FORESCOUT
Active Defense for the Enterprise of Things™

Segmentación Zero Trust simple y sin interrupciones para entornos de OT

Proteja con garantías las redes de OT ampliadas con gestión de riesgos y segmentación dinámica avanzadas

Los enfoques tradicionales de protección de dispositivos OT (tecnología operativa) en redes de OT/ICS han dependido desde hace mucho tiempo de garantizar la separación de las aplicaciones de las redes de IT y los usuarios con acceso remoto. Sin embargo, a medida que las organizaciones de OT modernizan su infraestructura con nuevas tecnologías, como Cloud SCADA, DCS (Sistemas de control distribuido) y MES (Sistemas de ejecución de fabricación) avanzado, las estrategias tradicionales de división por zonas ya no bastan para mantener protegidos los entornos de OT.

A continuación se incluyen los retos para los entornos de OT:

- Riesgo de desplazamiento lateral del malware y los ciberdelincuentes, amenazas interzonales procedentes de entornos de IT, y usuarios remotos que afecten a la infraestructura ciberfísica y de OT.
- Detección y mitigación de la propagación del malware y las amenazas interzonales que afectan a la infraestructura ciberfísica y de OT.
- Complejidad operativa por el hecho de tener varios proveedores e incoherencia en los controles de segmentación en entornos de OT ampliados.

La solución de Forescout: la mejor para entornos de OT

Si estos problemas le resultan familiares, ahora es un momento extraordinario para evaluar la solución de Forescout. Esta solución ayuda a simplificar la segmentación Zero Trust y a optimizar la gestión de riesgos en cuanto a los dispositivos IT, OT e ICS en su Enterprise of Things (EoT) heterogénea.

"Para 2021, el 80 % de los proyectos del IoT industrial (IIoT) tendrán requisitos de seguridad específicos de la tecnología operativa (TO), frente al 40 % actual"[1].

GARTNER

"Las tecnologías de dispositivos IoT y de conexión a redes han introducido un riesgo potencial en redes y empresas. Los equipos encargados de la seguridad deben aislar, proteger y controlar cada uno de los dispositivos de las redes, continuamente"[2].

FORRESTER RESEARCH

Con la plataforma Forescout puede:

- **Acelere la segmentación Zero Trust** en los grupos de IT y OT.
- **Conozca de forma instantánea el estado de segmentación de los entornos de IT-OT** en tiempo real y en cualquier dispositivo o lugar del entorno ampliado.
- **Visualice los flujos de tráfico** en función de la taxonomía lógica de usuarios, aplicaciones, servicios, funciones, ubicaciones, dispositivos y nivel de riesgo.
- **Reduzca la superficie de ataque y garantice el cumplimiento de normativas** mediante la segmentación dinámica en entornos de IT, IoT y OT.
- **Optimice los flujos de trabajo de IT-OT** y aproveche las inversiones actuales con una política de segmentación coherente en toda la empresa.
- **Reduzca el riesgo de incumplimiento y limite el coste gestionando el acceso entre redes de forma eficiente**, y con menos personal.

“Casi el 20 % de las empresas han observado al menos un ataque basado en el Internet de las cosas (IoT) en los tres últimos años”[3].

GARTNER

Gestión de riesgos y segmentación Zero Trust optimizadas para redes de IT-OT

La solución de Forescout proporciona una visibilidad de dispositivos en profundidad para redes de OT y permite la gestión eficaz y en tiempo real de un amplio espectro de riesgos operativos y de ciberseguridad. La solución responde a los retos de las empresas en cuanto a segmentación con varios dominios y casos de uso, y de mitigación de riesgos en los entornos de OT ampliados para acelerar la detección y respuesta a amenazas sin interrupciones.

Forescout eyeSegment le ayuda a diseñar y desplegar segmentación Zero Trust mediante la asignación automática de los flujos de tráfico a una taxonomía lógica de usuarios, aplicaciones, servicios, funciones, ubicaciones, dispositivos y niveles de riesgo en la toda red empresarial. Esto hace posible la creación de una línea base de tráfico de OT en tiempo real, sin desplegar agentes ni rediseñar la arquitectura. Además, le permite determinar el impacto de las directivas de segmentación antes de aplicarlas.

AMPLÍE EL VALOR DE SUS INVERSIONES EN SEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

- Responda al riesgo que presenta la convergencia de IT-OT (desplazamiento lateral) con un enfoque unificado de directivas de segmentación.
- Responda el riesgo relacionado con los dispositivos de OT con la planificación de directivas de segmentación granulares, la supervisión y la respuesta.
- Permita la segmentación dinámica y sin interrupciones para entornos de OT sensibles, aprovechando la inversión (infraestructura) existente.

Forescout eyeInspect (antes SilentDefense) protege la infraestructura crítica con inspección profunda de paquetes patentada y una enorme biblioteca de indicadores de amenazas específicas para ICS. eyeInspect supervisa las comunicaciones de red en tiempo real y proporciona información contextual detallada sobre activos de red, protocolos y contenido de las comunicaciones. Gracias a sus potentes funciones, como la agregación de alertas avanzada y la creación de una línea de base de activos, puede automatizar las tareas de detección de amenazas y cumplimiento de normativas que reducen el riesgo y contribuyen a la aplicación de la segmentación de OT.

Figura 1. La matriz de eyeSegment le permite centrarse en lo que es importante para que pueda analizar e investigar un patrón de tráfico concreto en su entorno. No importa dónde esté en la jerarquía de la matriz, puede crear de manera instantánea las directivas de eyeSegment deseadas para segmentar un patrón de tráfico específico y proteger su empresa al tiempo que garantiza la continuidad de la producción y de la actividad empresarial.

La solución de segmentación de la red de Forescout resuelve una amplia variedad de casos de uso de OT. En todos ellos, la flexibilidad de la plataforma Forescout ayuda a reducir el riesgo de interrupción de la actividad y minimiza los costes operativos asociados a los proyectos de segmentación. Estos son algunos casos de uso habituales:

- Mitigar el riesgo, garantizar el cumplimiento de normativas y reducir los costes operativos de las redes de OT.
- Conseguir visibilidad inmediata de los entornos de OT en tiempo real para crear directivas de segmentación que no generen interrupciones.
- Acelerar la segmentación Zero Trust de los entornos de IT-OT.

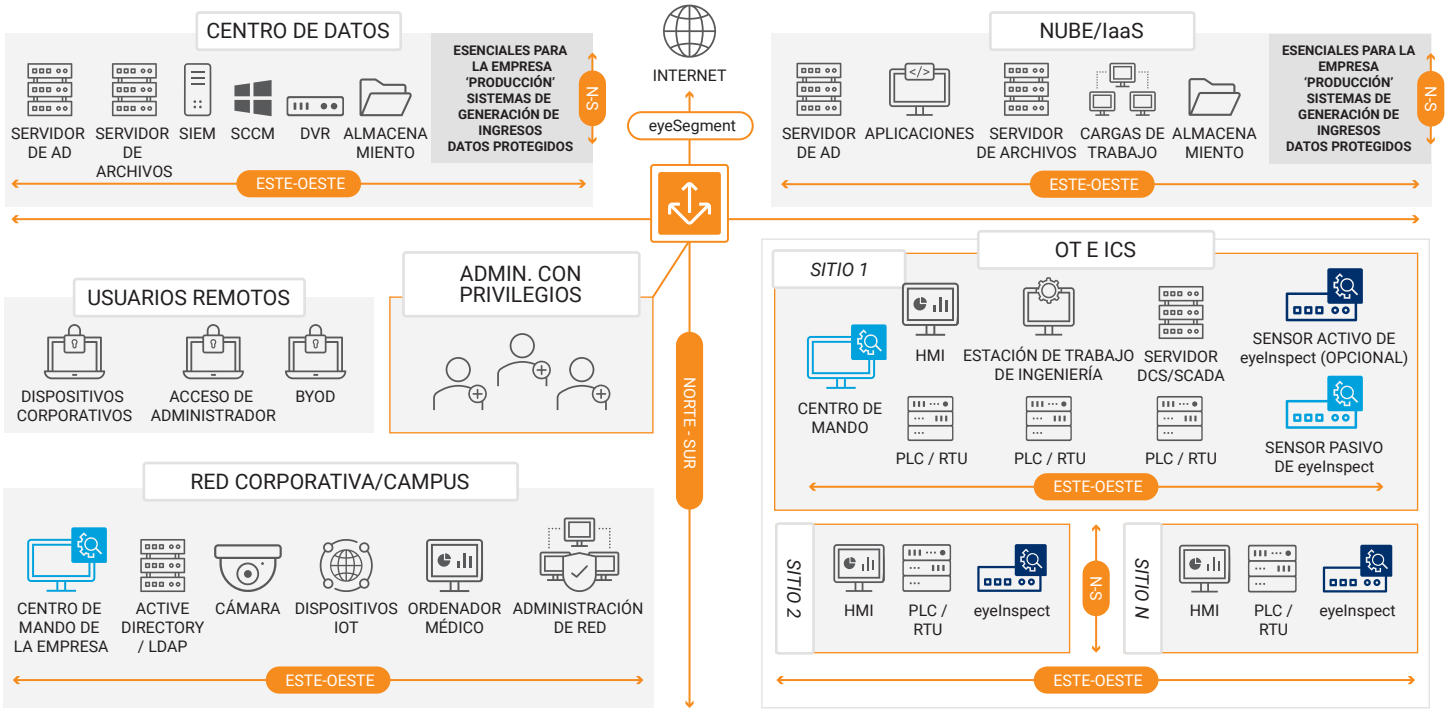

Figura 2. La solución de Forescout puede ayudarle a mitigar las amenazas y conocer de forma instantánea su estado de segmentación en tiempo real. En el ejemplo anterior, eyeSegment mantiene conectados los dispositivos de distintos dominios en el sector sanitario y de IT-OT.

1. Invest Implications: 'Cool Vendors in Industrial IoT and OT Security, Gartner Research, abril de 2018
2. Mitigating Ransomware With Zero Trust, Forrester Research, Inc., 8 de junio de 2020
3. IoT Security Primer: Challenges and Emerging Practices, Gartner, enero de 2020

No se conforme con verlo. Protéjalo.

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

forescout.com/platform/eyeSegment 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