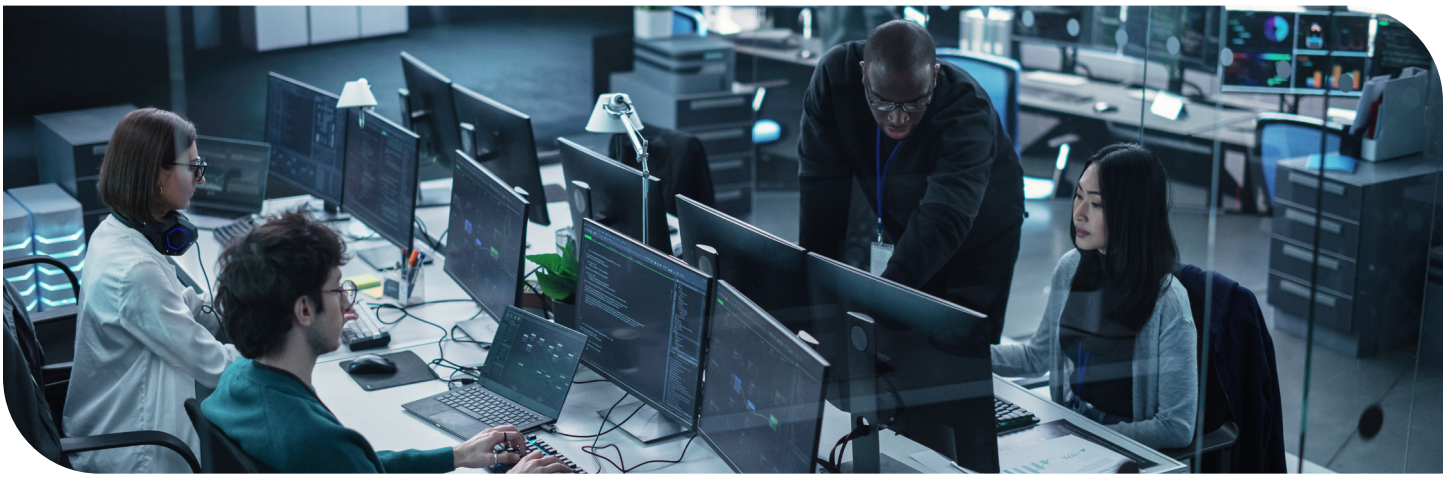
FORESCOUT

Gestión de riesgos y exposición

Identificar, cuantificar y priorizar riesgos y problemas de cumplimiento



"Las violaciones de la seguridad raras veces son furto de ataques muy planificados dirigidos por Estados o complejos métodos de ataque. Más bien son fruto de una serie de sencillos procesos, que se pueden evitar mediante medidas de seguridad básicas, como una gestión de vulnerabilidades basada en el riesgo"

Forrester Research, *The State of Vulnerability Risk Management, marzo de 2023*

La superficie de ataque crece de forma imparable, impulsada por el aumento de TI en la sombra, entornos de trabajo híbridos y el uso de nubes. Los equipos de seguridad y de red, que protegen su empresa y sus valiosos activos digitales, apenas pueden seguir el ritmo de este desarrollo. Las tecnologías obsoletas, los agujeros de seguridad no parcheados y los activos de TI menos "importantes" a menudo se saltan por alto, pero son objetivos fáciles. Los atacantes aprovechan estas vulnerabilidades para penetrar en redes y moverse después por la infraestructura para acceder a objetivos valiosos. Si los equipos confían en herramientas de seguridad reactivas, que no hacen saltar la alarma hasta que la seguridad ya está comprometida, esto puede conllevar tiempos de interrupción que se podrían evitar mediante controles de seguridad proactivos.

Las empresas necesitan un enfoque efectivo para entender sus superficies de ataque y desarrollar procesos de seguridad que no obstaculicen el funcionamiento empresarial ni estorben a los usuarios. Para ello, necesitan herramientas de equipo que ayuden a establecer prioridades en la gestión de activos y riesgos de forma proactiva y que, al mismo tiempo, aporten el contexto necesario para mitigar los incidentes de seguridad.

Mejora demostrable de la situación de riesgo

- Gestión simplificada de los activos de ciberseguridad
- Vista completa de los riesgos de los dispositivos
- Evaluación clara y precisa de la vulnerabilidad de los dispositivos
- Respuesta más rápida a incidentes
- Establecimiento proactivo de directrices de seguridad
- Mejor protección de IoT y equipos médicos

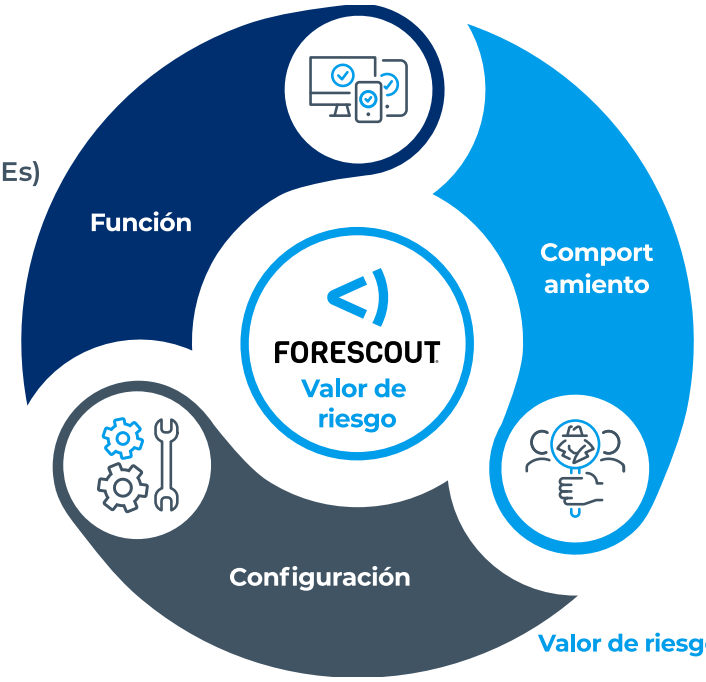
Refuerce la seguridad de su red mediante la priorización basada en el riesgo

Los equipos de seguridad, que se enfrentan a una superficie de ataque creciente y una falta de contexto debido a las herramientas aisladas, reciben con Forescout Risk and Exposure Management una herramienta completa de inteligencia de activos, que les proporciona una base fiable para la comprensión de la situación de seguridad. La solución vigila la efectividad de las medidas en todo el ecosistema de seguridad para reducir los riesgos y vulnerabilidades. Para eliminar los puntos débiles, aplica un enfoque automatizado y basado en el riesgo.

The Forescout® Risk and Exposure Management permite a las empresas no solo detectar los riesgos, sino también entenderlos. Los equipos de seguridad pueden:

- reducir el esfuerzo empresarial dedicado a la gestión de activos de ciberseguridad
- mejorar decisivamente la ciberhigiene averiguando la superficie de ataque completa
- comprender la configuración y el estado de cada equipo conectado y, sobre esta base, evaluar, clasificar y cuantificar de forma precisa el nivel de riesgo y la usabilidad
- demostrar la utilidad de las inversiones realizadas en tecnologías de seguridad y hacer un seguimiento de la efectividad de las medidas de control para reducir los riesgos paso a paso
- acelerar la revisión de incidentes y desarrollar proactivamente directrices para evitar otros incidentes

- **Configuración:**
  - Vulnerabilidades (CVEs)
  - Usabilidad (EPSS)
  - Servicios expuestos
- **Función:**
  - Criticalidad de los dispositivos
- **Comportamiento:**
  - Accesibilidad desde Internet



Valor de riesgo = f (indicadores de riesgo detectados, criticalidad de los dispositivos)

Información sobre dispositivos disponible a largo plazo y priorización de ciberriesgos

Forescout Risk and Exposure Management le ayuda a identificar, cuantificar y priorizar riesgos debidos a vulnerabilidades y configuraciones erróneas. Para ello se calcula un valor de riesgo multifactorial unívoco para cada dispositivo basándose en la configuración, la función y el comportamiento específicos del dispositivo.

Identificar

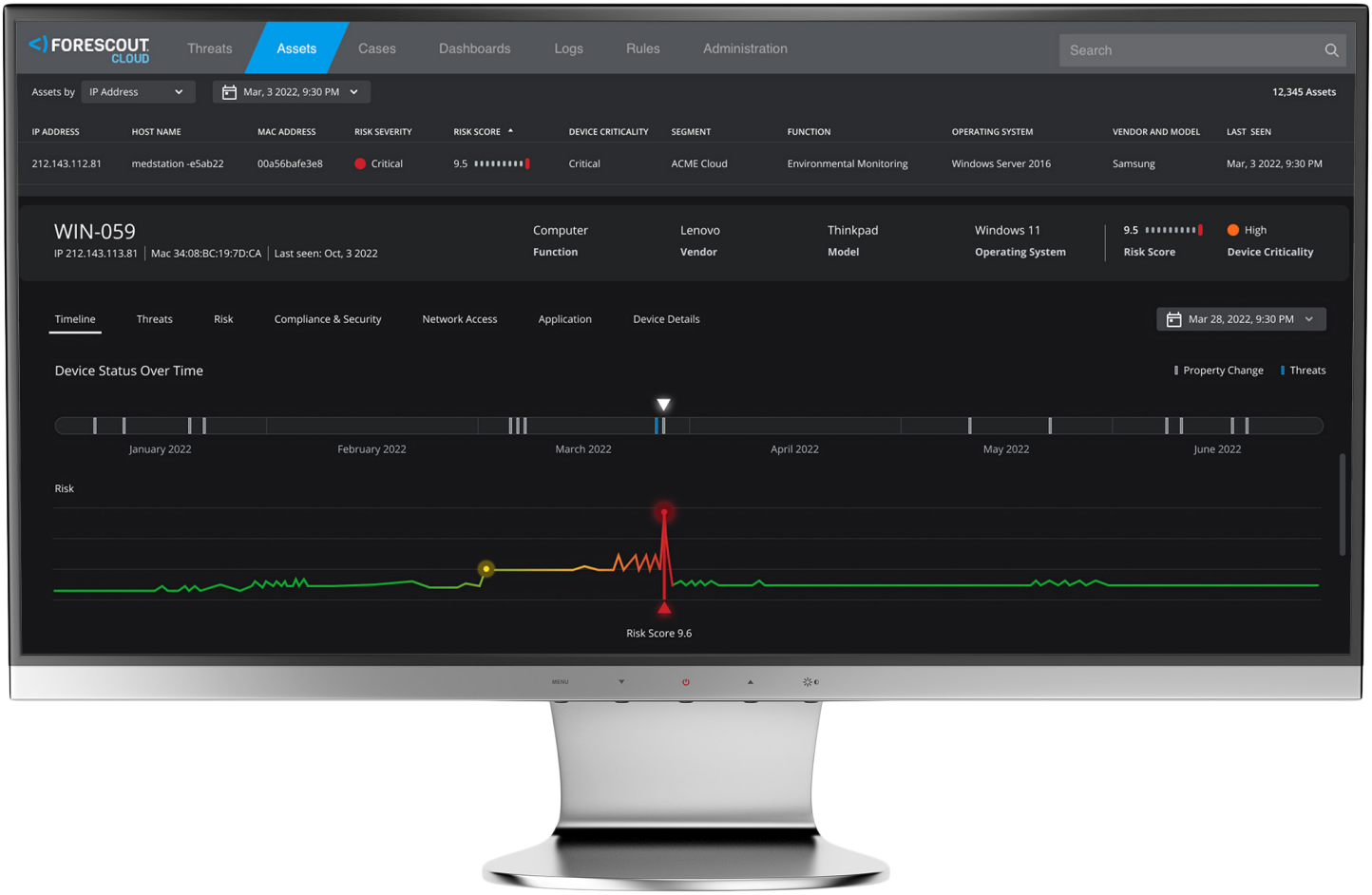
Gestión de activos de ciberseguridad optimizada gracias a conocimientos claros y precisos de cada dispositivo en la red

Benefíciese de un inventario preciso y duradero con datos históricos sobre el estado de los dispositivos y los cambios en la configuración, que se sirve de una clasificación basada en la nube de los dispositivos administrados y no administrados (TI, IoT, IoMT, TO/ICS).

Inventariado de la superficie de ataque – Clasificación fiable basada en la nube de dispositivos administrados y no administrados.

Datos de dispositivos contextuales persistentes – Buscables; conservación durante 90 días y seguimiento de datos de dispositivos contextuales completos, incluyendo los cambios en el estado y la configuración.

Filtrado de perfiles de vulnerabilidad – Las funciones de filtrado ampliadas permiten encontrar y hacer un seguimiento de los dispositivos que tengan en común con dispositivos comprometidos determinadas características de vulnerabilidad. Esto le permite solventar problemas de forma proactiva.



Por qué Forescout

1. Inventario persistente de todos los tipos de dispositivos en una superficie moderna
2. Valor de riesgo multifactorial unívoco, basado en la configuración, la función y el comportamiento
3. Clasificación fiable basada en la nube
4. Tecnología de inspección profunda de paquetes patentada
5. Correlación de la usabilidad de vulnerabilidades con la exposición de los dispositivos
6. Integraciones con productos de seguridad líderes y posibilidad de comprobar la efectividad
7. Conocimientos prácticos implementables sobre riesgos y vulnerabilidades
8. Lago de datos basado en la nube con información sobre riesgos y amenazas

Visite www.forescout.com para averiguar más sobre el enfoque que Forescout aplica en la gestión del riesgo y la exposición, y solicitar una demostración.

Cuantificar

Conocimientos completos de los riesgos de ciberseguridad

Haga un seguimiento continuo del riesgo de ciberseguridad que suponen todos los dispositivos conectados sirviéndose de un valor de riesgo multifactorial basado en la configuración, función y comportamiento. De este modo podrá proteger su red proactivamente.

Configuración – Registro de las exigencias de configuración específicas de cada dispositivo para establecer si es accesible para los atacantes y si presenta vulnerabilidades que estos puedan explotar:

- Vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés), correladas con el catálogo CISA de vulnerabilidades explotadas conocidas (KEV, por sus siglas en inglés)
- Exploit Prediction Scoring System (epss)
- Servicios expuestos y puertos abiertos, así como el potencial peligro (control o acceso)

Función – Establecer y evaluar la criticalidad de los dispositivos, partiendo de su función y uso.

Comportamiento – Seguimiento de los cambios en la configuración y el comportamiento de cada dispositivo para detectar anomalías que aumenten el riesgo de compromiso, por ejemplo, por parte de un atacante de Internet.

Priorizar

Revisión rápida de incidentes y desarrollo proactivo de medidas de remedio

Facilite a sus equipos de TI y de seguridad el acceso a datos de inventario persistentes y en tiempo real, para ayudarles a minimizar el riesgo proactivamente y examinar incidentes.

Información de dispositivos accesible en cualquier sitio – El portal Forescout Cloud ofrece a todos los equipos de TI y de seguridad un acceso fácil y fiable a información completa y contextual de los dispositivos

Priorización basada en el riesgo – Utilice las características de riesgo y vulnerabilidad en combinación con información sobre el estado de cumplimiento y de configuración de los dispositivos para revisar los incidentes y simplificar el desarrollo de medidas de remedio.

Contexto histórico de los dispositivos – Acelere el análisis de riesgo y la respuesta a incidentes para minimizar el radio de acción de los ataques y reducir el tiempo medio de reparación (MTTR).

FORESCOUT®

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

©2023 Forescout Technologies, Inc. Todos los derechos reservados. Forescout Technologies, Inc. es una empresa registrada en Delaware, EE. UU. Encontrará una lista de nuestras marcas y patentes en www.forescout.com/company/legal/intellectual-property-patents-trademarks. Otras marcas, productos o nombres de servicios pueden ser marcas o marcas de servicios de las correspondientes empresas. Versión 01_02