# ForeScout CounterACT
## Control de acceso a la red

Hoja de datos

## Aspectos destacados

### Características

- **Fácil de implementar.** No requiere agentes de extremos. No requiere cambios de infraestructura. Todo en una sola aplicación.
- **Rápido tiempo de amortización.** Visibilidad completa de toda la red en horas o días.
- **Cobertura del 100 %.** Dispositivos administrados y no administrados. LAN con cableado e inalámbricas. Servidores, equipos de escritorio, teléfonos inteligentes y tabletas.
- El potente motor de políticas lo ayuda a automatizar un amplio espectro de acciones para controlar el acceso a la red, corregir los extremos o enviar alertas al soporte técnico.

### Beneficios

- **Visibilidad.** Vea la red completa (dispositivos, extremos, usuarios, aplicaciones).
- **Seguridad.** Proteja los datos confidenciales y bloquee la actividad amenazante.
- **Productividad.** Otorgue el nivel correcto de acceso a cada persona y dispositivo, sin intervención intrusiva ni participación del personal.
- **Confiabilidad.** Mejore la estabilidad de red identificando y eliminando la infraestructura no autorizada.
- **Ahorros de costos.** Elimine el trabajo manual asociado con la apertura y el cierre de los puertos de red para el acceso de invitados, y la resolución de problemas y el tiempo de inactividad causado por los dispositivos de red no autorizados.

ForeScout

## Control de acceso a la red

ForeScout CounterACT™ es una plataforma de control de seguridad automatizada que le permite ver, supervisar y controlar todo lo que se encuentra en la red: todos los dispositivos, todos los sistemas operativos, todas las soluciones y todos los usuarios. ForeScout CounterACT permite que los empleados y los invitados sigan siendo productivos en la red a la vez que protege los recursos de red importantes y los datos confidenciales.

Basada en tecnologías de control de acceso a la red (NAC) de tercera generación, ForeScout CounterACT es fácil de instalar, porque no requiere software, agentes, actualizaciones de hardware ni reconfiguraciones. Todo se encuentra en una única aplicación.

### Riesgos de seguridad y puntos ciegos de la red

Tradicionalmente, la seguridad de la red se ha enfocado en el bloqueo de los ataques externos con cortafuegos y sistemas de prevención de intrusos. Estos dispositivos no hacen nada para proteger la red contra las amenazas internas, como estas:

- **Visitantes:** cuando los invitados y los contratistas van a su instalación, llevan sus equipos. Para seguir siendo productivos, los invitados necesitan acceso a Internet y los contratistas pueden necesitar recursos adicionales. Si brinda acceso ilimitado a estos visitantes, se arriesga a sufrir ataques de software malintencionado o comprometer los datos confidenciales.
- **Usuarios inalámbricos y móviles:** sus empleados desean utilizar sus teléfonos inteligentes y tabletas en la red. Si no tiene un control adecuado, estos dispositivos pueden infectar la red o ser fuentes de pérdida de datos.
- **Dispositivos no autorizados:** los empleados bienintencionados pueden extender la red con concentradores de cableado de bajo costo y puntos de acceso inalámbricos. Estos dispositivos pueden hacer que la red se vuelva inestable y ser fuentes de infección y pérdida de datos.
- **Software malintencionado y redes de bots:** estudios muestran que incluso las empresas bien administradas tienen equipos infectados debido a ataques de día cero o antivirus desactualizados. Una vez comprometido el equipo, pueden ocasionar «ataques dinámicos», en los que los extraños pueden analizar la red y robar los datos.
- **Cumplimiento:** los extremos pueden estar configurados incorrectamente, las máquinas virtuales pueden aparecer en la red con una configuración inadecuada y los controles de seguridad se pueden desactivar. Los sistemas que no cumplen con las políticas son riesgos de seguridad.

### Funcionamiento de ForeScout CounterACT

ForeScout CounterACT es diferente de la mayoría de las soluciones de control de acceso a la red (NAC) porque se implementa con facilidad y proporciona resultados rápidamente. Todo se encuentra en una aplicación simple que interactúa con la infraestructura de red existente. No debe instalar software ni agentes, ni actualizar hardware.

ForeScout CounterACT se implementa fuera de banda conectando al puerto SPAN de uno de los conmutadores existentes. Desde esa posición, CounterACT supervisa el tráfico de red y se integra con su infraestructura de red para poder ver los dispositivos nuevos en el momento en el que intentan acceder a la red. CounterACT otorga acceso automáticamente según el usuario, el dispositivo y la infraestructura de seguridad del dispositivo. Una vez que el dispositivo está en la red, CounterACT puede notificarle un problema de seguridad, solucionar el problema por usted o poner en cuarentena el extremo hasta que se resuelva el problema. CounterACT protege continuamente la red supervisando el comportamiento de todos los dispositivos y bloqueando los ataques.

*"Independientemente de cuál sea la estrategia de «Traer su propio dispositivo» (BYOD) seleccionada, será necesario contar la capacidad de detectar el uso de dispositivos no administrados con fines empresariales, y para eso se requiere NAC".*

**Gartner, "NAC Strategies for Supporting BYOD Environments" (Estrategias de NAC para admitir entornos de BYOD), 22 de diciembre de 2011, Lawrence Orans y John Pescatore**

## La diferencia de ForeScout

ForeScout CounterACT es considerablemente más fácil y rápido de implementar que los productos tradicionales de NAC. Este es el motivo:

- **Una caja, un día para instalar.** Todo se encuentra en una aplicación simple. La configuración es sencilla gracias a los asistentes de configuración incorporados.
- **ForeScout trabaja con lo que usted tiene.** Todos los conmutadores, enrutadores, cortafuegos, extremos, sistemas de administración de revisiones, sistemas antivirus, directorios, sistemas de vales existentes: ForeScout CounterACT trabaja con todos ellos. No requerimos cambios de infraestructura ni actualizaciones de equipos.
- **Sin software.** ForeScout CounterACT no tiene agentes, lo que significa que trabaja con todos los tipos de extremos: administrados y no administrados, conocidos y desconocidos, autorizados y no autorizados. No se debe instalar ningún cliente.
- **No interrumpe.** A diferencia de los productos de NAC de primera generación que en cuanto se los empleaba interrumpían a los usuarios con controles de acceso que requerían mucha intervención, ForeScout CounterACT se puede implementar con un enfoque en etapas, lo que minimiza la interrupción y acelera los resultados. En esta etapa inicial, CounterACT le brinda visibilidad de los puntos problemáticos. Cuando quiera implementar el control automatizado, podrá hacerlo gradualmente, comenzando con las ubicaciones más problemáticas y eligiendo la acción de cumplimiento apropiada.
- **Resultados acelerados.** ForeScout CounterACT ofrece resultados útiles el primer día, ya que le otorga visibilidad de los problemas de la red. La base de conocimiento incorporada lo ayuda a configurar políticas rápida y correctamente.

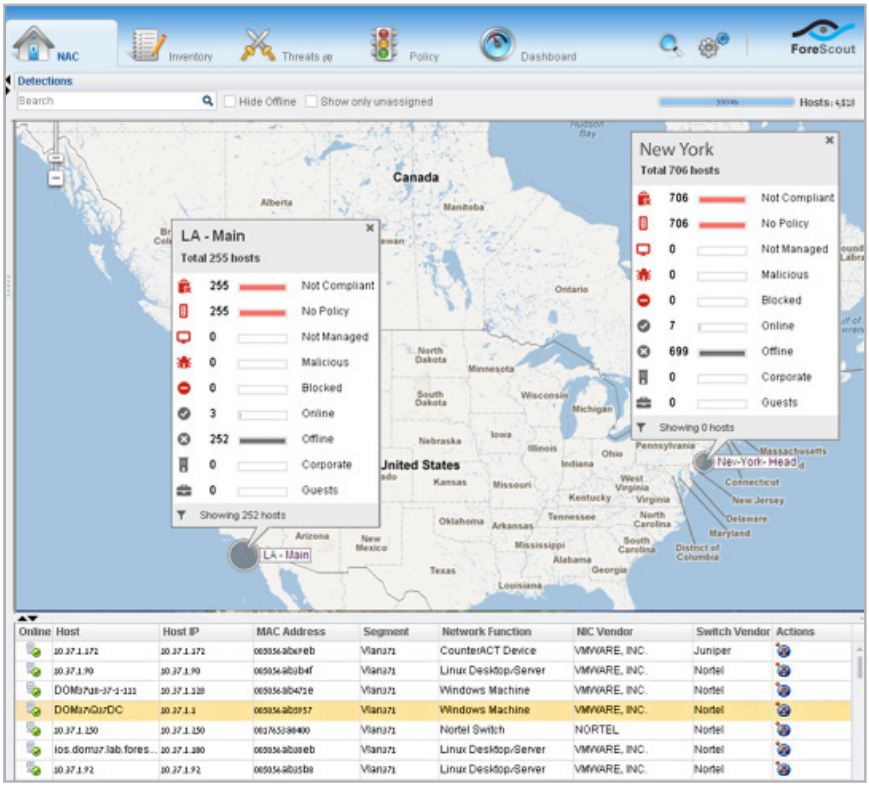


*Ilustración 1*: ForeScout CounterACT proporciona información de alto nivel y detallada de todos los dispositivos presentes en la red.

## Características

| General | | |
|---|---|---|
| **Tecnología ControlFabric™**<br>ForeScout CounterACT es el componente central de la arquitectura ControlFabric que permite que ForeScout CounterACT y otras soluciones intercambien información y solucionen una amplia variedad de problemas operativos, de red y de seguridad. | **Visibilidad**<br>El inventario de activos de ForeScout CounterACT proporciona visibilidad y control en tiempo real y en varios niveles, lo que permite rastrear y controlar usuarios, aplicaciones, procesos, puertos, dispositivos externos y más (consulte la ilustración 1). | **Integración en la infraestructura de TI**<br>A diferencia de los productos de NAC exclusivos, CounterACT es rápido y fácil de instalar, porque es compatible con una amplia gama de hardware y software de redes y seguridad de otros fabricantes, entre ellos, conmutadores de red, puntos de acceso inalámbricos, VPN, antivirus, administración de revisiones, sistemas de vales, SIEM, evaluación de la vulnerabilidad y administración de dispositivos móviles (MDM). |
| **Implementación fuera de banda**<br>ForeScout CounterACT se implementa fuera de banda, lo que elimina problemas sobre latencia y puntos potenciales de falla en la red. | **Administración de políticas**<br>ForeScout CounterACT le permite crear las políticas de seguridad apropiadas para su empresa. La configuración y la administración son rápidas y sencillas gracias al asistente de políticas integrado y la base de conocimiento de clasificaciones de dispositivos, reglas e informes de CounterACT. | **Escalabilidad**<br>ForeScout CounterACT se probó en redes de clientes que superaban los 250 000 extremos. Las aplicaciones de CounterACT están disponibles en una variedad de tamaños para adaptarse a redes de todos los tamaños. |
| **Informes**<br>ForeScout CounterACT cuenta con un motor de informes completamente integrado que lo ayuda a supervisar el nivel de cumplimiento de las políticas, cumplir con los requisitos normativos de auditoría y generar informes de inventario en tiempo real. | | |

| Extremos | | |
|---|---|---|
| **Cumplimiento de extremos**<br>ForeScout CounterACT puede garantizar que cada extremo de la red cumpla con las políticas de antivirus, que tenga las revisiones correspondientes y que no tenga software ilegal, como punto a punto (P2P). | **Detección de amenazas**<br>La tecnología patentada de detección de amenazas ActiveResponse™ de ForeScout CounterACT supervisa el comportamiento de los dispositivos después de la conexión. ActiveResponse bloquea las amenazas de día cero y autopropagación, y otros tipos de comportamiento malintencionado. A diferencia de otros enfoques, ActiveResponse no se basa en actualizaciones de firmas para mantener su efectividad, lo que se traduce en un costo bajo de administración. | **Detección de dispositivos no autorizados**<br>ForeScout CounterACT puede detectar infraestructura no autorizada, como conmutadores y puntos de acceso inalámbricos no autorizados, identificando si el dispositivo es un dispositivo traductor de direcciones de red (NAT) o si está en una lista de dispositivos autorizados, o reconociendo situaciones en las que un puerto de conmutador tiene varios hosts conectados. CounterACT puede detectar incluso dispositivos sin dirección IP, por ejemplo, dispositivos furtivos de captura de paquetes que están diseñados para robar datos confidenciales. |
| **Control de dispositivos móviles en tiempo real**<br>ForeScout CounterACT detecta y controla los dispositivos móviles portátiles conectados a su red Wi-Fi. Admite iPhone, iPad, Blackberry, Android, Windows Mobile y Nokia Symbian. | **Agente opcional**<br>ForeScout CounterACT no requiere un agente en el extremo, lo cual resulta importante al lidiar con BYOD. Si así lo desea, puede instalar el agente ligero de ForeScout en dispositivos con Android, iOS, Windows, Mac y Linux. Los agentes pueden instarse de manera automática cuando el dispositivo se conecta a la red y el usuario registra su identidad. | |

| Acceso | | |
|---|---|---|
| **Registro de invitados**<br>El proceso automatizado de ForeScout CounterACT permite a los invitados acceder a la red sin poner en riesgo la seguridad de la red interna. CounterACT incluye varias opciones de registro de invitados, lo que permite adaptar el proceso de admisión de invitados según las necesidades de la organización. | **Opciones flexibles de control**<br>A diferencia de los productos NAC de las primeras generaciones, que empleaban controles de acceso que requerían mucha intervención e implicaban 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. Las violaciones de bajo riesgo se pueden tratar 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). | **802.1x o no**<br>ForeScout CounterACT le permite elegir 802.1X u otras tecnologías de autenticación, como LDAP, Active Directory, 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 (consulte la ilustración 3). |
| **Acceso basado en funciones**<br>ForeScout CounterACT garantiza que solo los usuarios correctos con los dispositivos correctos tengan acceso a los recursos de red correctos. ForeScout aprovecha su directorio existente, en el que usted asigna funciones a las identidades de los usuarios. | **Autenticación**<br>CounterACT admite autenticación y directorios existentes basados en normas, como 802.1x, LDAP, RADIUS, Active Directory, Oracle y Sun. | **RADIUS incorporado**<br>ForeScout CounterACT incluye un servidor RADIUS incorporado para facilitar la implementación de 802.1X. También le permite aprovechar servidores RADIUS configurando CounterACT para que funcione como proxy RADIUS. |

| ALERTA Y CORRECCIÓN | RESTRICCIÓN DE ACCESO | TRANSFERENCIA Y DESHABILITACIÓN |
|---|---|---|
| Abrir vale problemático | Implementar un cortafuegos virtual firewall en un dispositivo infectado o que no cumple con las políticas | Reasignar el dispositivo de una VLAN de producción a una VLAN en cuarentena |
| Enviar notificación por correo electrónico | Reasignar el dispositivo a una VLAN con acceso restringido | Bloquear acceso con 802.1X |
| Capturas de SNMP | | Alterar las credenciales de inicio de sesión para bloquear el acceso |
| Syslog | Actualizar las listas de acceso (ACL) en los conmutadores, cortafuegos y enrutadores para restringir el acceso | Bloquear el acceso mediante autenticación de dispositivos |
| Secuestro del navegador HTTP | Transferir el dispositivo automáticamente a una red invitada preconfigurada | Desactivar el puerto del conmutador (802.1X o SNMP) |
| Confirmación de usuario final auditable | Secuestro de DNS | Bloqueo de puerto Wi-Fi |
| Autocorrección | | Bloqueo de VPN |
| Autocorrección | Implementar un cortafuegos virtual firewall en un dispositivo infectado o que no cumple con las políticas | Interrumpir aplicaciones ni autorizadas |
| Enviar a servicio web | | |
| Escribir en SQL y LDAP | | |
| Integrar con otros sistemas como SIEM, protección de extremos, administración de revisiones, evaluación de la vulnerabilidad, MDM, detección avanzada de amenazas, etc. | | |

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

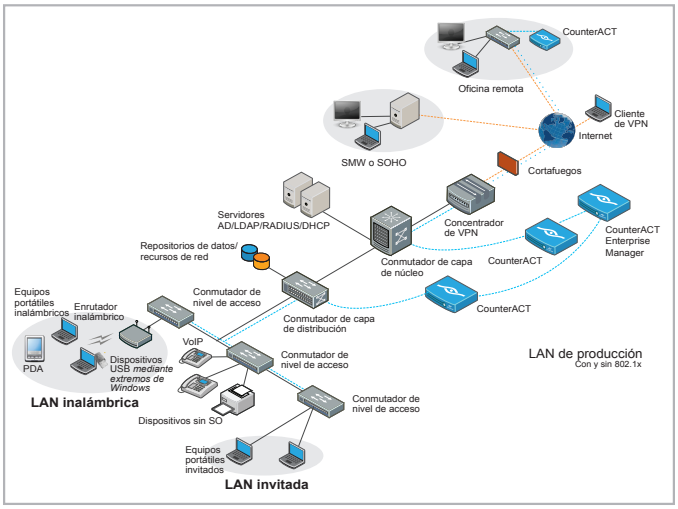


*Ilustración 3*: LAN de producción: con y sin 802.1x.

## Modelos escalables

ForeScout CounterACT se probó en redes de clientes que superaban los 250 000 extremos. Las aplicaciones de CounterACT están disponibles en una variedad de tamaños para adaptarse a redes de todos los tamaños. Las redes grandes que necesitan múltiples aplicaciones se pueden administrar centralmente con ForeScout CounterACT Enterprise Manager. ForeScout CounterACT está disponible en un factor de forma de aplicación física o virtual. Cada aplicación de ForeScout CounterACT incluye una licencia perpetua para una cantidad especificada de dispositivos de red. Las licencias están disponibles para 100, 500, 1000, 2500, 4000, y 10 000 dispositivos por aplicación. La solución ForeScout CounterACT está completamente integrada, con toda la funcionalidad en un único producto. Este modelo simple evita las cargas y los costos administrativos necesarios para mantener varios productos, componentes, portales y licencia.

A continuación, se muestran las especificaciones de la aplicación física. Para conocer las especificaciones de la aplicación virtual, visite **http://www.forescout.com/product/scalable-models.**

| | CT-R | CT-100 | CT-1000 | CT-2000 | CT-4000 | CT-10000 |
|---|---|---|---|---|---|---|
| **Dispositivos** | 100 | 500 | 1000 | 2500 | 4000 | 10 000 |
| **Ancho de banda** | 100 Mbps | 5 Mbps | 1 Gbps | 2 Gbps | Multi-Gbps | Multi-Gbps |
| **Puertos de red**<br>**Cobre**<br><br><br>**Fibra** | 4<br>10/100/1000<br><br>N/D | 4 a 8 (según el modelo específico)<br>10/100/1000<br><br>Opción disponible (hasta 2) | 4 a 8 (según el modelo específico)<br>10/100/1000<br><br>Opción disponible (hasta 4) | 4 a 8 (según el modelo específico) 10/100/1000<br><br>Opción disponible (hasta 4) | 4 a 8 (según el modelo específico)<br>10/100/1000<br><br>Opción disponible (hasta 4) | 4 a 8 (según el modelo específico)<br>10/100/1000<br><br>Opción disponible (hasta 4) |
| **Compatibilidad con E/S** | 1 puerto serie (RJ45) | 1 puerto serie (RJ45) | 1 puerto serie (RJ45) | 1 puerto serie (RJ45) | 1 puerto serie (RJ45) | 1 puerto serie (RJ45) |
| **Puertos USB** | 2, cumplen con USB 2.0 | 4 USB 2.0 en el panel trasero + 1 USB 1.1 en el panel delantero | 4 USB 2.0 en el panel trasero + 1 USB 1.1 en el panel delantero | 4 USB 2.0 en el panel trasero + 1 USB 1.1 en el panel delantero | 4 USB 2.0 en el panel trasero + 1 USB 1.1 en el panel delantero | 4 USB 2.0 en el panel trasero + 1 USB 1.1 en el panel delantero |
| **VGA** | 1 (DB15) | 1 (DB15) | 1 (DB15) | 1 (DB15) | 1 (DB15) | 1 (DB15) |
| **CD-ROM** | N/D | 1 | 1 | 1 | 1 | 1 |
| **Discos duros (HDD)** | 1 HDD | 3 HDD (RAID 1 + HS) | 3 HDD (RAID 1 + HS) | 3 HDD (RAID 1 + HS) | 3 HDD (RAID 1 + HS) | 3 HDD (RAID 1 + HS) |
| **Suministro de alimentación** | 1 hasta 60 W<br>100 a 240 V de CA (externa) | 1 hasta 650 W<br>100 a 240 V de CA | 2 hasta 650 W<br>100 a 240 V de CA | 2 hasta 750 W<br>100 a 240 V de CA | 2 hasta 750 W<br>100 a 240 V de CA | 2 hasta 750 W<br>100 a 240 V de CA |
| **Consumo de energía (máx.)** | 45,3 W | 648 W | 648 W | 744 W | 744 W | 744 W |
| **Temperatura**<br>**En funcionamiento**<br><br><br>**Almacenamiento** | 5 a 40 °C<br><br>0 a 70 °C | +10 °C a +35 °C (fluctuación no superior a 10 °C por hora)<br><br>-40 a +70 °C | +10 °C a +35 °C (fluctuación no superior a 10 °C por hora)<br><br>-40 a +70 °C | +10 °C a +35 °C (fluctuación no superior a 10 °C por hora)<br>-40 a +70 °C | +10 °C a +35 °C (fluctuación no superior a 10 °C por hora)<br><br>-40 a +70 °C | +10 °C a +35 °C (fluctuación no superior a 10 °C por hora)<br><br>-40 a +70 °C |
| **Requisito de refrigeración** | N/D | 2550 BTU/h | 2550 BTU/h | 2550 BTU/h | 2550 BTU/h | 2550 BTU/h |
| **Humedad** | 20 a 90 % | 90 %, sin condensación a 35 °C (sin funcionar) | 90 %, sin condensación a 35 °C (sin funcionar) | 90 %, sin condensación a 35 °C (sin funcionar) | 90 %, sin condensación a 35 °C (sin funcionar) | 90 %, sin condensación a 35 °C (sin funcionar) |
| **Chasis** | 1 U de escritorio (carcasa de acero de diseño compacto) | Bastidor de 1 U de 19″ | Bastidor de 1 U de 19″ | Bastidor de 2 U de 19″ | Bastidor de 2 U de 19″ | Bastidor de 2 U de 19″ |
| **Dimensiones** | Altura: 55 mm (2,17″)<br>Ancho: 335 mm (9,84″)<br>Profundidad: 213 mm (8,39″) | Altura: 43,2 mm (1,70″)<br>Ancho: 430 mm (16,93″)<br>Profundidad: 665,5 mm (26,2″) | Altura: 43,2 mm (1,70″)<br>Ancho: 430 mm (16,93″)<br>Profundidad: 665,5 mm (26,2″) | Altura: 87,30 mm (3,44″)<br>Ancho: 430 mm (16,93″)<br>Profundidad: 704,8 mm (25,75″) | Altura: 87,30 mm (3,44″)<br>Ancho: 430 mm (16,93″)<br>Profundidad: 704,8 mm (25,75″) | Altura: 87,30 mm (3,44″)<br>Ancho: 430 mm (16,93″)<br>Profundidad: 704,8 mm (25,75″) |
| **Envío** | Tamaño: 13,19 x 12,6 x 12,8″<br><br>Peso: 3,6 libras | Tamaño: 36 x 28 x 10″<br><br>Peso: 55 libras | Tamaño: 36 x 28 x 10″<br><br>Peso: 55 libras | Tamaño: 36 x 28 x 10″<br><br>Peso: 71 libras | Tamaño: 36 x 28 x 10″<br><br>Peso: 71 libras | Tamaño: 36 x 28 x 10″<br><br>Peso: 71 libras |

*Ilustración 4*: Especificaciones de la plataforma de CounterACT.

*NOTA:* Todos los dispositivos cumplen con la Parte 15 de las Reglas de la Comisión Federal de Comunicaciones (FCC), Clase A; CANADÁ y EE. UU: CSA 60950 y UL 60950 (seguridad); ROHS.

## Opciones de integración básicas

ForeScout CounterACT incluye una amplia variedad de opciones de integración con infraestructuras de TI y de red (conmutadores, controladores inalámbricos, VPN, enrutadores, directorios), extremos (Windows, Mac, Linux, iOS, Android, impresoras y otros dispositivos) y software de extremos (antivirus, mensajería instantánea, WMI, etc.). Estas opciones de integración están disponibles sin costo adicional mediante complementos de instalación sencilla. Estas opciones de integración básicas le confieren un enorme poder para descubrir y clasificar extremos; rastrear usuarios y aplicaciones; evaluar la infraestructura de seguridad; controlar el acceso a la red; aplicar políticas de cumplimiento y corregir brechas de seguridad, como agentes de seguridad de extremos dañados.

## Opciones de integración extendidas

Las opciones de integración extendidas de ControlFabric, desarrolladas y admitidas por ForeScout, aportan más valor a la aplicación CounterACT y están disponibles como módulos con licencia independiente que se pueden agregar a la aplicación CounterACT. Entre los módulos de integración actuales desarrollados y admitidos por ForeScout, se incluyen:

- Administración de eventos de información de seguridad (SIEM)
- Módulo de integración MDM
- Módulo de integración de detección avanzada de amenazas
- Módulo de integración de evaluación de la vulnerabilidad
- Módulo de integración McAfee ePO
- Módulo de seguridad móvil (integración con iOS y Android)

## Opciones de integración personalizadas

La interfaz abierta ControlFabric de ForeScout le permite a usted o a cualquier tercero implementar fácilmente nuevas opciones de integración basadas en protocolos que emplean estándares comunes. La interfaz ControlFabric se puede habilitar en la aplicación CounterACT mediante la compra de un módulo de integración de ControlFabric. Actualmente, el módulo de integración de ControlFabric admite los siguientes mecanismos basados en estándares: API de servicios web (disponible el cuarto trimestre de 2013), SQL, LDAP, Syslog.

## 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 ofrece seguridad de red dominante al permitir que las organizaciones supervisen y mitiguen de manera continua posibles brechas de seguridad y ataques cibernéticos. La aplicación CounterACT de la empresa identifica y evalúa de manera dinámica todos los usuarios, los extremos y las aplicaciones presentes en la red a fin de proporcionar visibilidad completa, inteligencia y mitigación basada en políticas de los problemas de seguridad. La tecnología ControlFabric abierta de ForeScout permite que una amplia variedad de sistemas de administración y productos de seguridad de TI compartan información e implementen acciones de corrección automatizadas. Gracias a que las soluciones de ForeScout son fáciles de implementar, discretas, flexibles y escalables, más de 1500 empresas y organismos de gobierno han manifestado su preferencia por ellas. Con sede en Campbell, California, ForeScout entrega las soluciones mediante su red de asociados autorizados globales. **Obtenga más información en www.forescout.com.**

ForeScout

**ForeScout Technologies, Inc.**
900 E. Hamilton Ave.,
Suite 300
Campbell, CA 95008
Estados Unidos

**Teléfono** 1-866-377-8771 (EE. UU.)
**Teléfono** 1-408-213-3191
(internacional)
**Fax** 1-408-213-2283 (internacional)
**www.forescout.com**



Doc: 2013.0016-P