FORESCOUT

Resumen de la solución

NAC moderno

Identifique todos los dispositivos, evalúe su estado de seguridad y aplique controles de acceso entre redes heterogéneas

> "Las herramientas de control de acceso a la red (NAC) son las más indicadas en la actualidad para ayudar a aislar dispositivos y entidades no aprobadas (usuarios, segmentos, dispositivos, etc.) para evitar que entren en "contacto" con la red. Utilice estas tecnologías NAC más modernas, de proveedores como Forescout, para mantener los elementos desconocidos y probablemente sin parches alejados de sus redes Zero Trust[1]".
>
> — Chase Cunningham, Analista principal, Forrester Research

Las redes actuales requieren una solución de control de acceso a la red (NAC) moderna, que sea no se limite a la mera autenticación de dispositivos. El control de acceso a la red moderno debe identificar dispositivos, evaluar el estado y el cumplimiento, aplicar controles de acceso entre redes heterogéneas, supervisar permanentemente todos los dispositivos conectados y automatizar la respuesta cuando se detectan incumplimientos de normativas o comportamientos inusuales.

Problemas

Las exigencias empresariales y de ciberseguridad siguen evolucionando, por lo que las organizaciones exigen mucho más a una solución NAC para hacer frente a estos problemas:

- El número de dispositivos no gestionados supera a los gestionados en muchas redes y no se pueden autenticar mediante métodos tradicionales.
- Cuantos más dispositivos gestionados hay, mayor es el riesgo y esto incluye la presencia de ángulos muertos.
- Las redes multiproveedor son muy habituales y necesitan alternativas a la autenticación 802.1X.
- Los sistemas corporativos remotos y BYOD que se conectan a la red generan nuevos problemas de administración de la seguridad.
- La incapacidad de automatizar la seguridad, el cumplimiento de normativas y las directivas de acceso genera un aumento de costes operativos y un exceso de trabajo manual.

La solución

Si estos problemas le resultan familiares, ahora es un momento extraordinario para evaluar el control de acceso a la red. La plataforma Forescout está redefiniendo el concepto de control de acceso a la red (NAC) y cómo puede resolver los problemas empresariales y de ciberseguridad a los que se enfrenta su empresa. Y con Forescout, el NAC moderno es fácil de desplegar y no genera interrupciones. Su empresa disfrutará de visibilidad completa de todos los dispositivos en cuestión de días a partir de la implementación, con controles basados en

directivas normalmente operativos en algunas semanas.

Nuestra plataforma de NAC ofrece funciones de seguridad de red fundamentales que no se limitan a la simple autenticación. Estas nuevas funciones incluyen la identificación granular de dispositivos/usuarios, la evaluación del estado y el cumplimiento de normativas, la supervisión permanente de dispositivos, las opciones de control flexibles y la respuesta automatizada.

Los enfoques de NAC tradicionales no pueden autenticar de forma segura los sistemas no tradicionales que se conectan a las redes de campus hoy día, como los dispositivos del Internet de las cosas (IoT). Además, dependen de agentes para evaluar el estado de seguridad y cumplimiento de los ordenadores tradicionales. Las funciones de detección e identificación de Forescout reconocen, clasifican y evalúan de forma precisa todos estos dispositivos para que pueda crear directivas de acceso con contexto. La plataforma Forescout trabaja con o sin agentes, con o sin autenticación 802.1X, y supervisa continuamente todos los dispositivos de su red.

"Nos dijeron que podríamos desplegar la plataforma Forescout en una tarde. Uno de los miembros de mi equipo y yo nos miramos y pensamos... sí, claro. Pero lo cierto es que la desplegamos en unas horas".

— Mike Roling, CISO, estado de Misuri

Identificación: descubrimiento, clasificación e inventario de todos los dispositivos conectados

Con la plataforma Forescout, los equipos de seguridad y de TI consiguen en tiempo real visibilidad íntegra de todos los dispositivos conectados mediante IP, en el momento en el que acceden a la red, lo que les permite disponer de un inventario de recursos preciso y actualizado.

- Elija entre más de 20 métodos de descubrimiento e identificación activos y pasivos, en función de su entorno empresarial, y garantice la disponibilidad permanente de la red.
- Los más de 12 millones de huellas digitales de dispositivos de Forescout Device Cloud le ofrecen funciones de clasificación de dispositivos tridimensional y de gran fiabilidad, para determinar la función, sistema operativo, proveedor, modelo, etc., del dispositivo.
- Consiga una cobertura total en todas las ubicaciones, redes y tipos de dispositivos (sin ángulos muertos), con o sin autenticación 802.1X.

Cumplimiento: evaluación del estado de seguridad y cumplimiento de normativas

Las herramientas de seguridad basadas en agente son incapaces de detectar los dispositivos gestionados que o bien carecen de agente o bien tienen un agente que está dañado o no funciona correctamente. Además, como no se pueden instalar agentes de seguridad en los dispositivos IoT, es imposible evaluarlos, lo que aumenta todavía más la superficie de ataque. Sin embargo, con la plataforma Forescout, puede automatizar la evaluación del estado y la corrección de todos los dispositivos basados en IP tras la conexión y, a partir de ahí, de manera permanente.

- Encuentre y corrija los dispositivos gestionados sin agentes o con los agentes dañados de sus herramientas de seguridad actuales.
- Detecte el incumplimiento de normativas en los dispositivos, los cambios en el estado de seguridad, las vulnerabilidades, las credenciales débiles, los indicadores de peligro (IoC), los intentos de suplantación y otros indicadores de alto riesgo, todo ello sin agentes.
- Evalúe y supervise continuamente los dispositivos no gestionados, incluidos los que no pueden aceptar agentes, para garantizar el cumplimiento de normativas de seguridad.

"Es increíble la cantidad de información que obtenemos con la plataforma Forescout. Es de lejos la mejor herramienta que jamás he utilizado para buscar, identificar y controlar adecuadamente los sistemas. Para nosotros ha sido tremendamente útil".

— Joseph Cardamone, analista sénior de seguridad de la información, Haworth International

Amplíe el valor de sus inversiones de seguridad y TI

La mayoría de las herramientas de seguridad se limitan a marcar las infracciones y a alertar a su personal.

La plataforma Forescout incluye módulos plug-and-play que amplían la visibilidad y el control para que pueda:

- Compartir contexto de dispositivos en tiempo real con sus herramientas de administración de seguridad y TI.
- Organizar los flujos de trabajo y automatizar las medidas de respuesta.
- Evaluar de manera permanente el estado de seguridad y garantizar el cumplimiento de normativas de los dispositivos autocorregidos.

Descubra cómo en www.forescouttechnologies.es.

"La plataforma y las funciones de [Forescout] para la seguridad de IoT/TO destacan frente a las de competencia. La máxima visibilidad, que se traduce en un excelente control operativo y, en última instancia, en mayor seguridad es el núcleo del enfoque de seguridad Zero Trust de Forescout[2]."

— Forrester Research

Conexión: aplicación de las directivas de acceso entre redes heterogéneas

La plataforma Forescout aplica un modelo de seguridad Zero Trust basado en la identidad de los dispositivos y usuarios, la higiene de dispositivos y el estado de cumplimiento en tiempo real, sin necesidad de aplicar actualizaciones de hardware o software en la infraestructura.

- Proporcione acceso de mínimo privilegio a los recursos empresariales según la función del usuario, el tipo de dispositivo y el estado de seguridad.
- Impida que se conecten dispositivos no autorizados, no fiables o que suplantan a otros.
- Afronte las auditorías internas y las normativas externas con confianza, sabiendo que los controles de seguridad desplegados garantizan el cumplimiento sin afectar al rendimiento de los usuarios.

Por qué Forescout:

1. Despliegue rápido, flexible y sin interrupciones.
2. Evaluación sin agente del estado y el riesgo.
3. Rápida creación de valor y rentabilidad.
4. Sin dependencia de proveedores; utilice su infraestructura actual.
5. Sin necesidad de actualizaciones de software ni hardware.
6. Integraciones con los principales productos de seguridad y TI.
7. Evite la complejidad y costes operativos de la autenticación 802.1X en redes cableadas.
8. Categoría empresarial: capacidad para un total de 2 millones de endpoints.
9. Motor de directivas robusto que automatiza la respuesta a incidentes para acelerar el tiempo medio de respuesta.
10. Plataforma Zero Trust de Forrester.

Dé un paso adelante:

- Solicite una demostración de Forescout
- Visite nuestro sitio web www.forescouttechnologies.es

***Notas**

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook, Forrester Research, 2 de enero de 2019
2. Forrester Wave™: Zero Trust eXtended Platform Providers, 4.º trim. 2019

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San José, CA 95134 EE. UU.

C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Soporte técnico +1-708-237-6591

Más información en forescouttechnologies.es