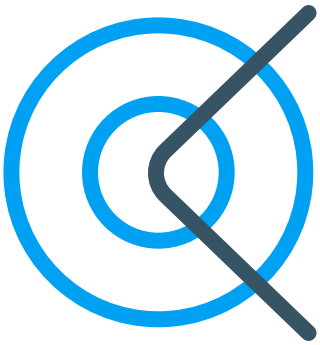
FORESCOUT



eyeSight

La fuente definitiva de la verdad para cada activo conectado en su terreno digital.

Sin Agentes
Obtenga un inventario unificado y en tiempo real de los activos conectados a la red, incluida su postura de riesgo y seguridad.

Preciso
Clasifique cada dispositivo para obtener contexto para políticas de se seguridad y cumplimiento proactivas.

Efectivo
Automatice las tareas repetitivas, como la medición y la elaboración de informes de cumplimiento y riesgo minimizando los errores humanos.

Eficiente
Confianza en tiempo real de que las herramientas de seguridad y los controles de cumplimiento esta trabajando como deberían.

Forescout eyeSight ofrece una visión sin precedentes de cada activo conectado a través de una profunda integración a su red.

- Descubra todo su inventario de activos con más de 30 técnicas activas y pasivas que revelan brechas de cobertura en todo su terreno digital, proporcionando una visión en tiempo real de su superficie de ataque.
- Automatice la clasificación de activos y cree perfiles completos que incluyan riesgos y vulnerabilidades conocidos con la inteligencia sobre amenazas impulsada por Vedere Labs.
- Prepárese para hacer frente a las nuevas amenazas a medida que surgen aprovechando el machine learning cloud que mejora continuamente nuestro centro de inteligencia propietario de dispositivos con más de 30,000 millones de endpoints llamada Forescout´s Device Could.
- Evalúe continuamente el estado de un activo, la postura de riesgo y el cumplimiento de las políticas sin necesidad de instalar un agente, lo cual es esencial para proteger los activos IoT, IoMT y OT.
- Multiplique sus fuerzas a la vez que minimiza el error humano con informes automatizados sobre la postura de cumplimiento y la exposición al riesgo cibernético, lo que le permite centrar sus esfuerzos en lo que más importa.

Descubra
Vea los dispositivos al instante que se conectan a la red. Monitoree continuamente los dispositivos temporales. Obtenga un inventario en tiempo real y reduzca los gaps de visibilidad.

Clasifique
Identifique diversos tipos de dispositivos de TI, IoT, IoMT y OT. Aproveche la potencia de Device Cloud para obtener el contexto completo del dispositivo. Mejore la eficacia, la cobertura y la velocidad de la autoclasificación

Evalúe
Identifique los gaps de cumplimiento y ciberseguridad. Evalúe su postura de cumplimiento a regulaciones internas y externas.

eyeSight Resuelve:

- **Gaps de Visibilidad**
  causada por equipos aislados y herramientas de seguridad no integradas
- **Riesgos Operativos y de negocio**
  debido a procesos manuales y propenso a errores
- **Inteligencia incompleta de dispositivos**
  No permite la ejecución de políticas de seguridad.
- **Gaps de Seguridad**
  cuando las herramientas basadas en agente no estan actualizadas o funcionan correctamente
- **Dispositivos no autorizados no detectados**
  o MAC spoofing
- **No complimiento**
  que puede surgir rápidamente entre escaneos

Descrubra

Descubrimiento profundo en tiempo real

Elimine los puntos ciegos y minimice los riesgos con una visibilidad completa de todas las facetas de su terreno digital:

- Infraestructura física y SDN, incluidos conmutadores, enrutadores, puntos de acceso inalámbricos y controladores.
- Ordenadores portátiles, tabletas, teléfonos inteligentes, sistemas BYOD/invitados, dispositivos para trabajar desde casa.
- Activos IoT en redes de campus, centros de datos, sucursales, emplazamientos remotos y redes periféricas.
- Instancias de nube pública y privada a través de Amazon Web Services, Microsoft Azure y entornos VMware.
- Tecnología operativa (OT) y sistemas de control industrial, incluidos HMI, SCADA, PLC, sistemas de gestión de edificios (BMS) y sistemas de automatización de edificios (BAS).
- Dispositivos IoMT en hospitales y redes de prestación de asistencia sanitaria (HDO), como bombas de infusión y equipos de diagnóstico.

Personalice las técnicas de detección y supervisión para su entorno

Aproveche la flexibilidad de más de 30 técnicas de supervisión activas y pasivas en redes cableadas, inalámbricas, VPN y virtuales/definidas por software para evitar la interrupción de activos sensibles a las técnicas de exploración activa.

ACTIVO A INFRAESTRUCTURA

Network infrastructure polling

SDN integration
- Meraki
- Cisco ACI

Public/Private cloud integration
- VMware
- AWS
- Azure

Query directory services (LDAP)

Query web applications (REST)

Query databases (SQL)

eyeExtend orchestrations

PASIVO A DISPOSITIVO

SNMP traps

SPAN traffic Flow analysis
- NetFlow
- Flexible NetFlow
- IPFIX
- sFlow

DHCP requests

HTTP user-agent

TCP fingerprinting

Protocol parsing

RADIUS requests

ACTIVO A DISPOSITIVO

Agentless Windows inspection
- WMI
- RPC
- SMB

Agentless macOS, Linux inspection
- SSH

NMAP

SNMP queries

HTTP queries

Forescout SecureConnector®

Clasificar

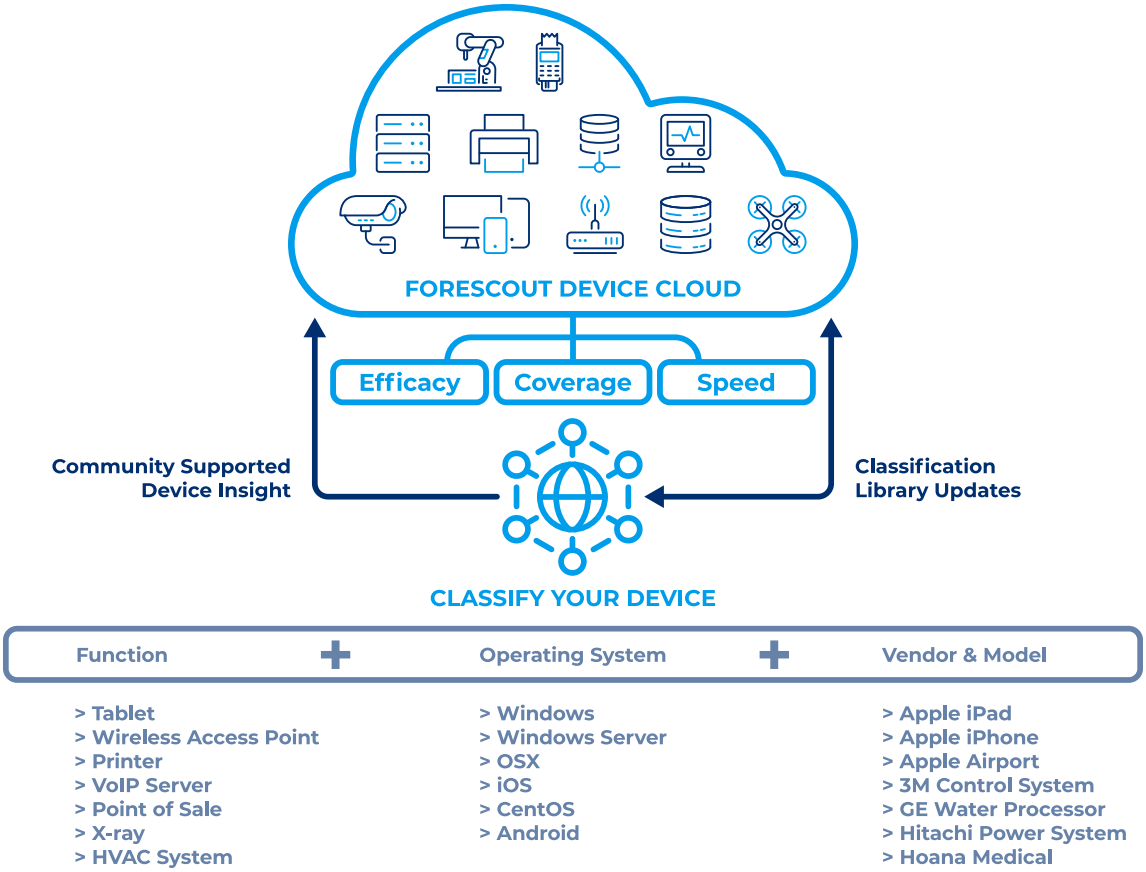
Autoclasificación inteligente

La aplicación de políticas de seguridad sin un contexto completo de los activos puede conducir a resultados no deseados que pueden poner en riesgo las operaciones. ForescoutDevice Cloud es el mayor repositorio de inteligencia de dispositivos recopilada de más de 50 millones de dispositivos y proporciona automáticamente un contexto completo para cada activo conectado. Nuestra taxonomía de clasificación multidimensional identifica la función y el tipo de dispositivo, el sistema operativo y la versión, y el proveedor y el modelo. Esto incluye:

- Más de 1,900 versiones diferentes de sistemas operativos
- Más de 7,700 fabricantes y modelos de dispositivos diferentes
- Dispositivos médicos de más de 400 proveedores líderes en tecnología médica.
- Miles de sistemas de control industrial y dispositivos de automatización utilizados en los sectores de fabricación, energía, petróleo y gas, servicios públicos, minería y otras infraestructuras críticas.

Clasificación automatizada mediante Forescout Device Cloud

Device Cloud, es el mayor repositorio de inteligencia de activos del mundo, proporciona la comprensión más completa y precisa del riesgo de activos dentro de cualquier organización.



Avaluar

Evaluación de la postura sin agentes

eyeSight descubre continuamente activos y evalúa inmediatamente la configuración, la postura y los indicadores de riesgo del activo para comprender si se adhieren a los mandatos de cumplimiento y a las políticas de seguridad. Las políticas pueden ayudar a cuantificar mejor el riesgo evaluando condiciones de cumplimiento como:

- Está el software de seguridad instalado, operativo y actualizado con los últimos parches?
- Es el activo crítico para las operaciones de la empresa?
- Algún activo ejecuta aplicaciones no autorizadas o infringe las normas de configuración?
- Los activos, especialmente los sistemas IoT, IoMT y OT, ¿utilizan contraseñas predeterminadas o débiles?
- Se han detectado activos fraudulentos, incluidos los que suplantan a activos legítimos?
- Cuáles de sus activos conectados son más vulnerables a las amenazas más recientes?

Monitorear

Ver información sobre cumplimiento

Obtenga información práctica a partir de paneles de control listos para usar que identifican, priorizan y mitigan de forma rápida y proactiva los riesgos en todo su terreno digital. Las vistas personalizables de los paneles ayudan a los analistas de seguridad y a los equipos SOC a:

- Evaluar el riesgo y el progreso del cumplimiento en todas las políticas o en cualquier subconjunto de ellas.
- Identificar dispositivos vulnerables y comprometidos para acelerar y centrar la respuesta a incidentes.
- Seguimiento de las tendencias de cumplimiento a lo largo del tiempo
- Personalice y comparta vistas preparadas para ejecutivos y auditores de los datos de riesgo y cumplimiento.
- Busque y filtre rápidamente activos por política o atributos de dispositivo.

Segmentar, orquestar y aplicar

La plataforma Forescout Continuum amplía el valor de eyeSight con un conjunto de capacidades automatizadas de ciberseguridad para diseñar e implementar políticas de seguridad unificadas para el control de acceso a la red, la segmentación dinámica de la red y proporciona la base para la seguridad Zero Trust.

Visite www.forescout.com/platform/para conocer la plataforma Continuum de Forescout.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com