Mitigación y diagnóstico continuos

Plataforma de seguridad CounterACT

La Plataforma de seguridad ForeScout CounterACT proporciona supervisión, control y corrección basada en políticas de los dispositivos administrados, no administrados y no tradicionales, todo ello en tiempo real, que puede actuar como un pilar para CDM. Esta es la forma en que lo logra:

Vea

- Detecte dispositivos en el instante en que se conectan con su red sin necesidad de agentes
- Reúna información sobre dispositivos, usuarios, aplicaciones y sistemas operativos, y clasifíquelos
- Supervise continuamente los dispositivos administrados, BYOD y extremos IoT

Controle

- Permita, deniegue o restrinja el acceso a la red basándose en el nivel del dispositivo y las políticas de seguridad
- Evalúe y corrija automáticamente extremos malintencionados o de alto riesgo
- Mejore el cumplimiento de las exigencias y normas de la industria

Instrumente

- Comparta conocimiento contextual con los sistemas de seguridad y administración de TI
- Automatice flujos de trabajo habituales, tareas de TI y procesos de seguridad en todos los sistemas
- Acelere la respuesta en todo el sistema para mitigar rápidamente los riesgos y violaciones de seguridad de datos

Para garantizar un nivel aceptable y uniforme de confidencialidad, integridad y disponibilidad de activos de información, las organizaciones de TI del gobierno deben cumplir con un número creciente de normas, directivas y estándares. Su objetivo principal es eliminar las intrusiones (confidencialidad), proteger información sensible (integridad) y mitigar la exposición a la denegación de ciberataques al servicio (disponibilidad).

El programa de Mitigación y diagnóstico continuo (CDM) representa un enfoque dinámico en el fortalecimiento de la ciberseguridad de las redes y los sistemas del gobierno. El CDM proporciona a los departamentos y las organizaciones federales capacidades y herramientas para identificar riesgos de ciberseguridad de forma continua, priorizar estos riesgos sobre la base de impactos potenciales y habilitar al personal de ciberseguridad para que puedan mitigar los problemas importantes en primer lugar. El Congreso estableció el programa CDM a fin de promover una ciberseguridad adecuada, basada en el riesgo y rentable que emplee recursos de ciberseguridad con mayor eficiencia.

Este requisito “continuo” en CDM no significa que necesariamente haya que trabajar las 24 horas del día los siete días de la semana, sino que significa recurrir a evaluaciones en intervalos según el valor de la información y el nivel calculado de riesgo. La publicaciones federales proporcionan directivas para determinar la frecuencia de la evaluación sobre la base de criterios tales como la volatilidad del control de seguridad, los niveles de impacto en el sistema en términos de la función protegida y las debilidades identificadas. Estas directivas definen la latencia de intervalos de detección (DIL) como la métrica que se usa en la medición y auditoría de los niveles aceptables de respuesta en un programa de seguridad de CDM.

Desafíos de cumplimiento con CDM

En vez de tener un enfoque de documentación y reacción pasiva, CDM exige una actitud proactiva, con enfoque en los datos y basada en el riesgo. Por lo general, esto requiere un leve cambio en la infraestructura de seguridad, dado que las integraciones de procesos y datos deben atravesar los límites de la organización, de los datos y de los sistemas. Dentro del marco de CDM, los procesos de recolección de datos, la gestión de activos y de riesgos tienen lugar de forma continua, no periódica, en todo el entorno. Los desafíos técnicos más grandes para las organizaciones de TI están vinculados con la integración y correlación de la transmisión por secuencias continua.

A medida que se ponen a disposición nuevos datos sobre el entorno de TI, el sistema de CDM necesita absorber los datos y responder con la elevación de los umbrales y la adaptación de directivas de red, así como tomar medidas de control en un bucle de comentarios perpetuos. CDM también requiere la transmisión de operaciones de seguridad costosas para colaborar con los funcionarios federales de alto rango a fin de que obtengan mayor visibilidad del estado de la seguridad de la organización y de la información sobre gestión de riesgos. Una implementación efectiva debe recopilar datos de procesos continuos, correlacionar múltiples factores contextuales, tomar medidas automáticamente en los casos apropiados y presentar los asuntos restantes en orden de prioridad.

Aspectos destacados

Visibilidad en tiempo real
Obtenga visibilidad en tiempo real automatizada de los extremos que se conectan a su red. Detecte también dispositivos analizadores de protocolos (sniffer) furtivos que no usan una dirección IP.

Administración eficaz de activos
Genere un inventario en tiempo real de su red: dispositivos, hardware, sistemas operativos, aplicaciones, niveles de parches, procesos, terminales abiertas, periféricos, usuarios y más.

Control de acceso basado en políticas Límite de acceso a la red a usuarios y dispositivos autorizados con o sin 802.1X para la seguridad del puerto del conmutador.

Supervisión continua Evalúe la seguridad y el nivel de cumplimiento los extremos en tiempo real antes y después de que se conecten a la red. Detecte las violaciones de configuración de extremos y los comportamientos maliciosos, y diseñe una respuesta basada en la gravedad de la violación.

Corrección automática Automatice la corrección de extremos sin cumplimiento mediante la actualización automática de los sistemas de protección y configuración de extremos, parches y actualizaciones, e instale, active o desactive aplicaciones o periféricos.

Integración con HBSS Aumente el conocimiento de la situación y la respuesta ante incidentes mediante la detección automática y la corrección de extremos con agentes del sistema de seguridad basado en host (HBSS) perdidos o dañados. Permita, deniegue o restrinja el acceso a la red basándose en los estándares de cumplimiento evaluados por HBSS.

Informes de cumplimiento
Genere informes en tiempo real que reflejen el nivel de cumplimiento con la política. Acorte el DIL mediante el inicio de escaneos de cumplimiento a medida que se conectan los hosts a la red en lugar de esperar a los escaneos basados en tiempo.

Requisitos de implementación

A fin de adoptar CDM, las organizaciones deben invertir en la gestión en tiempo real de detección de activos y vulnerabilidades, mecanismos de respuesta impulsados por medios inteligentes y automatizados, y comentarios continuos de datos en un sistema de gestión empresarial. Además, el sistema necesita debe ser de fácil implementación dentro del marco existente de TI.

Un sistema de gestión de vulnerabilidad y detección de activos en tiempo real debe usar una combinación de detección pasiva y activa más técnicas de control para detectar y elaborar un perfil de sistemas de red, independientes del sistema operativo o del factor de forma. Las técnicas de detección pasiva de tráfico controlan el tráfico para ver qué dispositivos están activos. Las técnicas de detección activa sondean la red en busca de dispositivos inactivos. En conjunto, se puede lograr la visibilidad completa y constante de los activos de TI. Tan pronto como se puede instalar o reconfigurar un dispositivo en la red, se puede detectar el cambio y es posible evaluar el dispositivo. Finalmente, el sistema de gestión de activos debería incluir la capacidad de evaluar las posturas de seguridad y las vulnerabilidades de los extremos de la red.

El mecanismo de respuesta automatizada debería poder tomar entradas del sistema de gestión de vulnerabilidades y detección de activos y, sobre la base de esta información más la advertencia sobre el comportamiento del extremo, generar un conjunto de respuestas inteligentes diseñado para reducir el riesgo empresarial. Las respuestas deben ser las adecuadas sobre la base de la gravedad de la violación al cumplimiento normativo y/o la conducta del extremo. Por ejemplo, el sistema de respuesta debe ser capaz de responder a las acciones tales como:

- Enviar una alerta al individuo o equipo de gestión de TI adecuado.
- Solucionar automáticamente el extremo o activar un sistema de terceros para solucionar el extremo.
- Limitar el acceso a la red.
- Bloquear el acceso a la red.

Las acciones de controles automatizados y datos de activos se deben comentar en otros aspectos del sistema de CDM a fin de optimizar la eficiencia y efectividad del sistema general (consulte la ilustración 1). Por ejemplo, los vínculos entre el sistema CDM y la Administración de eventos e información de seguridad (SIEM) de la organización ayudan a asegurar que los informes de cumplimiento generados por el sistema de SIEM sean exactos.

El sistema de CDM también debe aportar información en sistemas basados en agentes como antivirus, administración de parches y sistemas de administración de dispositivos móviles (MDM) a fin de asegurar que estos sistemas estén al tanto de extremos no administrados en la red.

Finalmente, el sistema de CDM debe ser fácil y rápido de implementar. Por ejemplo, el sistema debe poder hacer estas tareas:

- Implementarse dentro de la infraestructura de red existente sin necesidad de cambiar la arquitectura de la red.
- Integrarse en la infraestructura de redes existente.
- No confiar en la implementación en línea u otros puntos únicos de fallas.
- No solicitar la instalación de agentes de extremos adicionales.

Aspectos destacados (continuación)

Controles móviles e inalámbricos
Detecte y haga cumplir los controles de seguridad en dispositivos móviles como teléfonos inteligentes y tabletas. Garantice el cumplimiento inalámbrico mediante la integración con infraestructura de red inalámbrica.

Implementación sin interrupciones
CounterACT se puede implementar con un enfoque en etapas, lo que minimiza la interrupción y acelera los resultados.

Interoperabilidad de TI
Aproveche la integración con la infraestructura existente de TI con servicios de directorio, administración de parches, protección de extremos, evaluación de vulnerabilidades, sistemas SIEM y MDM.

ForeScout CounterACT como el pilar de CDM

ForeScout CounterACT aborda los requisitos de CDM y puede actuar como pieza clave en su solución de CDM. CounterACT proporciona visibilidad en tiempo real y control para los extremos de la red, entre ellos, teléfonos inteligentes, tabletas, netbooks y otros dispositivos móviles personales conectados a la red.

CounterACT usa una combinación de técnicas de detección para clasificar con precisión extremos a través de técnicas de interrogación pasivas y activas. ForeScout CounterACT es una solución sin agentes que permite trabajar con distintos tipos de extremos: administrados y no administrados, conocidos y desconocidos.

CounterACT puede evaluar la postura de seguridad de los extremos en su entorno LAN/WAN. Esto es especialmente importante en el caso de los extremos no administrados del tipo “traer sus dispositivos” (BYOD), ya que, en general, sus sistemas de gestión de extremos existentes no detectan estos dispositivos. CounterACT puede evaluar la postura de seguridad de los dispositivos administrados (computadoras conectadas al dominio) sin necesidad de implementar otro agente para esos dispositivos. Este es un factor clave que ayuda a la implementación rápida y a la facilidad de funcionamiento del sistema CounterACT. CounterACT puede evaluar la postura de seguridad de los dispositivos BYOD no administrados por la instalación de un agente ligero temporal. Este agente es compatible con Windows®, MacOS y Linux. Se puede implementar automáticamente cuando el usuario se conecta a la red y registra su identidad en el sistema. Independientemente de que se use un agente o no, CounterACT puede llevar adelante un amplio rango de verificaciones de cumplimiento, entre ellas, control de software necesario, versiones de software y de parches, configuración de dispositivo y vulnerabilidad de extremo, por mencionar algunas. Se integra con el sistema de red líder de seguridad basada en el host y con las plataformas de identidad para proporcionar inteligencia de extremos en tiempo real y atención en postura de seguridad.

ForeScout CounterACT incluye un amplio rango de acciones de solución de extremos sobre la base de la postura de seguridad del extremo. CounterACT puede hacer que el servidor de antivirus actualice automáticamente los hosts que están en infracción, que el sistema de administración de parches actualice el sistema operativo del dispositivo o puede deshabilitar el software no autorizado. Además, CounterACT es compatible con los sistemas SIEM para proporcionar detalles de configuración de extremos, correlacionar el acceso y las violaciones al cumplimiento y acelerar la respuesta ante incidentes. CounterACT incluye informes integrados que lo ayudan a supervisar el cumplimiento de las políticas, satisfacer los requisitos normativos de auditoría y generar informes de inventario en tiempo real.

ForeScout CounterACT se vende como un appliance virtual o físico que se implementa sin inconvenientes dentro de su infraestructura existente; por lo general, no requiere cambios a la infraestructura y no agrega latencia a las operaciones de la red.
La appliance CounterACT se instala fuera de banda y evita la latencia o el potencial de errores de red; además, se puede administrar centralmente para gestionar dinámicamente decenas o cientos de miles de extremos desde una consola.

ForeScout CounterACT emplea un enfoque comprobado de la gestión de riesgo de TI. Los dispositivos que acceden a la red se identifican, controlan, corrigen (si o desea) y supervisan continuamente para asegurar el cumplimiento y la protección. El motor de cumplimiento detectará los dispositivos o usuarios que no cumplan con la política de seguridad y rastreará a los usuarios que tienen un comportamiento riesgoso, como usar aplicaciones punto a punto (P2P), unidades de almacenamiento externo, teléfonos inteligentes, entre otras actividades no autorizadas. Los equipos o los usuarios que no cumplan con las normas se mostrarán en la consola principal, además del motivo del incumplimiento y detalles tales como ubicación del dispositivo.

Finalmente, CounterACT ayuda a los administradores de TI a lograr métricas de latencia de intervalos de detección (DIL) mediante la integración con escáneres de cumplimiento para agregar funcionalidad de escaneo basado en eventos. Mediante esta integración, CounterACT activa el escáner de cumplimiento cuando un host se conecta a la red. El agregado de escaneo basado en eventos mejorará considerablemente la métrica de DIL. ForeScout CounterACT se integra con una cantidad de dispositivos de escáneres de evaluación de vulnerabilidades (VA) principales, como Nessus de Tennable®, Retina de BeyondTrust® y Qualys®, además de otras integraciones que están en desarrollo.

Reduzca la complejidad y aumente la eficiencia

En el pasado, los gerentes de seguridad de TI tendían a abordar cada riesgo con una solución técnica específica. Las normas obligatorias se abordaban con controles especializados. Así se proporcionaba un nivel aceptable de seguridad y cumplimiento en el corto plazo. Hoy día, sabemos que las soluciones de seguridad independientes entre sí aumentan la complejidad, a su vez, la complejidad aumenta el riesgo y el costo de mano de obra de administración. La falta de interconectividad entre los controles de TI es un desafío principal que dificulta la labor de los departamentos de TI para administrar el riesgo de modo eficiente. Ello también resulta en una pobre conocimiento de la situación y en limitada información para una detección de amenazas rápidas y mitigación de riesgos.

ForeScout CounterACT ayuda a resolver este problema. CounterACT se integra con los sistemas existentes para crear un sistema de supervisión permanente preciso y de rápida respuesta sencillo que le proporciona mucha más eficiencia gracias a su nuevo diseño. Como resultado, el sistema le permite tener visibilidad en tiempo real, inspección profunda de los extremos, supervisión permanente y corrección automática, integración del sistema con otros sistemas de gestión de seguridad, rápida implementación y bajo costo total de propiedad.

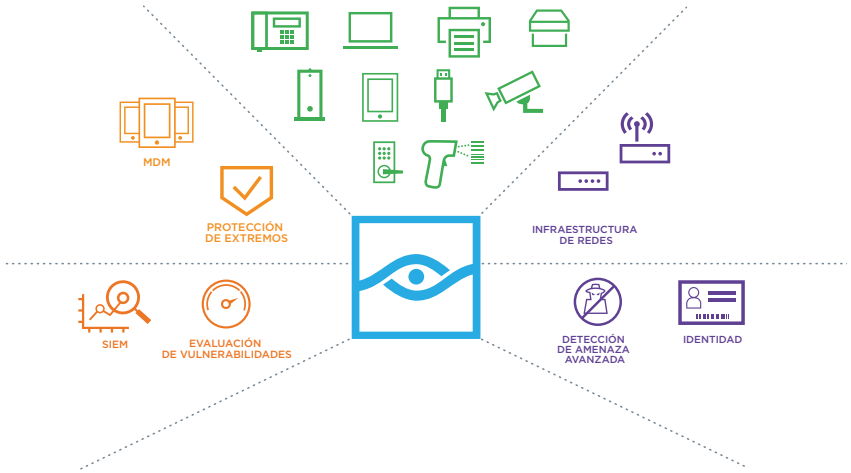

Ilustración 1: Estado deseado: ForeScout CounterACT proporciona visibilidad en tiempo real de la red y comparte información bidireccionalmente con la infraestructura de seguridad y operativa existente.

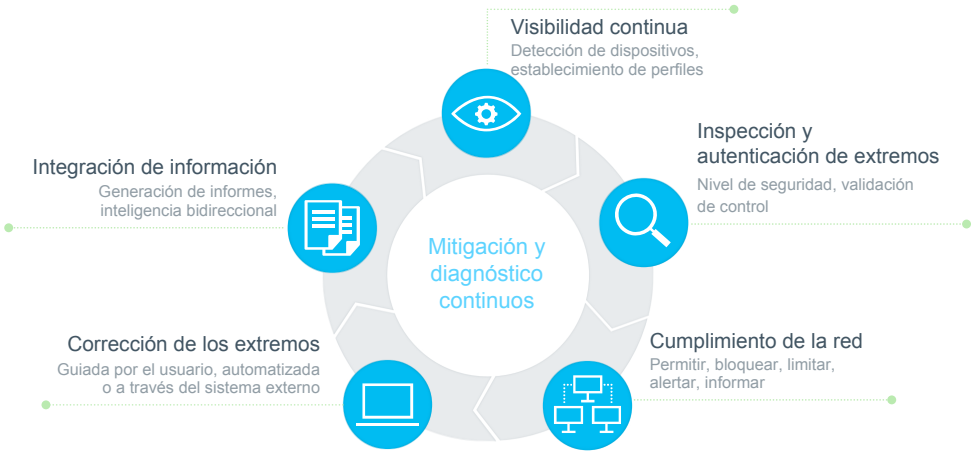

Ilustración 2: La plataforma de automatización de seguridad inteligente de ForeScout proporciona visibilidad en tiempo real y controles automatizados.

Criterios de mitigación y diagnóstico permanente[1]		ForeScout CounterACT
Detección y clasificación de activos	Detecte hardware no autorizado o no administrado en una red y detecte configuración de software no autorizada o no administrada en los activos de TI en una red.	CounterACT detecta dispositivos en la red en tiempo real y mantiene una base de datos integral de activos de hardware y software. Se puede buscar y organizar el inventario por varios atributos de hardware y software. Se pueden generar informes de inventario.
Evaluación	Se evalúa la postura de seguridad de los extremos, lo que permite obtener un inventario de software preciso y exacto esencial para dar soporte al conocimiento y control efectivo de las vulnerabilidades del software y a los ajustes de configuración de seguridad.	CounterACT puede evaluar la postura de seguridad de los extremos en su entorno LAN/WAN. Esto es especialmente importante en el caso de los dispositivos no administrados del tipo "traer sus dispositivos" (BYOD), ya que, en general, sus sistemas de gestión existentes no detectan estos dispositivos. CounterACT puede llevar adelante un amplio rango de verificaciones de cumplimiento, entre ellas, supervisión de software necesario, versiones de software y de parches, configuración de dispositivo y vulnerabilidad de extremo, por mencionar algunas. Se integra con otros agentes y herramientas basados en hosts y con escáneres de vulnerabilidad para obtener información adicional sobre cumplimiento.
Control de acceso y autenticación	Previene, elimina y limita las conexiones o los accesos a la red no autorizados para evitar que los atacantes atraviesen los límites de red externos e internos y luego alternen dentro y fuera de ellos para lograr un acceso a la red más profundo y/o capturar datos de la red activos o pasivos. Administra accesos a la cuenta, comportamientos de seguridad, credenciales y autenticación.	CounterACT puede bloquear o limitar el acceso a dispositivos no autorizados así como a dispositivos que pasan a estar sin cumplimiento mientras están conectados a la red. CounterACT está impulsada por eventos y reevalúa extremos ante cambios de la configuración del sistema operativo.
Mitigación y corrección automatizada	Previene la explotación del sistema mediante el diseño consciente del sistema a fin de minimizar debilidades y hacer que el sistema cumpla los estándares para reducir la superficie de ataque y aumentar el esfuerzo necesario para alcanzar las partes del sistema que permanecen vulnerables.	Cuando se detectan violaciones al cumplimiento, CounterACT puede responder según la gravedad de la violación mediante el envío de una alerta o de un aviso al personal de TI, o bien mediante la corrección automática, cuarentena o bloqueo de extremos sin cumplimiento. También tiene una interfaz con un sistema de terceros como administración de parches.
Conocimiento de la situación	El conocimiento del estado de un extremo de modo preciso y oportuno es clave para el control efectivo y el aviso de problemas de seguridad de red de una organización.	CounterACT aporta un conocimiento integral de la situación mediante la identificación de extremos de la red y la integración con otros sistemas de gestión de seguridad, tales como productos de gestión del ciclo de vida útil del extremo, sistemas de gestión de activos, bases de datos, SIEM, VA y productos de antivirus, lo que permite obtener una inteligencia de extremos en tiempo real y un conocimiento de la postura de seguridad. Además, es compatible con los sistemas SIEM para proporcionar detalles de configuración de extremos, correlacionar el acceso y las violaciones al cumplimiento.

[1]Referencia: "Criterios de mitigación y diagnóstico permanente"
https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f154da08471898c2e7a9ab05595c3df6

Arquitectura ForeScout ControlFabric®

La integración entre ForeScout CounterACT y su solución CDM es solo una de muchas integraciones de sistema de TI que aprovechan la arquitectura ControlFabric. ControlFabric es tecnología abierta que permite que ForeScout CounterACT y otras soluciones intercambien información y mitiguen con mayor eficiencia una amplia variedad de problemas de seguridad. Obtenga más información en www.forescout.com/controlfabric.

Acepte el desafío de ForeScout

Comuníquenos qué solución de ForeScout es la adecuada para usted y programaremos una evaluación in situ sin cargo.

Acerca de ForeScout

ForeScout Technologies, Inc. está transformando la seguridad a través de la visibilidad. ForeScout ofrece a las empresas de la lista Forbes Global 2000 y las organizaciones gubernamentales la capacidad única de ver los dispositivos, incluso los dispositivos no tradicionales, en el instante en que se conectan a la red. Asimismo, ForeScout le permite controlar estos dispositivos e instrumentar el intercambio de información y la operación con diversas herramientas de seguridad para acelerar la respuesta ante incidentes. A diferencia de las opciones tradicionales de seguridad, ForeScout lo logra sin necesidad de agentes de software o conocimiento previo del dispositivo. Las soluciones de la compañía se integran con las principales redes, elementos de seguridad, dispositivos móviles y productos de administración de TI para superar silos de seguridad, automatizar flujos de trabajo y permitir importantes ahorros en los costos. Más de 2000 clientes de más de 60 países mejoran la seguridad de sus redes y su nivel de cumplimiento con las soluciones de ForeScout*.

Obtenga más información en www.forescout.com.

Obtenga más información en
www.ForeScout.com

ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008, Estados Unidos

Número gratuito para llamadas en los EE. UU.
1-866-377-8771
Tel. (internacional) +1-408-213-3191
Asistencia técnica 1-708-237-6591
Fax 1-408-371-2284

* A partir de enero de 2016