Forescout eyeControl

Implementación y automatización de controles basados en directivas para reducir de forma proactiva su superficie de ataque y responder rápidamente a los incidentes

Los equipos de seguridad de TI se ven desbordados por una multitud de problemas de seguridad y cumplimiento de normativas que comunican un abundante número de herramientas de seguridad que generan alertas constantemente, sin posibilidad de realizar ninguna acción. Desafortunadamente, estas herramientas carecen del contexto sobre dispositivos necesario para priorizar o automatizar funciones que implementen controles encaminados a mitigar los riesgos. Como resultado, los equipos de profesionales especialistas en seguridad pierden el tiempo resolviendo manualmente problemas menores, mientras son incapaces de centrarse en la reducción proactiva de los riesgos o la rápida respuesta a amenazas.

Implementación de controles basados en directivas

Forescout eyeControl, gracias a un detallado contexto sobre dispositivos procedente de Forescout eyeSight, permite a los equipos de seguridad priorizar, implementar y automatizar con confianza controles basados en directivas. Las empresas pueden mejorar su higiene de seguridad, reducir su superficie de ataque y acelerar la respuesta y la corrección con el fin de mitigar rápidamente las amenazas, los incidentes de seguridad y los incumplimientos de normativas.

Según sus iniciativas de seguridad, mediante eyeControl puede llevar a cabo acciones tanto para la red y como para los endpoints. Para orquestar las acciones para la red, eyeControl se integra directamente con una infraestructura física y virtual heterogénea formada por conmutadores, dispositivos inalámbricos, VPN, conexiones definidas por software y la nube. Las medidas para los endpoints se pueden implementar sin necesidad de agentes, en endpoints Windows, Mac y Linux o mediante SecureConnector™.

eyeControl

Funciones principales

- Protege los datos confidenciales frente a amenazas externas.
- Impide que dispositivos infectados, vulnerables o no conformes propaguen malware.
- Evita que los ataques selectivos roben datos o provoquen una interrupción del funcionamiento de la red.
- Proporciona a los empleados, contratistas y clientes acceso y disponibilidad de la red.
- Garantiza el cumplimiento de las directivas internas y las normativas externas.
- Automatiza medidas de control para ofrecer acciones adecuadas para cada situación.

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

CONTROL MODERADO

Red

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

Host

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

AUTOMATIZACIÓN DEL CONTROL BASADO EN DIRECTIVAS

CONTROL ESTRICTO

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-homing)
- Desactivar dispositivos periféricos
- Activar acciones/sistemas de corrección

Automatización de controles con confianza

eyeControl aprovecha un motor de directivas intuitivo y flexible que permite a las empresas aplicar un control granular y selectivo. Se pueden implementar flujos de trabajo sofisticados y medidas combinadas con evaluaciones dinámicas fáciles de utilizar, lógica booleana y directivas en cascada. La gráfica de directivas facilita la creación de directivas precisas, el análisis del flujo de directivas y su ajuste, antes de activar las medidas de implementación.

Las medidas de control puede iniciarlas de forma manual el equipo de seguridad o bien, para incrementar la eficiencia de las operaciones de seguridad, se puede introducir la automatización de forma gradual. A partir de tareas básicas y repetitivas la automatización progresa hacia controles cada vez más complejos para liberar a los recursos de TI especializados de forma que puedan dedicarse a problemas más importantes. Este enfoque garantiza un mínimo de interrupción de la actividad y al mismo tiempo mejora enormemente el acceso a la red, el cumplimiento para los dispositivos, la segmentación de la red y las iniciativas de respuesta a incidentes.

> "Automatizar una acción para un endpoint es algo frecuente, pero cuando se requiere una intervención manual, basta con pulsar el botón derecho del ratón." – *Joseph Cardamone, Analista senior de seguridad de la información y Responsable de privacidad para Norteamérica, Haworth*

Problemas

- Los dispositivos no conformes o no autorizados en la red presentan un riesgo importante.
- Con redes homogéneas y sin segmentar, las empresas son vulnerables a las amenazas laterales.
- Incapacidad para responder de forma rápida y eficaz a los incidentes y amenazas de seguridad.
- Capacidad limitada para implementar una seguridad de dispositivos continua mediante el uso de las herramientas correspondientes.
- El riesgo de interrupción de la actividad empresarial coarta la automatización de controles de seguridad.

Implementación del acceso a la red

Control del acceso a los recursos de la empresa en función del perfil de los usuarios (invitado, empleado, contratista), la clasificación del dispositivo y el nivel de seguridad.

- Acceso diferenciado para invitados y dispositivos BYOD.
- Implementación de directivas de acceso a la red con o sin autenticación 802.1X.
- Medidas para gestionar dispositivos sospechosos, no autorizados o de TI en la sombra.
- Limitación o bloqueo del acceso a la red para dispositivos comprometidos o maliciosos.
- Cuarentena o aislamiento para los dispositivos no conformes hasta que se hayan solucionado los problemas de incumplimiento.

"Uno de los motivos por los que elegimos la plataforma de Forescout era porque esta tecnología no depende del protocolo 802.1X, lo que facilita enormemente el despliegue. No tener que instalar agentes redunda también en una mejora del rendimiento y la simplicidad".
—Juan Ignacio Gordon, Director de seguridad de TI, ACCIONA

Mejora del cumplimiento para los dispositivos

Automatización de la evaluación del cumplimiento 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.

- Garantía de que los endpoints están configurados correctamente y reparación de problemas de configuración graves, como el empleo de contraseñas predeterminadas o no seguras.
- Comprobación de que las aplicaciones y agentes de seguridad necesarios están instalados, activos y actualizados.
- Desactivación o bloqueo de aplicaciones no autorizadas que pudieran introducir riesgos o cargar sin necesidad el ancho de banda de la red o mermar la productividad de los recursos.
- Identificación de vulnerabilidades de alto riesgo y ausencia de parches críticos, e inicio de las medidas necesarias para repararlos.
- Aplicación proactiva de medidas de reparación como la instalación del software de seguridad necesario, la actualización de agentes o la aplicación de parches de seguridad.
- Implementación de directivas y automatización de controles de la idoneidad de la configuración en despliegues en la nube, como AWS, Azure y VMware®.

"Con la solución de Forescout, esperamos ahorrar millones, ya que las auditorías serán cada vez más rápidas, generarán menos hallazgos y necesitarán un menor trabajo de corrección".
— Phil Bates, Chief Information Security Officer, State of Utah

Implementación de segmentación dinámica de la red

Aplicación de directivas de segmentación dinámica de la red en tecnologías dispares en toda la empresa, a través de un marco de directivas común.

- Asignación dinámica de dispositivos a grupos de segmentación en función de sus propiedades, clasificación y nivel de seguridad.
- Aplicación de controles de segmentación a través de controles de VLAN, ACL, WLAN y del etiquetado en entornos de campus y OT.
- Aplicación de controles de segmentación a través de grupos de seguridad o etiquetas en entornos en la nube pública y privada, como AWS y VMware NSX.
- Segmentación de los dispositivos no conformes y vulnerables en zonas separadas —especialmente aquellos a los que solo se les pueden aplicar parches o correcciones dentro de un plazo de mantenimiento programado— para no afectar a la continuidad de la actividad y, al mismo tiempo, reducir la superficie de ataque.
- Implementación de directivas de segmentación para apartar los dispositivos y flujos de datos críticos del resto de la red, según dicten normativas como HIPAA, PCI y SWIFT CSP.

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.

- Identificación de dispositivos de alto riesgo que no se han contenido o reparado.
- 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).

"Forescout no solo aísla los dispositivos y lleva a cabo la segmentación de la red, sino que también descubre las redes que no se habían visto antes". –*Subdirector de seguridad de la información (CISO), gran empresa de asistencia sanitaria*

"Contar con Forescout es como tener un cazador de amenazas automático en el equipo, que captura amenazas constantemente en toda nuestra red global. Ahora podemos afrontar problemas que antes no podíamos gestionar. Además, realizamos en cuestión de minutos tareas que antes nos llevaban horas".
— Nick Duda, Ingeniero jefe de seguridad, HubSpot

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Teléfono gratuito (EE. UU.)
1-866-377-8771
Tel. (internacional) +1-408-213-3191
Soporte técnico 1-708-237-6591

Más información en Forescout.com