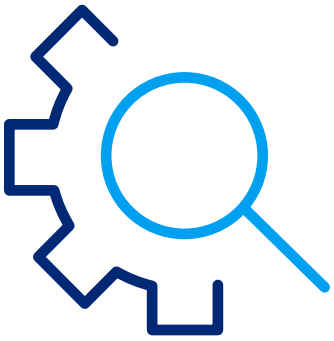

# eyeInspect

## Reducir riesgos en entornos de TO y de ICS, automatizar el cumplimiento y optimizar el análisis de amenazas

**Forescout eyeInspect** ofrece una vista general detallada de todos los dispositivos en las redes de TO/ICS y permite la mitigación efectiva de riesgos operativos y cibernéticos en tiempo real.

- Marco para los riesgos de los activos que permite determinar de forma exhaustiva la resiliencia de su red de TO.
- Total transparencia de dispositivos gracias al filtrado DPI (Deep Packet Inspection) o inspección profunda de paquetes) de más de 270 protocolos de red industriales y activos de línea basal
- Protección de la red con ayuda de miles de indicadores de amenazas específicos para TO y de una potente detección de anomalías

### Sin agentes

Inventariado consolidado en tiempo real de todos los dispositivos de TO e ICS conectados, con más de 30 técnicas de detección activas y pasivas.

### Preciso

Establecimiento de una línea basal de activos y protección de la red con ayuda de miles de indicadores de amenazas específicos para TO y de un potente detección de anomalías.

### Efectivo

Evaluación proactiva de riesgos, detección de amenazas, determinación de sus repercusiones en el negocio y rápida priorización de las medidas de remedio.

### Eficiente

Automatización de medidas que requieren tiempo relacionadas con el cumplimiento y la evaluación de riesgos, minimización de fallos humanos y mayor eficiencia.

### Visualizar

**Total transparencia de dispositivos mediante puertos SPAN y otras técnicas pasivas diversas, para garantizar una cobertura del 100 %**

**Análisis DPI (Deep Packet Inspection) patentados con más de 270 protocolos de TI y TO**

### Detectar

**Registro de información exhaustiva sobre los activos de TO; protocolización de todos los cambios de configuración para análisis de seguridad y exámenes forenses**

**Detección, contención y eliminación de amenazas con herramientas para el examen y el tratamiento de alertas**

### Responder

**Cumplimiento simplificado de estándares importantes como NERC CIP, Directiva NIS UE, NIST CSF, IEC 62aa3 y TSA Pipeline Security**

**Paneles de control (dashboards) para una cooperación más eficiente y detalles exhaustivos sobre alarmas para dar una respuesta efectiva a los incidentes**

## eyeInspect es la solución para:

- **la falta de transparencia en TO** debida a redes de dispositivos heterogéneos y dispersos geográficamente.
- **brechas en la defensa y riesgos de vulnerabilidades** cuando no se instalan parches o las aplicaciones están expuestas a amenazas.
- **riesgos operativos y cibernéticos** debido a la avalancha de alertas y la mala priorización de medidas de remedio.
- **información incompleta sobre amenazas,** que impide la ejecución de las directrices de protección.
- **tareas de cumplimiento,** que conllevan un gran esfuerzo y el riesgo de multas elevadas.

# Visualizar

**Visualizar miles de dispositivos en una sola vista**

- Registro preciso en tiempo real del inventario de activos con técnicas pasivas y sin interrumpir el funcionamiento de la empresa
- Visualización de dispositivos serie e IP, incluidos HMI, SCADA, SPS, sistemas de gestión y automatización de edificios (BMS y BAS, por sus siglas en inglés)
- Priorización de alertas y visualización de protocolos según diferentes parámetros, incluyendo tiempo, dispositivos, ubicación de la red y tipo de alarma

# Detectar

**Detección de amenazas y gestión de riesgos inteligente**

- Detección de ciberamenazas conocidas y desconocidas con ayuda de miles de comprobaciones específicas para TO/ICS e indicadores de compromiso (IOC, por sus siglas en inglés)
- Detección de riesgos operativos y cibernéticos; priorización según su urgencia y sus posibles repercusiones para el negocio
- Detección de infracciones de cumplimiento por parte de dispositivos y directrices en toda la red
- Detección en tiempo real de cambios en la red, incluyendo nuevos dispositivos, cambios en la infraestructura y actividades empresariales llamativas

# Responder

**Responder con rapidez con la solución de seguridad para TO más inteligente y escalable del mundo**

- Evaluaciones de riesgo comprensibles de forma intuitiva, que sirven de ayuda para tomar decisiones en la respuesta a amenazas operativas y cibernéticas
- Flujos de trabajo, reglas y medidas correctivas automatizadas para respuestas en tiempo real a las nuevas amenazas que surjan
- Respuesta a cambios de cumplimiento con ayuda de normas, parámetros e informes que se corresponden con las líneas basales de activos definidas

## Exigencias del Enterprise Command Center

| | DESCRIPCIÓN DEL PRODUCTO |
|---|---|
| **Hardware/Hypervisor** | Servidor en racks de 19 pulgadas o, como mínimo, VMware ESXi |
| **Procesador** | CPU de 4 núcleos (Intel®) de 64 bits > 2.4 GHz |
| **Capacidad de memoria** | 16-32 GB |
| **Disco duro** | > 250 GB |
| **Interfaz de red** | Interfaz para la comunicación con el centro de mando (Command Center) y acceso a aplicaciones web |

## Exigencias del Command Center

(*) El tamaño de la memoria de trabajo solo es válido para la licencia de eyeSight

| | Implementación pequeña (≤ 5 sensoren) | Implementación mediana (≤10 sensoren) | Implementación grande (>10 sensoren ≤100) |
|---|---|---|---|
| **Hypervisor** | Como mínimo, VMware ESXi 5 | | |
| **Factor de forma** | Servidor en racks de 19 pulgadas o dispositivos virtuales | | |
| **Procesador** | CPU de 4 núcleos de 64 bits | CPU de 4/6 núcleos (Intel) de 64 bits | CPU de 12 núcleos (Intel) de 64 bits |
| **Capacidad de memoria** | 16(*)-64 GB | 32(*)-64 GB | 64-256 GB |
| **Disco duro** | 500 GB | 1 TB | >1 TB |
| | (Con una conservación de datos de 90 días) | | |
| **Interfaz de red** | Interfaz para la comunicación con los sensores y acceso a aplicaciones web | | |

## Exigencias del sensor pasivo

| | Implementación pequeña (≤ 5 sensoren) | Implementación mediana (≤10 sensoren) | Implementación grande (>10 sensoren ≤100) |
|---|---|---|---|
| **Ejemplo de modelo de hardware** | Foxguard® IADIN-FS1 | Dell® Embedded PC 5000 | Dell® PowerEdge R640 |
| **Descripción de la implementación** | Implementación en redes pequeñas y en condiciones ambientales difíciles | Implementación en redes pequeñas, en condiciones ambientales difíciles | Implementación en redes grandes e instalaciones en un centro de computación |
| **Factor de forma** | Pequeño ordenador industrial/ montaje en rieles DIN | Ordenador industrial mediano | Servidor en racks de 19 pulgadas 1U |
| **Procesador** | CPU de 2 o 4 núcleos (Intel) de 64 bits | CPU de 4 o 6 núcleos (Intel) de 64 bits con 8 GT/s | CPU de 6 núcleos (Intel) de 64 bits > 2.4 GHz |
| **Capacidad de memoria** | 8-16 GB | 16-32 GB | 64-256 GB |
| **Disco duro** | 64-500 GB para ordenadores industriales (se deberían utilizar SSD con un amplio rango de temperatura) | | |
| **Interfaz de monitorización** | Hasta 4 puertos de monitorización | Hasta 8 puertos de monitorización | Hasta 8 puertos de monitorización |

## Exigencias del sensor activo

| INTEGRADO EN EL SENSOR PASIVO |
| --- |
| eyeInspect se puede integrar directamente en cualquier sensor pasivo para implementaciones pequeñas, medianas y grandes. |

| | Autónomo | Virtual |
| --- | --- | --- |
| **Procesador** | CPU de 2-4 núcleos | 4 vCPU |
| **Capacidad de memoria** | 4 GB RAM | 4 GB RAM |
| **Interfaz de red** | ≥ 1 | ≥ 1 |

Encontrará más información sobre las exigencias de hardware aquí: https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/

## Protocolos

Encontrará una lista completa de todos los protocolos estándar de TO, TI y TO de propietario en este enlace: https://www.forescout.com/company/resources/eyeinspect-protocols/

## Orquestar, segmentar, controlar

La plataforma de Forescout incrementa las utilidades de eyeInspect con una suite de productos para la elaboración e implementación de directrices y medidas automatizadas para la gestión de activos, la conformidad de dispositivos, los accesos a la red, la segmentación de la red y la respuesta a incidentes.

Para averiguar más sobre la plataforma de Forescout, visite www.forescout.com/platform/

FORESCOUT

**Forescout Technologies, Inc.**

Gratuita (EE. UU.) 1-866-377-8771
Tel. (internac.) +1-408-213-3191
Asistencia +1-708-237-6591

Descubra más en Forescout.com