FORESCOUT
Active Defense for the Enterprise of Things™

Control de acceso a la red moderno

Por qué la visibilidad y control de dispositivos sin agentes es fundamental para una ciberseguridad eficaz

Visibilidad y control de dispositivos: Por qué es necesario

A capacidad de detectar, clasificar, evaluar y controlar todos los dispositivos que se conectan a la red es una condición indispensable para conseguir una seguridad Zero Trust. Solo el conocimiento en tiempo real de todos los endpoints de cada segmento, la información detallada sobre el estado de la seguridad y un control de acceso y corrección automatizados basados en directivas le permitirán garantizar con fiabilidad la seguridad de datos y sistemas, y al mismo tiempo responder con rapidez y precisión a los incidentes.

100%

VISIBILIDAD EN TIEMPO REAL

Los agresores buscan continuamente dispositivos no gestionados y desprotegidos, y tarde o temprano acaban por encontrar y aprovechar los puntos ciegos. La visibilidad y el control sin agentes son las piedras angulares de la seguridad y el cumplimiento de las normativas. También juegan un papel fundamental a la hora de hacer frente a un buen número de desafíos empresariales. Por ejemplo, una visibilidad de dispositivos continua en profundidad genera un **inventario de activos en tiempo real** preciso, que permite al personal de seguridad y de TI reducir los costes operativos, al tiempo que ayuda a garantizar el cumplimiento de normativas y a evitar auditorías fallidas.

forescout.com/solutions/network-access-control info-espana@forescout.com Tel. (internacional) +1-408-213-3191

Por qué es difícil contar con visibilidad y control

El método convencional de administrar los endpoints de una red consistía en instalar un agente de software en cada dispositivo. Esto funcionaba bastante bien cuando los endpoints eran estáticos, y cuando se utilizaban PC y servidores propiedad de la empresa. Pero la movilidad, la diversidad de tipos de dispositivos y la virtualización han complicado mucho la visibilidad y control contextual.

El aumento explosivo del número y la diversidad de dispositivos ha alterado radicalmente el panorama de dispositivos. Los sistemas ciberfísicos, como los dispositivos del Internet de las cosas (IoT) y los sistemas de tecnología operativa (OT) se conectan ahora a la red corporativa. Muchos de los empleados trabajan desde casa, y algunos se conectan a la nube. La empresa moderna ha evolucionado rápidamente para convertirse en **Enterprise of Things** (Empresa de las cosas), y la mayoría de las "cosas" no admiten agentes de administración. Incluso en los casos en los que los admiten, un enfoque basado en agentes genera problemas:

- Los sistemas basados en agentes no funcionan cuando el agente no está presente, está roto o desactivado.
- Los métodos basados en agentes y en autenticación 802.1X generan ángulos muertos en su red y crean complejidad operativa, que a menudo da lugar a despliegues incompletos.
- Las herramientas aisladas para el cumplimiento de los dispositivos carecen de una vista unificada, y perpetúan los ángulos muertos.
- El número de dispositivos no gestionados supera a los gestionados en muchas redes y no se pueden autenticar mediante métodos tradicionales.
- Los dispositivos móviles, BYOD, de invitados y los empleados que trabajan desde casa convierten la seguridad basada en agentes en una tarea laboriosa e ineficaz.
- Las redes multiproveedor son muy habituales y necesitan alternativas a la autenticación 802.1X que no requieran actualizaciones de hardware ni software.

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].

DR. CHASE CUNNINGHAM
ANALISTA PRINCIPAL, FORRESTER RESEARCH

La solución de Forescout el control de acceso a la red moderno (NAC) moderno

Forescout Technologies es el precursor de una estrategia de seguridad de control de acceso a la red sin agentes que aborda los desafíos habituales de los entornos dinámicos y variados de nuestros días.

La plataforma Forescout proporciona una visión continua y unificada de todos sus dispositivos en campus, datacenters, la nube y redes de OT. Ofrece visibilidad continua y detallada de:

- Dispositivos en redes de campus: portátiles, tablets, smartphones, sistemas BYOD/de invitados y dispositivos IoT
- Infraestructuras de datacenters: máquinas virtuales, hipervisores, servidores físicos y otros componentes de redes virtuales y físicas
- Infraestructuras de nube pública y privada: AWS®, Microsoft® Azure® y máquinas virtuales VMware®
- Sistemas de control industrial (ICS) y OT: dispositivos médicos, industriales y de automatización de edificios
- Infraestructuras de red físicas y definidas por software: conmutadores, routers, firewalls, VPN, puntos de acceso inalámbricos y controladoras

La visibilidad de dispositivos más completa: sin ángulos muertos

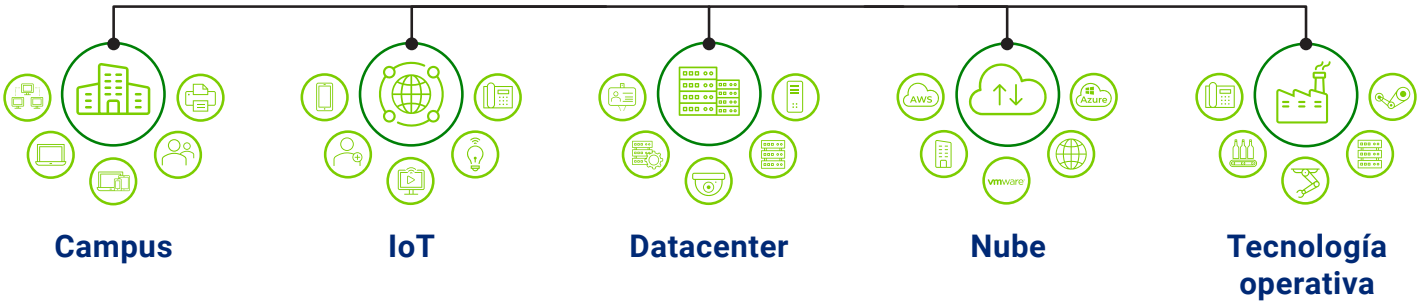


Figura 1: La visibilidad de dispositivos de Forescout se adapta a toda la empresa para proporcionar un inventario de activos detallado y en tiempo real de todo lo que se conecta a la red.

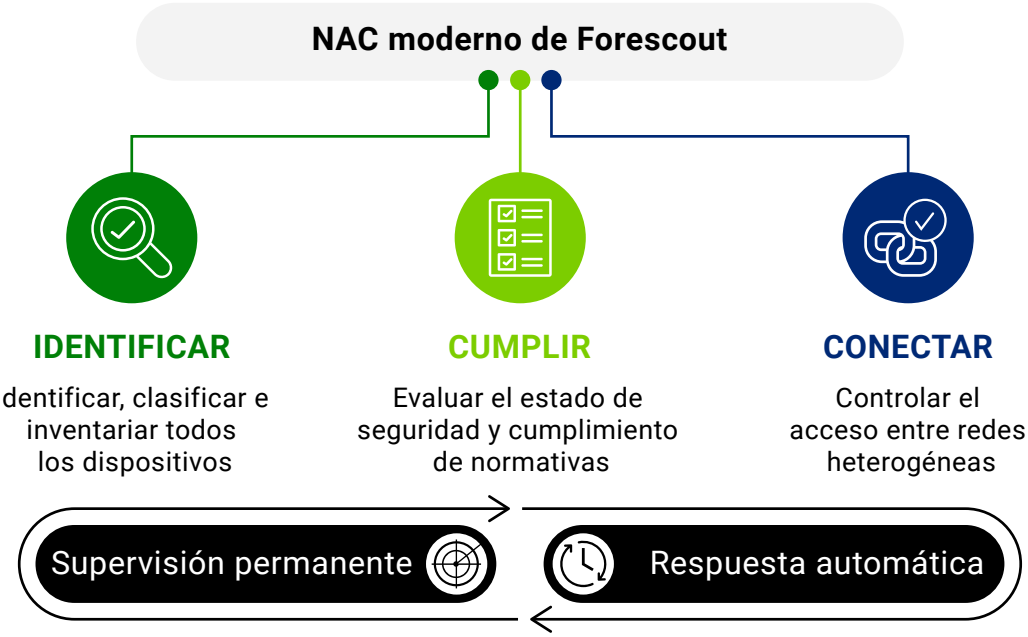


Figura 2: La solución de control de acceso a la red moderno de Forescout aporta funciones esenciales para cualquier red heterogénea sin necesidad de agentes de software ni autenticación 802.1X.

Nuestra estrategia

La solución de control de acceso a la red (NAC) moderno de Forescout permite a las organizaciones de TI:

- Elegir entre más de 20 técnicas activas y pasivas para disfrutar del descubrimiento de dispositivos sin agente más completo en todas las ubicaciones, redes y tipos de dispositivos, sin ángulos muertos.
- Clasificar de forma automática y precisa los dispositivos según su función, sistema operativo y versión, proveedor y modelo.
- Crear y mantener automáticamente un inventario de activos en tiempo real de cada dispositivo conectado mediante IP en su red ampliada.
- Evaluar y supervisar de forma permanente el estado de seguridad de todos los dispositivos, sin agentes.
- Cumplir con las directivas de seguridad y normativas de la industria mediante la automatización de la corrección de endpoints.
- Aplicar controles de red flexibles basados en la autenticación, la función del usuario, el tipo de dispositivo y el estado de seguridad, en cualquier red cableada, inalámbrica o VPN heterogénea.
- Aplicar el control de acceso con privilegios mínimos para una seguridad de confianza cero o Zero Trust.

Cómo identificamos todos los dispositivos de todas las redes

La plataforma Forescout ofrece más de 20 técnicas configurables de recopilación de información que disfrutan de una profunda integración con conmutadores, routers, puntos de acceso inalámbrico, firewalls, concentradores VPN, datacenters y soluciones en la nube de proveedores líderes de IT y OT. La plataforma escucha pasivamente el tráfico de la red, analiza numerosas secuencias de protocolos y puede interaccionar directamente tanto con la infraestructura de red como con los endpoints.

Las técnicas de visibilidad de Forescout incluyen:

- Métodos **pasivos tanto para la red como para el dispositivo final**. Algunos ejemplos son: recepción de capturas SNMP de conmutadores y controladoras inalámbricas, supervisión de puertos SPAN y análisis de secuencias de protocolos en el tráfico (Forescout incluye inspección profunda de paquetes para más de 150 protocolos de IT y OT), recopilación y análisis de datos de flujos y evaluación de solicitudes DHCP y tráfico de agentes de usuario HTTP. Si se implementa autenticación 802.1X, Forescout también supervisa solicitudes RADIUS mediante un servidor incorporado o externo.
- Métodos **activos en la infraestructura de red**. Un ejemplo sería la petición de una lista de las máquinas virtuales y los dispositivos conectados a conmutadores, concentradores VPN, controladoras inalámbricas y controladoras de nube privada y pública. Para obtener datos de usuarios y dispositivos, la plataforma Forescout consulta los servicios de directorio, las aplicaciones web o las bases de datos externas.
- Métodos **activos en el dispositivo final**. Algunos ejemplos son el análisis de los segmentos de la red en busca de dispositivos conectados con NMAP, la inspección remota de dispositivos Windows con WMI o de dispositivos Mac y Linux con SSH y la identificación del perfil de los endpoints mediante consultas SNMP.

Técnicas de visibilidad de dispositivos

TÉCNICAS PASIVAS	ACTIVAS EN INFRAESTRUCTURA	ACTIVAS EN DISPOSITIVO FINAL
Capturas SNMP	Sondeo de la infraestructura de red física	Inspección sin agente Windows (WMI, RPC, SMB)
Tráfico SPAN • Solicitudes DHCP • Agente de usuario HTTP • Huella digital TCP • Análisis de protocolos médicos (20 protocolos) • Análisis de protocolos ICS de OT (más de 70 protocolos)	Integración en la infraestructura de red basada en controladora • Juniper Mist • Cisco ACI, Cisco Meraki	Inspección sin agente macOS, Linux (SSH)
Análisis de flujo • NetFlow • Flexible NetFlow • IPFIX • sFlow	Integración en nube privada (infraestructura virtual) • VMware	NMAP
Solicitudes DHCP (vía IPhelper)	Integración en nube pública • AWS • Azure	Consultas SNMP a endpoints
Agente de usuario HTTP (vía redirección de URL)	Consulta de servicios de directorio (LDAP)	Inspección basada en agente (SecureConnector)
Solicitudes RADIUS	Consulta de aplicaciones web (REST)	
OUI MAC	Consulta de bases de datos externas (SQL)	
	Coordinación (ITSM, UEM, EPP, EDR, VA)	

Figura 3: Métodos de visibilidad de dispositivos de Forescout

Ventajas de contar con múltiples métodos de visibilidad de dispositivos

Al ofrecer muchos métodos diferentes, fácilmente configurables durante la instalación (y fácilmente modificables después), la plataforma Forescout es inigualable en flexibilidad, eficacia y efectividad.

Despliegue rentable y simplificado en grandes entornos: la capacidad para elegir entre más de 20 técnicas activas y pasivas ofrece la flexibilidad de conseguir visibilidad de dispositivos en cualquier red heterogénea, independientemente de la complejidad, tamaño o número de ubicaciones remotas de la red, todo sin necesidad de actualizaciones de infraestructura (software/hardware) ni el despliegue de un dispositivo local en cada sitio/oficina remota.

Sin ángulos muertos: no es infrecuente que los clientes empresariales tengan ubicaciones remotas que no pueden desplegar dispositivos adicionales ni ofrecer tráfico SPAN. Nuestra capacidad de aprovechar varias técnicas pasivas y activas resuelve las limitaciones de red y aporta una cobertura de dispositivos total, sin ángulos muertos.

Detección, clasificación y evaluación solo pasiva en redes del sector sanitario y OT/ICS críticas: las redes críticas suelen ser entornos inadecuados para las técnicas activas de sondeo y búsqueda que podrían alterar los sistemas médicos y de control de procesos. La plataforma Forescout proporciona visibilidad de dispositivos en las redes del sector sanitario y OT a través de una combinación de técnicas completamente pasivas, incluida la supervisión del tráfico SPAN para la inspección profunda de paquetes en más de 150 protocolos específicos de IT, sector sanitario y OT. Lo que distingue a la solución de Forescout es que una vez identifica de forma precisa los dispositivos, puede aplicar selectivamente métodos activos en dispositivos específicos para una evaluación adicional sin el riesgo de interrumpir la actividad empresarial.

Además de descubrimiento, clasificación y evaluación: la posibilidad de utilizar técnicas de reconocimiento en capas pasivas y activas permite a la plataforma Forescout ir mucho más allá de la simple identificación de dispositivos por dirección MAC e IP. La clasificación es el proceso de adquirir y correlacionar numerosas capas de contexto para crear un perfil enormemente detallado de cada dispositivo. La evaluación es el proceso de comparar las propiedades de estado del dispositivo detectado con las directivas de seguridad como base para las decisiones de control de acceso y reparación. Ambos métodos merecen un examen más pormenorizado.

Clasificación automática inteligente

Contar con contexto completo para cada dispositivo es esencial para crear directivas granulares. Debe conocer el fin operativo de cada dispositivo para decidir cómo protegerlo y gestionarlo mejor. Dados el crecimiento y la diversidad de dispositivos, es casi imposible recopilar manualmente este contexto, pero crear directivas sin el contexto adecuado pone en riesgo las operaciones. Forescout clasifica automáticamente dispositivos tradicionales, IoT y OT mediante una taxonomía multidimensional que identifica la función y el tipo de dispositivo, el sistema operativo y la versión, así como el proveedor y el modelo.

La plataforma clasifica automáticamente:

- Más de 575 versiones de sistemas operativos diferentes
- Más de 5700 productos y modelos de distintos proveedores de dispositivos
- Dispositivos médicos de más de 400 proveedores de tecnología sanitaria
- Miles de dispositivos de control y automatización industrial que se utilizan en infraestructuras de fabricación, energía, gas y petróleo, servicios públicos, minería y otros sectores críticos

Forescout Device Cloud facilita la clasificación automática en la plataforma y garantiza que esta rica fuente de contexto esté siempre actualizada a medida que crezca el número y la diversidad de los dispositivos. Como el mayor lago de datos del mundo con inteligencia sobre dispositivos obtenida de manera colaborativa, Forescout Device Cloud proporciona una única fuente de verdad intersectorial sobre huellas digitales, comportamientos y perfiles de riesgo de más de 12 millones de dispositivos de clientes empresariales. Forescout Research publica frecuentemente nuevos perfiles para mejorar la eficacia, cobertura y velocidad de la clasificación en la totalidad del panorama de dispositivos.

Evaluación de estado y corrección automática sin agente

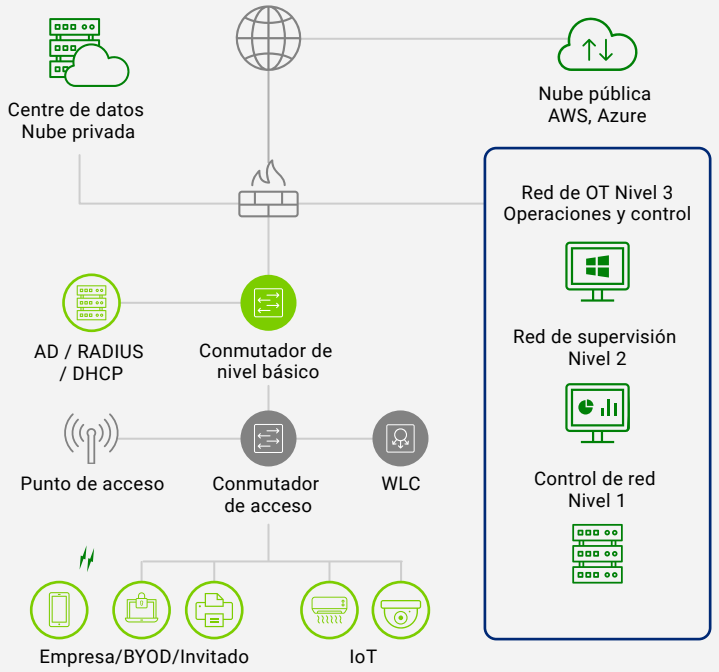
La clasificación de los dispositivos ofrece contexto operativo referente a su objetivo, es decir, qué es cada dispositivo. Sin embargo, para obtener un contexto completo, se requiere otra perspectiva que mida la salud y la higiene de cada dispositivo. Forescout supervisa continuamente la red y evalúa la configuración, el estado y la seguridad de los dispositivos conectados con el fin de determinar sus perfiles de riesgo y averiguar si cumplen las directivas y normativas de seguridad. Da respuesta a cuestiones clave, como:

- ¿Utilizan los dispositivos sistemas operativos aprobados? ¿Tienen instalados los últimos parches del SO?
- ¿Está el software de seguridad instalado, operativo y actualizado con los últimos parches?
- ¿Hay algún dispositivo que tenga activas aplicaciones no autorizadas o que infrinja los estándares de configuración?
- ¿Utilizan los dispositivos contraseñas predeterminadas o poco seguras (muy arriesgado en concreto para los dispositivos IoT)?
- ¿Se han detectado dispositivos no autorizados, como los que se hacen pasar por dispositivos legítimos mediante técnicas de falsificación?
- ¿Cuáles de los dispositivos conectados son más vulnerables a las últimas amenazas?

Después de contestar a estas cuestiones críticas, la **plataforma Forescout aplica el cumplimiento de dispositivos mediante la automatización de la corrección de dispositivos** con controles nativos o de terceros. Entre sus funciones más importantes se incluyen:

- Garantía de que los endpoints están configurados correctamente y reparación de problemas de configuración graves, como el empleo de contraseñas predeterminadas o no seguras.
- Garantía permanente de que los agentes de seguridad funcionan correctamente (están instalados, en ejecución y actualizados).
- Desactivación o bloqueo de aplicaciones no autorizadas que puedan introducir riesgos, cargar sin necesidad el ancho de banda de la red o mermar la productividad de los recursos.
- Identificación de vulnerabilidades de alto riesgo y ausencia de parches críticos, e inicio de las medidas necesarias para repararlos.
- Aplicación proactiva de medidas de reparación, como la instalación del software de seguridad necesario, la actualización de agentes o la aplicación de parches de seguridad.
- Implementación de directivas y automatización de controles de la idoneidad de la configuración en despliegues en la nube, como AWS, Azure y VMware.

Clasificación y evaluación de dispositivos



¿QUIÉN?
- Usuario
- Nombre
- Correo electrónico
- Título
- Grupo
- Suscripción/Cuenta
- Función/Responsable de IAM

¿QUÉ?
- Función
- SO
- Proveedor/Modelo
- Dirección IP
- Agente del navegador
- Puertos
- Virtual/Físico
- Dirección MAC

¿ESTADO?
- Aplicaciones
- Servicios
- Procesos
- Versiones
- Registro
- Parches
- Cifrado
- Antivirus

¿DÓNDE?
- Conmutador
- Controladora
- Puerto de conmutación /SSID/VLAN
- AWS/Azure
- Región
- VNet/VPC
- Nivel de Purdue

Figura 4: La plataforma Forescout clasifica rápidamente los dispositivos por tipo, aclara si están gestionados por la empresa o no, si son IoT u OT, físicos o virtuales, y ayuda a evaluar su nivel de cumplimiento de las normas.

"Las tecnologías de dispositivos IoT y de red han introducido un riesgo potencial en redes y empresas. Cada dispositivo introduce nuevas vías de código y activos que deben localizar los equipos de seguridad y tratar como infraestructura no fiable. Los equipos de seguridad deben aislar, proteger y controlar todos los dispositivos de la red, continuamente". [2]

FORRESTER

8 DE JUNIO DE 2020

Uso de la visibilidad para facilitar el control

Las redes de los clientes son todas diferentes. De ahí que sus requisitos varíen, y sus directivas de seguridad sean exclusivas. Y que resulte fundamental desplegar una solución flexible para proteger todas las redes: cableadas, inalámbricas y VPN. Por ejemplo, los clientes de grandes empresas generalmente despliegan una solución de Forescout **sin autenticación 802.1X en sus redes cableadas**. Eligen esta opción porque es fácil de desplegar, no requiere actualizaciones de infraestructura de hardware/software ni complejas configuraciones de conmutadores ni endpoints, como ocurre con autenticación 802.1X, y funciona con una infraestructura de red única o multiproveedor. Esta práctica se ajusta a la recomendación de Gartner de no utilizar autenticación 802.1X en redes cableadas para facilitar el despliegue y reducir costes operativos. Sin embargo, en redes inalámbricas, el despliegue de 802.1X para la autenticación de dispositivos de IT de usuarios corporativos es una práctica estándar. Las opciones de despliegue híbridas y flexibles de Forescout admiten fácilmente ambas prácticas.

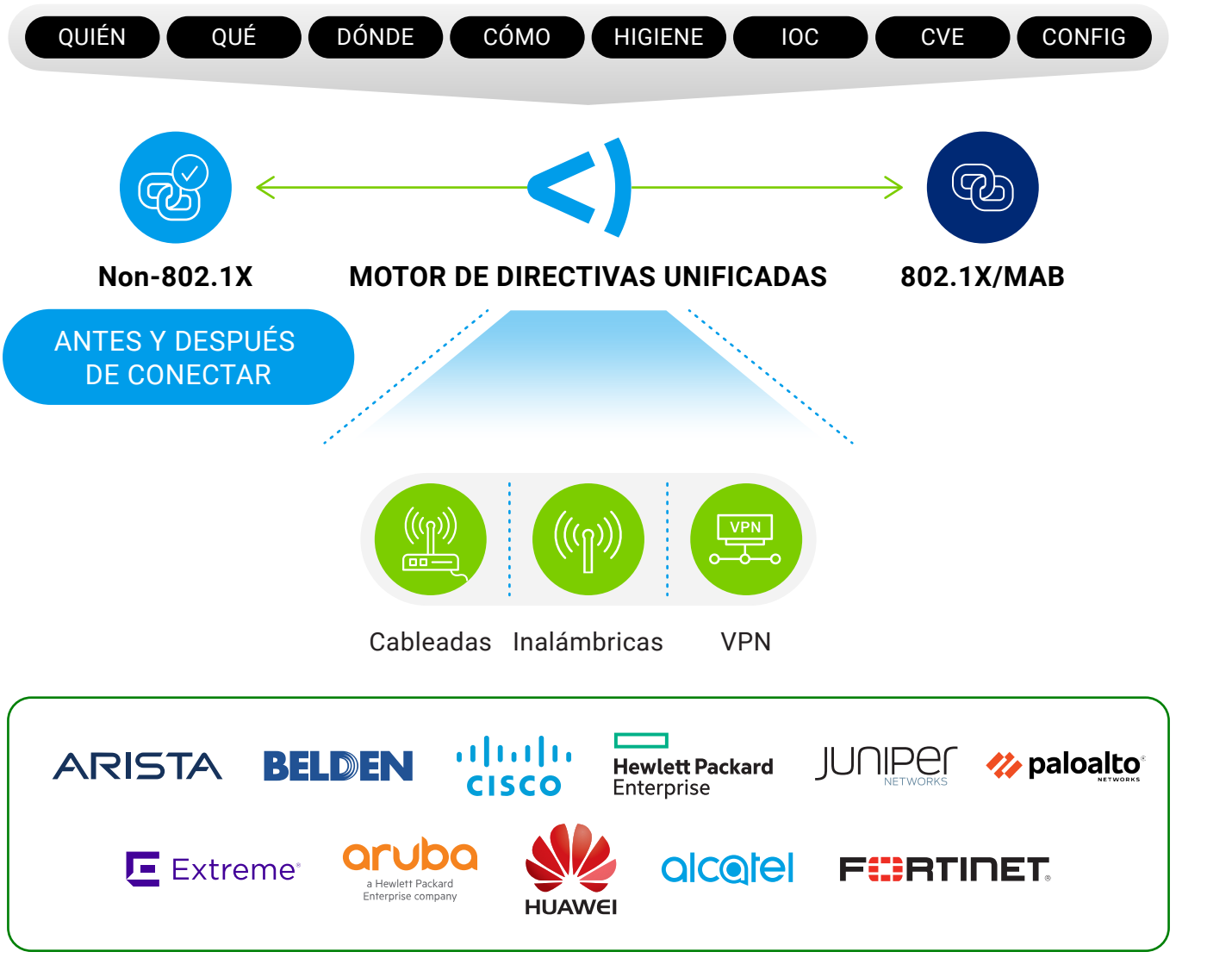


Figura 5: Forescout ofrece opciones con y sin autenticación 802.1X para proteger los endpoints en redes cableadas, inalámbricas y VNP multiproveedor.

Estas son algunas de las ventajas fundamentales del uso de la plataforma Forescout para proteger el acceso a las redes:

Mayor flexibilidad

- Amplia variedad de métodos de control de acceso, con o sin autenticación 802.1X
- Arquitectura cableada robusta sin 802.1X; sin interrupciones, fácil de desplegar, requisitos de configuración mínimos, sin actualizaciones de infraestructura, opciones antes de conectar y después de conectar, rápida creación de valor y rentabilidad.
- Motor de directivas unificadas para implementar acceso seguro diferenciado (dispositivos de invitados, BYOD, corporativos e IoT) y Zero Trust.

Sin actualizaciones

- Utiliza la infraestructura existente y no requiere actualizaciones de software/hardware.
- Trabaja con el proveedor de infraestructura de red que elija (por ejemplo, conmutador, controladora inalámbrica, IaaS), lo que reduce la dependencia de un solo proveedor.
- Rápida creación de valor y rentabilidad

Heterogénea

- Integración directa (a través de SNMP, SSH, Telnet y RADIUS) con cientos de conmutadores y controladoras inalámbricas con versiones de sistemas operativos distintas de más de 30 proveedores de infraestructuras de red, lo que permite aplicar el acceso de red en cualquier red multiproveedor.
- Solución flexible sin interrupciones, que reduce los costes operativos, de despliegue y mantenimiento.
- Compatibilidad heterogénea que permite a una empresa compradora conseguir una rápida visibilidad y control de los activos después de una fusión/adquisición.

Segmentación en toda la empresa

- Aproveche la información de visibilidad de la plataforma Forescout para conocer el estado de segmentación en tiempo real sobre todos los dispositivos, dondequiera que estén.
- Diseñe y simule las directivas de segmentación lógica para conocer el impacto antes de la aplicación.
- Supervise el estado de la segmentación en tiempo real y responda a las violaciones de directivas en toda la empresa ampliada.

Encontrará más información sobre la solución de segmentación en toda la empresa de Forescout aquí.

MEJORES PRÁCTICAS PARA DESPLIEGUE DE NAC

Forescout recomienda las siguientes mejores prácticas para desplegar el control de acceso a la red:

Red inalámbrica: 802.1X es una práctica estándar para autenticar dispositivos de IT de usuarios corporativos en redes inalámbricas. Una vez autenticados, Forescout identifica y evalúa sin agente el cumplimiento de los dispositivos para ordenadores Windows, macOS y Linux.

Con el motor de directivas de Forescout, los clientes pueden elegir corregir automáticamente y aplicar los controles de red adecuados para respetar las directivas de seguridad (por ejemplo, notificar al usuario, corregir, bloquear y/o compartir contexto con herramientas de terceros).

Red cableada: en redes cableadas, Forescout recomienda una arquitectura sin autenticación 802.1X. La complejidad del despliegue y administración de 802.1X y MAB en redes cableadas hace que la mayoría de los clientes elijan una opción sin autenticación 802.1X. Los clientes empiezan por el descubrimiento, la identificación y la evaluación del estado/cumplimiento de los dispositivos y, a continuación, aplican los niveles adecuados de acceso a la red mediante controles no basados en 802.1X en cualquier red heterogénea. Nota: Forescout también es totalmente compatible con la autenticación 802.1X en redes cableadas.

Coordinación con productos de IT y de seguridad

En todo el proceso de control de acceso a la red, Forescout puede trabajar con sus herramientas existentes para intercambiar contexto de dispositivos en tiempo real y automatizar los flujos de trabajo de respuesta. Esto no solo acelera la mitigación de riesgos, sino que le permite maximizar la rentabilidad de las inversiones en administración de seguridad y de IT. A través de integraciones con eyeExtend inmediatas y apps de eyeExtend Connect, ayudamos a los clientes a convertir la administración de la seguridad aislada en un sistema de respuesta automatizada para toda la empresa que defiende activamente su Enterprise of Things.

A continuación incluimos algunas ventajas de la coordinación con herramientas de seguridad existentes durante el proceso de control de acceso a la red (NAC):

Comparta contexto de dispositivos

- Comparta contexto de dispositivos con sus herramientas de administración de activos existentes para ayudarle a garantizar que siempre dispone del inventario más actualizado y preciso.
- Proporcione contexto de dispositivos en tiempo real a los equipos de operaciones de seguridad y aplicaciones para la correlación y priorización de incidentes.

Inicie los flujos de trabajo al conectar

- Las herramientas existentes pueden pasar por alto la evaluación de vulnerabilidades de los dispositivos en tránsito ya que realizan análisis puntuales. Forescout trabaja con las herramientas de seguridad para activar análisis de vulnerabilidades en el momento de la conexión.
- Inicie la aplicación de parches y las actualizaciones de seguridad inmediatamente en el momento de la conexión para reducir la superficie de ataque.

Evalúe el estado de seguridad

- Compruebe que los agentes de seguridad existentes están en funcionamiento e identifique dispositivos con riesgos e indicadores de peligro (IoC).
- Detecte cuentas obsoletas o con privilegios ilegítimos al conectar los dispositivos.

Automatice las acciones de respuesta

- Contenga, ponga en cuarentena o bloquee los dispositivos vulnerables, comprometidos o de alto riesgo.
- Inicie acciones de mitigación y reparación basadas en directivas para responder a los incidentes.

> **Forescout domina en la actualidad el subgrupo del mercado de NAC sin agentes, con una cuota del 64,7 % y se le atribuye además el mayor porcentaje de despliegues NAC híbridos del sector. Este crecimiento se debe en gran medida al importante conjunto de funciones de Forescout dedicadas principalmente a cumplir las demandas de la parte de mayor crecimiento de este mercado de dispositivos no gestionados y que no admite agentes, que inevitablemente requieren un enfoque sin agente.**
>
> **IDC**
> **MAYO DE 2020[3]**

No se conforme con verlo. Protéjalo.

La solución de control de acceso a la red (NAC) moderno moderna de Forescout ofrece una alternativa sin agentes, flexible y sin interrupciones hacia la seguridad Zero Trust. Revise esos recursos para obtener más información sobre cómo Forescout proporciona defensa activa para el Enterprise of Things:

Lea la guía de mercado tecnología NAC de Gartner: Descubra por qué Gartner llama a Forescout "Una de las soluciones NAC más populares del mercado".

Visite el sitio web de Forescout: obtenga más información sobre la solución de control de acceso a la red (NAC) moderno de Forescout, incluidos los casos de uso que aborda, cómo ayuda al cumplimiento de los dispositivos y las opiniones de los clientes de Forescout.

Realice un Test Drive: experimente el antes y el después de la plataforma Forescout con un Test Drive que le mostrará seis convincentes casos de uso.

Solicite una demo: visite la página de demos de Forescout para solicitar una demostración personal y acceder a toda una serie de demostraciones y vídeos complementarios bajo demanda.

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook (El ecosistema Zero Trust eXtended: Plan estratégico para redes: Manual de arquitectura y operaciones de seguridad), Forrester Research, 2 de enero de 2019
2. Forrester Research, Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles and Techniques (Mitigación del ransomware con Zero Trust: fortalezca sus defensas con principios y técnicas Zero Trust), 8 de junio de 2020
3. IDC, Worldwide NAC Market Shares, 2019: Diverse Market Demands Expand NAC's Addressable Market (Un mercado diverso exige la ampliación del mercado objetivo de NAC), mayo de 2020

No se conforme con verlo. Protéjalo.

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

forescout.com/solutions/network-access-control 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