FORESCOUT
Active Defense for the Enterprise of Things™

eyeSight

Visibilidad completa de dispositivos

SIN AGENTE

Ofrece un inventario unificado en tiempo real de todos los dispositivos conectados a la red.

PRECISIÓN

Clasifica todos los dispositivos para obtener el contexto necesario que permita diseñar directivas proactivas de seguridad y cumplimiento de normativas.

EFECTIVIDAD

Identifica los dispositivos no autorizados, vulnerables o no conformes, y crea directivas para limitar el riesgo.

FIABILIDAD

Ofrece certeza en tiempo real de que las herramientas de seguridad y los controles de cumplimiento funcionan.

EFICIENCIA

Mide automáticamente e informa del estado de cumplimiento y la exposición a ciberriesgos, minimizando la posibilidad de error humano y aumentando la eficacia.

Descubrimiento, clasificación y evaluación continuas de todos los dispositivos conectados en toda la empresa

Forescout eyeSight le ofrece una visión inigualable de la totalidad de su empresa de las cosas (EoT, Enterprise of Things), sin interrumpir los procesos empresariales críticos.

- Descubra de todos los dispositivos conectados mediante IP.
- Clasifique los dispositivos automáticamente y consiga contexto completo.
- Evalúe el cumplimiento de directivas y el estado de seguridad de los dispositivos.

DESCUBRIMIENTO

Vea los dispositivos en el instante en que se conectan a la red.

Supervise continuamente la conexión y desconexión de los dispositivos.

Obtenga un inventario de activos en tiempo real, sin interrumpir la actividad empresarial.

CLASIFICACIÓN

Identifique distintos tipos de dispositivos IT, IoT y OT

Aproveche las ventajas de Forescout Device Cloud.

Mejore la eficacia de clasificación automática, la cobertura y la velocidad.

EVALUACIÓN

Identifique brechas en la seguridad y en el cumplimiento de normativas.

Evalúe el cumplimiento de las normas internas y externas.

Consiga información del riesgo cibernético y operativo.

DESCUBRIMIENTO

Descubrimiento continuo sin agentes

Elimine los ángulos muertos y minimice el riesgo operativo con visibilidad completa de toda su empresa de las cosas:

- Portátiles, tablets, smartphones, sistemas BYOD/de invitados, dispositivos de teletrabajo
- Dispositivos IoT en redes de campus, centros de datos, sucursales, sitios remotos y redes perimetrales
- Instancias de redes públicas y privadas en entornos de AWS, Azure y VMware
- Sistemas de tecnología operativa (OT), incluidos dispositivos médicos, industriales y de automatización de edificios
- Infraestructuras de red físicas y definidas por software, con conmutadores, routers, puntos de acceso inalámbrico y controladoras

Aproveche la flexibilidad de más de 20 técnicas de supervisión activa y pasiva en redes alámbricas, inalámbricas, VPN, virtuales y definidas por software. Evite dispositivos especialmente sensibles a técnicas de sondeo y análisis activos.

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 Análisis de flujo • NetFlow • Flexible NetFlow • IPFIX • sFlow	Integración SDN • Meraki • Cisco ACI	Inspección de macOS, Linux sin agente • SSH
Solicitudes DHCP	Integración de la nube pública/privada • VMware • AWS • Azure	NMAP
Agente de usuario HTTP	Consulta de servicios de directorio (LDAP)	Consultas SNMP
Huella digital TCP	Consulta de aplicaciones web (REST)	Consultas HTTP
Análisis de protocolos	Consulta de bases de datos (SQL)	SecureConnector®
Solicitudes RADIUS	Orquestaciones de eyeInspect	

CLASIFICACIÓN

Clasificación automática inteligente

Las directivas Zero Trust solo pueden aplicarse sobre la base de un contexto de dispositivos completo. La recopilación manual de este contexto es prácticamente imposible, y las directivas Zero Trust implementadas sin contexto de dispositivos completo pueden poner en riesgo las operaciones. Gracias a la inspección profunda de paquetes de más de 150 protocolos de IT y OT, eyeSight proporciona una identificación profunda de todos los dispositivos IT, IoT y OT. La taxonomía multidimensional identifica la función y el tipo de dispositivo, el sistema operativo y la versión, así como el proveedor y el modelo, incluidos:

- Más de 600 versiones de sistemas operativos diferentes
- Más de 5700 proveedores y modelos distintos
- Dispositivos médicos de más de 400 proveedores líderes en tecnología sanitaria
- Miles de sistemas de control y automatización industrial que se utilizan en infraestructuras de fabricación, energía, gas y petróleo, servicios públicos, minería y otros sectores críticos

EYESIGHT RESUELVE:

Lagunas de visibilidad provocadas por equipos aislados y herramientas de seguridad distintas.

Riesgos operativos y comerciales debidos a procesos manuales propensos a errores.

Inteligencia sobre dispositivos incompleta, lo que obstaculiza la ejecución de las directivas Zero Trust de protección.

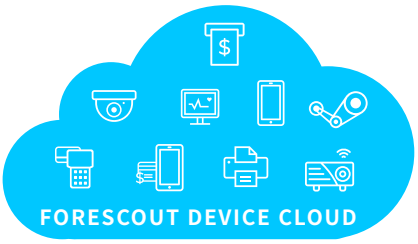
Brechas de seguridad cuando las herramientas basadas en agentes no están actualizadas o no funcionan correctamente.

Dispositivos no autorizados que no se han detectado o problemas de suplantación.

Incumplimiento que puede surgir rápidamente entre análisis puntuales.

Clasificación automática basada en Forescout Device Cloud

Device Cloud, el mayor lago de datos del mundo con inteligencia sobre dispositivos obtenida de manera colaborativa, proporciona el conocimiento más completo y preciso de todos los riesgos asociados a los dispositivos dentro del contexto de cualquier empresa.



EFICACIA COBERTURA VELOCIDAD

Información de dispositivos obtenida mediante crowdsourcing

Actualizaciones de bibliotecas de clasificación

CLASIFIQUE SUS DISPOSITIVOS

Función		Sistema operativo		Proveedor y modelo	
• Tablet	• Servidor VoIP	• Windows 7	• iOS	• iPad de Apple	• Purificador de agua de GE
• Pto de acceso inalámbrico	• Punto de venta	• Windows Server 2016	• CentOS	• iPhone de Apple	• Sistema eléctrico de Hitachi
• Impresora	• Rayos X	• OS X 10.7 Lion	• Android	• Airport de Apple	• Hoana Medical
	• Sistema HVAC	• OS X 10.10 Yosemite		• Sistema de control de 3M	

EVALUACIÓN

Evaluación del estado de los dispositivos

Otro elemento esencial de las directivas Zero Trust es la incorporación de la higiene de seguridad y el perfil de riesgo de los dispositivos que se conectan. eyeSight supervisa continuamente la red y evalúa la configuración, el estado de la seguridad y los indicadores de riesgos de los dispositivos conectados y averigua si cumplen las directivas y normativas de seguridad. Las directivas Zero Trust se pueden basar en condiciones de riesgo y cumplimiento 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 infrinja los estándares de configuración?
- ¿Utilizan los dispositivos, en particular los sistemas IoT y OT, contraseñas predeterminadas o débiles?
- ¿Se han detectado dispositivos no autorizados, como los que suplantan dispositivos legítimos?
- ¿Cuáles de los dispositivos conectados son más vulnerables a las últimas amenazas?

No se conforme con verlo. Protéjalo.

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

SUPERVISIÓN

Visibilidad y cumplimiento de EoT

Consiga información práctica de paneles disponibles y personalizables para detectar, priorizar y mitigar de forma rápida y proactiva los riesgos de sus “cosas” conectadas. Las vistas dinámicas ayudan a los analistas de seguridad y equipos de operaciones de seguridad (SOC) a:

- Evaluar el progreso del riesgo y el cumplimiento de todas las directivas o en cualquier subgrupo.
- Identificar los dispositivos vulnerables y comprometidos para acelerar la respuesta a incidentes.
- Realizar un seguimiento de las tendencias de cumplimiento a lo largo del tiempo.
- Personalizar y compartir vistas del riesgo y el cumplimiento, destinadas a directivos y auditores.
- Buscar y filtrar rápidamente activos de EoT por directiva o por atributos de dispositivos

Segmentación, organización e implementación

Amplíe el valor de eyeSight con una suite de productos de Forescout para diseñar e implementar directivas Zero Trust para disponer de control de acceso a la red, seguridad de IoT, segmentación de la red y seguridad del IoT.

Visite www.forescout.com/platform/ para obtener más información sobre los productos eyeSegment, eyeControl, eyeInspect y eyeExtend de Forescout.

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