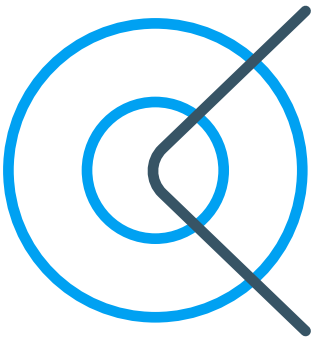
FORESCOUT



eyeSight

La fuente de información decisiva sobre cada dispositivo conectado en su entorno de TI

Sin agentes
Inventario completo en tiempo real de todos los dispositivos conectados a la red, incluyendo su estado de seguridad y riesgo.

Preciso
Clasificación de todos los dispositivos para conseguir un contexto que ayude a elaborar directrices de seguridad y cumplimiento proactivas.

Efectivo
Automatización de tareas rutinarias, por ejemplo, en la gestión de cumplimiento y de riesgos, para aliviar la carga de los equipos y minimizar los fallos humanos.

Eficiente
Información en tiempo real acerca de si las herramientas de seguridad y los controles de cumplimiento funcionan correctamente.

Forescout eyeSight se integra profundamente en sus estructuras de red para proporcionarle una vista general única de todos los dispositivos conectados.

- Detección de todos los activos con más de 39 técnicas activas y pasivas, que muestran las brechas de cobertura en su entorno de TI y ofrecen una visión en tiempo real de todas sus superficies de ataque
- Clasificación automática de dispositivos y elaboración de perfiles completos, incluyendo riesgos y vulnerabilidades conocidos basándose en inteligencia de amenazas de Vedere Labs
- Preparación temprana de amenazas futuras gracias al aprendizaje automatizado basado en la nube que optimiza de forma continua la Forescout Device Cloud, una fuente de información sobre dispositivos de propietario con más de 39 mil millones de puntos de datos individuales
- Evaluación continua del nivel de estado, riesgo y cumplimiento de los dispositivos, sin que sea necesario instalar un agente; algo esencial para la protección de activos de IoT, TO e IoMT
- Informes automatizados sobre el estado de cumplimiento y el peligro que suponen los ciberriesgos ayudan a ahorrar tiempo, minimizar fallos humanos y concentrarse en los esencial

Detectar
Detección de dispositivos en cuanto se conectan con la red
Vigilancia continua de los dispositivos que inician y finalizan una sesión
La inventarización en tiempo real descubre brechas de transparencia

Clasificar
Detección de diferentes tipos de dispositivos de TI, IoT, IoMT y TO
Uso de la potente Device Cloud para un contexto completo de dispositivos
Clasificación automática más eficiente, completa y rápida

Evaluar
Detección de riesgos de seguridad y de brechas de cumplimiento
Evaluación del cumplimiento de directrices internas y externas
Vista general de los riesgos operativos y cibernéticos existentes

eyeSight es la solución para:

- **brechas de transparencia,** causadas por equipos aislados y herramientas de seguridad de diferentes tipos
- **riesgos operativos y empresariales** debido a procesos manuales propensos a generar fallos
- **información sobre dispositivos incompleta,** que impide la ejecución de directrices de seguridad
- **Brechas de seguridad,** debido a herramientas no basadas en agentes que no están actualizadas o no funcionan correctamente.
- **Dispositivos desconocidos no autorizados,** oder MAC-Spoofing
- **Infracciones de cumplimiento,** que pueden darse fácilmente entre escáneres puntuales

Detectar

Detección detallada en tiempo real

Evite puntos ciegos y minimice riesgos gracias a una total transparencia sobre su entorno de TI:

- infraestructura física y de sdn-i, incluyendo conmutadores, enrutadores, WAP y controladores
- ordenadores portátiles, tabletas, móviles inteligentes, sistemas byod/invitados, dispositivos usados en teletrabajo
- activos de IoT en redes de campus, centros de computación, filiales, sedes alejadas y redes de borde (Edge)
- instancias de nube públicas o privadas en entornos aws, Microsoft Azure y VMware
- Sistemas de control industriales y de TO (tecnología operativa), incluyendo HMI, SCADA, SPS, gestión y automatización de edificios (BMS y BAS, por sus siglas en inglés)
- dispositivos IoMT en hospitales y otros organismos sanitarios, por ejemplo, bombas de infusión y equipos de diagnóstico

Adaptación de las técnicas de detección y supervisión a su entorno según las necesidades

Aproveche la flexi-ilidad de más de 30 técnicas de monitorización activas y pasivas para VPN y redes alámbricas, inalámbricas, virtuales y definidas por software. Esto le permite evitar interrupciones en dispositivos que reaccionen de forma sensible a técnicas de escaneo activas.

DETECCIÓN DE INFRAESTRUCTURA ACTIVA

Acceder a la infraestructura de red

Integración SDN
- Meraki
- Cisco ACI

Integración de nubes públicas y privadas
- VMware
- AWS
- Azure

Consulta de servicios de directorio (LDAP)
Consulta de aplicaciones web (REST)
Consulta de -ases de datos (SQL)
Orquestaciones de eyeExtend

DETECCIÓN PASIVA DE DISPOSITIVOS

SNMP-Traps

Tráfico de datos
Análisis de flujos de datos NetFlow
- Flexible NetFlow
- IPFIX
- sFlow

Consultas DHCP
HTTP-Useragent
TCP-Fingerprinting
Análisis de protocolo
Consultas RADIUS

DETECCIÓN ACTIVA DE DISPOSITIVOS

Examen sin agentes de dispositivos Windows
- WMI
- RPC
- SMB

Examen sin agentes de dispositivos macOS y Linux
- SSH

NMAP
Consultas SNMP
Consultas HTTP Forescout
SecureConnector®

Clasificar

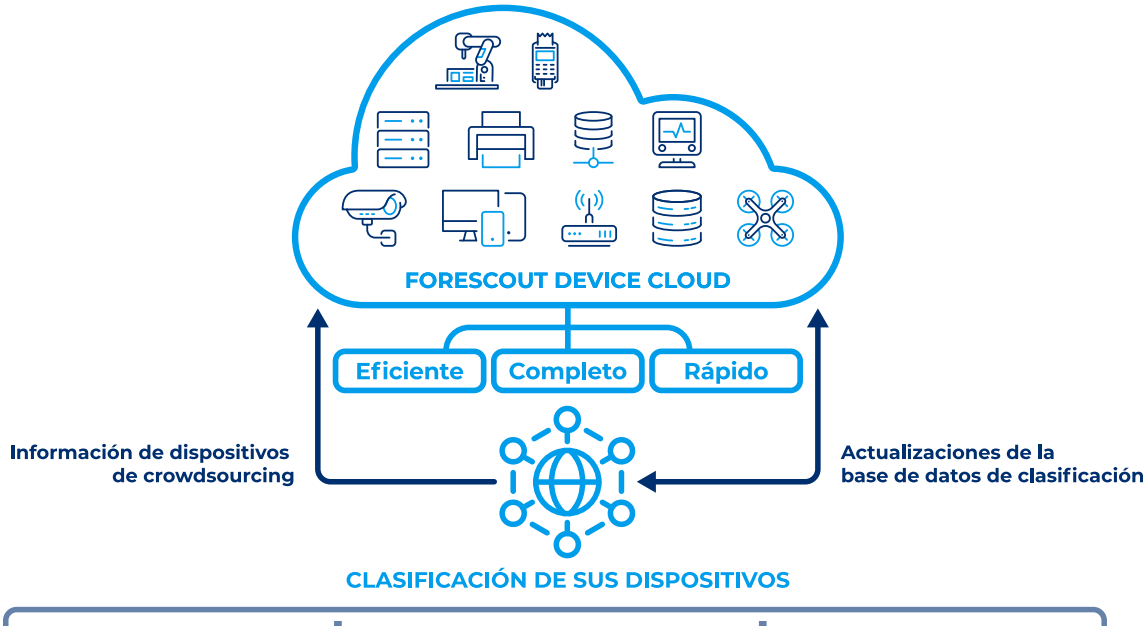
Clasificación automática inteligente

Si se implementan las directrices de seguridad sin un contexto de dispositivos completo, esto puede conducir a resultados indeseados y poner en peligro los procesos empresariales. La Forescout Device Cloud, el mayor repositorio de datos de dispositivos, recogidos de más de 50 millones de activos, aporta automáticamente un contexto completo para cada dispositivo conectado. Nuestro esquema de clasificación multidimensional abarca la función y el tipo de dispositivo, el sistema operativo y su versión, así como el fabricante y modelo, entre ellos:

- más de 1900 versiones de sistemas operativos distintos
- más de 7700 fabricantes y modelos de dispositivos distintos
- dispositivos médicos de más de 400 proveedores líderes
- miles de sistemas de control industriales y dispositivos de automatización que se utilizan en la fabricación, el sector energético, la industria petrolera y de gas, las empresas de suministro, la minería y en otros sectores de infraestructura crítica

Clasificación automática basada en la Forescout Device Cloud

La Device Cloud, el mayor repositorio del mundo de información sobre dispositivos, ofrece los conocimientos más completos y precisos sobre los riesgos de los dispositivos en empresas de todo tipo.



Evaluar

Evaluación sin agentes del estado de los dispositivos

eyeSight vigila continuamente la red y comprue-a de inmediato la configuración de los dispositivos detectados, su estado de seguridad y su perfil de riesgo, para esta-lecer si son conformes con las disposiciones de cumplimiento y las directrices de seguridad. Para cuantificar mejor los riesgos, se pueden aplicar directrices para la compro-ación de las condiciones de conformidad, como las siguientes:

- ¿Está el software de seguridad instalado, activado y actualizado?
- ¿Es el dispositivo crítico para el negocio?
- ¿Se han descu-ierto dispositivos en los que se ejecutan aplicaciones no autorizadas o que infringen los estándares de configuración?
- ¿Hay dispositivos, especialmente sistemas IoT, IoMT y TO, que utilicen contraseñas estándar o dé-iles?
- ¿Se han descu-ierto dispositivos ilícitos, incluidos aquellos que se hacen pasar por legítimos mediante técnicas de suplantación?
- ¿Qué dispositivos conectados son más vulnera-les a las amenazas más nuevas?

Vigilar

Recibir información de cumplimiento

Extraiga conocimientos prácticos implementa-les a través de paneles de mando (dash-oards) preconfigurados, para detectar con rapidez riesgos en todo el entorno, priorizarlos y contenerlos de forma proactiva. Las vistas adapta-les de los paneles de mando facilitan a los analistas de seguridad y los equipos del SOC numerosas tareas:

- Evaluación de los riesgos y avances de cumplimiento para todo tipo o un su-grupo cualquiera de directrices
- Localización de dispositivos vulnera-les o comprometidos, para poder reaccionar de forma más rápida y específica a incidentes
- Seguimiento a largo plazo de tendencias de cumplimiento
- Adaptación de vistas del estado de riesgo y de cumplimiento para su entrega a directivos e inspectores
- Rápida búsqueda y filtrado de activos por directrices o características del dispositivo

Segmentar, orquestar, implantar

La plataforma de Forescout aumenta las utilidades de eyeSight con soluciones de ciberseguridad automatizadas que permiten la elaboración e implementación de directrices unificadas para el control de acceso a la red, así como una segmentación dinámica de la red, y crea la base para una seguridad de conformidad cero.

UPara averiguar más sobre la plataforma de Forescout, visite www.forescout.com/platform/

Forescout Technologies, Inc.

Gratuita (EE. UU.) 1-866-377-8771
Tel. (internac.) +1-408-213-3191
Asistencia +1-708-237-6591

Descubra más en Forescout.com