eyeControl

Implementación de controles basados en políticas

Implemente y automatice acciones de control en redes heterogéneas

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

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

Eficaz
Motor de políticas unificado para implementar el acceso a la red de Zero Trust.

Sin actualizaciones
Se integra perfectamente en la infraestructura existente sin necesidad de actualizaciones de software o hardware.

Menor costo de propiedad
La reducción de los costos de despliegue, mantenimiento y funcionamiento se traduce en un retorno de la inversión más rápido.

Forescout eyeControl brinda un control de acceso a la red flexible y con menos interrupciones para redes empresariales heterogéneas. Aplica y automatiza políticas de seguridad de Zero Trust para el acceso con menos privilegios a todos los activos administrados y no administrados en todo el terreno digital. Los controles basados en políticas pueden imponer continuamente el cumplimiento de los activos, reducir la 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 la postura de seguridad
- Despliegue con o sin autenticación 802.1X en redes heterogéneas

Garantía de cumplimiento para dispositivos

- Automatización del cumplimiento de las políticas de seguridad, las normas del sector y normativas gubernamentales
- Inicio de flujos de trabajo de corrección y mitigación de riesgos en tiempo real

Automatización de respuesta a incidentes

- Automatiza la respuesta a los incidentes de seguridad
- Contención de amenazas para minimizar la propagación y la interrupción

Automatización de controles con confianza

Las políticas 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 usa un amplio contexto de dispositivos procedente de eyeSight para aplicar y automatizar los controles de seguridad Zero Trust con confianza.

En la base de eyeControl hay un motor de políticas unificado y flexible que le permite aplicar controles granulares y específicos. Este motor unificado de políticas proporciona:

- Agrupación dinámica y evaluación de dispositivos por lógica empresarial y contexto.
- Condiciones y acciones combinadas mediante lógica booleana y políticas en cascada para implementar sofisticados flujos de trabajo de control.
- Gráficos de políticas para la creación precisa de políticas, el análisis del flujo de políticas 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 políticas se activan y evalúan 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 política.

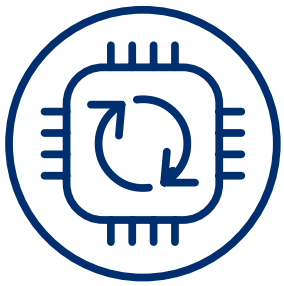
Moderado

Red

- Trasladar a la red de invitados
- Cambiar el rol del usuario inalámbrico
- Asignar a VLAN de autocorrección
- Limitar la infraestructura o dispositivos no autorizados

Host

- Iniciar aplicaciones y procesos obligatorios
- Actualizar antivirus o agentes de seguridad
- Aplicar actualizaciones/parches del SO
- Garantizar el cumplimiento para unidades externas



Automatización del control basado en políticas

Severo

Red

- Poner el dispositivo en cuarentena (VLAN, Firewall virtual)
- Desactivar el puerto de conmutación
- Bloquear el acceso inalámbrico o VPN
- Utilizar listas de control de acceso (ACL) para limitar el acceso

Host

- Cerrar las aplicaciones no autorizadas
- Desactivar NIC/doble conectividad de red (dual-homed)
- Desactivar dispositivos periféricos
- Activar medidas o sistemas de corrección

Figura 1. Implementación de políticas en la red y en los puntos de conexión, incrementando la automatización progresivamente.

eyeControl detecta:

- **Dispositivos no autorizados, fraudulentos o suplantados** en la red que plantean riesgos y problemas de cumplimiento.
- **Brechas de seguridad** cuando las herramientas basadas en agentes no están actualizadas o no funcionan correctamente.
- **Redes homogéneas y sin segmentar** que dejan a las organizaciones expuestas a las amenazas y aumentan el radio de acción.
- **Riesgos de interrupción de la actividad** debido a la existencia de dispositivos vulnerables, falta de parches críticos y aplicaciones no autorizadas.
- **Propagación lateral** de las amenazas causada por la incapacidad de contener rápidamente los dispositivos comprometidos o maliciosos.
- **Incumplimiento** debido a la incapacidad de supervisar y aplicar continuamente la política de los dispositivos conectados.
- **Problemas de implementación NAC** en entornos heterogéneos, de múltiples proveedores, y redes cableadas.

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 través de redes cableadas e inalámbricas para todos los dispositivos gestionados y 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 puntos de conexión a través del motor de políticas Zero Trust unificado
- Interoperatividad con la infraestructura existente y no requiere actualizaciones de software o 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 corrección con el fin de garantizar un cumplimiento continuo de políticas de seguridad internas, reglamentos externos y normativas del sector.

- Asegúrese de que los puntos de conexión están configurados correctamente e inicie la corrección de problemas de configuración graves.
- Identifique y repare los dispositivos gestionados con agentes de seguridad dañados o no presentes.
- 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 corregirlos.
- Implementación de acciones de corrección y mitigación de riesgos en dispositivos Windows, Mac, Linux, IoT y OT
- Implementación de políticas y automatización de controles de la idoneidad de la configuración en despliegues en la nube, como Amazon Web Services, Microsoft Azure and VMware

Automatización

Acelere la respuesta ante incidentes

Contenga rápida y eficazmente las amenazas y responda a los incidentes de seguridad para minimizar la interrupción de las operaciones y el impacto en la empresa.

- Automatice las tareas de respuesta a incidentes básicas y repetitivas; y libere recursos especializados para centrarse en problemas y prioridades de mayor impacto.
- Identifique indicadores de peligro (IOC) y riesgos en los dispositivos en tiempo real para reducir el tiempo medio de respuesta (MTTR).
- Aísle y contenga automáticamente los activos comprometidos o maliciosos para limitar el radio de acción potencial al evitar la propagación lateral del malware.
- Automatice la respuesta a incidentes e inicie flujos de trabajo de corrección de dispositivos en tiempo real.
- Reduzca el tiempo medio de respuesta al proporcionar información importante sobre los dispositivos (conexión, ubicación, clasificación y estado de seguridad) a los equipos multifuncionales de respuesta a incidentes y a las tecnologías aisladas.

Descubrir, evaluar, gobernar

Forescout Platform aumenta el valor de eyeControl al proporcionar un 100% de visibilidad de los dispositivos, cumplimiento continuo, segmentación de la red y una base sólida para zero trust.

Consulte www.forescout.com/products para más información.

Forescout Technologies, Inc.

No. gratuito (EE.UU.) 1-866-377-8771
Tel (Internacional) +1-408-213-3191
Asistencia +1-708-237-6591

Más información en Forescout.com