FORESCOUT
Active Defense for the Enterprise of Things™

eyeControl

Implementación de controles basados en directivas

SIN INTERRUPCIONES

Despliegue flexible y variedad de opciones de control de acceso, con o sin autenticación 802.1X.

SIN AGENTES

Evaluación de la higiene de dispositivos y corrección automática de los dispositivos para garantizar el cumplimiento, sin agentes.

CON EFICACIA

Motor de directivas unificado para implementar un acceso seguro Zero Trust.

SIN ACTUALIZACIONES

Utiliza la infraestructura existente y no requiere actualizaciones de software o hardware.

MENOR COSTE TOTAL DE PROPIEDAD

Solución flexible, sin interrupciones, sin agentes y compatible con varios proveedores, que reduce los costes operativos, de despliegue y de mantenimiento. Rentabilidad de la inversión más rápida.

Implemente y automatice medidas de control para el Enterprise of Things en redes heterogéneas

Forescout eyeControl ofrece el control de acceso a la red más flexible y con menos interrupciones para las redes empresariales heterogéneas. Aplica y automatiza directivas Zero Trust para el acceso con el mínimo de privilegios para todos los dispositivos gestionados y no gestionados del Enterprise of Things (EoT). Se pueden aplicar controles basados en directivas para formar el cumplimiento de normativas en los dispositivos, reducir su superficie de ataque de forma proactiva y responder rápidamente a los incidentes.

ACCESO SEGURO A LA RED

Implementación del acceso a la red según el usuario, identidad del dispositivo y estado

Despliegue con o sin autenticación 802.1X en redes heterogéneas

GARANTÍA DE CUMPLIMIENTO PARA DISPOSITIVOS

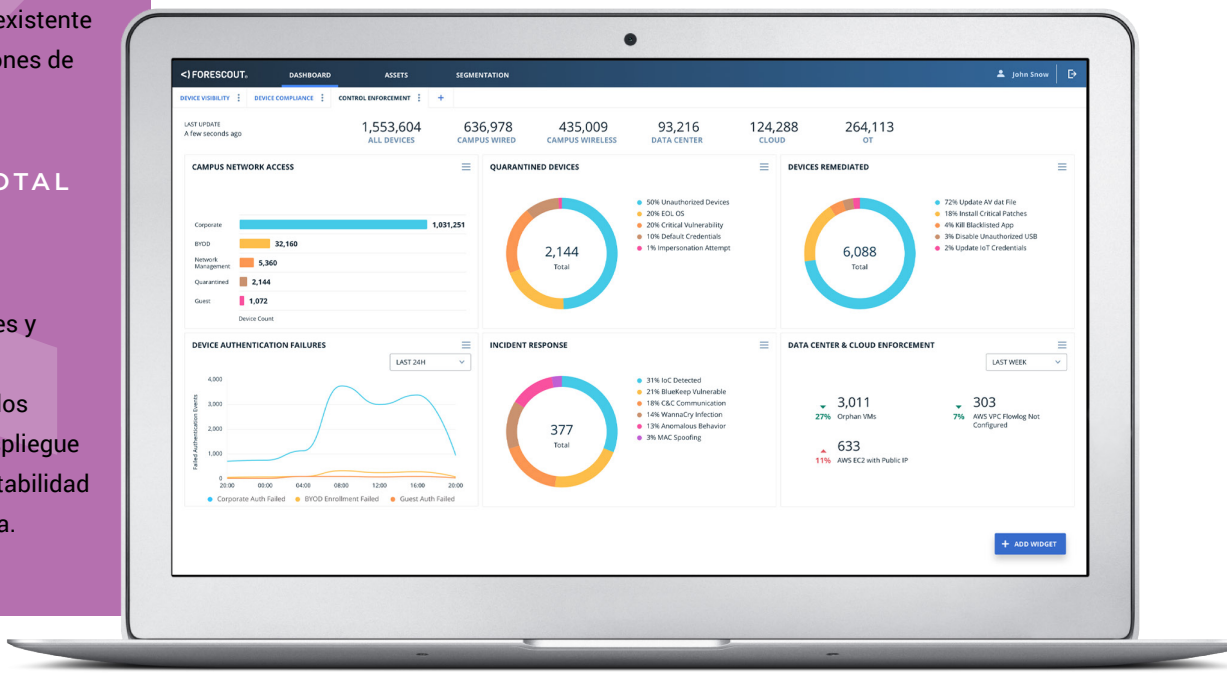
Cumplimiento de directivas, normativas y reglamentos de seguridad

Inicio de flujos de trabajo de corrección y mitigación de riesgos

AUTOMATIZACIÓN DE RESPUESTA A INCIDENTES

Automatización de respuesta a incidentes de seguridad

Contención de amenazas para minimizar la propagación y la interrupción



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

AUTOMATIZACIÓN DE CONTROLES CON CONFIANZA

Las directivas Zero Trust solo pueden aplicarse sobre la base de un contexto de dispositivos completo. Esto incluye conocimiento en tiempo real de la identidad del usuario y el dispositivo, el estado de seguridad y el perfil de riesgo de todos los dispositivos que se conecten. Los controles que se implementan sin visibilidad total pueden interrumpir la actividad y poner las operaciones en riesgo. eyeControl utiliza amplio contexto de dispositivos procedente de eyeSight para aplicar los controles Zero Trust con confianza.

En la base de eyeControl hay un motor de directivas intuitivo y flexible que le permite aplicar controles granulares y selectivos. Este motor de directivas Zero Trust proporciona:

- Agrupación dinámica y evaluación de dispositivos mediante lógica empresarial y contexto de los dispositivos
- Condiciones y acciones combinadas mediante lógica booleana y directivas en cascada para implementar flujos de trabajo de control sofisticados
- Gráfica de directivas para la creación de directivas precisa, el análisis del flujo de directivas y su ajuste, antes de activar las medidas de implementación
- Capacidad para empezar con acciones de control iniciadas manualmente y aplicar lentamente la automatización para aumentar la eficacia de las operaciones de seguridad

Las directivas se activan y evalúan automáticamente en tiempo real con los eventos y cambios que se producen en un dispositivo determinado o en la red. La Figura 1 muestra la gama de acciones de control disponibles en eyeControl cuando se activa una directiva.

MODERADO		ESTRICTO
Red		**Red**
Trasladar a la red de invitados		Poner el dispositivo en cuarentena (VLAN, firewall virtual)
Cambiar la función del usuario inalámbrico		Desactivar el puerto de conmutación
Asignar a la VLAN de autocorrección		Bloquear el acceso inalámbrico o VPN
Limitar la infraestructura o los dispositivos no autorizados		Utilizar listas de control de acceso (ACL) para limitar el acceso
Host		**Host**
Iniciar aplicaciones y procesos obligatorios		Cerrar las aplicaciones no autorizadas
Actualizar antivirus/agentes de seguridad		Desactivar NIC/doble conectividad de red (dual-homing)
Aplicar actualizaciones/parches del SO		Desactivar dispositivos periféricos
Cumplimiento para unidades externas		Activar medidas/sistemas de corrección

AUTOMATIZACIÓN DEL CONTROL BASADO EN DIRECTIVAS

Figura 1. Implementación de directivas en la red y los endpoints, incrementando la automatización progresivamente.

CONTROL

Acceso seguro a la red

eyeControl proporciona la solución de control de acceso a la red más flexible, heterogénea y sin interrupciones para las organizaciones. Con eyeControl, puede aplicar el acceso seguro a las redes cableadas e inalámbricas para todos los sistemas de EoT gestionados o no gestionados, cumplir los requisitos de auditoría, reducir la superficie de ataque y mitigar rápidamente las amenazas. Incluye las siguientes funciones:

- Provisión de acceso a la red Zero Trust para dispositivos de empleados, invitados, contratistas y BYOD
- Identificación y bloqueo de dispositivos no fiables, no autorizados, de TI en la sombra y que suplantan dispositivos legítimos
- Puesta en cuarentena y aislamiento de dispositivos no conformes y de alto riesgo hasta que se aplique la corrección
- Amplia variedad de métodos de control de acceso, con o sin autenticación 802.1X
- Incorporación de evaluación de estado sin agente y aplicación de acciones a redes y endpoints a través del motor de directivas Zero Trust unificado
- Interoperatividad con la infraestructura existente y no requiere actualizaciones de software/hardware.
- Integración directa con más de 30 proveedores de infraestructura de red en cientos de modelos de productos

CUMPLIMIENTO

Garantía de cumplimiento para dispositivos

Automatización de la evaluación del estado de seguridad e implementación de controles de reparación con el fin de garantizar un cumplimiento continuo de directivas de seguridad internas, reglamentos externos y normativas del sector.

- Asegúrese de que los endpoints están configurados correctamente e inicie la reparación de problemas de configuración graves
- Identifique y repare los dispositivos gestionados con agentes de seguridad dañados o no presentes

eyeControl DETECTA:

Los dispositivos **no autorizados, no fiables o de suplantación** en la red, que suponen riesgos y problemas de cumplimiento de normativas.

Brechas de seguridad cuando las herramientas basadas en agentes no están actualizadas o funcionando correctamente.

Redes homogéneas y sin segmentar que hacen que las empresas sean vulnerables a las amenazas y aumentan el radio de acción.

Riesgos de interrupción de la actividad debido a la existencia de dispositivos vulnerables, aplicaciones no autorizadas o falta de parches críticos.

Propagación lateral de las amenazas debido a la incapacidad para contener rápidamente los dispositivos comprometidos o maliciosos.

Incumplimiento por la incapacidad para aplicar y supervisar continuamente el estado de los dispositivos conectados.

Problemas de implementación NAC en entornos heterogéneos y multiproveedor, y redes cableadas.

- Detección y desactivación de las aplicaciones no autorizadas que introducen riesgos, afectan al ancho de banda de la red o reducen la productividad.
- Identificación de dispositivos con vulnerabilidades de alto riesgo y ausencia de parches críticos, e inicio de las medidas necesarias para repararlos.
- Implementación de acciones de reparación y mitigación de riesgos en dispositivos Windows, Mac, Linux, IoT y OT
- Implementación de directivas y automatización de controles de la idoneidad de la configuración en despliegues en la nube, como AWS, Azure y VMware.

AUTOMATIZAR

Aceleración de la respuesta a incidentes

- Contención de las amenazas y respuesta a incidentes de seguridad de forma rápida y eficaz, para minimizar las interrupciones de las operaciones y daños en la empresa. Automatice las tareas de respuesta a incidentes básicas y repetitivas, y libere recursos especializados para que se centren en problemas y prioridades de mayor impacto.
- Identificación de los indicadores de riesgo (IoC) en los dispositivos en el momento de la conexión, con el fin de reducir el tiempo medio de respuesta.
- Aislamiento y contención rápidos de los dispositivos comprometidos o maliciosos para evitar la propagación lateral del malware.
- Automatización de la respuesta ante incidentes e inicio de flujos de trabajo de reparación en dispositivos comprometidos.
- Reducción del tiempo medio de respuesta proporcionando a los equipos interdisciplinares de respuesta a incidentes información práctica del contexto de los dispositivos (conexión, ubicación, clasificación y nivel de seguridad del dispositivo).

No se conforme con verlo. Protéjalo.

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

forescout.com/platform/eyeControl 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