ForeScout CounterACT®

Obtenga supervisión, control y corrección basada en políticas de los dispositivos administrados, no administrados y no tradicionales, todo en tiempo real.

ForeScout CounterACT® es un appliance de seguridad sin agente que identifica y evalúa extremos y aplicaciones de redes en forma dinámica, apenas se conectan a la red. CounterACT determina rápidamente el usuario, el propietario y el sistema operativo, al igual que la configuración del dispositivo, el software, los servicios, el estado de parches y la presencia de agentes de seguridad. Luego, proporciona corrección, control y supervisión continua de estos dispositivos.

CounterACT realiza estas acciones en extremos corporativos, en los personales del tipo "traiga su propio dispositivo" (BYOD) y en dispositivos no tradicionales, sin que sean necesarios agentes de software ni conocimientos previos del dispositivo. Se implementa rápidamente dentro del entorno existente y solo en escasas ocasiones requiere cambios de infraestructura, actualizaciones o reconfiguración de extremos.

¿Por qué los clientes prefieren CounterACT?

Compatibilidad heterogénea. Funciona con sistemas operativos, infraestructuras de red, software de extremos y soluciones de seguridad de terceros más frecuentes.

Sin agente. No se necesitan agentes de extremo para la autenticación y el control de acceso a la red.

Visibilidad excepcional. Se visualizan los dispositivos que otras soluciones no pueden ver:

- Computadoras de escritorio y portátiles, servidores, enrutadores, teléfonos inteligentes y tabletas.
- LAN e impresoras con cable e inalámbricas.
- Dispositivos IoT (proyectores, controles industriales, cuidado de la salud, fabricación, dispositivos POS, entre otros).

Control automatizado. Se automatizan una amplia gama de acciones:

- Permitir, denegar o restringir el acceso a la red según las políticas de seguridad y el nivel del dispositivo.
- Poner en cuarentena y corregir extremos malintencionados o de alto riesgo.

Rápido tiempo de amortización. Se implementa rápidamente y se gana visibilidad de la red en cuestión de horas.

Cumplimiento de políticas. Se aplica control de acceso a la red, cumplimiento de extremos y seguridad del dispositivo móvil.

Productividad. Se otorga el nivel correcto de acceso a cada persona y dispositivo, sin intervención intrusiva ni participación del personal.

Confiabilidad. Mejora la estabilidad de la red identificando y eliminando la infraestructura no autorizada.

Ahorros de costos. Se elimina el trabajo manual asociado con la apertura y el cierre de los puertos de red para el acceso de invitados.

Cumplimiento. Se identifican automáticamente las violaciones de las políticas, se corrigen las deficiencias de los extremos y se mide el cumplimiento de los mandatos.

Riesgos de seguridad y puntos ciegos de la red

Tradicionalmente, la seguridad de redes se ha enfocado en el bloqueo de los ataques externos con firewalls y sistema de prevención de intrusiones. Sin embargo, estas herramientas de seguridad no hacen nada para proteger a la red contra el aluvión de amenazas internas que causan cada vez más incidentes y violaciones de seguridad. Se encuentran entre las amenazas:

- **Visitantes:** Los invitados y los contratistas van a su instalación y llevan sus propios equipos. Ambos necesitan acceso a Internet, y es posible que los contratistas requieran otros recursos. Si otorga acceso ilimitado a estos invitados, se arriesga a que la red sufra algún ataque.
- **Usuarios inalámbricos y móviles (BYOD):** Los empleados desean utilizar sus propios teléfonos inteligentes, tabletas y computadoras portátiles en la red. Sin un control adecuado, estos dispositivos pueden infectar la red o causar la pérdida de datos.
- **Dispositivos de Internet de las cosas (IoT):** Los dispositivos no tradicionales siguen expandiendo la superficie de ataque porque agregan dispositivos no administrados, tales como proyectores con dirección IP, termostatos, controles de iluminación, cámaras de seguridad y más.
- **Dispositivos no autorizados:** Los empleados bienintencionados pueden extender la red con concentradores de cableado de bajo costo, servidores departamentales, enrutadores y puntos de acceso inalámbricos que pueden causar inestabilidad y vulnerabilidad en la red.
- **Malware y redes de bots:** Una vez en riesgo la red, los dispositivos conectados a ella pueden ocasionar "ataques pivotes", en los que los terceros pueden examinar la red y robar datos.
- **Cumplimiento:** Los extremos y las máquinas virtuales mal configurados pueden incluir configuraciones o software incorrectos. Además, el usuario o un malware pueden deshabilitarlos intencionalmente, lo que desactiva los controles de seguridad.

No se puede proteger lo que no se ve.

La visibilidad restringida genera puntos ciegos en la seguridad. La mayoría de los sistemas de seguridad de extremos requiere agentes actualizados en cada dispositivo para poder visualizarlos y administrarlos. Normalmente, los administradores de seguridad de TI no tienen visibilidad de extremos BYOD no administrados ni del número creciente de dispositivos IoT que aparecen en las redes todos los días.

Funcionamiento de ForeScout CounterACT®

ForeScout CounterACT ofrece la capacidad única de visualizar los dispositivos con dirección IP conectados a la red, controlarlos e instrumentar el intercambio de información y la operación con diversas herramientas de seguridad. Esta es la forma en que lo logra:

Visualizar El appliance CounterACT se implementa fuera de banda en la red. Desde allí, controla el tráfico de la red de forma permanente y se integra con la infraestructura de la red para identificar los dispositivos apenas acceden a la red. CounterACT tiene la capacidad única de visualizar una gran variedad de extremos con dirección IP, usuarios y aplicaciones. En realidad, las sofisticadas tecnologías de CounterACT detectan dispositivos que son invisibles para los productos de la competencia.

CounterACT no se limita a ello. A continuación, clasifica con precisión los extremos en la red a través de técnicas de interrogación pasivas y activas. CounterACT puede identificar el tipo de dispositivo, la ubicación, el usuario y si el dispositivo es miembro de su dominio, así como otros tipos de información básica. También obtiene información detallada sobre el nivel de seguridad del dispositivo al utilizar credenciales administrativas para interrogar a los dispositivos corporativos.

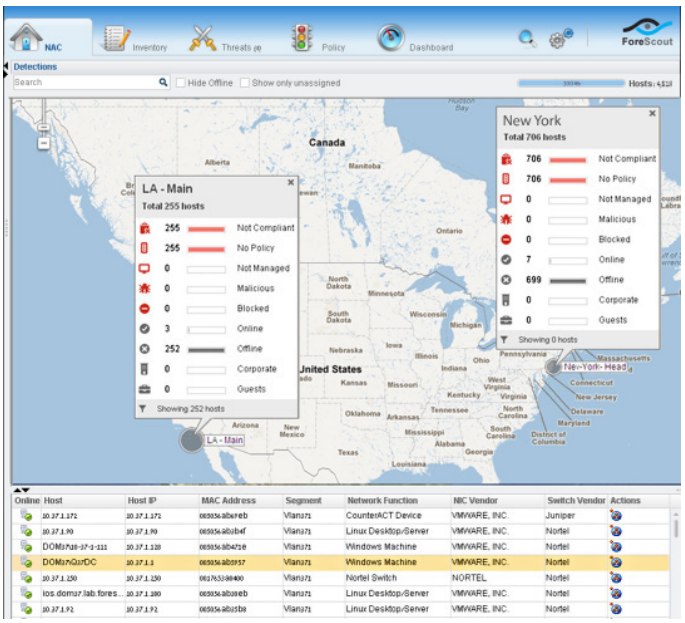

Ilustración 1: ForeScout CounterACT proporciona información detallada y de alta calidad de todos los dispositivos en la red.

Controlar. Una vez que CounterACT detecta un problema de seguridad en un extremo, su sofisticado administrador de políticas puede ejecutar automáticamente una serie de respuestas que varían según la gravedad del problema. Las violaciones menores pueden generar un mensaje de advertencia al usuario final. Los empleados y contratistas que traen sus propios dispositivos pueden ser redireccionados a un portal interno automatizado. Las violaciones graves generan diversas acciones, como bloqueo o cuarentena del dispositivo, reinstalación de un agente de seguridad, reinicio de un agente o proceso, activación del extremo para capturar un parche del sistema operativo o realizar otras acciones correctivas.

Los analistas, clientes y socios eligen CounterACT:

- ForeScout ha sido designada Gartner Magic Quadrant for Network Access Control** (Cuadrante mágico de Gartner para el control de acceso a la red [NAC]) por su capacidad de ejecución y la integridad de visión (cuatro informes consecutivos).
- La mejor solución de NAC según SC Magazine, junio de 2015.
- La mejor compra según SC Magazine, octubre de 2014.

> Necesitábamos una solución de NAC de rápida implementación, que no presentara el riesgo de interrupción de la actividad. Además, debía ser compatible con nuestra infraestructura de TI mixta de Aruba® y Cisco®. ForeScout CounterACT nos ofreció todo esto y mucho más, incluso magníficas capacidades de integración con nuestras herramientas de seguridad FireEye® y ArcSight®. Por este motivo, llamamos a CounterACT "el cuchillo del ejército suizo" de nuestro departamento de seguridad de información, ya que facilita varios controles de seguridad y verificaciones de cumplimiento automatizados de la manera más eficiente".
>
> **Ali Kutluhan Aktaş, jefe de seguridad de la información/ administración de riesgos en KKB.**

El valor de la arquitectura ControlFabric

La arquitectura ControlFabric es el cemento que une las capacidades de ForeScout CounterACT con aquellas de los productos de red, seguridad, movilidad y administración de TI de terceros. Elimina los silos de administración de seguridad para lograr lo siguiente:

- Unificar la administración de seguridad en todo el sistema.
- Alcanzar mayores eficiencias operativas.
- Acelerar la respuesta a amenazas.
- Potenciar el rendimiento de la inversión en seguridad.
- Mejorar considerablemente la seguridad de la red y el nivel de cumplimiento.

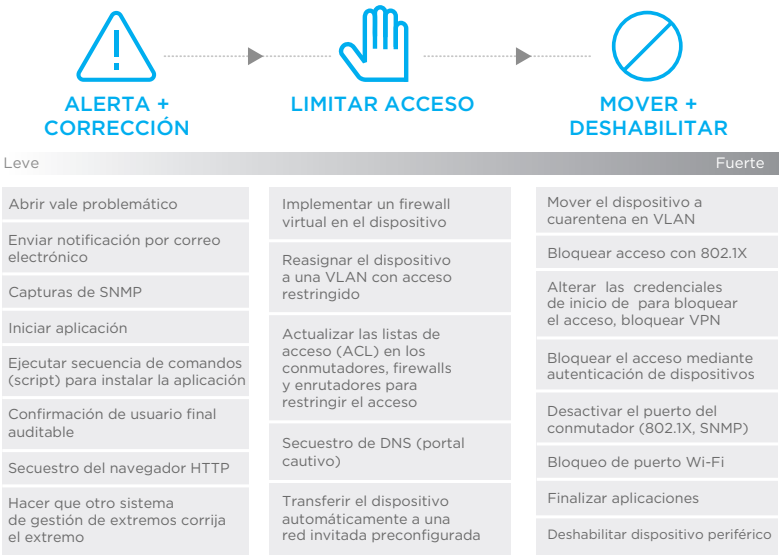

Ilustración 2: ForeScout CounterACT gestiona el espectro completo de acciones de control.

Instrumentar. CounterACT aprovecha la arquitectura ForeScout ControlFabric® para instrumentar el intercambio de información y la operación entre las herramientas de seguridad y de administración del sistema que ya posee. La arquitectura ControlFabric le permite lograr esto a través de integraciones personalizadas o módulos de software del tipo "conectar y usar" (Plug and play). Desarrollados con nuestros socios tecnológicos, los módulos básicos y extendidos de ForeScout permiten aprovechar el poder de CounterACT en más de 70 productos* líderes de redes, seguridad, movilidad y administración de TI con estos fines:

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

Características

General

Implementación fuera de banda: Se implementa fuera de banda en la red sin agregar latencia ni un posible punto de falla.

Visibilidad: La función de inventario de activos proporciona visibilidad y control en tiempo real y multidimensional, lo que permite rastrear y controlar usuarios, aplicaciones, procesos, puertos, dispositivos externos y más (consulte la ilustración 1).

Interoperabilidad abierta: CounterACT funciona con los conmutadores, enrutadores, VPN, firewalls, extremos, sistemas operativos (Windows®, Linux, iOS, OS X y Android), sistemas de administración de parches, sistemas antivirus, directorios y sistemas de tickets más populares, sin necesidad de cambios ni actualizaciones en la infraestructura.

Informes: Un motor de informes completamente integrado lo ayuda a supervisar su nivel de cumplimiento de las políticas, satisfacer los requisitos normativos de auditoría y generar informes de inventario en tiempo real.

Escalabilidad: Trayectoria comprobada en redes de clientes con más de 1.000.000 de extremos. Los appliances de CounterACT se presentan en una variedad de tamaños.

Certificaciones: CounterACT tiene nivel militar y cumple con las siguientes certificaciones:

- Autorización de funcionamiento (ATO) del Cuerpo de Marines de los Estados Unidos.
- Certificado de aptitud de red (CoN) del Ejército de los Estados Unidos.
- Lista de productos aprobados con capacidades unificadas (UC APL).
- Nivel de aseguramiento de evaluación de criterios comunes (EAL) L4+.

No interrumpe: Se implementa sin impacto sobre los usuarios o los dispositivos. Cuando quiera avanzar hacia control automatizado, podrá hacerlo gradualmente, comenzando con las ubicaciones más problemáticas y eligiendo las acciones de cumplimiento apropiadas.

Administración de políticas: Cree las políticas de seguridad apropiadas para su empresa. La configuración y la administración son rápidas y sencillas gracias las plantillas integradas de políticas, normas e informes.

Arquitectura ControlFabric: La arquitectura ControlFabric® ofrece una amplia interoperabilidad con productos de terceros y una arquitectura de integración abierta.

Extremos

Sin agente: Identifique, clasifique, autentifique y controle el acceso a la red sin agente. Realice una exhaustiva inspección de los extremos sin agente, en la medida en que CounterACT tenga credenciales administrativas en el extremo. En situaciones en las cuales CounterACT no tiene credenciales administrativas, tales como BYOD, la inspección exhaustiva se puede realizar con la ayuda de nuestro agente SecureConnector opcional, que está incluido en CounterACT sin gastos adicionales.

Cumplimiento de extremos: Garantice que los extremos de la red cumplan con las políticas de antivirus, que tengan los parches correspondientes y que no tengan software ilegal. CounterACT identifica automáticamente las violaciones de las políticas, corrige las deficiencias de seguridad de los extremos y mide el cumplimiento de los mandatos normativos.

Detección de amenazas: La supervisión permanente aporta conocimientos más precisos y oportunos que las exploraciones de vulnerabilidad en momentos puntuales, ya que algunos dispositivos pueden entrar en la red y salir de ella.

Detección de dispositivos no autorizados: Detecte infraestructura no autorizada, tal como conmutadores y puntos de acceso inalámbricos no autorizados. CounterACT incluso puede detectar dispositivos sin dirección IP, por ejemplo, dispositivos furtivos de captura de paquetes que están diseñados para robar información confidencial.

Acceso

Registro de invitados: Deje que los invitados accedan a la red sin poner en riesgo la seguridad de la red interna. Varias opciones de registro de invitados le permiten adaptar el proceso de admisión de invitados según las necesidades de la organización.

Acceso basado en funciones: CounterACT garantiza que solo los usuarios correctos con los dispositivos adecuados tengan acceso a los recursos de red apropiados. Aprovecha el directorio existente en el que haya asignado funciones a las identidades de usuarios.

Opciones flexibles de control: A diferencia de los productos NAC "de las primeras generaciones", que emplean controles de acceso que requieren mucha intervención e implican interrupciones para los usuarios, ForeScout CounterACT proporciona un espectro completo de opciones de implementación que le permiten adaptar la respuesta al contexto de la situación. Resuelva las violaciones de bajo riesgo mediante el envío de una notificación al usuario final o la corrección automática del problema de seguridad, lo que permite al usuario mantener la productividad mientras se realizan las tareas de corrección (consulte la ilustración 2).

Autenticación 802.1X o no: Puede elegir la autenticación 802.1X u otras tecnologías de autenticación, como LDAP, Active Directory®, RADIUS®, Oracle® y Sun. El modo híbrido le permite utilizar varias tecnologías simultáneamente, lo que agiliza la implementación de NAC en los entornos grandes y diversos.

RADIUS incorporado: Un servidor RADIUS incorporado facilita la implementación de 802.1X. También le permite aprovechar servidores RADIUS configurando CounterACT para que funcione como proxy RADIUS.

Modelos ampliables

CounterACT tiene una trayectoria comprobada en redes de clientes con más de 1.000.000 de extremos. Se presenta en una variedad de opciones de appliances virtuales y físicos para satisfacer las necesidades específicas de su empresa. Las redes grandes que necesitan múltiples appliances se pueden administrar de forma centralizada con CounterACT Enterprise Manager. Cada appliance de CounterACT incluye una licencia perpetua para una cantidad especificada de dispositivos de red. Para consultar detalles de licencia, visite www.forescout.com/licensing.

Administración y control centralizados

CounterACT Enterprise Manager se puede implementar como appliance virtual o físico para proporcionar administración y control centralizados de las implementaciones de CounterACT. Supervisa las actividades y políticas de CounterACT, y recopila información sobre actividad malintencionada en cada appliance, así como las acciones de identificación, notificación, restricción y corrección ejecutadas por CounterACT. Esta información está disponible para visualización e informe en la consola CounterACT.

Obtenga más información en
www.ForeScout.com

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.
** Gartner, Inc., "Magic Quadrant for Network Access Control" (Cuadrante mágico de Gartner para el control de acceso a la red [NAC]), Lawrence Orans y Claudio Neiva, 10 de diciembre de 2014. Gartner no respalda a ningún proveedor, producto ni servicio al que se haga referencia en sus publicaciones de investigación, y no aconseja a los usuarios de tecnología que seleccionen solo a aquellos proveedores con las calificaciones más altas ni otra designación. Las publicaciones de investigación de Gartner constan de sus opiniones de la organización de investigación y no deben interpretarse como declaraciones de hechos. Gartner no se hace responsable de ninguna garantía, explícita o implícita, con respecto a esta investigación, incluso cualquier garantía de comerciabilidad o aptitud con un propósito en particular.