FORESCOUT

Device Visibility and Control: Visibilidad y control de dispositivos sin agentes

Funciones primordiales para una ciberseguridad eficaz

> "La visibilidad es la clave para defender los recursos de valor. Cuanta más visibilidad se tenga de la red en todo el ecosistema de la empresa, mayores serán las posibilidades de detectar rápidamente cualquier indicio de violación de seguridad y de detenerla"[1].
>
> **— Dr. Chase Cunningham, Analista principal, Forrester Research**

Device Visibility and Control: por qué son necesarios

La capacidad de detectar, clasificar, evaluar y controlar todos los dispositivos que se conectan a la red es la condición indispensable para proteger sus sistemas y su negocio. Solo el conocimiento en tiempo real de todos los endpoints de cada segmento, la información detallada sobre la configuración y el estado de la seguridad y un control de acceso automatizado basado en directivas le permitirán garantizar con fiabilidad la seguridad de datos y sistemas, responder con rapidez y precisión a los incidentes, cumplir las normativas, gestionar los riesgos para la empresa y las infraestructuras y optimizar la eficacia de la seguridad . 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 son las piedras angulares de la seguridad y el cumplimiento de las normativas.

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. Esta medida funcionaba bastante bien cuando la mayoría de los endpoints eran estáticos, PC o servidores propiedad de la empresa, pero la movilidad, la diversidad de tipos de dispositivos y la virtualización han complicado enormemente la visibilidad y el control. En los entornos empresariales actuales, los segmentos en la nube y los centros de datos bullen con cargas de trabajo que llegan de forma dinámica, se procesan en máquinas virtuales y se conectan a través de redes virtuales. Los segmentos en campus están repletos de portátiles, tablets y smartphones personales que carecen de agentes de seguridad, así como de dispositivos del Internet de las cosas (IoT) incompatibles con ellos. Los segmentos de Tecnología Operativa (OT, Operational Technology) suman grandes cantidades de dispositivos que no admiten agentes, se comunican con protocolos propios, gestionan procesos de gran importancia y no toleran intrusiones internas. Las organizaciones de IT necesitan con urgencia una solución sin agentes que pueda ofrecer visibilidad y control exhaustivos en todos estos entornos diferentes.

La solución de Forescout: Device Visibility and Control, Visibilidad y control de dispositivos sin agentes

Forescout Technologies es el precursor de una estrategia de seguridad de red sin agentes que aborda los retos de la visibilidad y el control de dispositivos en los entornos dinámicos y variados de nuestros días. La plataforma de visibilidad y control de dispositivos de Forescout proporciona una visión continua y unificada de todos sus dispositivos en campus, centros de datos, la nube y redes de OT.

La plataforma Forescout detecta:

- Dispositivos en redes de campus: portátiles, tablets, smartphones, sistemas BYOD/de invitados y dispositivos IoT
- Infraestructuras de centros de datos: máquinas virtuales, hipervisores, servidores físicos y 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

Figura 1: La visibilidad de dispositivos de Forescout se adapta a toda la empresa.

> "La visibilidad y la evaluación de zonas de riesgo y confianza y el intercambio de datos de contexto constituyen el sistema inmunitario de las empresas digitales"[2].
>
> **— Neil MacDonald, VP, Analista, Gartner**

Nuestra estrategia

Forescout brinda a las organizaciones de IT la posibilidad de:

- Detectar todos los dispositivos conectados por IP a todas las redes: dispositivos físicos y virtuales en campus, centros de datos, la nube y entornos industriales.
- Clasificar en tiempo real los distintos dispositivos de IT, IoT y OT/ICS, así como máquinas virtuales e instancias de la nube, mediante la identificación de tipo, función, proveedor, modelo, sistema operativo y versión.
- Evaluar y supervisar continuamente el estado de seguridad de los dispositivos para cumplir las normativas.
- Cumplir las directivas, las normativas del sector y las mejores prácticas, como la segmentación de la red.
- Limitar, bloquear o poner en cuarentena los dispositivos no conformes o comprometidos.
- Automatizar las medidas de control de endpoints, redes y terceros.

Cómo detectamos todos los dispositivos conectados por IP y sistemas de OT en todos los segmentos

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, centros de datos 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 100 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 802.1X, Forescout puede supervisar un servidor RADIUS, ya sea 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
Capturas SNMP
Tráfico SPAN
Solicitudes DHCP
Agente de usuario HTTP
Huella digital TCP
Análisis de protocolo DICOM (dispositivos de obtención de imágenes médicas)
Análisis de protocolos ICS de TO (más de 60 protocolos)
Análisis de flujo
NetFlow
Flexible NetFlow
IPFIX
sFlow
Solicitudes DHCP (vía IP-helper)
Agente de usuario HTTP (vía redireccionamiento de URL)
Solicitudes RADIUS
OUI MAC

ACTIVO A INFRAESTRUCTURA
Sondeo de la infraestructura de red física
Integración en la infraestructura de red basada en controladora
Meraki
Cisco ACI
Integración en nube privada (infraestructura virtual)
VMware
Integración en nube pública
AWS
Azure
Consulta de servicios de directorio (LDAP)
Consulta de aplicaciones web (REST)
Consulta de bases de datos externas (SQL)
Coordinación (ITSM, UEM, EPP, EDR, VA)

ACTIVO A DISPOSITIVO FINAL
Inspección sin agente Windows (WMI, RPC, SMB)
Inspección sin agente macOS, Linux (SSH)
NMAP
Consultas SNMP a endpoints
Inspección basada en agente (SecureConnector)

Figura 2: 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.

Detección, clasificación y evaluación solo pasiva en redes de OT: las redes de OT suelen ser entornos inadecuados para las técnicas activas de sondeo y búsqueda que puedan alterar los sistemas de control de procesos y las operaciones empresariales. Los métodos activos pueden aplicarse selectivamente cuando los dispositivos se conocen mejor. La plataforma Forescout proporciona visibilidad de dispositivos en todas las redes de OT mediante una combinación completamente pasiva de duplicación de tráfico SPAN e inspección profunda de paquetes en casi 100 protocolos específicos de OT. Forescout admite los protocolos estándar del sector, como BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 60850, IEEE C37.118, Modbus/TCP, OPC, PROFINET y Siemens S7. También admitimos los protocolos privados de los principales fabricantes, como ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, Schneider Electric y Yokogawa.

Despliegue rentable en grandes entornos: la capacidad de usar técnicas de visibilidad remotas puede reducir el coste general de despliegue al facilitar la supervisión de centros pequeños sin necesidad de un appliance local.

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 procesos merecen un examen más pormenorizado.

Clasificación automática inteligente

Contar con contexto completo para cada dispositivo es esencial para crear directivas granulares. Debe conocer el contexto operativo o el propósito 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 500 versiones de sistemas operativos diferentes
- Más de 5000 productos y modelos de distintos proveedores de dispositivos
- Dispositivos médicos de más de 350 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. Forescout Research emplea inteligencia de más de 8 millones de dispositivos del mundo real en Forescout Device Cloud* y publica estos nuevos perfiles con frecuencia para mejorar la eficacia de clasificación, la cobertura y la velocidad en su entorno de dispositivos completo.

Evaluación del estado de los dispositivos

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 infrinjan 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?

Clasificación y evaluación de dispositivos

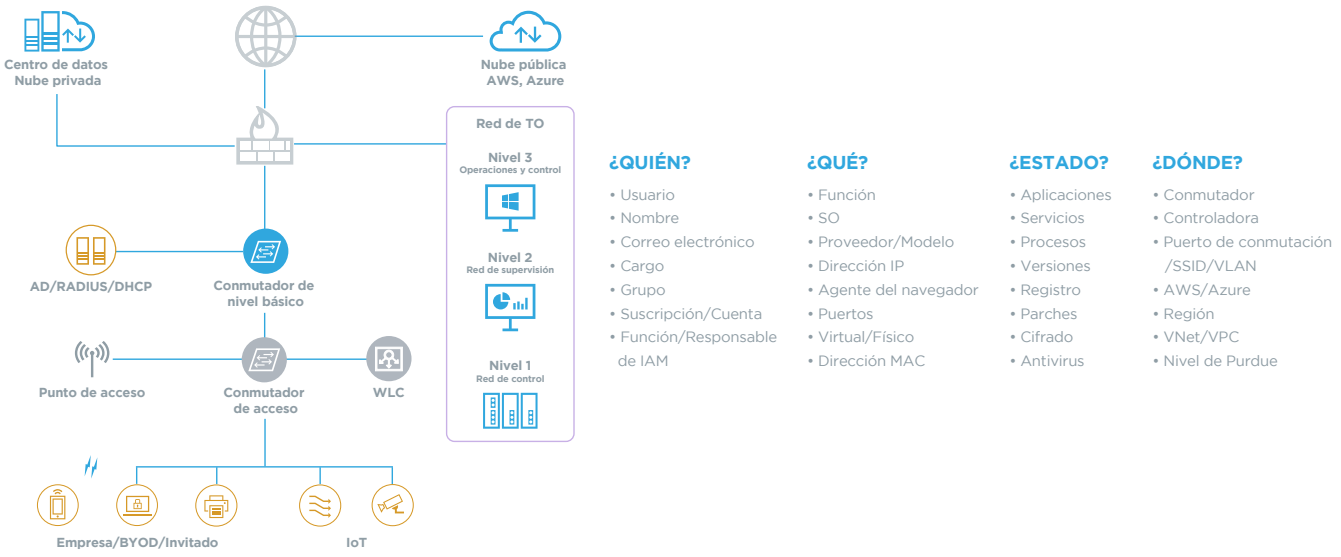

Figura 3: La plataforma Forescout clasifica rápidamente los dispositivos por tipo, aclara si están gestionados por la empresa o no, si son IoT o OT, físicos o virtuales, y ayuda a evaluar su nivel de cumplimiento de las normas.

Uso de la visibilidad para facilitar el control

La plataforma Forescout incluye un motor de directivas que comprueba continuamente si los dispositivos cumplen el conjunto de directivas personalizables que dictan su comportamiento en la red, lo que significa que se supervisan constantemente en tiempo real hasta dos millones de dispositivos. Las directivas se activan en tiempo real con los eventos que se producen en un dispositivo determinado o en la red. Puede tratarse de eventos de admisión en la red, como la conexión a un puerto de conmutación o el cambio de una dirección IP, o de eventos de autenticación, como los que recibe un servidor RADIUS. Las directivas también pueden activarse por cambios en los atributos de los dispositivos. La Figura 4 muestra la gama de medidas de control disponibles en la plataforma Forescout cuando se activa una directiva.

Medidas de control de Forescout

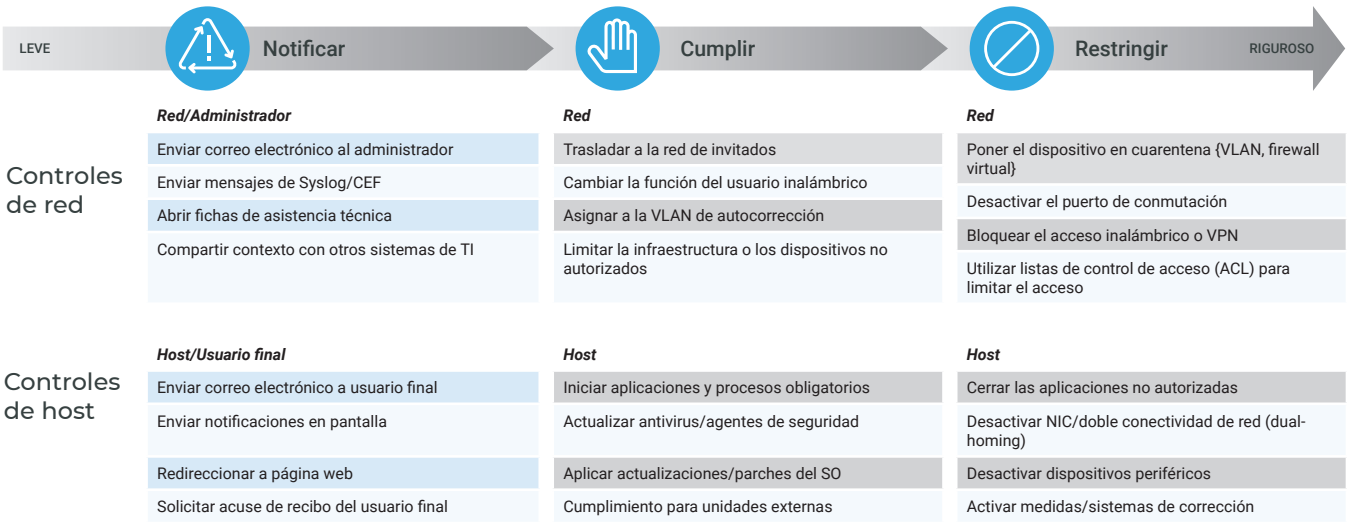

Figura 4: Las medidas de control personalizables le permiten aplicar el nivel de control correcto —de leve a riguroso— en función de sus directivas de seguridad.

El motor de directivas recurre a dos variedades de funciones de control. La primera es nativa de Forescout. La segunda se obtiene mediante el intercambio de datos y la integración coordinada de controles de productos líderes en gestión de IT y seguridad.

Funciones de control nativas

Las funciones nativas de Forescout incluyen controles basados en la red y en el host. Los controles de la red proporcionan segmentación basada en directivas, lo que autoriza o restringe el acceso según la identidad del usuario, su cargo y el estado de su dispositivo. Los controles basados en el host emplean medidas de higiene en los dispositivos para iniciar y detener aplicaciones, actualizar antivirus y otros agentes de seguridad para hosts o desactivar dispositivos periféricos. El motor de directivas aplica estas directivas automáticamente, sea cual sea la ubicación o el movimiento del dispositivo en la red corporativa y el centro de datos o la nube.

Funciones de control ampliadas

La plataforma Forescout automatiza la aplicación de directivas, acelera la respuesta en todo el sistema y mitiga los riesgos compartiendo el contexto de los dispositivos en tiempo real y coordinando flujos de trabajo en muchos tipos distintos de productos de gestión de IT y seguridad. Forescout ofrece integración con los principales proveedores de estas categorías:

- Detección de amenazas avanzadas
- Herramientas de gestión de clientes
- Gestión de movilidad empresarial
- Protección, detección y respuesta de endpoints
- Gestión de servicios de IT
- Firewalls de próxima generación
- Gestión de acceso privilegiado
- Administración de información y eventos de seguridad
- Evaluación de vulnerabilidades

Esta integración permite a Forescout desplegar una seguridad coordinada que abarca toda la infraestructura y facilitar controles basados en directivas según la clasificación de usuarios, dispositivos, aplicaciones y tráfico. Las directivas de acceso son granulares y proporcionan un control preciso y flexible de los recursos, lo que permite a las organizaciones de IT aplicar una segmentación dinámica de la red y crear directivas de seguridad que reconocen y tienen en cuenta el contexto en tiempo real.

Medidas de control que podemos adoptar

Forescout ofrece una combinación de funciones de control nativas y ampliadas, profundamente enraizadas en el control de acceso a la red, que confieren a su plataforma una variedad extraordinaria de prestaciones de control de dispositivos, prestaciones que a su vez proporcionan a las organizaciones de IT un potente arsenal de herramientas de seguridad de la red.

La plataforma Forescout autoriza el acceso a los recursos de la empresa en la red en función del perfil de los usuarios (invitado, empleado, contratista), la clasificación del dispositivo y el nivel de seguridad. Para ello, dispone de lo siguiente:

- Acceso diferenciado para invitados y dispositivos BYOD.
- Implementación de directivas de acceso a la red con o sin autenticación 802.1X.
- Medidas para gestionar dispositivos sospechosos, no autorizados o de IT en la sombra.
- Limitación o bloqueo del acceso a la red para dispositivos comprometidos o maliciosos.
- Cuarentena o aislamiento para los dispositivos no conformes hasta que se hayan solucionado los problemas de incumplimiento.

La plataforma Forescout mejora el cumplimiento normativo de los dispositivos al automatizar la evaluación del cumplimiento y la implementación de controles de reparación con el fin de garantizar el cumplimiento continuo de las directivas de seguridad internas, los reglamentos externos y las normativas del sector. 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.
- Comprobación de que las aplicaciones y los agentes de seguridad necesarios están instalados, activos 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.

La plataforma Forescout implementa la segmentación dinámica de la red aplicando directivas de segmentación en tecnologías dispares en toda la empresa a través de un marco de directivas común. La plataforma Forescout:

- Asigna de forma dinámica los dispositivos a grupos de segmentación en función de sus propiedades, clasificación y nivel de seguridad.
- Aplica la segmentación a través de controles de VLAN, ACL y WLAN y del etiquetado en entornos de campus y OT.
- Aplica controles de segmentación a través de grupos de seguridad o etiquetas en entornos en la nube pública y privada, como AWS y VMware NSX®.
- Segmenta los dispositivos no conformes y vulnerables en zonas separadas —especialmente aquellos a los que solo se les pueden aplicar parches o correcciones dentro de un plazo de mantenimiento programado— para no afectar a la continuidad de la actividad y, al mismo tiempo, reducir la superficie de ataque.
- Implementa directivas de segmentación para apartar dispositivos específicos y flujos de datos críticos del resto de la red, según dicten normativas como HIPAA, RGPD, PCI y SWIFT CSP.

La plataforma Forescout acelera la respuesta a incidentes conteniendo las amenazas y respondiendo a incidentes de seguridad de forma rápida y eficaz, para minimizar las interrupciones de las operaciones y los daños en la empresa. Esta solución de visibilidad y control de dispositivos:

- Identifica dispositivos de alto riesgo que no se han contenido o reparado.
- Funciona con soluciones de ATD para identificar indicadores de riesgo (IoC) en los dispositivos en el momento de su conexión con el fin de reducir el tiempo medio de respuesta.
- Aísla y contiene con rapidez los dispositivos comprometidos o maliciosos para evitar la propagación lateral del malware.
- Automatiza la respuesta ante incidentes e inicia flujos de trabajo de reparación en dispositivos comprometidos.
- Reduce el tiempo medio de respuesta proporcionando a los equipos interdisciplinares de respuesta a incidentes información práctica del contexto de los dispositivos (conexión, ubicación, clasificación y nivel de seguridad).

La seguridad empieza por la visibilidad

Hay un motivo por el que los mandos militares siempre quieren tomar y mantener posiciones elevadas: estas les permiten ver las fuerzas que se aproximan y activar las defensas antes de que se inicie el ataque. La plataforma Forescout ofrece a las organizaciones de IT una vista dominante del terreno que deben defender en la red. Al detectar, clasificar, evaluar y controlar continuamente todos los dispositivos allí donde se conecten, Forescout hace del campo de batalla un territorio visible, inteligible y manejable.

Evalúe personalmente la plataforma Forescout

La mejor manera de informarse a fondo de las funciones de visibilidad y control de dispositivos sin agentes de Forescout es verlas de primera mano. Forescout le ofrece muchas maneras de conocer mejor la plataforma Forescout:

Haga la prueba: experimente el antes y el después de la plataforma Forescout con una prueba práctica que le mostrará seis convincentes casos de uso.

Obtenga el informe "Absolute Visibility and Risk Report" (Informe de visibilidad absoluta y riesgos) de Forescout: consiga una evaluación de detallada de los riesgos y la visibilidad de los dispositivos. Póngase en contacto con su representante local de Forescout para obtener más información.

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.

Utilice la herramienta de cálculo de rentabilidad/valor de negocio de Forescout: cuantifique el valor de negocio que la plataforma Forescout puede ofrecer a su organización (según el modelo de IDC para calcular el valor de negocio) en solo 10 minutos.

*A domingo, 31 de marzo de 2019

1 "The Zero Trust eXtended (ZTX) Ecosystem" (El ecosistema Zero Trust eXtended (ZTX)", Forrester Research, enero de 2018

2 Zero Trust Is an Initial Step on the Roadmap to CARTA (Zero Trust es el primer paso del camino a CARTA), Gartner, diciembre de 2018

FORESCOUT

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

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

Más información en Forescout.com