FORESCOUT
Active Defense for the Enterprise of Things™

NAC moderno

Seguridad Zero Trust, sin agente, flexible y sin interrupciones
Empresa de las cosas

En la actualidad, las empresas necesitan una forma de implementar y mantener acceso de confianza cero (Zero Trust) para todos los tipos de redes y sistemas que conectan: ordenadores de campus, dispositivos de visitantes, portátiles para el teletrabajo, o dispositivos del IoT, OT e inteligentes. Además, requieren una plataforma de control de acceso a la red (NAC) que pueda:

- Identificar continuamente todos los componentes que se conectan.
- Evaluar su estado.
- Aplicar directivas de acceso.
- Implementar de forma automática controles para comportamientos que no cumplen las normativas o son inusuales

La estrategia Zero Trust es más difícil de lo que parece

Controlar absolutamente todo lo que se conecta a las redes corporativas no es tarea fácil. Los técnicos informáticos y los arquitectos de seguridad que implementan estos sistemas se enfrentan a obstáculos como los siguientes:

- Las soluciones NAC antiguas no funcionaron debido a su complejidad o a los riesgos de que se produjera un impacto negativo en las operaciones empresariales.
- Los dispositivos IoT y OT que proliferan en las redes empresariales no se pueden autenticar o controlar con agentes tradicionales.
- Los controles basados en 802.1X no se pueden aplicar en redes de varios proveedores.
- Los análisis de redes programados no tienen en cuenta los intentos de suplantación y otras amenazas que pueden surgir en cualquier momento.
- Muchas de las alternativas de acceso Zero Trust cuestan demasiado y/o requieren demasiado esfuerzo manual.

> **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 MISSOURI**

forescout.com/platform/eyeControl info-espana@forescout.com Tel. (internacional) +1-408-213-3191

Forescout: la mejor solución de NAC moderna de su categoría

Si conoce estos obstáculos que hemos citado, ahora es un momento extraordinario para evaluar el control de acceso a la red Forescout. Podemos satisfacer sus necesidades y superar sus expectativas mediante:

La visibilidad más integral

Consiga un 100 % de visibilidad de todos los dispositivos conectados a sus redes ampliadas, en tiempo real, debido a nuestras más de 20 técnicas activas y pasivas.

Zero Trust para todos los dispositivos conectados

Contenga el impacto de los ataques, gracias la supervisión continua sin agente y con un motor de directivas unificadas que segmenta y aísla de manera dinámica todo lo que se conecte a su empresa.

Despliegue sin interrupciones, con ventajas inmediatas para su red

Consiga visibilidad total en días y control automatizado en semanas, gracias a un software sin agente que no necesita actualizaciones de infraestructura ni configuración de 802.1X.

Demostrada para redes empresariales ampliadas

Nuestros miles de clientes del Fortune 1000 satisfechos, algunos con 2 millones de endpoints, avalan las funciones y la confianza que les otorga Forescout para garantizar la seguridad de sus redes.

AMPLÍE EL VALOR DE SUS INVERSIONES EN SEGURIDAD E IT

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 e IT.
- 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.

“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

IDENTIFICACIÓN

Descubrimiento, clasificación e inventario de todos los dispositivos conectados

Con la plataforma Forescout, los equipos de seguridad y de IT 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 los dispositivos IoT no admiten agentes de seguridad, es imposible evaluarlos, lo que aumenta todavía más la superficie de ataque. Sin embargo, con la plataforma Forescout, puede automatizar la evaluación del estado de todos los dispositivos basados en IP y su corrección, al conectarse y, a partir de ahí, de manera permanente.

- Encuentre y corrija los dispositivos gestionados que no tienen agentes o tienen agentes de sus herramientas de seguridad actuales que están dañados o no funcionan.
- Detecte en los dispositivos el incumplimiento de normativas, 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.

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

- Evalúe y supervise continuamente los dispositivos no gestionados, incluidos los que no pueden aceptar agentes, para garantizar el cumplimiento de normativas de seguridad.

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 basado en un mínimo de privilegios 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.
- Implemente controles flexibles en la infraestructura cableada, inalámbrica y de VPN, con o sin 802.1X.

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook, Forrester Research, 2 de enero de 2019

2. Forrester WaveTM: Zero Trust eXtended Platform Providers, 4.º trim. 2019

La plataforma y las funciones [de Forescout] para la seguridad de IoT/OT 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

No se conforme con verlo. Protéjalo.

Póngase en contacto con nosotros hoy mismo para proteger su Empresa de las cosas.

forescout.com/platform/eyeControl info-espana@forescout.com Tel. (internacional) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

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