Desafíos organizativos

- Mejorar la seguridad de la red general.
- Proteger datos confidenciales contra amenazas externas.
- No obstaculizar el acceso de empleados, contratistas y clientes.
- Cumplir con las políticas internas y la normativa externa.
- Mantener el valor de las inversiones de seguridad existentes.

Desafíos técnicos

- Detectar dispositivos desconocidos en la red que no están equipados con agentes de software.
- Identificar tipo y ubicación del dispositivo, identidad y función del usuario, y nivel de cumplimiento.
- Impedir que dispositivos infectados o sin cumplimiento propaguen malware.
- Evitar que ataques dirigidos roben datos o fuercen tiempo de inactividad de la red.
- Encontrar una solución de NAC para proporcionar la acción correcta para cada situación automáticamente, sin intervención humana.
- Medir la efectividad de los controles de seguridad y demostrar el cumplimiento de las normas.

Control de acceso a la red

Obtener visibilidad en tiempo real y control de los dispositivos apenas acceden a la red

ForeScout Technologies, Inc. ofrece soluciones únicas para el control y la gestión de los números y tipos de dispositivos de acceso a redes que crecen cada día más. Nuestro producto estrella, ForeScout CounterACT®, le ofrece visibilidad en tiempo real, lo que le permite detectar al instante dispositivos autorizados *y* no autorizados... y controlar el acceso como mejor le parezca.

El desafío

Las redes empresariales actuales abastecen una gran variedad de dispositivos tradicionales y no tradicionales, y otros extremos, desde computadoras, tabletas y teléfonos inteligentes hasta controles industriales, servidores virtualizados, puntos de acceso inalámbricos y aplicaciones en la nube. Y, sin duda, el alcance de los desafíos relacionados con los dispositivos se expandirá a medida que los BYOD*, la IoT*, los entornos de TI híbridos y la sofisticación de los hackers continúan haciendo progresos. Por lo tanto, su solución de Control de acceso a la red (NAC) debe gestionar los dispositivos corporativos y de propiedad de los empleados de los que tiene conocimiento, así como del creciente número de dispositivos no autorizados, "bajo el radar" que no conoce.

Aquí hay algunos hechos que refuerzan la necesidad de una solución de seguridad NAC integral y altamente inteligente:

- 26.000 millones de dispositivos en red y conectados se usarán para 2020[1].
- El 75 % de las aplicaciones móviles no pasarán las pruebas básicas de seguridad[2].
- El 98,7 % de los registros en riesgo fueron el resultado de pirateo externo en 2014[3].

Como gerente de sistemas de seguridad o de TI, tiene que saber si los dispositivos y los sistemas que intentar acceder a su red, o que ya han iniciado la sesión, están cumpliendo con las normas de seguridad de la organización.

La solución de ForeScout

ForeScout CounterACT® ofrece capacidades de NAC integrales y mucho más, basadas en la visibilidad en tiempo real de dispositivos apenas acceden a la red. Escanea continuamente la red y supervisa la actividad de dispositivos conocidos, corporativos, además de dispositivos desconocidos, como extremos personales y no autorizados. Y le permite automatizar y aplicar control de acceso a la red basado en políticas, cumplimiento de extremos y seguridad del dispositivo móvil. De hecho, ForeScout CounterACT ofrece una amplia gama de controles automatizados que preservan la experiencia del usuario y mantienen las operaciones del negocio en la medida de lo posible.

Las bases de la funcionalidad e inteligencia de CounterACT pueden resumirse en tres palabras:

Ver CounterACT ofrece la capacidad única de detectar dispositivos apenas se conectan a la red, sin necesidad de agentes de software o conocimientos previos del dispositivo. Genera un perfil y clasifica los dispositivos, usuarios, aplicaciones y sistemas operativos mientras supervisa continuamente los dispositivos administrados, dispositivos personales y otros extremos.

Controlar CounterACT permite, deniega o restringe el acceso a la red según el nivel del dispositivo y políticas de seguridad. Al evaluar y corregir los extremos maliciosos o de alto riesgo, mitiga la amenaza de violaciones de datos y ataques de malware que, de lo contrario, pondría a su organización en riesgo. Además, por el control y la supervisión continuas de los dispositivos de su red según las políticas de seguridad, CounterACT agiliza muchísimo su capacidad de demostrar el cumplimiento de la normativa y de los mandatos de la industria.

Orquestar CounterACT se integra con más de 70 productos** de red, seguridad, movilidad y gestión de TI mediante la arquitectura ForeScout ControlFabric®. Esta capacidad de compartir inteligencia de seguridad en tiempo real entre los sistemas y de aplicar una política de seguridad de red unificada reduce la exposición a vulnerabilidades mediante la automatización de la respuesta a amenazas en todo el sistema. Además, le permite obtener un mayor rendimiento de la inversión en sus herramientas de seguridad existentes y, al mismo tiempo, ahorrar tiempo a través de la automatización del flujo de trabajo.

ForeScout CounterACT recopila conocimientos contextuales profundos sobre el extremo, su ubicación, el propietario y el contenido. Puede asegurar lo siguiente:

- Los dispositivos no autorizados y las aplicaciones no sancionadas no acceden a la red.
- Los dispositivos autorizados están configurados con los últimos sistemas operativos; el software antivirus actualizado está instalado y funcionando, y las vulnerabilidades tienen sus respectivos parches.
- Los agentes de prevención de pérdida de datos y cifrado están trabajando.
- Los usuarios no pueden ejecutar aplicaciones no autorizadas o dispositivos periféricos en la red.

Cuando los extremos no están al nivel de los estándares de la organización, CounterACT inicia automáticamente una o más acciones de corrección y aplicación basadas en políticas, que van desde una notificación de incumplimiento por correo electrónico hasta corrección obligatoria (como actualización de software) y prevención de acceso o cuarentena absoluta. No hay necesidad de intervención humana ni trabajo manual asociados con la gestión de acceso de invitados, la ubicación de sistemas y la apertura o el cierre de puertos de red. El acceso a la red está controlado según la política.

Para más de 2000 empresas en más de 60 países**, ForeScout proporciona control de acceso a la red inteligente y rentable que cumple con los estándares más altos de seguridad y cumplimiento de la normativa, así como facilidad de uso e implementación. CounterACT se vende como un appliance virtual o físico que se implementa dentro de su infraestructura existente y, por lo general, no requiere cambios a la configuración de la red. El appliance de CounterACT se instala físicamente fuera de banda, por lo que evita la latencia o las cuestiones relacionadas con la posibilidad de fallo de red. Puede administrarse centralmente para gestionar decenas o cientos de miles de extremos de una consola.

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

1 Gartner Research, http://www.gartner.com/newsroom/id/2636073.
2 Gartner Research, septiembre de 2014 http://www.scmagazine.com/gartner-75-percent-of-mobile-apps-will-fail-security-tests-through-end-of-2015/article/372424/.
3 Investigación Privacy Rights Clearinghouse, http://www.securityweek.com/data-breaches-numbers.

* Traer sus dispositivos (BYOD), Internet de las cosas (IoT).
** A partir de enero de 2016.