
VANTELIS
CYBER OT

El crecimiento de OT impulsado por la regulación y la digitalización

ESCENARIO

Los ciberataques se multiplicaron por 22 el año pasado

Impulso regulatorio global: CISA en EE. UU., NIS2 y CRA en Europa, CSS e IPART en Medio Oriente y APAC.

Sin embargo… implementar ciberseguridad industrial tiene bajo ROI

PROPUESTA

Certificado por los principales proveedores de automatización

Casos de uso con los líderes del mercado de ciberseguridad OT

Sin costos ocultos:

VALOR ENTREGADO

Continuidad del negocio

Mitigación de riesgos

Cumplimiento de normas:

Petróleo y gas

Minería y metales

Agua y saneamiento

Edificios inteligentes

Planta industrial

LA SOLUCIÓN VANTELIS ES TOTALMENTE AGNÓSTICA AL SEGMENTO DE MERCADO Y AL PROVEEDOR DE AUTOMATIZACIÓN

La automatización tiene restricciones de seguridad distintas

Sistema industrial (OT):

Protección de los recursos de produc
Vida útil de hasta 20 años
Rara vez se actualiza

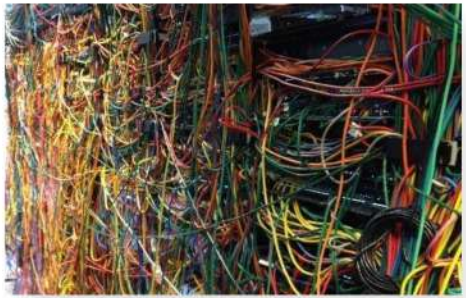
Las técnicas de seguridad de TI no se pueden aplicar directamente a la infraestructura OT

Oficina (IT):

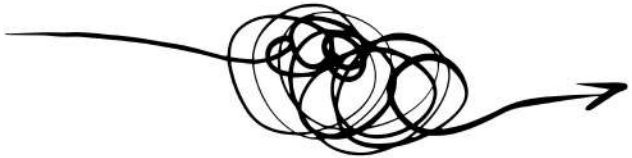
Protección de la infraestructura de IT
Vida útil de 3 a 5 años
Fácil de actualizar

Resultados en horas, no en meses

Red OT real

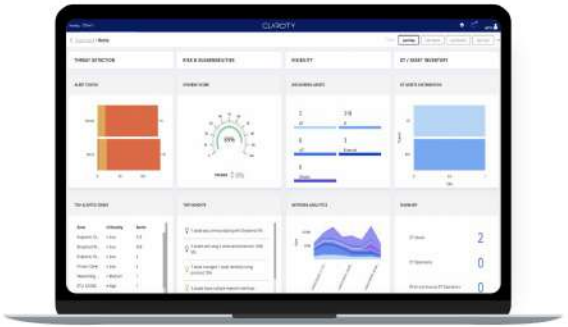


El tortuoso camino hacia la protección



Meses de inactividad operativa

Visibilidad y protección activas



- **Evaluaciones costosas (spoiler: la respuesta siempre es " hay que actualizar el sistema")**
- **Hojas de ruta de implementación de varios años**
- **Reconstrucciones completas de la red, incluyendo tendido de cable nuevo, reconfiguración del sistema y más**

Soluciones Vantelis: una capa de seguridad sin fricción

- Asegura toda la comunicación de red, incluidos los dispositivos legacy
- Incluye un stack completo de capacidades de protección
- Se implementa en minutos, con tiempo de inactividad despreciable

Ocultamiento de activos

Adquisición de datos

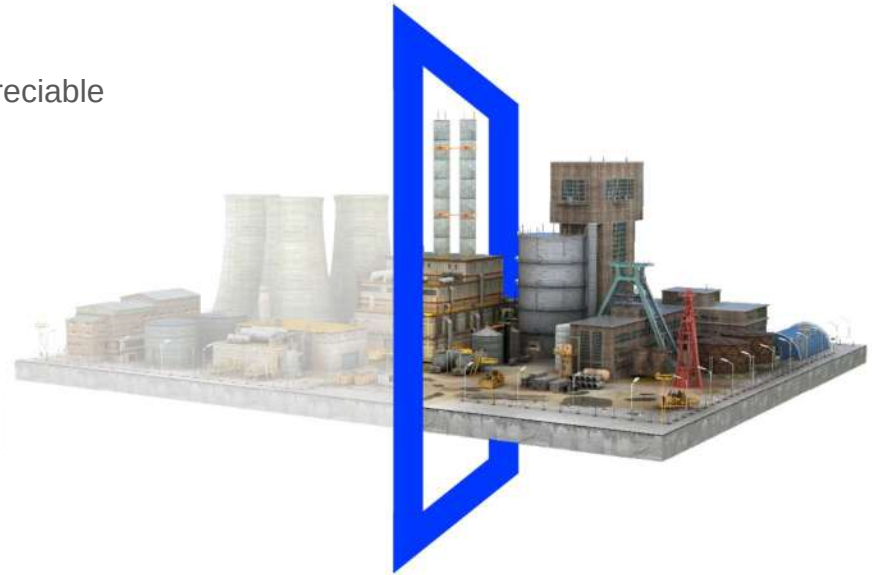
Tap en línea

Descubrimiento de activos OT

Segmentación instantánea

Zero Trust

Consola central



Optimización del costo total de propiedad y el tiempo de valor

Costo de compra

Costo oculto

- Planificar los cambios de red
- Modificaciones a la arquitectura de red
- Proyectos de reacondicionamiento
- Mantenimiento de varios productos
- Cambios de software vinculados a la red - VLANs, etc.
- Tiempos de inactividad en producción por el despliegue y las pruebas
- Demoras en la puesta en marcha

Los objetivos de OT no deberían implicar bloqueos ni cuellos de botella

PLATAFORMA *DE* ADQUISICIÓN DE DATOS OT

- Simplifica la generación de inventarios de activos y conexiones OT.
- Propuesta más competitiva que el enfoque tradicional (sensores, taps, NPB, etc.)
- Implementa el IDS más rápido
- Evita el vendor lock-in

PROTECCIÓN

- Reduce el costo de proteger activos valiosos
- Quick win: resultado inmediato
- Protege servidores y maquinaria legacy que no pueden cambiar su IP
- Es compatible con activos legacy y todos los proveedores

1- Plataforma de adquisición de datos

Combinación ganadora: Vantelis + plataformas de detección de anomalías

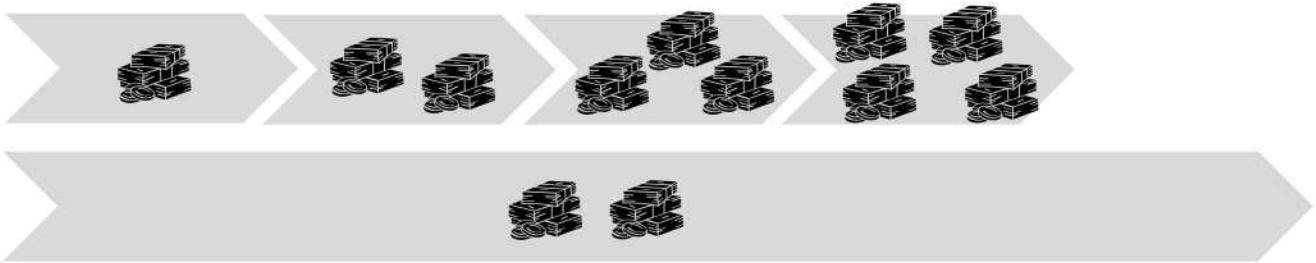
Empresa estatal que opera trenes de carga y pasajeros, con más de 7.000 km de vías y 1.000 estaciones

Desafío: conectar de forma segura distintos sistemas de automatización y consolidar la información de uso en una aplicación de analítica. Costos de implementación y dependencia de proveedor.

Solución de Vantelis:
- **90% de compresión de tráfico.**
- **Una persona puede implementar 8 estaciones por día.**
- **Gestión transparente de certificados y adquisición segura de datos en distintos entornos.**
- **Simplificación de la arquitectura y de la cantidad de hardware y tecnologías.**
- **Habilita visibilidad y protección al mismo tiempo, minimizando costos.**

Simplificación de la arquitectura y minimización de costos

PROBLEMA / SOLUCIÓN	TAP	Sensor	Packet Broker	Agregador de tráfico	VANTELIS CYBER OT
Switches legacy	■				■
Análisis y compresión de tráfico		■			■
Enviar tráfico a través de la red			■		■
Agregar tráfico de distintos sitios				■	■



Enfoque integral de Vantelis:

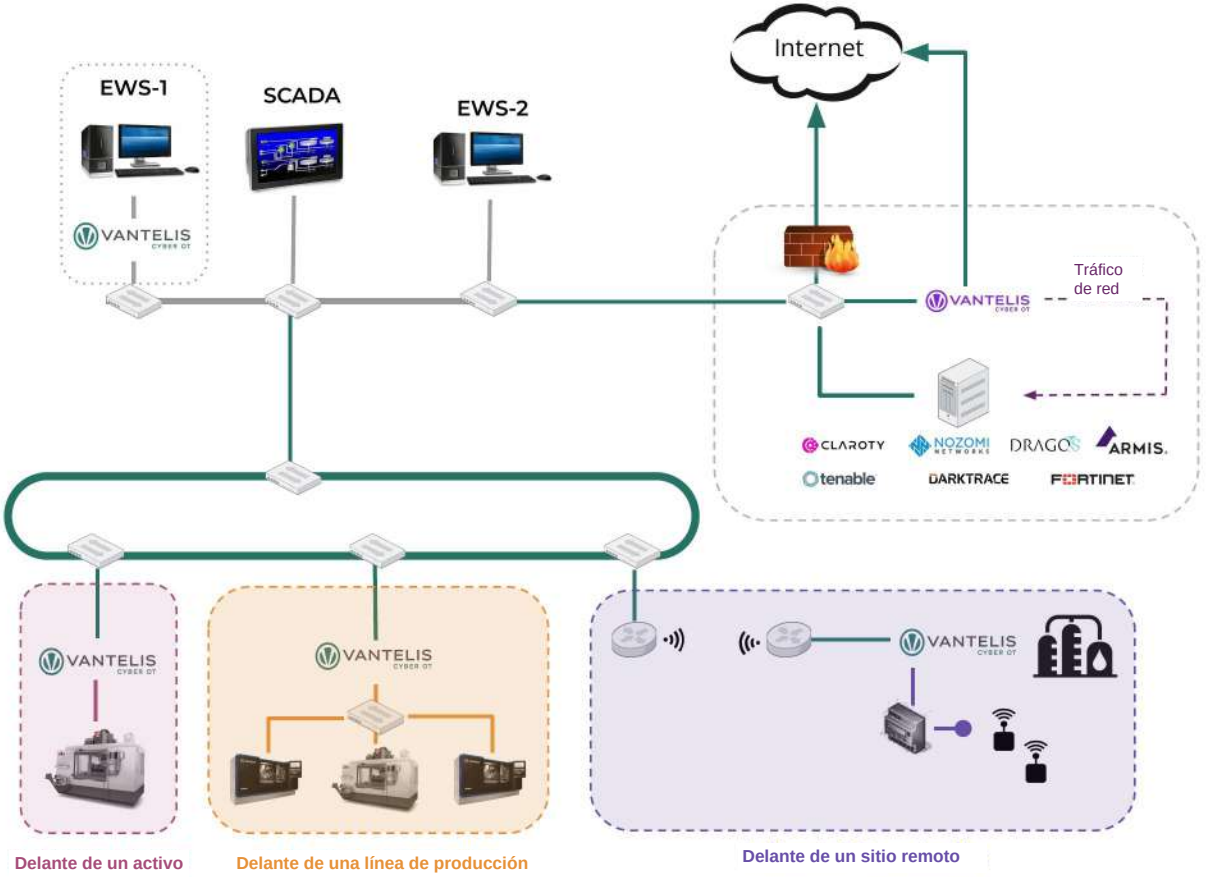
- simplifica la arquitectura.
- minimiza la cantidad de componentes
- reduce los costos asociados a la implementación y la infraestructura

NOZOMI NETWORKS · tenable · DARKTRACE · CLAROTY · CYLUS · DRAGOS · FORESCOUT · ARMIS · Microsoft Defender for IoT

Arquitectura escalable

Vantelis Orchestrator (consola de gestión)
- Se instala en una VM en una ubicación central (DMZ, etc.)
- Puede orquestar miles de VIA
- Puede actuar como TAP, Sensor, Packet Broker y agregador de tráfico para soluciones de visibilidad y monitoreo de terceros

Appliances Vantelis Via
- Appliance física o imagen de VM (contenerizada)
- Se conecta a un switch (Span o directo) o en línea
- Bypass físico en caso de falla del appliance (cable en vivo)



Desafíos + beneficios de Vantelis

DESAFÍOS	VANTELIS CYBER OT BENEFICIOS	+ MINIMIZAR EL TIEMPO Y RIESGO DE IMPLEMENTACIÓN
Recolección de datos insegura	La PKI integrada gestiona los certificados de forma transparente	Implementación segura en la red industrial
Los recolectores tienen limitaciones de ancho de banda	Tasa de compresión del 90% Sin impacto en el rendimiento	Solo 2 interfaces
		Bypass físico
Sin capacidad de respuesta ante un ataque	Brinda capacidad de respuesta	Escalable
		Consola central
Interfaces adicionales	Altamente escalable	Nativo de OT
		Incluye funciones básicas de visibilidad
Colisión de IP al recolectar datos de múltiples ubicaciones	Conversión de IP para el tráfico reenviado desde múltiples sitios	Anti-manipulación

2- Protección de activos legacy

Valor inmediato para fabricantes (OEM) y clientes finales

Problema: el sistema operativo es Windows XP y el fabricante de la máquina discontinuó el soporte de ciberseguridad.

Como no está permitido modificar la configuración de la máquina, se descarta el enfoque clásico por su alto costo de instalación y el tiempo de inactividad asociado (cambios de red y de proceso, validación e interrupciones sostenidas durante la implementación).

Solución: la plataforma drop-in de Vantelis protege las máquinas legacy frente a ransomware y amenazas avanzadas, sin interrumpir las operaciones.

Beneficios:
- aprovisionamiento zero-touch
- cero tiempo de inactividad operativa
- sin necesidad de rediseñar la red
- protección activa
- monitoreo mejorado

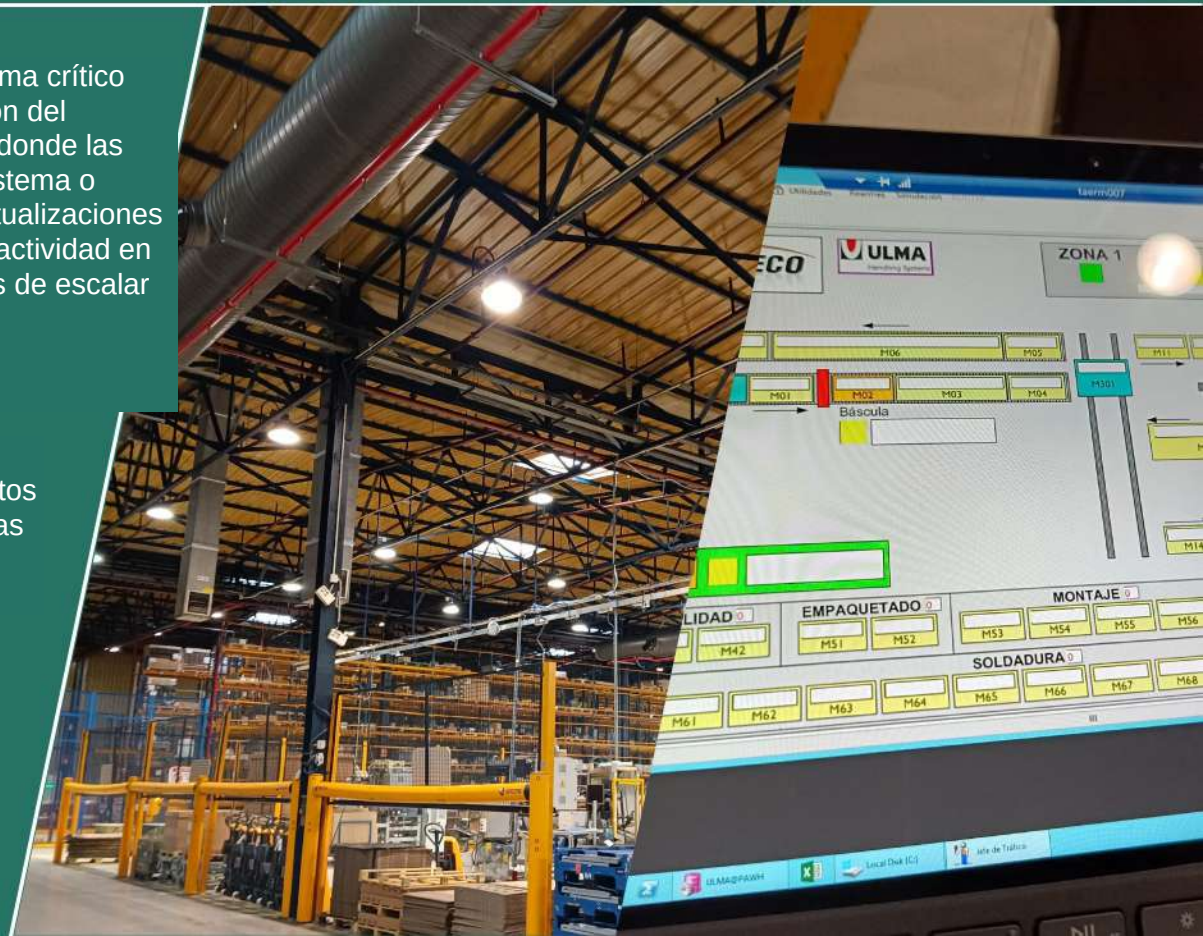
Protección de subsistemas - Ejemplo: depósito automatizado

Problema: el depósito automatizado es un subsistema crítico con muy poca tolerancia a la inactividad. La solución del fabricante (OEM) se basa en arquitecturas legacy, donde las mejoras de seguridad exigirían rediseñar todo el sistema o hacer cambios mayores. Como resultado: ● las actualizaciones se demoran o no son viables ● hay que evitar la inactividad en producción ● las mejoras de seguridad son difíciles de escalar

Solución: se implementó el gateway de Vantelis delante del subsistema, definiendo zonas y conductos y protegiendo sus comunicaciones sin interrumpir las operaciones

Beneficios:

- Se implementa en minutos
- No requiere cambios en los sistemas existentes
- Alineado con los principios de la norma IEC 62443
- Protege todo el subsistema sin impactar en las operaciones



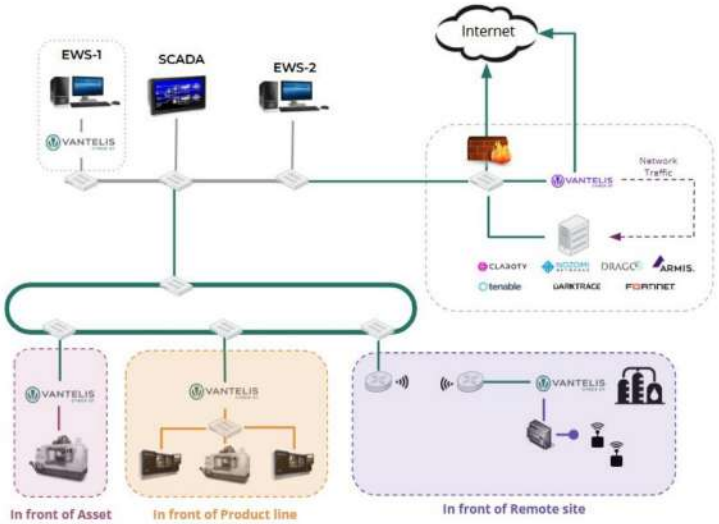
Después de la visibilidad, el próximo desafío es la protección

Identificación de activos a proteger

Implementación de Vantelis

Zonas y conductos

Ocultamiento de activos



Sin agentes,

protección no intrusiva

Escenario geopolítico: catalizador inmediato

CYBERSECURITY ADVISORY

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure

Release Date: April 07, 2026 **Alert Code:** AA26-097A

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Advisory at a Glance

Title	Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure
Original Publication	April 7, 2026
Executive Summary	Iran-affiliated advanced persistent threat (APT) actors are conducting exploitation activity targeting internet-facing operational technology (OT) devices, including programmable logic controllers (PLCs) manufactured by Rockwell Automation/Allen-Bradley. This activity has led to PLC disruptions across several U.S. critical infrastructure sectors through malicious interactions with the project file and

CISA recomienda explícitamente implementar un proxy de red, gateway, firewall o VPN delante de los PLC: exactamente la propuesta de valor de Vantelis

Follow-up steps to strengthen security posture:

- **Implement multifactor authentication (MFA)** [CPG 3.E] for access to the OT network from an external network.
- If remote access is required, **implement a network proxy, gateway, firewall, and/or virtual private network (VPN) in front of the PLC to control network access**.
  - A VPN or gateway device can enable MFA for remote access even if the PLC does not support MFA. Implement security rules on these higher-level network security mechanisms that prevent the type of repeated and sustained login attempts that would be seen during a brute force attack. When possible, implement a device control list for workstations sending messages or connecting to OT components.
  - Use the device control list to monitor for logon activity for unexpected or unusual access to devices from the internet.
- **Keep PLC devices updated with the latest software patches by the manufacturer.** Use established downtime windows to install patches. Known Exploited Vulnerabilities may need to be prioritized outside a downtime window.
- **Configure external and internal firewalls to block traffic using common ports** associated with network protocols that are unnecessary for the particular network segment.
- **Disable any unused authentication methods, logic, or features,** such as default authentication keys, as well as unused or needed services such as Teletype Network (Telnet), File Transfer Protocol (FTP), Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and web services.
- **Monitor asset management systems for device configuration changes**, which can be used to understand expected parameter settings.
- **Monitor the content of network traffic** for the following:
  - Unusual logins to internet-connected devices or unexpected protocols to/from the internet.
  - Functions of industrial control systems (ICS) management protocols that change an asset's operating mode or modify programs.

Protección de un depósito automatizado de una empresa del Forbes 200 en 1 hora, sin tiempo de inactividad

Implementación en 3 sitios en 2 horas

No requiere configuración específica ni rediseño

VANTELIS
CYBER OT

Implementado en una planta de agua para 2,5 millones de habitantes en 3 h

Protege sistemas de salud en horas

Remediar y proteger maquinaria de producción crítica en una empresa multinacional. Implementación sin interrumpir la producción

500 estaciones de tren

1 persona puede implementar

8 estaciones por día

Seguridad para una empresa de alimentos y bebidas a nivel nacional en horas, no en meses

VANTELIS
CYBER OT

Implementado en la planta solar más grande de Europa

Seguridad de la red eléctrica con criptografía poscuántica y latencia despreciable

CONTACT

EBRAX ATM SECURITY LLC.

·901 N. Market St. suite 705 Wilmington,
New castle county. Delaware 19801·

Mailling Address

777 Brickell Ave. Suite 1210, Miami, FL, 33131

info@ebrax.net

+549 11-6743-6697

www.ebrax.net