Forescout eyeSegment

Diseñe, cree y despliegue la segmentación de la red con confianza y a escala

Forescout eyeSegment acelera el diseño, la planificación y el despliegue de la segmentación dinámica de la red, en toda la empresa ampliada. Simplifica el proceso de creación de directivas de segmentación con contexto y permite la visualización y la simulación de las directivas antes de aplicarlas, para poder ajustarlas y validarlas de manera proactiva.

eyeSegment amplía las funciones de la plataforma Forescout para dar respuesta a los retos de la segmentación con varios dominios y varios casos de uso. Esta solución permite a las empresas adoptar los principios del modelo de seguridad Zero Trust para todos los sistemas conectados por IP, como los dispositivos del Internet de las cosas (IoT) y las tecnologías operativas (OT). El resultado es una rápida aceleración de los proyectos de segmentación en toda la empresa para reducir la superficie de ataque, limitar la propagación lateral y la onda expansiva, y mitigar el riesgo de incumplimiento de normativas corporativas y oficiales.

Problemas

- Falta de confianza para avanzar en proyectos de segmentación.
- Riesgo de exposición debido al potencial de desplazamiento lateral de las amenazas en redes planas.
- Contexto incompleto de dispositivos, aplicaciones y usuarios.
- Crecimiento descontrolado de las directivas e incapacidad para implementar de manera coherente los controles en tecnologías diferentes.
- Complejidad operativa por el hecho de tener varios proveedores e incoherencia en los controles de segmentación en distintos dominios de red.
- Falta de profesionales cualificados, recursos y herramientas para diseñar, crear y desplegar con eficacia la segmentación de la red, en toda la empresa ampliada.

eyeSegment

Ventajas

- Acelerar los proyectos de segmentación de la red con confianza.
- Determinar de manera proactiva el impacto de las directivas para minimizar las interrupciones de la actividad empresarial.
- Reducir el riesgo de interrupción de la actividad.
- Implementar de manera uniforme el control de tecnologías de implementación y dominios de red diferentes a través de un solo marco de directivas.
- Adaptarse a los requisitos de cumplimiento y normativas oficiales.
- Reducir la complejidad operativa de los proyectos de segmentación.
- Poner en práctica un modelo de seguridad Zero Trust (Confianza Cero) para implementar controles de seguridad granulares.

Funciones principales

- Cree directivas de segmentación que tengan en cuenta el contexto mediante una taxonomía empresarial lógica de usuarios, apps, servicios y dispositivos.
- Conozca rápidamente el impacto antes de aplicar las directivas de segmentación.
- Supervise y valide continuamente la higiene de segmentación.
- Responda con rapidez a las infracciones de las directivas de segmentación en toda la empresa.

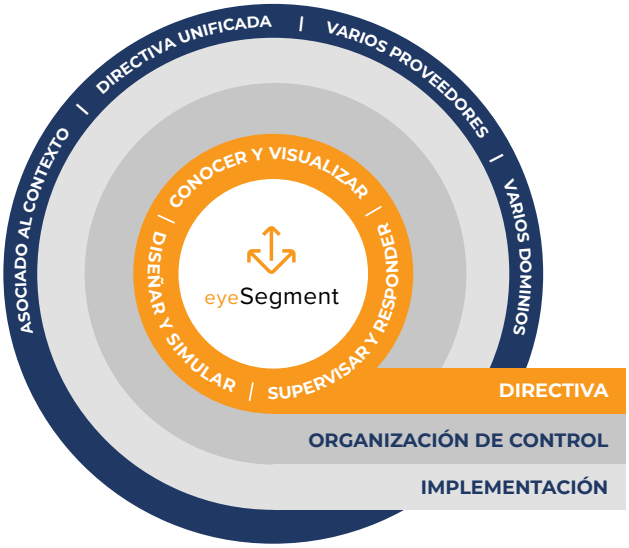

Figura 1: Forescout recomienda utilizar una arquitectura de tres capas para la segmentación de la red en toda la empresa, comenzando por una "capa de directivas" que hace uso de eyeSegment.

Transformación de la segmentación de la red en toda la empresa

Forescout eyeSegment aprovecha la visibilidad integral de los dispositivos y el contexto detallado en tiempo real que proporciona Forescout eyeSight. Esta solución permite visualizar los flujos de tráfico y las dependencias entre usuarios, aplicaciones, servicios y dispositivos y, a continuación, diseñar, simular y supervisar las directivas para conocer el impacto que tienen en su entorno. A través de Forescout eyeControl y eyeExtend, las directivas se organizan en varios puntos de implementación de segmentación en redes de campus, centros de datos y la nube. eyeSegment ayuda a las empresas a diseñar, crear y desplegar la segmentación de la red a escala para poder aplicarla a toda la empresa.

Conozca y visualice los flujos de tráfico

Forescout eyeSegment asigna automáticamente los flujos de tráfico a una taxonomía lógica de usuarios, aplicaciones, servicios y dispositivos en la red empresarial completa, sin desplegar agentes. De esta forma, le permite supervisar el tráfico de su red en tiempo real y crear directivas de segmentación granulares con información del contexto. Un uso típico sería diseñar controles para asegurarse de que solo los empleados del departamento financiero tengan acceso a las aplicaciones de pago que se utilizan en distintos dominios. Otro sería determinar los servicios comunes que necesitan los dispositivos médicos que tienen sistemas operativos obsoletos y, a continuación, separarlos.

La tabla de conectividad de eyeSegment (Figura 2) ayuda a visualizar los flujos de tráfico. Crea una línea base de tráfico, mantiene los datos de tráfico a lo largo del tiempo y muestra los flujos en tiempo real entre las zonas de origen y destino, tal y como se define en la directiva de segmentación.

Figura 2: Tabla de conectividad de eyeSegment que muestra los flujos de tráfico lógicos de la empresa.

Diseñe y simule las directivas de segmentación

Forescout eyeSegment le ayuda a diseñar, crear y ajustar directivas de segmentación eficaces basadas en una taxonomía empresarial lógica que pueda aplicarse en las tecnologías subyacentes existentes. Puede simular de forma proactiva la implementación de las directivas antes de ponerlas en práctica en el entorno, minimizando así la posibilidad de que se interrumpa la actividad empresarial.

Cree directivas de segmentación unificadas y granulares

Una directiva de segmentación es un grupo de reglas para permitir todo el tráfico, denegar todo el tráfico o permitir solamente determinado tráfico entre zonas de origen y destino específicas. Las zonas se basan en grupos de directivas estándar que pueden indicarse de forma manual o bien a través de una directiva. Las direcciones IP únicas y los objetos de segmentos de Forescout que son grupos también pueden ser zonas. Cada zona de segmentación puede designarse como zona de origen, zona de destino o ambas.

Puede crear directivas de segmentación desde una sola consola para denegar o autorizar de forma explícita determinado tráfico a través de distintas tecnologías y dominios de red. Cada directiva puede aplicarse a tráfico de una zona de origen concreta a una zona de destino determinada. De forma predeterminada, se autoriza todo el tráfico desde una zona de origen cualquiera a una zona de destino cualquiera. La directiva y sus excepciones determinan qué tráfico se permite y qué tráfico se deniega. Así puede definir distintas acciones para subgrupos y servicios.

Visualice las directivas y las dependencias de tráfico

La visualización de directivas y las dependencias de tráfico permiten observar las directivas de segmentación creadas y su estado en la tabla de conectividad, como se muestra a continuación. Las funciones de filtrado permiten ir a una directiva concreta para filtrar el tráfico por servicio y/o la intersección de zonas de la tabla con filtro de origen y destino.

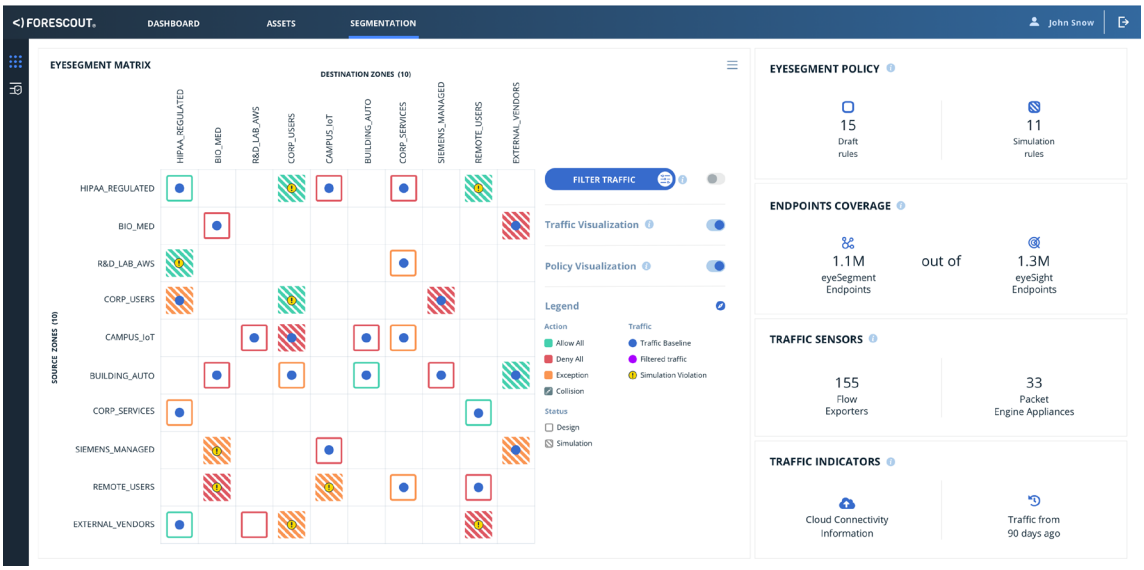

Figura 3: Visualización de directivas y simulación.

Supervise y responda

La administración de directivas unificada y el panel único de eyeSegment le permiten supervisar de forma centralizada los flujos de tráfico entre las zonas de origen y destino. La posibilidad de supervisar de manera continua y responder a las directivas de segmentación abstraídas de los controles subyacentes puede ser importante como paso gradual para el control, o cuando el control de una infraestructura no está disponible. eyeSegment también ayuda a supervisar de forma continua los controles de la infraestructura empresarial y a garantizar que se implementen controles de segmentación y que funcionen con eficacia tras aplicar los controles en toda la empresa.

Casos de uso

La plataforma Forescout responde a muy diversos casos de uso de segmentación de la red. 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:

Protección de aplicaciones empresariales fundamentales	• Proteger las aplicaciones esenciales para la empresa, asegurarse de que los controles se implementan de manera eficaz y supervisar para garantizar una protección continua. Mantener controles de servicios dentro de la empresa y entre empresas, a través de distintos servicios, aplicaciones y dominios • Controlar el acceso del usuario a servicios esenciales de la empresa en distintos dominios. Proteger las aplicaciones esenciales frente a un uso inadecuado por parte de los usuarios, asegurarse de que los controles se implementan de manera eficaz y supervisar para garantizar una protección continua
Implementar acceso a la infraestructura de IT crítica en función de privilegios	• Limitar el acceso de administrador de IT a dispositivos confidenciales de la red (conmutadores, NGFW, etc.) y cargas de trabajo de centros de datos/nube (Active Directory/LDAP, Domain Name System, Oracle Cluster, etc.) en función de administradores definidos (según la función), el estado del endpoint de administración de IT (cifrado, incorporado a un dominio, etc.) y la comunicación segura (puerto/servicio específico)
Protección de dispositivos de IoT/OT de la empresa (impresoras, cámaras, VoIP, lectores de tarjetas, HVAC, etc.)	• Proteger la red de IT de los dispositivos de IoT/OT • Proteger los dispositivos de IoT/OT frente a ataques
Garantía de segmentación en toda la empresa	• Asegurarse de que todos los puntos de implementación de diferentes dominios (campus, centros de datos e IoT), gestionados por otros equipos, cumplen los requisitos de las directivas de segmentación y están configurados como deben
Contención de dispositivos vulnerables	• Limitar el acceso entre (desde y hacia) dispositivos vulnerables (WannaCry, sin parches, fin de vida, etc.) y el resto de la red
Protección de dispositivos con aplicaciones/sistemas operativos obsoletos	• Reducir la superficie de ataque separando los dispositivos que tienen instalados sistemas operativos y aplicaciones obsoletos • Mitigar el riesgo de amenazas a los dispositivos que utilizan sistemas operativos antiguos

FORESCOUT

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 Forescout.com