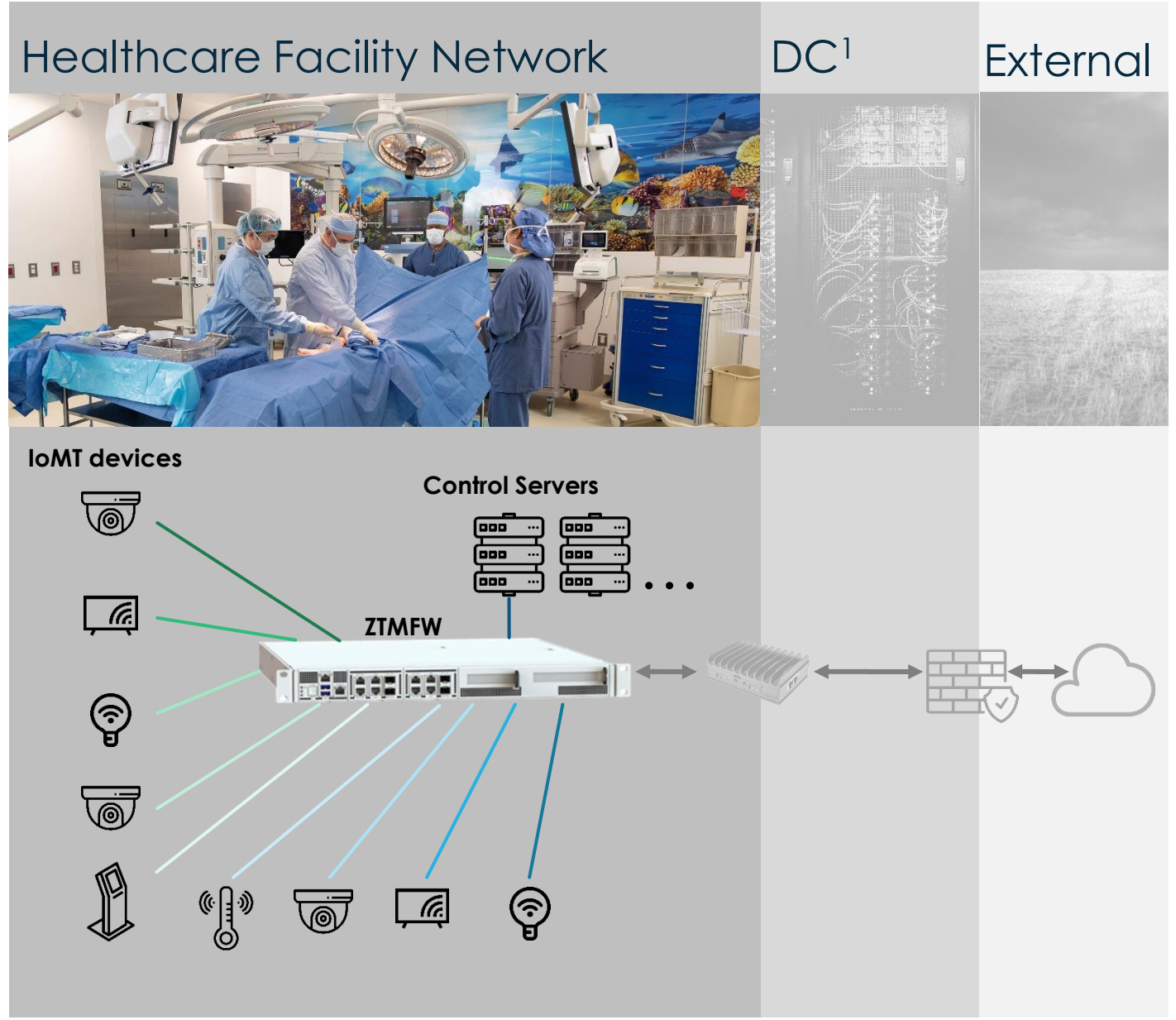
ZTMFW Use Case for Hospital Networks

For a connected Hospital network a major risk is that adversaries would **compromise IoMT device and access other devices from it**. Healthcare facilities CISOs want to make sure there is no way to access other IoMT devices from a compromised device.

Using ZTMFW:

- ▶ Communication to IoMT devices is **isolated**
- ▶ **Lateral** movement blocked
- ▶ Each device can **only** communicate with the **designated server**
- ▶ Each request is analyzed for **anomalies**
- ▶ **Protocol** specific **rules** can be enabled

56%² had at least one IoMT cyber attack in 24m
45%² of IoT/IoMT attacks resulted in adverse impact on patient care







1: Data Center; 2: Source: Cynerio – Insecurity of Connected Devices in Healthcare 2022

Comparison with a typical NGFW

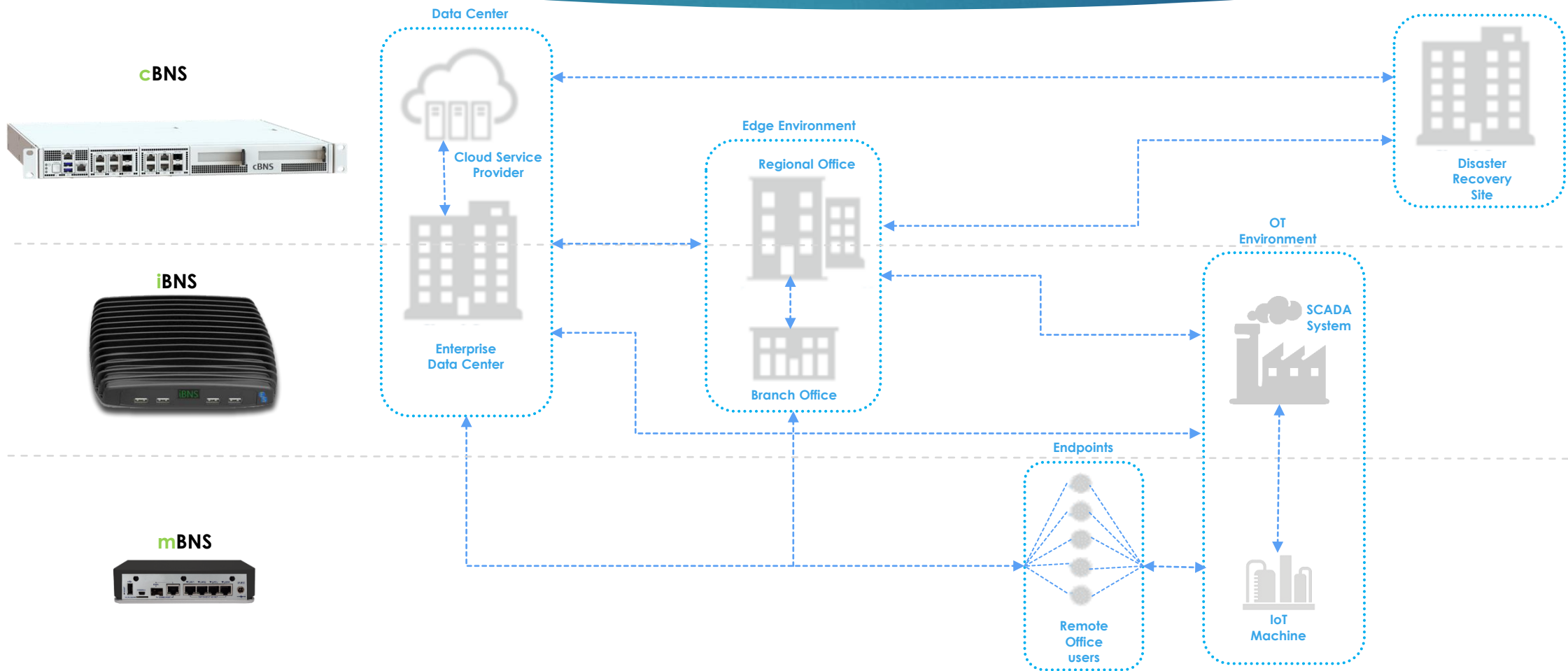
	ES iBNS	FGR 70F¹
Invisible to outside attackers	V	X
Invisible to inside attackers	V	X
Passwordless Encryption	V	X
Quantum Ready, WBC Encryption	V	X
Encryption Latency	4nano seconds	unspecified, likely X100 higher
Encrypted with Rules Throughput	up to 100Gbit	up to 580Mb/s
Packet adjustment/ redirection	V	X
Layer 2 AI IDS/IPS	V	X
Airborne Ready	DO-178, DO-254	X
MIL Standard	MIL-STD 810G, MIL-STD 704, MIL-STD 461	X
Compliance	IEC 62443, ISO/IEC 15408 EALs 1-7, others	X

ES portfolio needs by industry

	IT Network Security			OT Network Security		rBNS 	BNS 	ZTMFW 	Dada Diode 
	Firewall zero day protection	Multi branch tunneling	Multi level security subnet Separation	IT/OT separation	OT-OT Micro-segmentation				
Government (incl. City)	High	High	High	High	High		High	High	High
Defense	High	High	High	High	High	High	High	High	High
Energy ¹	High	High	High	High	High		High	High	High
Oil & Gas ²	High	High	High	High	High		High	High	High
Water Utilities	High	High	High	High	High		High	High	High
Critical Facilities (other)	High	High	High	High	High		High	High	High
Manufacturing (incl. Auto)	High	High	High	High	High		High	High	High
Transportation	High	High	High	High	High	High	High	High	High
Healthcare	High	High	High	Mid	Mid		High	Mid	Low
Telecom	High	High	High	Mid	Mid		High	Mid	Low
Retail	High	High	High	Mid	Mid		High	Mid	Low
IT	High	High	High	Low	Low		High	Low	Low
Education	High	High	High	Low	Low		High	Low	Low
Financial Services	High	High	High	Mid	Mid		High	Low	Low
Enterprises	High	High	High				High		
SMB	High						High		
Smart Building	High	High	High	High	High		High	High	Low

1: Including Generation, Nuclear, Hydro. 2: Including Upstream, Midstream, Downstream

BNS sectorial usage



Time it Takes a hacker to brute force a password in 2023

- Passwords can no longer be relied upon for critical users
- Using other techniques such as dictionaries, accelerate the breach even further

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Stuxnet: A New Era of Cyber Warfare

Background of Stuxnet:

- Stuxnet is a malicious computer worm, first identified in 2010, but with development likely starting in 2005.
- Believed to be developed by the United States and Israel to attack Iran's nuclear program.
- It marked a significant shift in cyber warfare, being one of the first instances of a cyber weapon causing physical damage to a facility.

How Stuxnet Works:

- Stuxnet targeted Windows machines using four zero-day exploits.
- It propagated through local networks and USB drives.
- Upon identifying its target, Siemens' Step7 software on systems controlling a specific configuration of centrifuges, it initiated its payload.

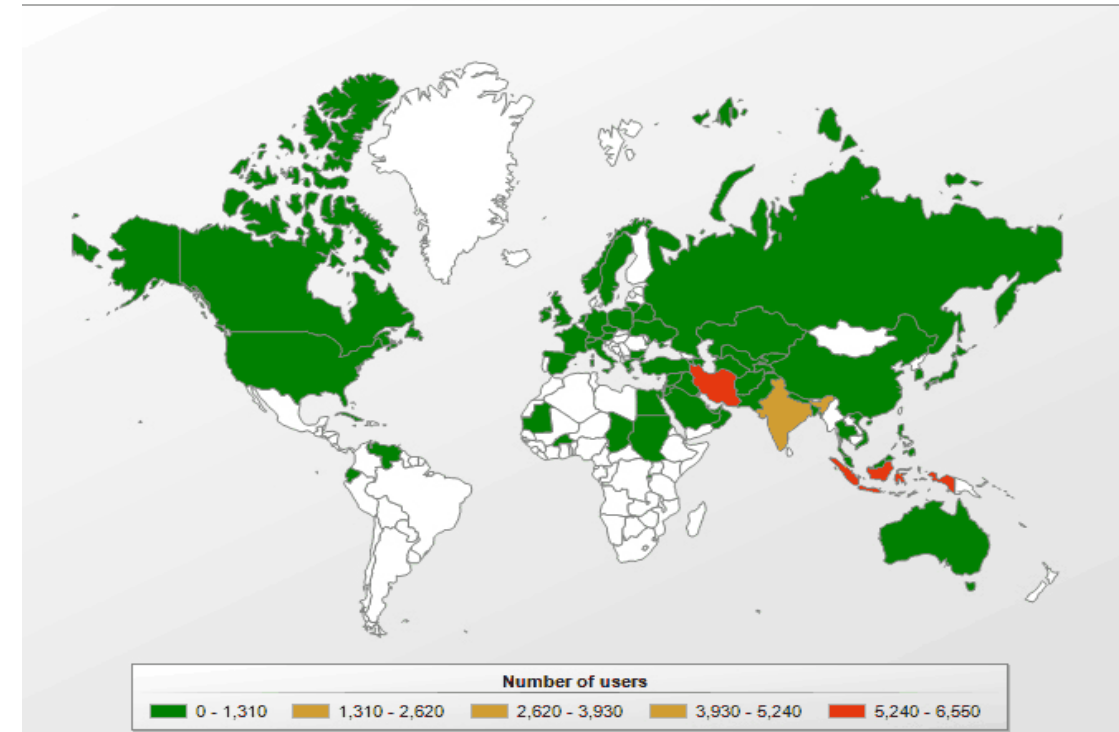
The Impact of Stuxnet:

- Caused significant disruption to Iran's nuclear program by damaging a large number of their centrifuges.
- The worm was eventually discovered and analyzed, revealing the potential for cyber warfare to have real-world impact.

Implications for Power Utilities:

- Stuxnet demonstrated that industrial control systems, like those used in power utility companies, are vulnerable to sophisticated cyber attacks.
- There's a need for constant vigilance, state of the art cybersecurity controls, and robust incident response plans to protect against such

Rootkit.Win32.Stuxnet geography



Centrifuges Damaged: Stuxnet damaged around **1,000 – 2,000** of Iran's centrifuges.

Attack Sophistication: Stuxnet used four **zero-day exploits** and two stolen digital certificates.

Global Infection: Despite its target, Stuxnet infected tens of thousands of systems in **155 countries**.

Attack Duration: Stuxnet operated **undetected** for about five years from 2005 to 2010.

Rising Threats: Operational technology (**OT**) attacks have increased by **over 2000%** since 2018.

BNS would stop Stuxnet in its tracks

BNS:

OT/IT Separation:

BNS provides robust separation of OT/IT networks, limiting potential spread of malware and enabling Zero Trust Microsegmentation.

Invisibility:

With no IP or MAC address, BNS can't be targeted or exploited like traditional network devices.

Firewall Stealth:

BNS can hide an existing firewall, maintaining its filtering activity without exposure to direct attacks.

Anomaly Detection:

BNS can identify and block unusual traffic based on various parameters, helping to stop the propagation of worm-like threats.

Advanced Encryption:

BNS uses white box cryptography to encrypt every frame with a unique algorithm and key, creating a secure tunnel impervious to password cracking. Additionally, it can use standard AES encryption.

Honeypot Redirection:

BNS can redirect suspicious traffic to a honeypot, further protecting the main network.

