Forescout eyeSight

Descubrimiento, clasificación y evaluación continuos de los dispositivos para obtener información de la situación y reducir el riesgo

Los CIO están asumiendo la responsabilidad de proteger un número cada vez mayor de sistemas conectados a la red, concretamente dispositivos IoT y de OT. Como reza nuestro lema, You can't secure what you can't see™, no se puede proteger lo que no se ve, y este incremento en el número (y los tipos) de dispositivos ha hecho aumentar la sensación colectiva de necesidad urgente de visibilidad de todos los dispositivos físicos y virtuales. Entre ellos se incluyen los dispositivos gestionados, no gestionados y desconocidos que conectan los empleados, contratistas y clientes, o incluso el personal de operaciones con buena intención. Estén donde estén en la red —en campus, centros de datos, la nube pública o privada, o entornos de OT/ICS— estos dispositivos deben detectarse, clasificarse y contabilizarse convenientemente.

Figura 1: Visibilidad detallada en campus, IoT, centros de datos, la nube y tecnologías operativas (OT).

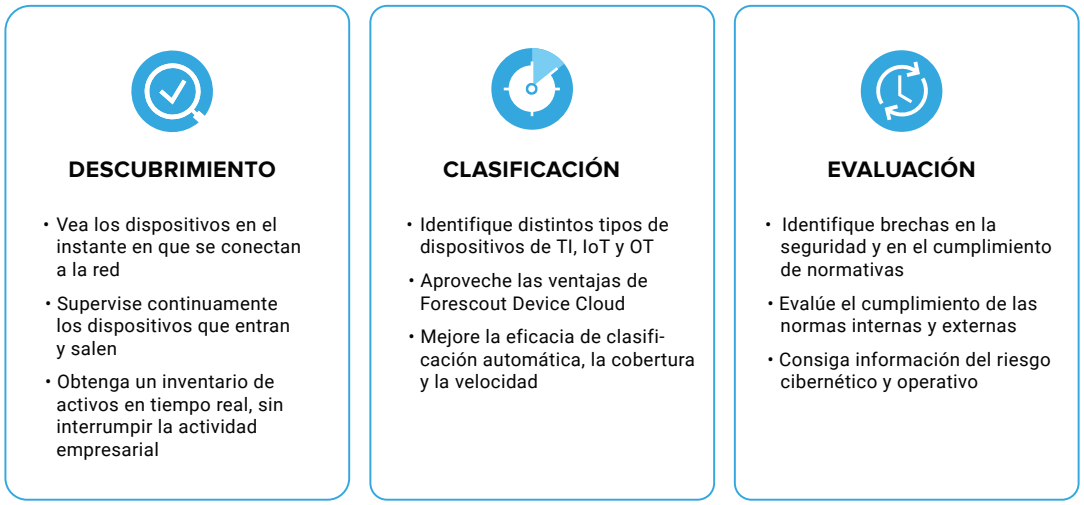
Forescout eyeSight le ofrece una visión inigualable de la totalidad de sus dispositivos, sin interrumpir los procesos empresariales críticos. Empieza por descubrir cada uno de los dispositivos conectados por IP a sus redes empresariales ampliadas. Pero el descubrimiento es solo el primer paso para conseguir la visibilidad total. Para tomar las decisiones adecuadas en cuanto a directivas y control, es fundamental contar con contexto global. Tras descubrir los dispositivos conectados, eyeSight los clasifica automáticamente y los evalúa según las directivas de la empresa. La eficaz combinación de estas tres características —descubrimiento, clasificación y evaluación— proporciona la visibilidad de dispositivos necesaria para aplicar las directivas y llevar a cabo las acciones adecuadas.

eyeSight

Funciones principales

- Ofrece un inventario unificado en tiempo real de todos los dispositivos conectados a la red, sin necesidad de agentes
- Clasifica con precisión los dispositivos para obtener el contexto que permita diseñar directivas proactivas de seguridad y cumplimiento de normativas
- Identifica los dispositivos no autorizados, vulnerables o no conformes, y crea directivas para limitar el riesgo
- Ofrece certeza en tiempo real de que las herramientas de seguridad y los controles de cumplimiento funcionan
- Mide con eficacia e informa del estado de cumplimiento y la exposición a ciberriesgos
- Automatiza tareas habituales para minimizar la posibilidad de error humano e incrementar la eficiencia

Figura 2: Funciones esenciales de visibilidad que ofrece eyeSight



Descubrimiento continuo, sin agentes

Los dispositivos IoT y de OT presentan retos especiales para la visibilidad. El ingente número de dispositivos de este tipo crea un problema de escala, que imposibilita el descubrimiento manual. Además, muchos de estos dispositivos no admiten agentes, y son especialmente sensibles a técnicas de sondeo y análisis activos que podrían provocar la interrupción de los sistemas y de la actividad de la empresa. eyeSight utiliza más de 20 técnicas de supervisión activa y pasiva (véase la Figura 3) para evitar posibles lagunas de visibilidad, mediante el descubrimiento de:

- Portátiles, tablets, smartphones, sistemas BYOD/de invitados y dispositivos IoT en redes de campus
- Máquinas virtuales, hipervisores y servidores físicos en centros de datos
- Instancias de AWS, Azure y VMware en nubes públicas y privadas
- Dispositivos médicos, industriales y de automatización de edificios en redes de tecnología operativa (OT)
- Infraestructuras de red físicas y definidas por software, con conmutadores, routers, VPN, puntos de acceso inalámbrico y controladoras

Estas funciones de descubrimiento se combinan para minimizar el riesgo operativo y eliminar los puntos ciegos de visibilidad con el fin de obtener un inventario de dispositivos completo y continuo en toda la empresa.

Figura 3: Técnicas de descubrimiento activo y pasivo.

PASIVO A INFRAESTRUCTURA	PASIVO A DISPOSITIVO FINAL	ACTIVO A DISPOSITIVO FINAL
Capturas SNMP	Sondeo de la infraestructura de red	Inspección de Windows sin agente • WMI • RPC • SMB
Tráfico SPAN	Integración SDN • Meraki • Cisco ACI	Inspección de macOS, Linux sin agente • SSH
Análisis de flujo • NetFlow • Flexible NetFlow • IPFIX • sFlow	Integración de la nube pública/privada • VMware • AWS • Azure	NMAP
Solicitudes DHCP	Consulta de servicios de directorio (LDAP)	Consultas SNMP
Usuario-agente HTTP	Consulta de aplicaciones web (REST)	Consultas HTTP
Huella digital TCP	Consulta de bases de datos (SQL)	SecureConnector®
Análisis de protocolos	Orquestaciones de eyeExtend	
Solicitudes RADIUS		

Problemas

- Los equipos, herramientas de seguridad y procesos aislados generan lagunas de visibilidad.
- Los procesos manuales, propensos a provocar errores, generan un riesgo operativo y para el negocio.
- Una inteligencia incompleta sobre dispositivos ofrece al equipo de TI poco contexto para poder construir directivas de defensa.
- Incapacidad para verificar qué herramientas de seguridad hay instaladas, configuradas y funcionando correctamente.
- Si no se detectan los dispositivos no autorizados se crean riesgos innecesarios de seguridad e incumplimiento de normativas.
- Los análisis puntuales realizados hace demasiado tiempo generan una falta de confianza en el estado de cumplimiento.

Clasificación automática inteligente

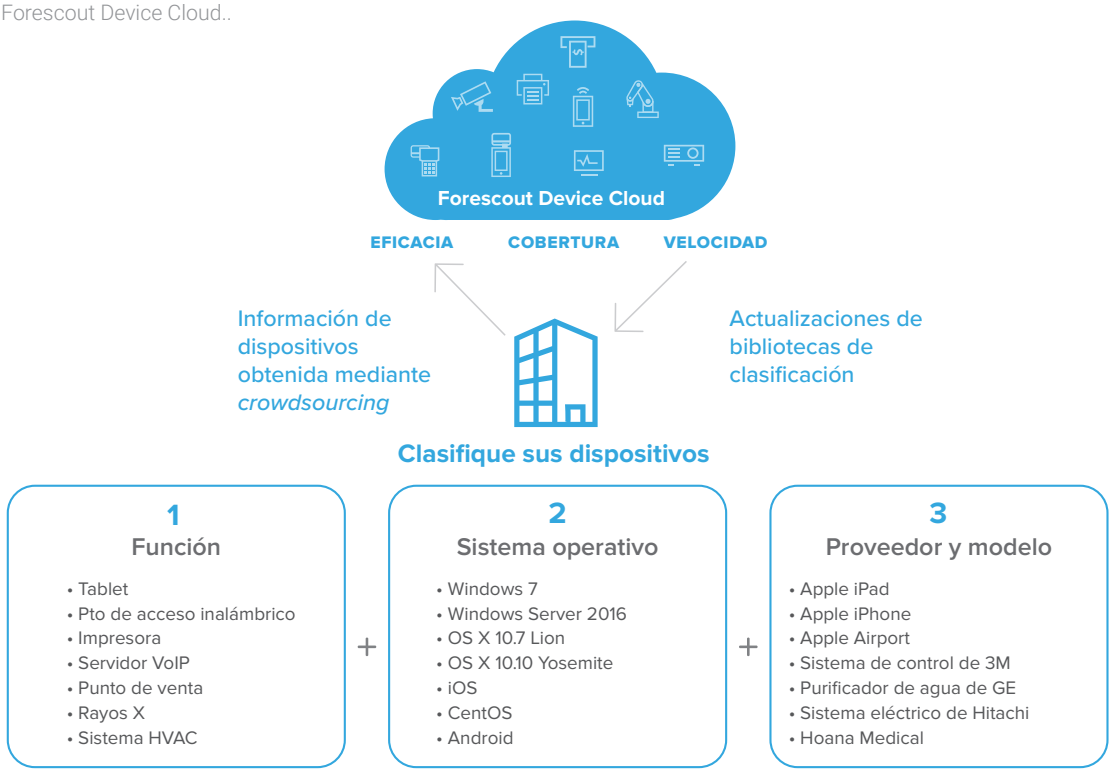
Contar con contexto completo para cada dispositivo es esencial para crear directivas granulares. Debe conocer el contexto operativo o el propósito de cada dispositivo para decidir cómo protegerlo y gestionarlo mejor. Dado el crecimiento y la diversidad de dispositivos es casi imposible recopilar manualmente este contexto, y crear directivas sin el contexto adecuado pone en riesgo las operaciones. eyeSight clasifica automáticamente los dispositivos IoT y de OT mediante una taxonomía multidimensional para identificar la función y el tipo de dispositivo, el sistema operativo y la versión, así como el proveedor y el modelo. La inspección profunda de paquetes de más de 100 protocolos de TI y OT permite a eyeSight obtener información detallada sobre la identidad de los dispositivos IoT y de OT.

eyeSight clasifica de forma automática :

- Más de 500 versiones de sistemas operativos diferentes
- Más de 5000 proveedores y modelos distintos
- Dispositivos médicos de más de 350 proveedores líderes en 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 eyeSight, garantizando que esta rica fuente de contexto esté siempre actualizada a medida que crezca el número y diversidad de los dispositivos. Forescout Research emplea inteligencia de más de 8 millones de dispositivos del mundo real en nuestra nube de dispositivos*, y publica estos nuevos perfiles con frecuencia con el fin de mejorar la eficacia de clasificación, la cobertura y la velocidad en su entorno de dispositivos completo.

Figura 4: Forescout Device Cloud..



*31 de diciembre de 2018.

Evaluación del estado de los dispositivos

La clasificación de los dispositivos ofrece contexto operativo referente su objetivo, es decir, qué es cada dispositivo. Sin embargo, para obtener un contexto completo, se requiere otra perspectiva para medir la salud e higiene de cada dispositivo. eyeSight 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. eyeSight da respuesta a cuestiones clave, como:

- ¿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 (y si están o no conectados a la red)?
- ¿Cuáles de los dispositivos conectados son más vulnerables a las últimas amenazas?

El poder de la inteligencia de dispositivos

La visibilidad de los dispositivos que ofrece eyeSight a través del descubrimiento, descripción, clasificación automática y evaluación ya se aprecia en la consola de Forescout. Sus paneles personalizables proporcionan una visión general y permiten compartir estas imágenes de cómo progresa en la consecución de sus objetivos de riesgo y cumplimiento. Estas vistas dinámicas pueden ayudar a los equipos a:

- Evaluar si una directiva concreta se ha implementado correctamente.
- Identificar dispositivos vulnerables en caso de violación de la seguridad para acelerar la respuesta a incidentes.
- Realizar un seguimiento del cumplimiento de requisitos específicos a lo largo del tiempo.
- Crear vistas del riesgo y el cumplimiento, así como posibles vulnerabilidades, destinadas a directivos y auditores.
- Acceder a datos detallados para abordar áreas problemáticas relacionadas con directivas, tipos de dispositivos, ubicaciones, etc. concretos.

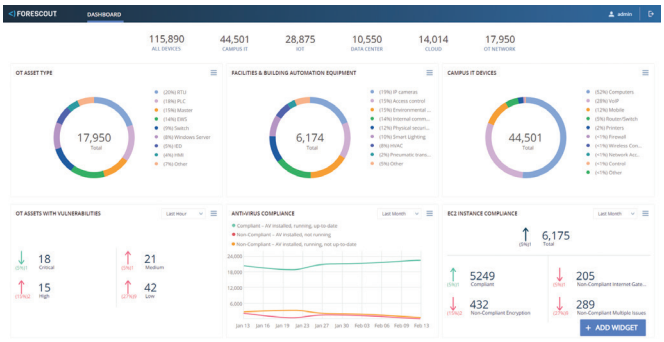


Figura 5. Personalización del panel para ofrecer a distintos interesados el contexto que necesitan.

La visibilidad de dispositivos que ofrece eyeSight se puede compartir también con interesados de otras áreas de TI a través de notificaciones e interfaces API. La cartera de productos de eyeExtend comparte este contexto de dispositivos con otros productos líderes en seguridad y TI a fin de automatizar los flujos de trabajo y orquestar una respuesta para todo el sistema.

Sin el contexto sobre dispositivos fundamental que aporta eyeSight, las empresas no tienen la confianza necesaria para implementar directivas de control, ya que si las medidas no se basan en suficiente inteligencia, pueden poner en riesgo las operaciones empresariales. eyeSight le proporciona la información profunda que necesita para diseñar y aplicar directivas granulares, así como automatizar acciones para la gestión de activos, el cumplimiento para dispositivos, el acceso a la red, la segmentación de red y la respuesta a incidentes. Después, mediante Forescout eyeControl y Forescout eyeExtend, puede establecer controles eficaces basados en directivas y organizar las acciones con confianza.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Teléfono gratuito (EE. UU.)
1-866-377-8771
Tel. (internacional) +1-408-213-3191
Soporte técnico 1-708-237-6591

Más información en Forescout.com

© 2019 Forescout Technologies, Inc. Reservados todos los derechos. Forescout Technologies, Inc. es una empresa de Delaware. Encontrará una lista de marcas comerciales y patentes en https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Los demás nombres de marcas, productos o servicios pueden ser marcas comerciales o marcas de servicios de sus respectivos propietarios. Version 05_19