Рішення Fortinet для захисту промислових мереж

Приклад реалізації проекту в енергетичній компанії в Україні

Чемерис Олександр,
Менеджер по роботі с ключовими замовниками Fortinet в Україні

R3-06-2021

FORTINET

Fortinet - глобальний лідер в сфері кіберзахисту

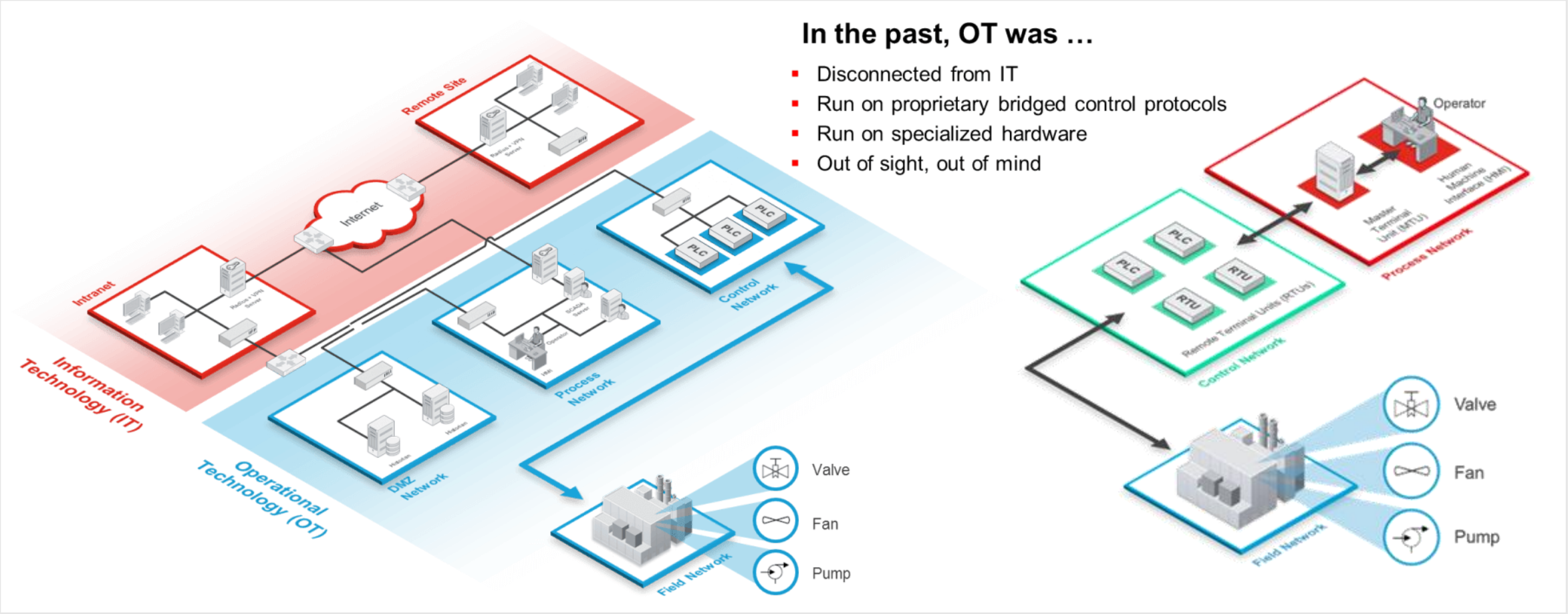
$3.09 млрд
FY2020
Фінансова стабільність

30B+ капіталізація 31 Mar 21
Nasdaq: FTNT
S&P 500

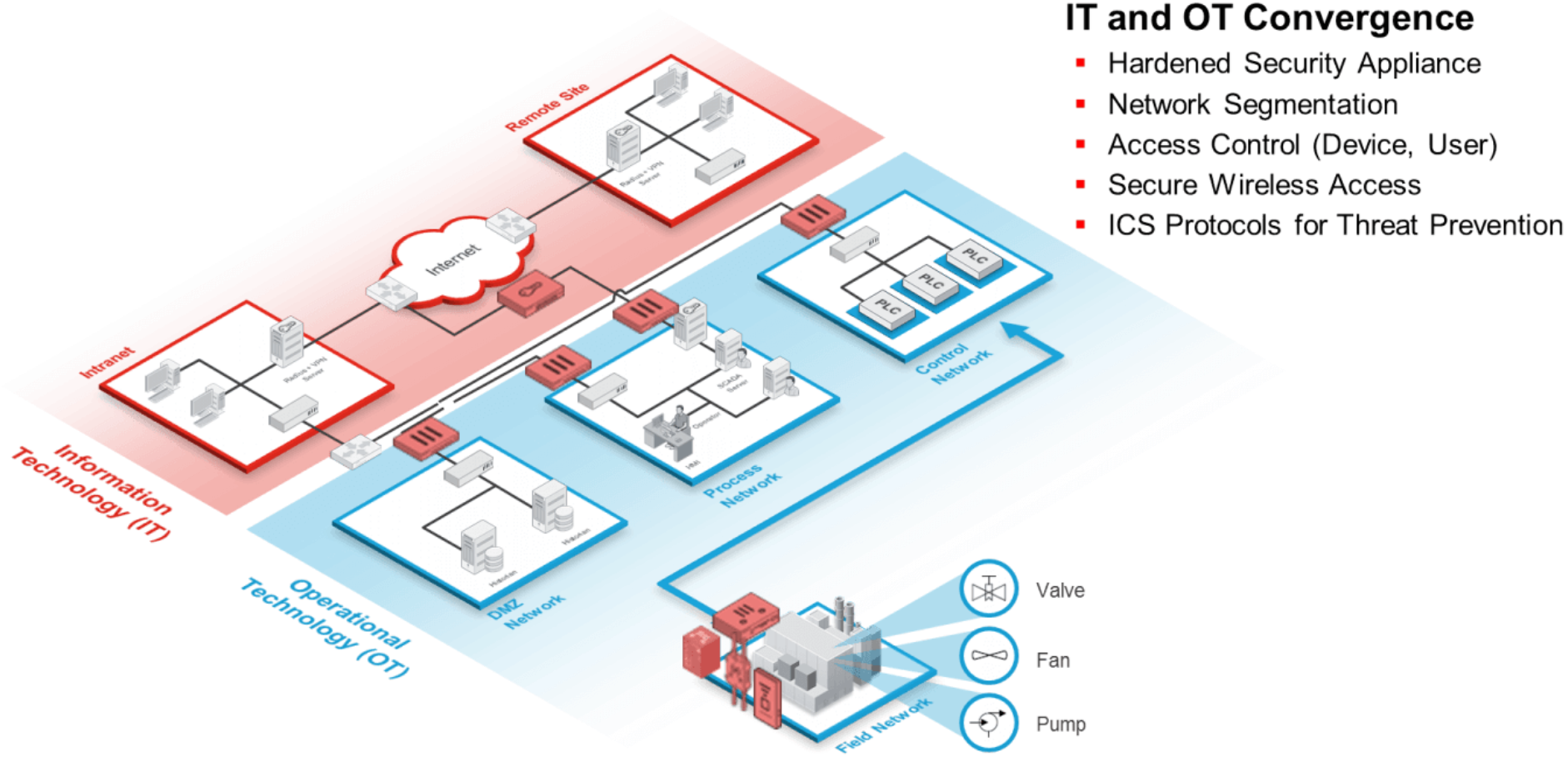
50
Інтегрованих рішень
Продуктова лінійка

500,000+
Замовників в світі
Клієнтська база

IT (Information Technology) та OT (Operational Technology) в минулому



Сучасний стан: безпечна взаємодія IT and OT



IT and OT Convergence

- Hardened Security Appliance
- Network Segmentation
- Access Control (Device, User)
- Secure Wireless Access
- ICS Protocols for Threat Prevention

Рішення Fortinet для захисту OT

1. Розуміємо промислові стандарти та інформацію - FortiGuard Industrial Security Service

Map 2021

ICS/OT протоколи – 1800+ додатків (Application Control) та 300+ IPS сигнатур

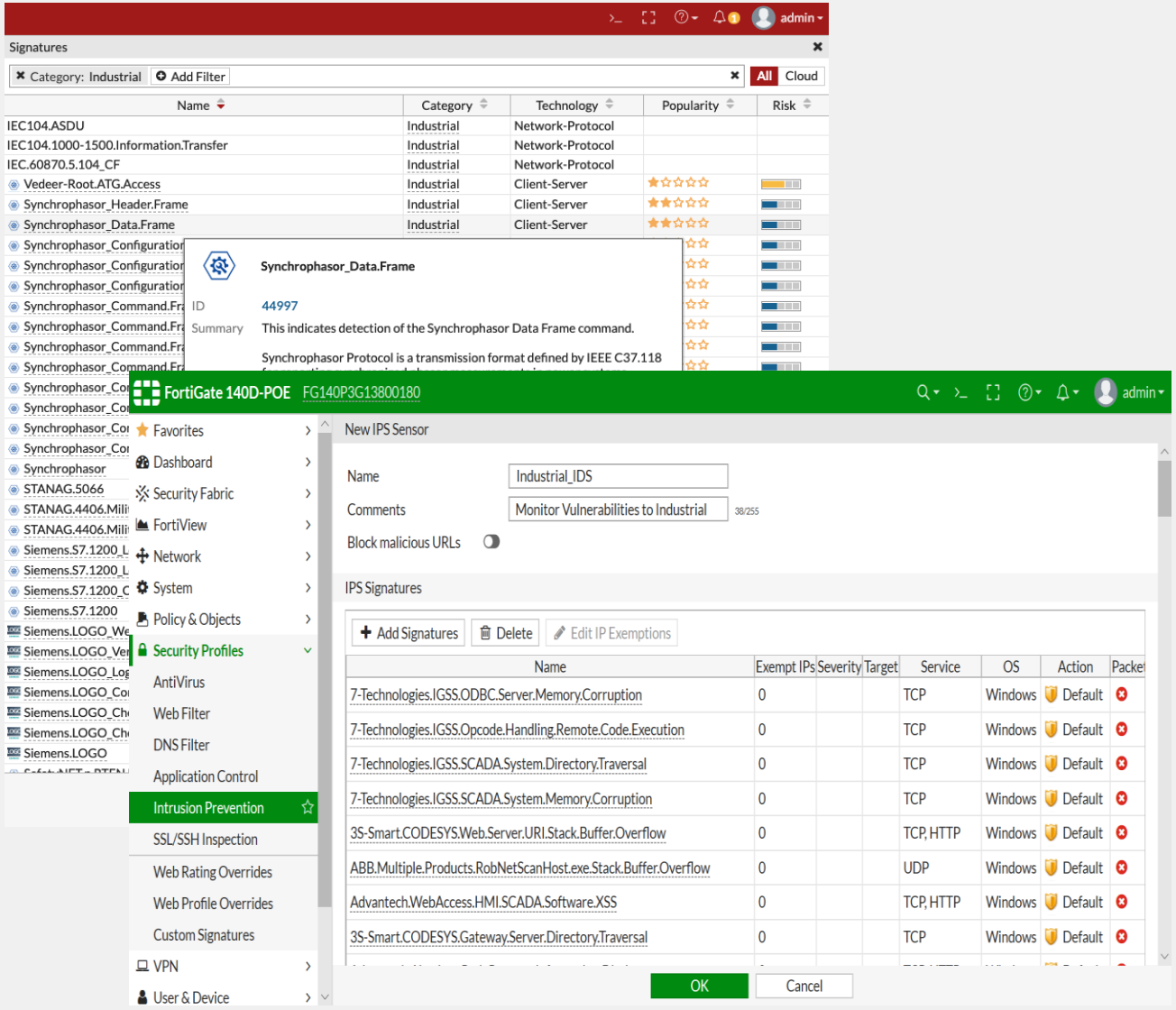
(EIA/CEA-852)	• GE SRTP (GE Fanuc)	• Modbus TCP / MOXA Modbus RTU ⇶	• SafetyNet p
	• HART-IP	• MOXA	• Siemens S7, S7Plus, LOGO
M	• HL7	• MQTT	• STANAG 4406
/ RealPort DNP3	• IEC 60870-5-104 (IEC 104) ⇶	• MTConnect	• STANAG 5066
NET Lite	• IEC 60870-6 (TASE.2/ICCP)	• Net C/X (Digi RealPort)	• TriStation
M 90	• IEC 61850 MMS	• Niagara Fox	• Vedeer-Root
• Emerson DeltaV	• IEC 61850 R-GOOSE	• OPC Classic (DA, HDA, AE)	
• Ether-S-Bus	• IEC 61850 R-SV	• OPC UA	

Детальна актуальна інформація на fortiguard.com

FortiGuard Industrial Protocol Coverage

Application Control	Intrusion Prevention

Гранульована ідентифікація та розпізнавання індустріальних протоколів, запобігання вторгненням



- **Application Signatures**
  - Визначення індустріальних протоколів
  - Гранульована ідентифікація типів
  - Визначення та керування Whitelist політиками
  - Можливість створення власних сигнатур
  - Packet Logging
  - Можливість Source Quarantine

2. Вміємо працювати у відповідних умовах Rugged Solutions – NGFW, комутатори, AP

Захищені міжмережеві екрани NGFW – FortiGate Rugged Series

FGR-30D
- IP20, Indoor Use
- Dual power input
- Industry Certified

FGR-35D
- IP67, Outdoor Use
- Industry Certified

FGR-60F
- IP20, Indoor Use
- SoC4 Powered
- By-pass port
- Industry Certified

FGR-60F 3G4G
- IP20, Indoor Use
- SoC4 Powered
- By-pass port
- Industry Certified
- Embedded 3G/4G/LTE

Industry Certifications

Захищені комутатори та точки доступу – FortiSwitch and FortiAP Rugged Series

FortiSwitch Rugged 112D-POE
- IP30, Indoor Use
- Dual power input
- DIN-rail or wall-mountable
- PoE and PoE+ capable
- Industry Certified

FortiSwitch Rugged 124D
- IP40, Indoor Use
- Dual power input
- Rack-mountable
- Industry Certified

FortiAP Rugged 234F
- Internal Antennas
- IP67, Indoor/Outdoor Use
- PoE Powered
- Ceiling, T-Rail, and Wall-mountable
- Industry Certified

FortiAP Rugged 432F
- External Antennas
- IP67, Indoor/Outdoor Use
- PoE Powered
- Ceiling, T-Rail, and Wall-mountable
- Industry Certified

3. Екосистема технологічних альянсів та партнерів

ТЕХНОЛОГІЧНІ АЛЬЯНСИ / ВАЛІДОВАНІ ДИЗАЙНИ

Виробники систем автоматизації та контролю

Альянси

GE
Schneider Electric
SIEMENS

Технологічні проекти

ABB
SEL Schweitzer Engineering Laboratories
EMERSON
HIRSCHMANN A BELDEN BRAND
YOKOGAWA
Rockwell Automation
Honeywell

Глобальні партнери

Hewlett Packard Enterprise
Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING
Orange Cyberdefense
HCL
IBM
NTT
accenture
Atos

Інше

Baker Hughes
T-Systems
Johnson Controls
Cognizant
World Wide Technology, Inc.
Eleven Paths

ТЕХНОЛОГІЧНІ ПАРТНЕРИ

Видимість активів / Запобігання загрозам

NOZOMI NETWORKS
CYBERX BATTLE-TESTED INDUSTRIAL CYBERSECURITY
DRAGOS
CLAROTY
INDUSTRIAL DEFENDER
SCADAfence
tenable

Операції, Оркестрація, Автоматизація

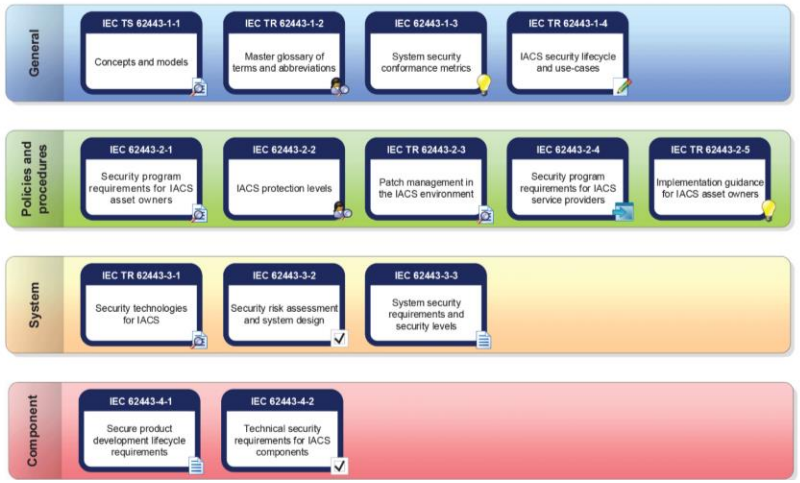
OTORIO
splunk>
tdi
rubrik
np network perception
SKYBOX SECURITY
BACKBOX
servicenow

Інше

SIEMENS RUGGEDCOM INDUSTRIAL STRENGTH NETWORKS
FORESCOUT
radiflow
RAD
DARKTRACE
OWL Cyber Defense

4. Відповідність індустріальним стандартам та кращим практикам

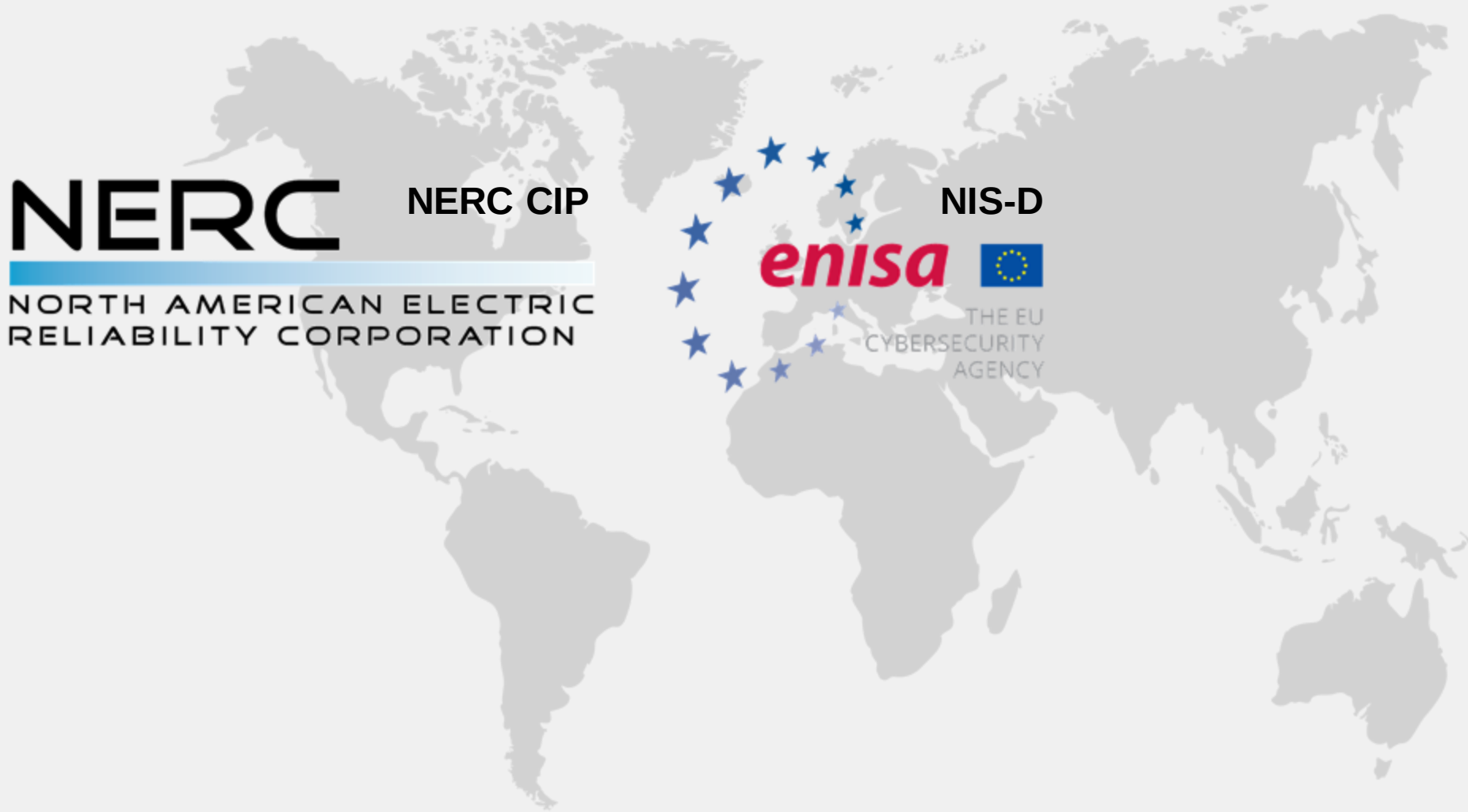
ISO 27001
Information Security Management System



IEC 62443
Cybersecurity Standards
(серія стандартів захисту промислових комунікаційних мереж)

NIST Cybersecurity Framework

Відповідність регуляторним стандартам



inet Security Fabric

датки

тформи

режі

Proxy

Tokens Proxy

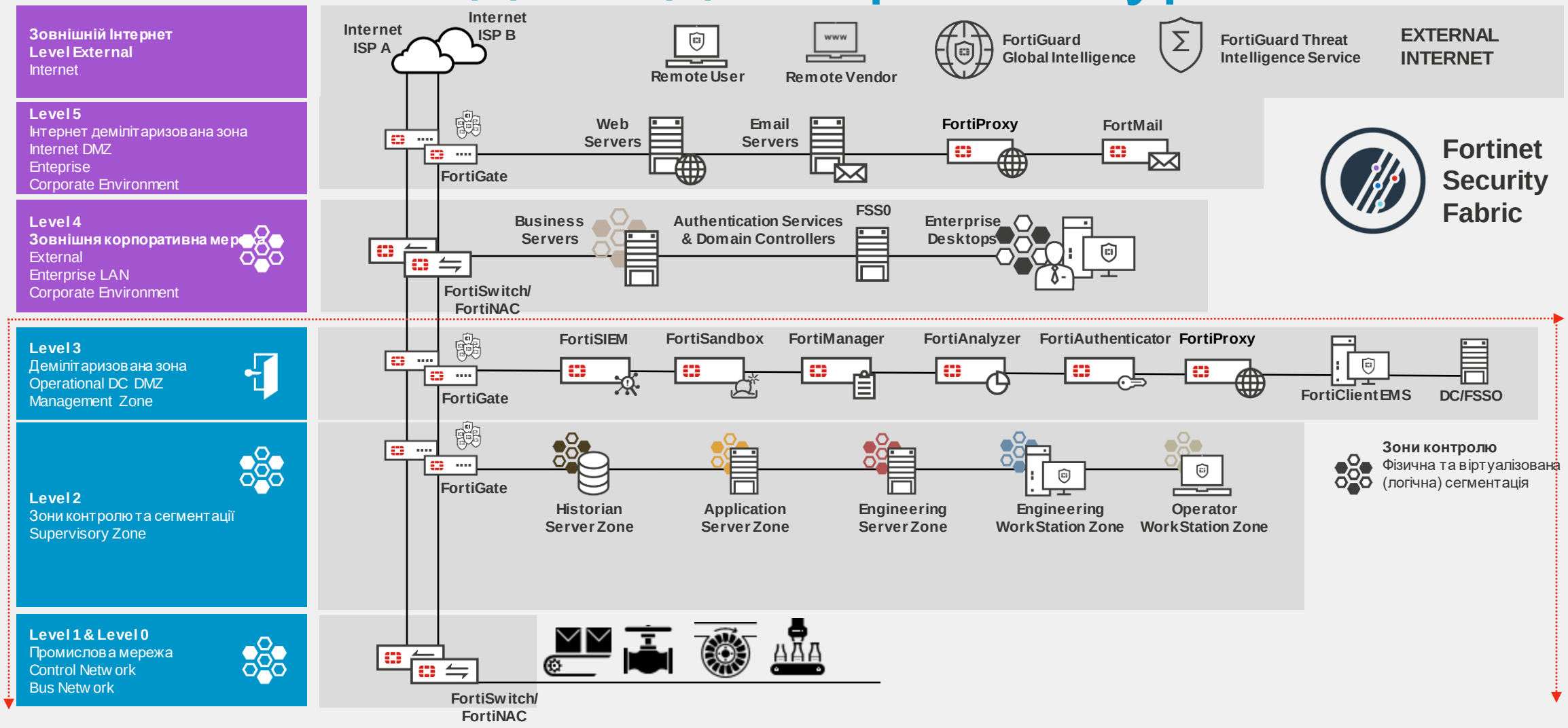
Tester

Керованість

Захист загрозам (Threat Intelligence)

Інтегрованість

IEC 62443 відповідна архітектура



net Security Fabri

тованих рішень та конне

Fabric Connectors

Fortinet-developed deep integration automating security operations and policies

IBM Cloud · Microsoft Azure · servicenow · Symantec

Fabric APIs

Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

ARISTA · ASAVIE · DELL · DRAGOS · EQUINIX · intel · SIEMENS Ingenuity for life · splunk> · TIGERA · tufin

Fabric DevOps

Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration

aws · Google Cloud · HashiCorp · Microsoft Azure · openstack. · ORACLE · RED HAT ANSIBLE Automation · refactr · vmware

Extended Ecosystem

Integrations with threat sharing initiatives and other vendor technologies

CYBER THREAT ALLIANCE · MITRE · STIX · INTERPOL

Firewalls · Switching · Wireless · Endpoint Security

Figures as of March 31, 2021

Note: Logos are a representative subset of the Security Fabric Ecosystem