



Security Summit OT

Milano 24 settembre 2026



**La visibilità non protegge:
conoscere le vulnerabilità non basta per proteggere gli ambienti OT**

Marcello Romeo, TXOne Networks

La sola Visibilità non Protegge



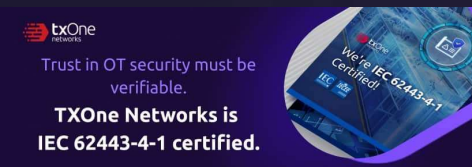
Marcello Romeo - Presales Manager South Europe
Marcello_Romeo@txone.com
TXOne Networks



TXOne Networks Company Profile

Keep the Operation Running

About TXOne Networks



TXOne Networks offers cybersecurity solutions for ICS and OT environments, employing the OT zero trust methodology for Cyber-Physical Systems (CPS)

- Founded in 2019
- 400 TXOners in 30 countries



- Global customers: 5000+
- Large enterprise customers: 350+

Semiconductor

Manufacturing Equipment	8 of Top 10
Fabrication Plant	6 of Top 10
Packaging and Testing	5 of Top 10
Pharmaceutical	5 of Top 10
Automotive	5 of Top 10
Aviation	5 of Top 10



TXONE NETWORKS IS IEC 62443-4-1 CERTIFIED

Trust in OT security must be verifiable.

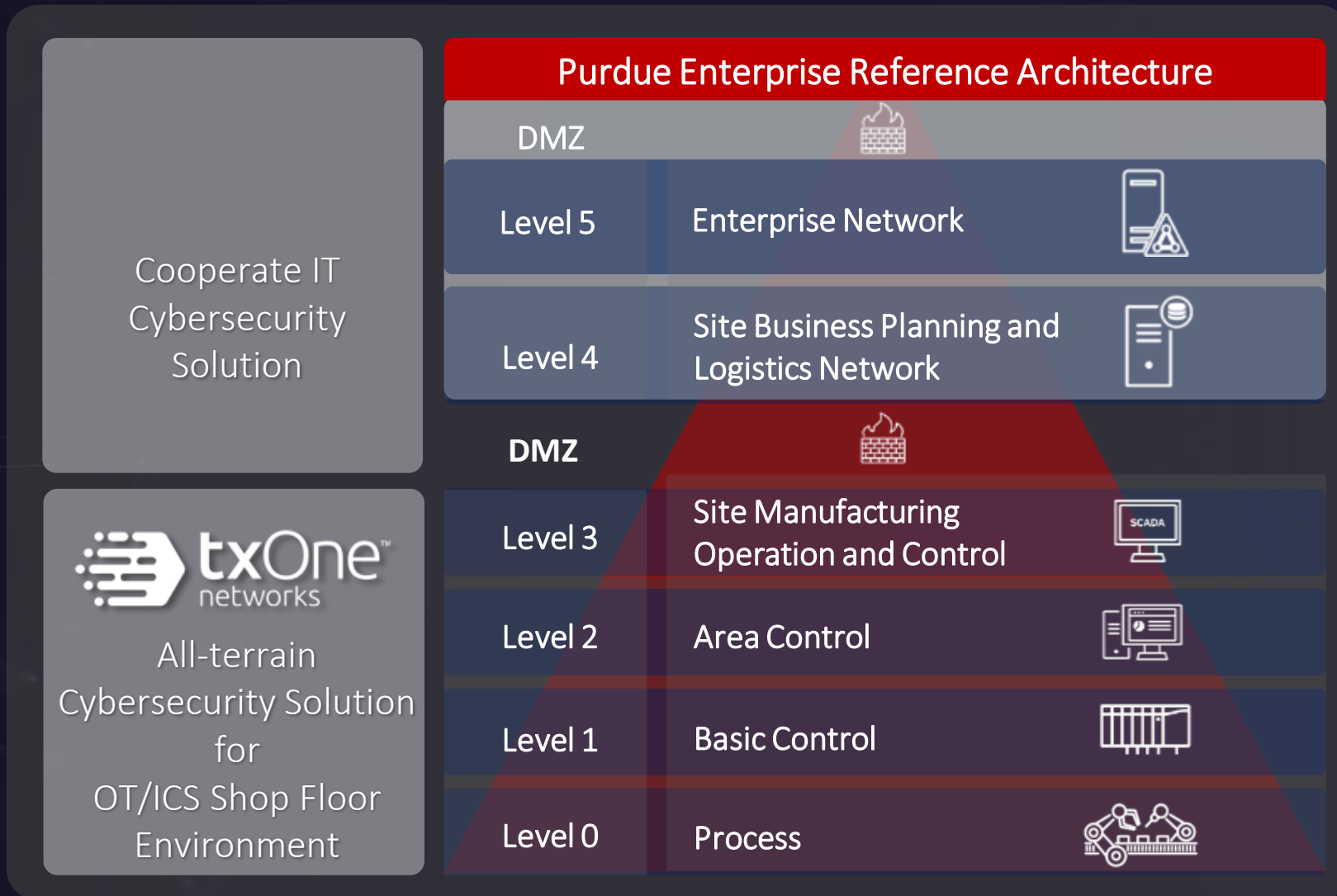
We are proud to announce that TXOne Networks has achieved IEC 62443-4-1 certification for our Secure Product Development Process.

This milestone reaffirms our commitment to embedding security at every stage of the product lifecycle, ensuring that our customers and partners can rely on solutions that are secure by design.



TXOne si occupa solo di OT Security

Evitare il Fermo Impianto con approccio OT-ZERO TRUST



Proteggiamo la
Produzione da
Incidenti Cyber



Le soluzioni Cyber IT non funzionano in OT

Keep the Operation Running

Quali sono le cause delle vulnerabilità in OT?



Worm/Malware brought in, or Misuse of PLC and critical assets, by Intentional or unintentional insiders.

Insider Threat Human Factor

Legacy Assets

Massive number of assets with complex and mixture systems included legacy, EOL operating systems

No network segmentation, in many cases the whole network is a big flat L2 network

Flat Network

Patching Absent

Difficult to conduct the patching and updating process due to several practical reasons



Le Tipiche soluzioni di sicurezza IT non funzionano in OT

Nessun
Supporto per
sistemi LEGACY

Sistemi critici come
machine SCADA
funzionano per oltre 20
anni.

Funzionano solo
se hanno un
update continuo e
connessione
cloud

I Sistemi OT molto
raramente hanno una
connettività internet o
CLOUD

Carenza o assenza
totale di supporto
per protocolli OT

Comprensione limitata e
suscettibile di falsi
positivi

Nessuna
conoscenza del
funzionamento
delle applicazioni
critiche OT

Troppe risorse richieste e
troppi falsi allarmi

Il Firewall protegge?



Firewall

- Basic firewall si just filtering/routing traffic considering static rules
- Rules are based on IP, MAC and Port Number



IPS (Intrusion Prevention System)

- Deep Packet inspection of all traffic, detect, identify and BLOCK Threats
- Real-time inspection, signatures based to prevent attacks reaching their targets
- Zero day attack prevention for Advanced IPS

**La Visibilità è solo
la prima fase
di un processo...**

A large graphic consisting of two concentric circles. The outer circle is a thick, light purple ring, and the inner circle is a solid, dark purple circle. The text is centered within the inner circle.

*Visibility That
Fuels Protection
Rollout*

Solution Portfolio Summary

Security Inspection

Element Series



PI-Pro



SAFEPORT

An ultimate security inspection, streamlining operations and relieving overworked teams

Installation-free, supporting **air-gapped environments** on the target ICS

Removable media sanitizer before bringing it into the working environment.

Easy operation to make the process convenient for any user

Endpoint Protection

Stellar



ICS endpoint protection for both modernized and legacy assets

Minimal downtime for mass deployment

4-in-1 lockdown for legacy and un-patchable devices

ICS-NGAV for modernized and patchable devices

Network Defense

Edge Series



Security appliances to segment the network with zero-trust protection

Easier deployment on the rack or in the cabinet

Robust hardware to support wide temperature range and long MTBF

Fail-safe without interrupting production even on hardware failure

CPS Platform

SENNINONE



Comprehensive security platform for monitoring and managing OT infrastructure

Asset lifecycle management across TXOne security solutions

Vulnerability management and monitoring of critical assets

CPSDR detects and response to potential OT threats

SENNINONE

Approach

Attack Surface
Management

Lifecycle
Protection

Threat Detection &
Response

Element



SenninOne

Stellar



Edge



Value

Holistic Visibility

Collaborative
Insights

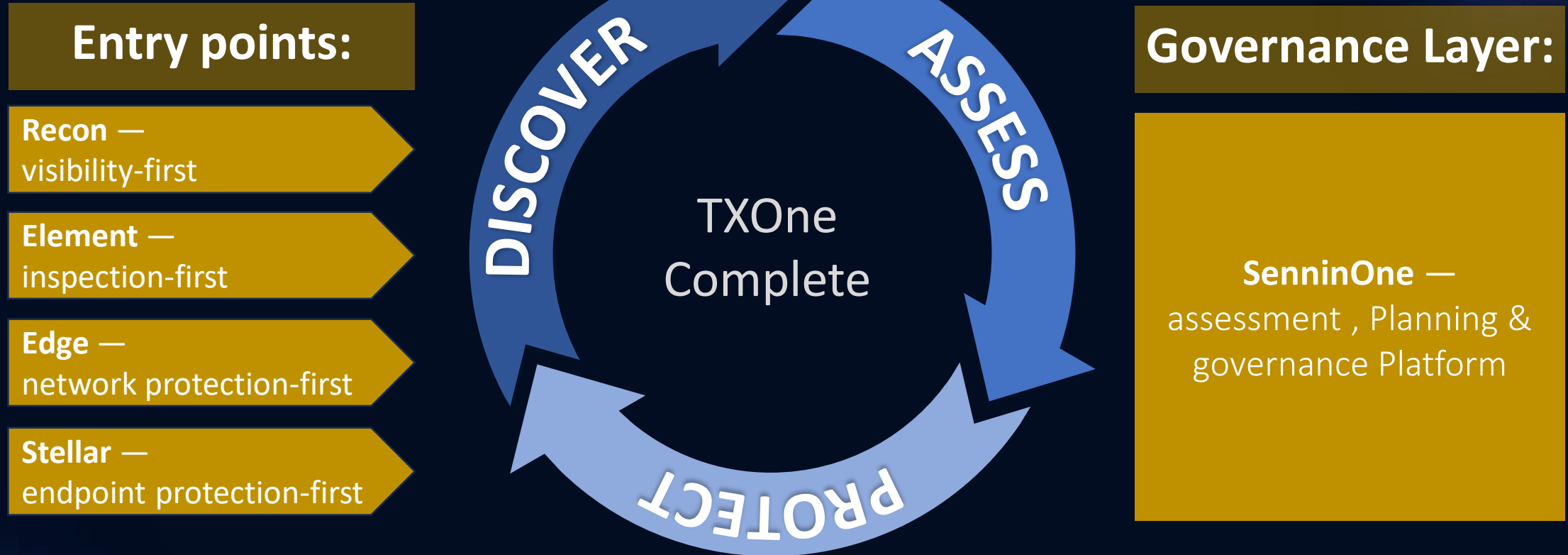
Simplified
Management

Goal

Operation
Resilience



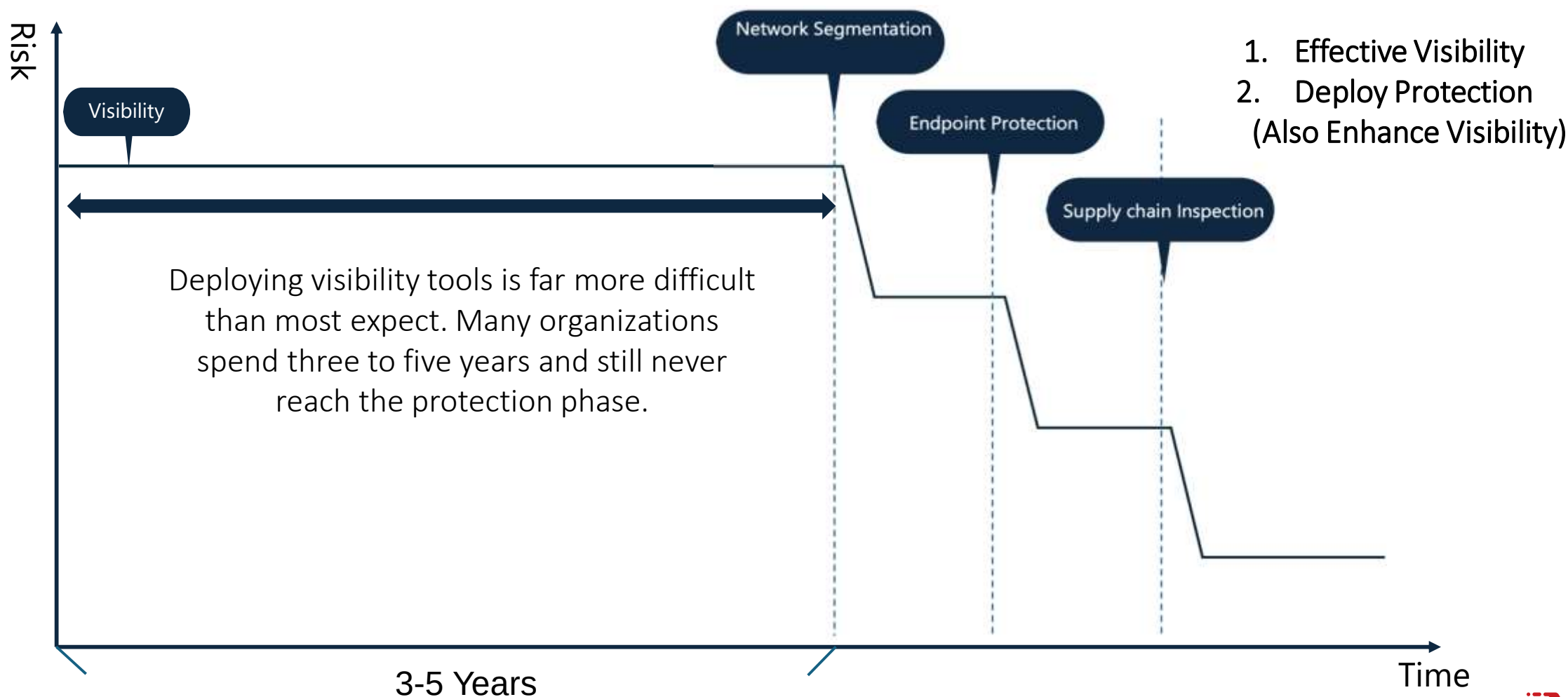
TXOne Complete with SENNINONE: Discover. Assess. Protect.



Shared Asset Model | Shared Risk Score | Shared Telemetry

La sola Visibility ritarda la Riduzione del Rischio

You don't need complete visibility before taking action to protect.



L3



You Can't Protect What You Can't See

“Cybersecurity **governance** is a comprehensive cybersecurity strategy that integrates with organizational **operations** and **prevents the interruption** of activities due to cyber threats”

- Cybersecurity & Infrastructure Security Agency, CISA

L3



You Can't Protect IF... You **only** See





Le soluzioni applicate a CASI REALI

Keep the Operation Running

Alcuni casi di successo



Caso di successo

La sicurezza OT diventa plug & play: facile per gli operatori, potente per l'IT.

Terna



Caso di successo

Innovazione e OT Cybersecurity:
Il Gruppo Edison accelera con le
soluzioni TXOne Networks

Gruppo Edison



Caso di successo

ansaldo energia

La tecnologia come alleato
strategico nella protezione degli
ambienti produttivi

Ansaldo Energia



ANSALDO ENERGIA

Dalle esigenze alla soluzione

ANSALDO ENERGIA

Ansaldo Energia è un gruppo presente in oltre 30 Paesi nel mondo, con più di 3.500 dipendenti. Il core business di Ansaldo Energia comprende la progettazione e la produzione di turbine a gas, turbine a vapore e generatori, oltre alla realizzazione di impianti completi per la produzione di energia.



- ❑ Un incidente Cyber in uno degli impianti ha conseguenze ed impatti sia sull'ambiente che sulla SAFETY
- ❑ Le Normative sono sia quelle di settore che la NIS2
- ❑ Gli attacchi si propagano da IT, dalla SupplyChain, o per errore umano ed impattano principalmente su sistemi molto vulnerabili, «LEGACY».
- ❑ Molti asset critici sono considerati «Intoccabili», nessuna modifica o installazione è consentita.
- ❑ Nessun interruzione alla produzione

ANSALDO ENERGIA: alcuni dei problemi affrontati...e risolti

- ❑ La protezione dei sistemi critici con pieno supporto degli ambienti LEGACY
- ❑ I sistemi critici, ma anche «fragili» dove nulla può essere installato a protezione
- ❑ Contenere il rischio di veicolo di infezione tramite chiavette USB generiche
- ❑ Sistemi Vulnerabili presenti in rete, per i quali non esistono più le patches o che non è possibile avviare verso cicli di patching continui.



ANSALDO ENERGIA: il valore delle soluzioni

- ❑ **EDGE IPS - Virtual Patching**: protezione garantita senza impatti e senza modifiche della rete e dell'asset. Protegge Asset Vulnerabili, non più aggiornabili, che non possono essere fermati, o comunque modificati.



- ❑ **STELLAR - LifeTime Protection** - Protezione degli asset legacy (EOS), a partire da Windows XP..fino ai sistemi Moderni. Incluso Linux.



- ❑ **Portable Inspector Pro**: Evitare chiavette generiche. Ispezione e Sanificazione di Asset dove l'agent non può essere installato. Nessun Reboot e nessuna modifica al sistema.



- ❑ **SAFEPORT**: Ispezione e sanificazione di storage rimovibili come Chiavette USB



Protezione e Visibilità sono un traguardo Congiunto

La visibilità
non è la destinazione finale: è solo il punto
di partenza

