FORESCOUT

Novedades de Forescout 8.2

"Para 2023, el número total de dispositivos IoT "conectados en todo el mundo aumentará hasta superar los 35 200 millones".

– Worldwide Internet of Things Infrastructure Forecast, 2019-2023, IDC

Los ataques de la pasada década nos han enseñado que basta un solo punto débil en una red para que una empresa sea vulnerable a violaciones de la seguridad. En un momento en que aumenta el número de dispositivos IoT y no gestionados que se conectan a las redes empresariales para impulsar la transformación digital, existe la urgente necesidad de equilibrar la innovación con el igualmente crítico objetivo de proteger estos dispositivos y proteger las redes.

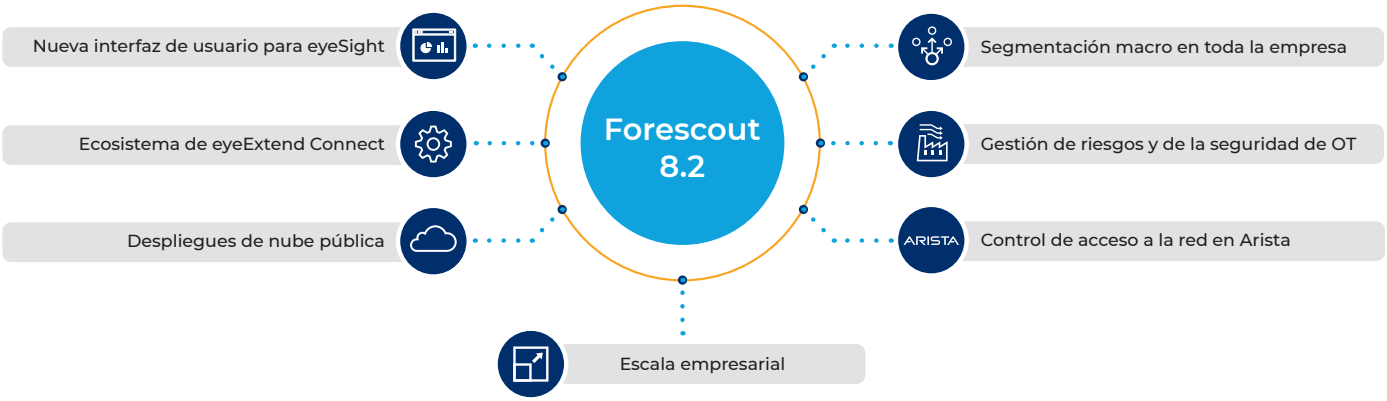
Sin una visión completa de los dispositivos conectados en todos los dominios de red, la capacidad de actuar rápidamente para mitigar los riesgos es prácticamente nula. Es necesario identificar todos los dispositivos antiguos y vulnerables, los endpoints no conformes y mal configurados, y las tecnologías operativas y del Internet de las cosas (IoT). Resulta absolutamente imprescindible evaluar continuamente los riesgos de todas las redes interconectadas en todas las ubicaciones. Una visibilidad completa otorga el poder de actuar rápido.

Forescout 8.2: identificar y actuar más rápidamente

Forescout 8.2 acelera la capacidad de identificar todos los dispositivos conectados, los problemas de incumplimiento y los riesgos de su red. Le permite actuar con confianza y rapidez para mitigar los riesgos de seguridad y reducir el tiempo medio de respuesta en sus redes empresariales ampliadas.

Las características principales son:

- Nueva interfaz de usuario centrada en las personas para Forescout eyeSight, con contexto de dispositivos práctico para identificar, priorizar y mitigar de forma proactiva los riesgos.
- Forescout eyeExtend Connect, un nuevo ecosistema de apps comunitarias que permite a clientes y partners desarrollar, consumir y compartir apps más fácilmente para integrarse con la plataforma Forescout.
- Nueva flexibilidad de despliegue y rentabilidad más rápida para las empresas que priorizan la nube, que desean desplegar appliances Forescout en sus entornos de nube pública de AWS y Microsoft Azure.
- Segmentación en toda la empresa con Forescout eyeSegment para permitir a las empresas diseñar y aplicar con confianza directivas en todos los dominios de red y puntos de implementación diversos.
- Integración con Forescout SilentDefense™, así como sensores de IT/OT integrados en el mismo appliance para disponer de una visibilidad unificada en todos los dominios de IT y OT, incluidas las redes clonadas con rangos de IP superpuestos.
- Control de acceso a la red a través de la integración directa con la infraestructura de Arista sin necesidad de agentes ni dependencia de 802.1X para dispositivos IT e IoT.



Nueva interfaz de usuario

Todos los interesados se benefician de un contexto basado en personas e información práctica distribuida a través de la nueva interfaz de usuario basada en la web. Los paneles visualizan los dispositivos conectados, alertan a los equipos sobre las áreas de mayor riesgo e indican el progreso respecto a los objetivos de cumplimiento. El inventario de dispositivos en tiempo real con funciones de análisis descendente detallado permite a los operadores buscar los dispositivos rápidamente para ayudar a su empresa a adelantarse a las amenazas. Opciones de personalización y uso compartido sencillas que facilitan la comunicación del riesgo a todas las funciones de IT para acelerar la respuesta.

Consiga información más rápidamente. La visibilidad de dispositivos inmediata y los paneles de cumplimiento le permiten:

- Identificar la función, el sistema operativo, el proveedor y el modelo de todos los dispositivos conectados.
- Definir un umbral de cumplimiento y controlar que se cumplan todas las directivas activas.
- Identificar los dispositivos de alto riesgo, como:
  - Dispositivos IoT con credenciales débiles, puertos abiertos u otros errores de configuración.
  - Dispositivos Windows a los que les faltan actualizaciones de seguridad o que tienen vulnerabilidades.
  - Dispositivos con agentes de seguridad dañados o aplicaciones no autorizadas.
  - Dispositivos de OT con vulnerabilidades y riesgos comunes críticos (CVE).
- Identificar las infracciones de directivas, incluidos los errores más frecuentes, así como los dispositivos que no cumplen varias directivas (por ejemplo, ejecutan aplicaciones P2P sin firewall ni antivirus).

Resuelva las brechas de forma proactiva. Utilice la nueva vista de activos basada en la web para:

- Buscar rápidamente el inventario de dispositivos en entornos de campus, centros de datos, la nube y OT.
- Filtrar rápidamente por directiva, segmento de red y cualquier propiedad del dispositivo.
- Identificar la ubicación de los dispositivos para reducir el tiempo medio de respuesta.

Ecosistema de apps de eyeExtend Connect

Los clientes aprovechan la plataforma Forescout para integrar sus otras tecnologías de IT y de ciberseguridad, y compartir el contexto de los dispositivos, organizar los flujos de trabajo y automatizar la respuesta. La cartera actual de módulos de eyeExtend de Forescout ofrece integraciones inmediatas con más de 25 productos líderes y le permite aumentar el valor de sus inversiones existentes. Además de estas opciones integradas y admitidas de Forescout, Forescout 8.2 ofrece un nuevo ecosistema de aplicaciones comunitarias para permitir las integraciones con otras tecnologías.

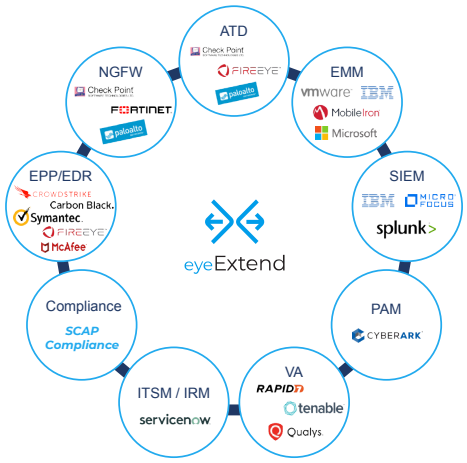
eyeExtend Connect aprovecha el poder de la colaboración y permite tanto a clientes como a partners desarrollar, consumir y compartir rápidamente apps para la conexión con la plataforma Forescout. Puede compartir fácilmente el contexto de los dispositivos con otras herramientas, automatizar flujos de trabajo y actuar para acelerar la respuesta de todos los sistemas con el fin de reducir el tiempo medio de respuesta.

Fácil de desarrollar. Disfrute de flexibilidad para crear sus propias apps mediante scripts universales Python y el estándar de intercambio de datos JSON para conseguir una rentabilidad más rápida.

Fácil de consumir. Seleccione entre una amplia variedad de apps de la comunidad, fáciles de desplegar y personalizar, y que además se pueden portar entre entornos de red.

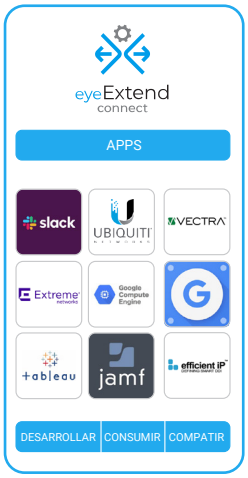
Fácil de compartir. Contribuya y aprenda de las mejores prácticas de la comunidad, comparta apps con sus compañeros y aproveche la colaboración para aumentar el valor de sus inversiones en IT.

Módulos de eyeExtend



Desarrolladas por Forescout

Apps de eyeExtend



NUEVO

Desarrolladas por la comunidad

Segmentación macro en toda la empresa

Forescout 8.2 complementa eyeSegment con las últimas innovaciones de eyeSight y eyeControl para la segmentación en toda la empresa en varios dominios de red y puntos de implementación diversos. Gracias a esta experiencia, puede diseñar e implementar con confianza la segmentación de la red y seguridad Zero Trust a gran escala.

- Asigne y visualice los flujos de tráfico entre una taxonomía lógica de usuarios, dispositivos, aplicaciones y dispositivos.
- Diseñe, simule y perfeccione las directivas de segmentación lógica para conocer el impacto antes de la aplicación.
- Supervise el estado de la segmentación en tiempo real y responda a las violaciones de directivas.
- Aplique controles de segmentación con confianza entre dominios de red y puntos de implementación diversos.

Gestión de riesgos y de la seguridad en entornos de OT

Aproveche la integración entre SilentDefense y Forescout 8.2 para cubrir una amplia variedad de casos de uso de gestión de riesgos y de la seguridad en entornos de OT y convergentes.

- Comparta la clasificación de dispositivos de OT y las vulnerabilidades de SilentDefense con eyeSight y utilice la nueva interfaz de usuario de eyeSight para disponer de una visibilidad unificada en las redes de IT y OT.
- Despliegue sensores de IT y OT integrados en el mismo appliance, para descubrir y clasificar dispositivos en entornos convergentes.
- Identifique los dispositivos de forma exclusiva y aplique las directivas en entornos de red clonadas que reutilizan los intervalos de direcciones IP en varios sitios, líneas de producción o plantas.
- Utilice las últimas funciones de SilentDefense en entornos de OT, incluida la notificación de cumplimiento de NERC CIP mejorada, la inspección selectiva y activa no intrusiva para una mayor visibilidad y un marco de riesgos de activos que agrega varios factores de riesgo a las calificaciones basadas en el impacto.

Control de acceso a la red en entornos de Arista

Forescout 8.2 incluye integración directa con la infraestructura de Arista para implementar los controles de acceso a la red en Arista, así como a entornos heterogéneos. Esto le permite identificar y regular tanto dispositivos de IT como IoT, sin necesidad de agente ni dependencia de 802.1X.

- Identifique y evalúe todos los dispositivos IoT e IT en tiempo real cuando se conecten a la red.
- Proporcione el acceso de red adecuado basado en eyeSight y contexto de terceros, incluido el tipo de dispositivo, el propietario, función del usuario, y estado de cumplimiento y seguridad del dispositivo.
- Mitigue riesgos mediante la automatización de una amplia variedad de respuestas de red en función de la situación, como la restricción, segmentación, puesta en cuarentena o bloqueo de dispositivos.

Despliegues de nube pública

Las empresas que adoptan un enfoque que prioriza la nube frente a la tecnología se han limitado a despliegues físicos in situ o virtuales en lo que relativo a la visibilidad y control de dispositivos. Con Forescout 8.2, puede desplegar los appliances sensor y la administración empresarial de Forescout a sus entornos de nube de Amazon Web Services o Microsoft Azure sin presencia in situ. También puede conseguir la flexibilidad para mezclar despliegues de nube pública con appliances físicos y virtuales en la infraestructura de nube privada de VMware, Hyper-V o KVM.

Físico | Virtual | Nube pública | Híbrido
Combinación de alguno o de todos

Escala empresarial

Forescout 8.2 proporciona escalabilidad inigualable para satisfacer los estrictos requisitos de las grandes empresas y mantener el ritmo del explosivo rendimiento de dispositivos conectados en el campus, centros de datos, nube y entornos IoT y OT.

- Clasifique los dispositivos utilizando la mayor base de conocimientos de dispositivos, con más de 11 millones de dispositivos empresariales, para una identificación más rápida y precisa de los activos IoT, OT e IT conectados.
- Administre dos millones de dispositivos en un solo despliegue, con independencia de que se trate de implementaciones físicas, virtuales, de nube o híbridas.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Drive
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