eyeControl

Implantación de controles basados en directrices

Implantar y automatizar medidas de control en redes heterogéneas

Continuo
Opciones flexibles para la habilitación y controles de acceso, con o sin 802.1X.

Sin agentes
Valoración continua del estado de los activos e implantación de cumplimiento automática sin instalación de agentes.

Efectivo
Módulo flexible para directrices unificadas con el fin de implementar accesos de confianza cero más seguros.

No se requieren Upgrades
Integración sin fisuras en la infraestructura existente sin mejoras de software o hardware.

Menos costes empresariales en total
Réditos rápidos gracias a menores costes para la habilitación, el mantenimiento y el funcionamiento.

Forescout eyeControl ofrece un control de acceso a la red flexible y fluido para redes de empresa heterogéneas. La solución implanta y automatiza directrices de seguridad de confianza cero (Zero Trust) para accesos de mínimo privilegio (Least Privilege) a todos los activos administrados y no administrados en su entorno digital. Los controles basados en directrices permiten implantar de forma continua la conformidad de los dispositivos, reducir proactivamente su superficie de ataque y responder rápidamente a los incidentes.

Acceso seguro a la red

- Implantación de accesos a red conformes con las directrices y basados en la identidad de los usuarios y dispositivos y en el estado de seguridad
- Habilitación con o sin 802.1X en redes heterogéneas

Implantación de la conformidad de los dispositivos

- Cumplimiento automatizado de directrices de seguridad, estándares de sector y disposiciones legales
- Activación de medidas de corrección y flujos de trabajo para la minimización de riesgosRisikominimierung in Echtzeit

Respuesta automatizada a incidentes

- Respuesta automatizada a incidentes de seguridad
- Contención de amenazas para minimizar su expansión y las perturbaciones que conllevan

Automatización fiable de controles

Las directrices de confianza cero solo se pueden implantar si se basan en una total transparencia de los dispositivos y un contexto completo. Esto incluye información en tiempo real sobre la identidad de los usuarios y dispositivos, sobre el estado de la seguridad y el perfil de riesgo de todos los dispositivos conectados. Los controles que se implementan sin tener una visión de conjunto completa pueden causar perturbaciones y obstaculizar los procesos empresariales. Por eso, eyeControl utiliza el contexto de dispositivos completo de eyeSight para implantar y automatizar de forma fiable controles de confianza cero.

El núcleo de eyeControl consiste en un módulo flexible para directrices unificadas, que le permitirá aplicar medidas de control detalladas y específicas. El módulo ofrece:

- sondeo dinámico y agrupación de activos basándose en la lógica del negocio y el contexto
- definición de condiciones y medidas complejas con lógica booleana y directrices en cascada, para implementar procesos de control exigentes
- función de grafos para la elaboración de directrices precisas, el análisis de flujos de directrices y la optimización de directrices antes de activar medidas de implementación
- posibilidad de empezar con controles iniciados manualmente y pasar a la implementación automática paso a paso, para aumentar la eficiencia de las medidas de seguridad

Si se producen eventos y cambios en un dispositivo determinado o en la red, las directrices se van activando y evaluando en tiempo real. La figura 1 a continuación muestra la amplitud de las medidas de control posibles con eyeControl cuando se activa una directriz.

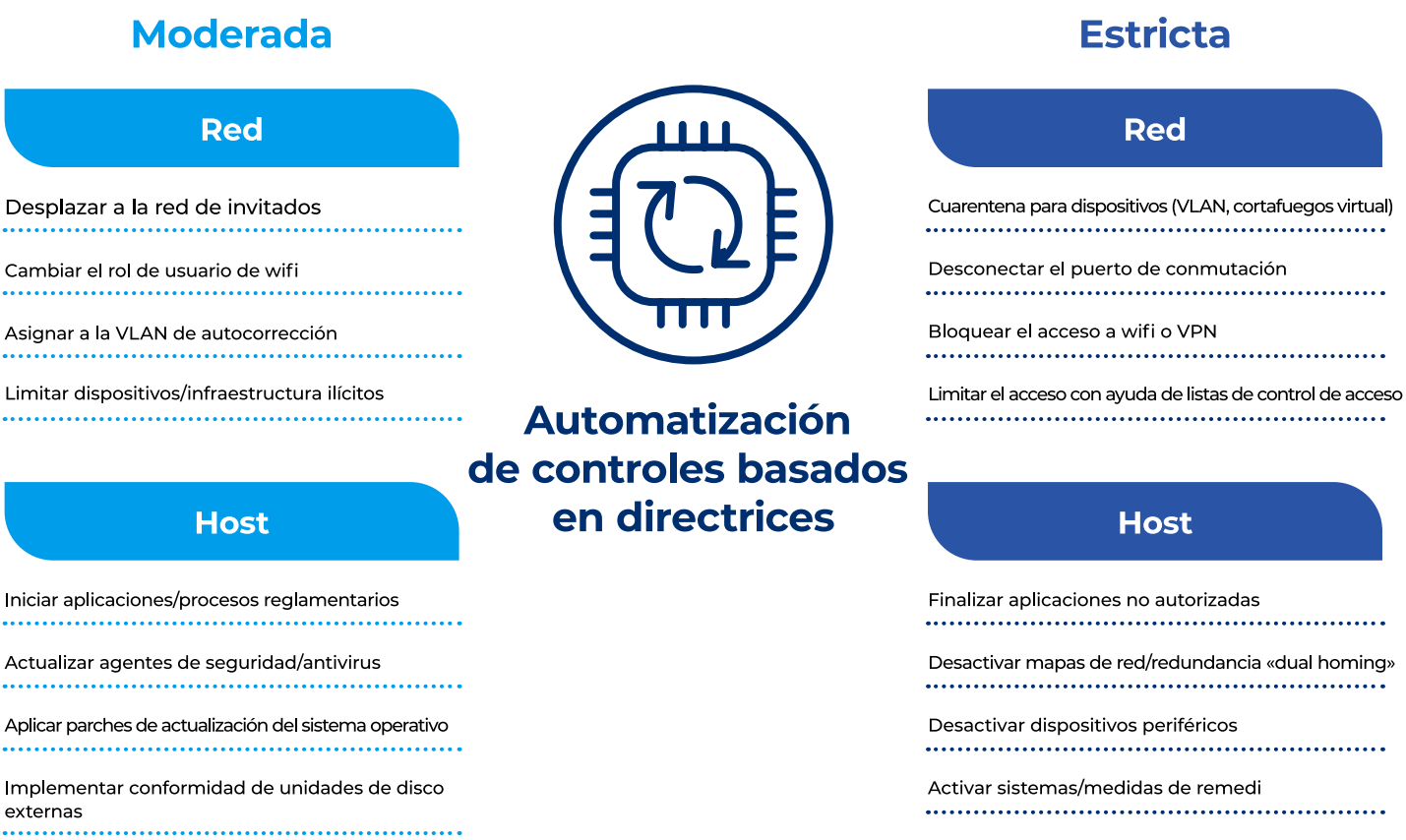

Fig. 1. Implantación da diractricas an la rad y an dispositivos finalas con un grado da automatización prograsivo.

eyeControl es la solución para:

- **dispositivos no autorizados, ilícitos o de suplantación (spoofing)** en la red, que suponen riesgos o problemas de cumplimiento.
- **agujeros de seguridad,** debido a herramientas no basadas en agentes que no están actualizadas o no funcionan correctamente.
- **redes planas, apenas segmentadas,** que hacen a las empresas más vulnerables a las amenazas y aumentan el radio de acción de los ataques.
- **riesgos para los procesos empresariales** debido a dispositivos vulnerables, en los que faltan parches importantes, o bien aplicaciones no autorizadas.
- **la propagación lateral** de amenazas cuando no se pueden desactivar rápidamente activos comprometidos o maliciosos.
- **infracciones de cumplimiento,** cuando no se pueden supervisar e implantar de forma constante directrices para los dispositivos conectados.
- **problemas en la implementación del NAC** en entornos heterogéneos con múltiples proveedores y redes alámbricas

Controlar

Acceso seguro a la red

eyeControl es la solución de control de acceso a la red más flexible para empresas con redes heterogéneas y trabaja sin perturbar los procesos de negocio. Con eyeControl puede garantizar el acceso seguro de todos los activos administrados y no administrados a redes alámbricas e inalámbricas, el cumplimiento de exigencias de auditoría, la reducción de la superficie de ataque y la mitigación rápida de amenazas. Las funciones abarcan:

- la implementación de accesos a red de con fianza cero para dispositivos de empleados, invitados y proveedores de servicios, así como dispositivos BYOD
- la detección y el bloqueo de dispositivos ilícitos, no autorizados y de suplantación de identidad, incluida TI en la sombra
- cuarentena/aislamiento de dispositivos no conformes y muy amenazados hasta la solución del problema
- uso de métodos diversos para el control de acceso, con o sin autenticación 802.1X
- implementación de controles, sin agente, del estado de los dispositivos; implantación de medidas en la red y en dispositivos finales con un módulo para directrices unificadas de confianza cero
- interoperabilidad con la infraestructura existente sin mejoras de software o hardware
- integración directa con más de 30 proveedores de infra estructura de red para cientos de modelos de producto

Cumplir

Implantación de la conformidad de los dispositivos

eyeControl permite la evaluación automatizada del estado de seguridad y la implantación de medidas correctivas. Así podrá cumplir de forma continua las directrices de seguridad internas, los estándares externos y las regulaciones específicas del sector.

- Validación de la configuración correcta de dispositivos finales e introducción de medidas para remediar vulnerabilidades graves en la configuración
- Detección de activos administrados que carecen de agentes de seguridad, o bien los que tienen son defectuosos, y ejecución de medidas correctivas
- Detección y desactivación de aplicaciones no autorizadas que generan riesgos, limitan la amplitud de la red u obstaculizan la productividad
- Detección de dispositivos con vulnerabilidades peligrosas o que carecen de parches importantes; introducción automática de medidas de remedio
- Implantación sin agentes de medidas para la corrección y la reducción de riesgos en dispositivos Windows, Mac, Linux, IoT, IoMT y OT
- Implementación de directrices y automatización de controles para configuraciones conformes con las disposiciones legales en implementaciones de nube (por ejemplo, Amazon Web Services, Microsoft Azure, VMware)

Automatizar

Respuesta más rápida a incidentes

Contenga rápidamente las amenazas y responda con efectividad a los incidentes de seguridad para minimizar las interrupciones en los procesos empresariales y las repercusiones en el negocio.

- Automatización de medidas de respuesta a incidentes básicos y reiterativos, para que los equipos puedan dedicar su tiempo a tareas más complejas
- Detección de indicadores de compromiso (iocs) y riesgos para activos en tiempo real con el fin de reducir el tiempo medio de respuesta (MTTR, por sus siglas en inglés)
- Aislamiento y contención automática de activos comprometidos o maliciosos para evitar la propagación de malware en la red y así limitar el potencial radio de acción
- Respuesta automatizada a incidentes e introducción en tiempo real de flujos de trabajo correctivos en dispositivos
- Reducción del mttr proporcionando un contexto de dispositivos valioso (conexión, sede, clasificación y estado de seguridad) a los equipos de respuesta a incidentes multidisciplinares y tecnologías aisladas

Detectar, evaluar, dirigir

La plataforma de Forescout aumenta las utilidades de eyeControl con soluciones que permiten una transparencia total de dispositivos, un cumplimiento continuo y una segmentación de redes, y crean una base sólida para estrategias de confianza cero.

Para más información, visite www.forescout.com/products.

Forescout Technologies, Inc.

Gratuita (EE. UU.) 1-866-377-8771
Tel (internac.) +1-408-213-3191
Asistencia +1-708-237-6591

Descubra más en Forescout.com