FORESCOUT
Active Defense for the Enterprise of Things™

# eyeInspect

Antes SilentDefense™

## SIN AGENTE

Consiga en tiempo real un inventario de activos de OT completo y unificado para dispositivos conectados mediante IP y en serie.

## PRECISIÓN

Utilice una base de referencia para controlar sus activos y proteja su red con miles de indicadores de amenazas específicos para OT y una potente detección de anomalías basada en aprendizaje automático.

## EFECTIVIDAD

Evalúe de forma proactiva los riesgos, descubra las amenazas, mida el impacto en el negocio y priorice las tareas de corrección.

## FIABILIDAD

Tenga en tiempo real la certeza de que las herramientas de seguridad y los controles de cumplimiento funcionan.

## EFICIENCIA

Automatice las tareas de evaluación de riesgos y cumplimiento de normativas, que llevan mucho tiempo, mientras minimiza los errores humanos e incrementa la eficiencia.

# Reducción del riesgo, automatización del cumplimiento y optimización del análisis de amenazas para entornos de ICS y OT

Forescout eyeInspect ofrece visibilidad de los dispositivos en profundidad para redes de OT y permite abordar de manera eficaz y en tiempo real una gama completa de riesgos de ciberseguridad y operativos.

- Cree una base de referencia de comportamientos de red admisibles, utilizando miles de consultas e indicadores de amenazas específicos para ICS/OT.
- Agregue miles de alertas y millones de registros según su nivel de riesgo y su causa.
- Clasifique y evalúe automáticamente los dispositivos para garantizar el cumplimiento de normativas y directivas.

### VISUALIZACIÓN

Vea los dispositivos en el instante en que se conectan a la red.

Supervise continuamente la conexión y desconexión de los dispositivos.

Obtenga un inventario de activos en tiempo real, sin interrumpir la actividad empresarial.

### DETECCIÓN

Identifique distintos tipos de dispositivos de OT conectados por IP y en serie.

Cree una base de referencia para los dispositivos y grupos de dispositivos.

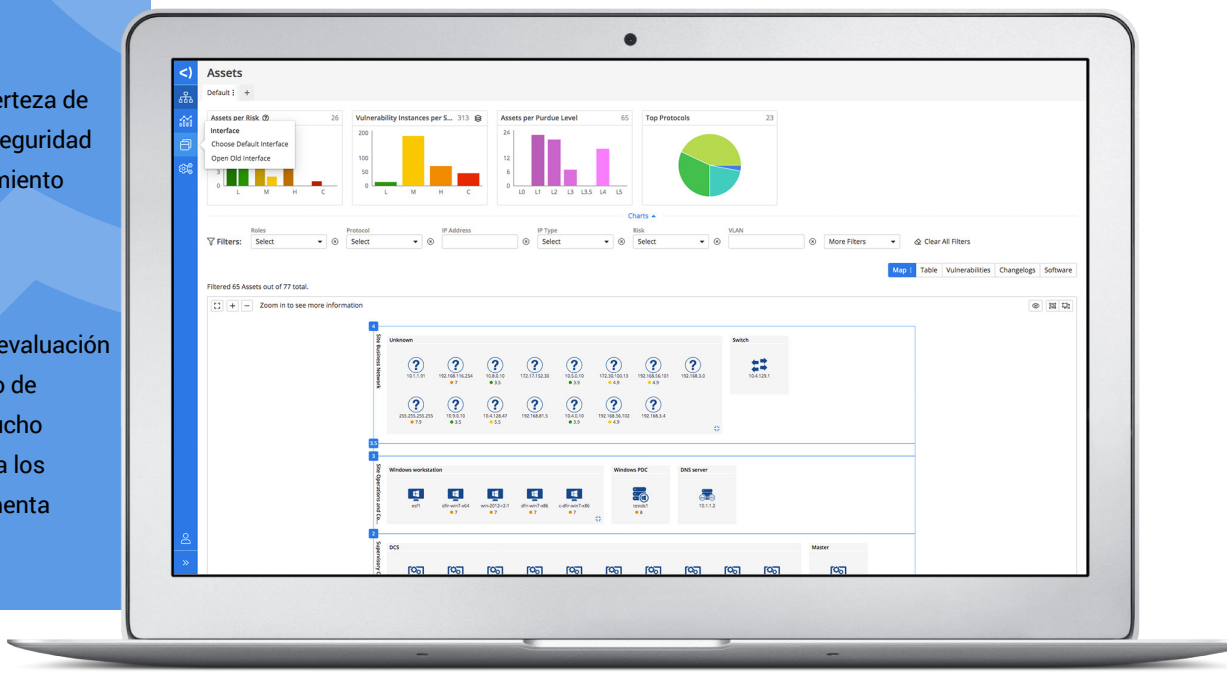
Optimice la eficacia de la clasificación automática y la supervisión continua.

### RESPUESTA

Automatice las evaluaciones de cumplimiento.

Evalúe el riesgo con calificaciones intuitivas.

Consiga información del estado de riesgo de ciberseguridad y operativo.



## VISUALIZACIÓN

### Visualice miles de dispositivos en una sola pantalla

- Véalo todo. Elimine los puntos ciegos asociados con dispositivos que se acaban de conectar o que no están autorizados.
- Obtenga un inventario de activos detallado, preciso y en tiempo real.
- Vea los dispositivos conectados por IP o en serie, como sistemas HMI, SCADA, PLC, controladoras, sensores, contadores y aparatos de E/S.

## DETECCIÓN

### Detecte las amenazas y gestione los riesgos de manera inteligente

- Detecte las ciberamenazas conocidas y desconocidas con miles de verificaciones e indicadores de riesgo específicos para ICS/OT.
- Detecte los riesgos operativos y cibernéticos, y asígneles una prioridad según el nivel de urgencia y su impacto potencial en el negocio.
- Detecte los dispositivos no conformes y las directivas que no se cumplen en toda la red.
- Detecte los cambios en la red, como la incorporación de nuevos dispositivos, las modificaciones n la infraestructura y toda actividad operativa irregular.

## RESPUESTA

### Responda con la solución de seguridad de OT más inteligente y escalable del mundo

- Responda a las ciberamenazas y las amenazas operativas según una calificación clara.
- Responda a las alertas con reglas, medidas de corrección y flujos de trabajo predefinidos y automatizados.
- Responda a los cambios relativos al cumplimiento con reglas, parámetros e informes definidos conforme a la base de referencia de activos.
- Vea los sistemas de administración de instalaciones (BMS) y los sistemas de automatización de edificios (BAS), incluidos los dispositivos HVAC y de control de acceso.
- Vea otras Infraestructuras de red físicas y definidas por software, como los conmutadores, routers, VPS, puntos de acceso inalámbrico y controladoras.
- Vea las alertas y registros, según distintos parámetros, como la hora, dispositivos, ubicación en la red y tipo de alerta.

## Requisitos de Enterprise Command Center

| Requisitos mínimos | |
|---|---|
| Hardware/Hipervisor | Servidor de 19 pulgadas o como mínimo VMware ESXi 5 |
| Procesador | CPU de 4 núcleos (Intel®), 64 bits ≥ 2,4 GHz |
| Tamaño de memoria | 16-32 GB |
| Unidad de disco duro | > 250 GB |
| Interfaz de red | Interfaz para la comunicación con el Command Center y el acceso a aplicaciones web |

## Requisitos de Command Center

| | Despliegue pequeño | Despliegue mediano (≤10 sensores) | Despliegue grande (>10 sensores ≤100) |
|---|---|---|---|
| Hipervisor | Mínimo VMware ESXi5 | | |
| Factor de forma | Servidor de 19 pulgadas o dispositivo virtual | | |
| Procesador | CPU de 4 núcleos, 64 bits | CPU de 4/6 núcleos (Intel), 64 bits | CPU de 12 núcleos (Intel), 64 bits ≥ 2,4 GHz |
| Tamaño de memoria | 16(*)-64 GB | 32(*)-64 GB | 64-256 GB |
| Unidad de disco duro | 500 GB | 1 TB | >1 TB |
| | (Basado en la retención de datos de 90 días) | | |
| Interfaz de red | Interfaz para la comunicación con el sensor y el acceso a aplicaciones web | | |

*(*) tamaño de memoria solamente para la licencia de eyesight*

## Requisitos del sensor pasivo

| | Piccola distribuzione (fino a 100 Mb/s) | Media distribuzione (fino a 500 Mb/s) | Grande distribuzione (fino a 1 Gb/s) |
|---|---|---|---|
| Modelo de hardware de ejemplo | Foxguard® IADIN-FS1 | Dell® Embedded PC 5000 | Dell® PowerEdge R640 |
| Descripción del despliegue | Despliegues en redes pequeñas y entornos difíciles | Despliegues en redes medianas y entornos difíciles | Despliegues en redes grandes e instalaciones de centros de datos |
| Factor de forma | PC en riel DIN industrial de tamaño pequeño | PC industrial de tamaño mediano | Servidor en bastidor 1U de 19 pulgadas |
| Procesador | CPU de 2/4 núcleos (Intel), 64 bits | CPU de 4/6 núcleos (Intel), 64 bits, 8 GT/s | CPU de 6 núcleos (Intel), 64 bits ≥ 2,4 GHz |
| Tamaño de memoria | 8-16 GB | 16-32 GB | 64-256 GB |
| Unidad de disco duro | 64 GB – 500 GB en PC industriales (deben usarse SSD que admiten alta temperatura) | | |
| Interfaz de supervisión | Hasta 4 puertos de supervisión | Hasta 8 puertos de supervisión | Hasta 8 puertos de supervisión |

## Requisitos mínimos de Active Sensor

| Integrado con sensor pasivo |
|---|
| eyeInspect puede integrarse directamente en cualquier sensor pasivo para despliegues pequeños, medianos y grandes. |

| | Autonomo | Virtuale |
|---|---|---|
| Procesador | CPU de 2/4 núcleos | 4 vCPU |
| Tamaño de memoria | 4 GB RAM | 4 GB RAM |
| Interfaz de red | ≥ 1 | ≥ 1 |
| Unidad de disco duro | 50 GB | |

Para obtener más información sobre los requisitos de hardware, consultar: https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/

## PROTOCOLOS

Encontrará una lista completa de todos los protocolos de sistemas estándar de OT e IT, y OT propietarios en: https://www.forescout.com/company/resources/eyeinspect-protocols/

## ORGANIZACIÓN, SEGMENTACION Y CONTROL

Forescout amplía el valor de eyeInspect y la plataforma Forescout con una suite de productos para diseñar e implementar directivas y acciones automatizadas para la gestión de activos, el cumplimiento de normativas para dispositivos, el acceso a la red, la segmentación de la red y la respuesta ante incidentes. Visite www.forescout.com/platform/ para descubrir los productos Forescout eyeSight, eyeSegment, eyeControl, eyeManage y eyeInspect.

## eyeINSPECT SOLUCIONA LOS PROBLEMAS RELATIVOS A:

**Lagunas de visibilidad de OT** provocadas por redes de dispositivos distribuidos geográficamente y no homogéneas.

**Protección y vulnerabilidad** cuando no se aplican los parches y se dejan las aplicaciones desprotegidas.

**Riesgo de ciberseguridad y operativo** debido a una sobrecarga de alertas y a una priorización inadecuada de las tareas de corrección.

**Inteligencia de amenazas incompleta** que dificulta la ejecución de directivas de defensa.

**Cumplimiento de normativas** que requiere muchos recursos y expone a su empresa a riesgos de multas importantes.

# No se conforme con verlo. Protéjalo.

Póngase en contacto con nosotros hoy mismo para proteger su Empresa de las cosas.

forescout.com/platform/eyeInspect info-espana@forescout.com Tel. (internacional) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San José, CA 95134 EE. UU.

C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Soporte técnico +1-708-237-6591

Más información en Forescouttechnologies.es