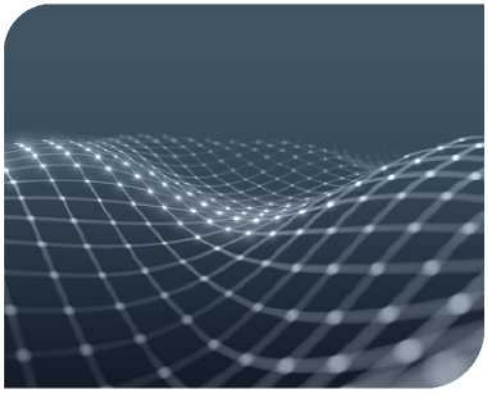

Plataforma Forescout Continuum

Alinee su realidad digital con su marco de seguridad

La transformación digital provoca un crecimiento explosivo de los activos de TI, IoT, IoMT y TO/ICS que se conectan a las redes organizativas. Innovaciones como el acceso remoto, operaciones distribuidas y fuerzas laborales móviles han mejorado la eficiencia, pero al mismo tiempo han ampliado la superficie del ciberataque. Esta es su realidad digital: la suma de todo lo que está conectado a su red, desde el campus hasta la nube y desde el centro de datos hasta el perímetro.

Cada organización también cuenta con su propio marco de seguridad, que es una combinación de las mejores prácticas de la industria, mandatos de la junta directiva y requisitos regulatorios, junto con las políticas de seguridad y prácticas de gestión de riesgos de la organización. El objetivo es que su realidad digital se alinee con su marco de seguridad.

Por desgracia, los cambios constantes desajustan su realidad digital de ese marco. Incluyen cambios cotidianos como el deterioro de dispositivos, fallos de software y la rotación de personal, así como eventos importantes como fusiones y adquisiciones corporativas, que pueden introducir cambios masivos de una sola vez.

Estos cambios amplían constantemente la brecha en la postura de riesgo de seguridad, lo que se traduce en riesgo empresarial: su próxima disrupción, fallo de auditoría, preocupación por la seguridad operativa o disrupción de la producción. Mientras tanto, la reserva de talentos en seguridad está disminuyendo y los equipos de TI están más desbordados que nunca.

No puede esperar para eliminar el riesgo. Pero es absolutamente posible gestionarlo con una plataforma que aborde automática y continuamente este vacío y le mantenga alineado.

Forescout Continuum

"Forescout es un **multiplicador de fuerzas. La visibilidad** y la capacidad de **automatización** que proporciona al departamento de seguridad son **invaluables**"

- CISO, importante centro médico de Florida

Cada entorno es diferente, pero los pasos para alinear su realidad digital con su marco de seguridad siguen el mismo continuo:

Gestión de activos de ciberseguridad: ¿Qué se conecta a su ecosistema y dónde se encuentra, física y lógicamente? La visibilidad es la base: no se puede proteger lo que no se ve.

Cumplimiento de activos: ¿Se puede instalar un agente en el activo? En caso afirmativo, ¿los agentes correctos están instalados y configurados correctamente? ¿Quién está conectado? ¿Se están ejecutando aplicaciones no autorizadas? Debe estar seguro de que los activos están en el estado deseado.

Cumplimiento de riesgos: ¿Es crítico este activo para la empresa? ¿Es vulnerable? ¿Funciona como se espera? No se puede corregir lo que no se conoce.

Segmentación de la red: ¿Cuáles son los hábitos de comunicación del activo? ¿Con qué otros tipos de activos se comunica, a través de qué puertos y protocolos? Las políticas de segmentación conscientes del contexto pueden reducir la superficie de ataque sin interrumpir el flujo de comunicación deseado.

Control de acceso a la red: ¿Hay que limitar o bloquear la comunicación? Los controles proactivos pueden autorizar el acceso y asignar usuarios y dispositivos a segmentos de red o poner en cuarentena dispositivos en función de su postura de seguridad.

Organización de la seguridad: ¿Qué información podemos obtener sobre el activo a partir de otras soluciones de ciberseguridad? ¿Está el activo correctamente parcheado? ¿Hay malware? No puede tomar decisiones sensatas sin toda la información disponible.

Automatización del flujo de trabajo: ¿Cuál es la acción o cadena de acciones correcta? Quiere utilizar conocimientos colectivos entre productos de seguridad para impulsar las acciones de corrección mediante la generación automática de tickets, la gestión automática de ciberactivos, la remedición automática, entre otras.

Estos pasos son sencillos en teoría, pero no en la práctica. La mayoría de los equipos informáticos no pueden evaluar todos los dispositivos en tiempo real y confirmar que cada uno cumple la normativa. Ha invertido potencialmente en docenas de herramientas de seguridad para gestionar su red, pero eso significa que la información está fragmentada y carece de una única fuente de verdad. Las instantáneas desfasadas y puntuales no pueden ser confiables. Aunque pudiera identificar los dispositivos que no cumplen la normativa, tiene una capacidad limitada para aplicar controles de políticas e imponer políticas de cumplimiento continuo en una mezcla de tecnologías de infraestructura de red y seguridad.

Necesita una plataforma única que automatice cada paso del proceso continuo de ciberseguridad. Necesita un multiplicador de fuerza.

Descubra - Evalúe - Controle

La Plataforma Forescout Continuum alinea automáticamente su realidad digital con su marco de seguridad al automatizar el descubrimiento, evaluación y control de todos los ciberactivos en su entorno.

Descubra y realice un inventario continuo de todos los ciberactivos de su red.

La gestión completa de activos de ciberseguridad requiere el descubrimiento continuo y la clasificación de cada dispositivo en todo su entorno de TI, IoT, TO e IoMT. Además de saber cuántos activos se conectan, tiene que saber cuáles son, cómo se conectan (por cable o inalámbricamente), dónde se encuentran físicamente (edificio, armario, puerto de conmutación) y lógicamente (VLAN, dirección IP), y cuál es su propósito.

Forescout es el único proveedor que ofrece un descubrimiento continuo de todos los ciberactivos mediante más de 30 técnicas activas y pasivas, incluida la inspección profunda de paquetes pasiva de activos TO/ICS e IoMT sensibles. Forescout Continuum también utiliza integraciones inalámbricas de conmutadores y VPN listas para usar para descubrir todos los activos, se estén comunicando o no, en todas las ubicaciones y redes.

Los datos recopilados mediante estas técnicas se comparan con los datos de más de 15 millones de dispositivos en la Nube de Dispositivos de Forescout. Además, la clasificación de activos se enriquece con contexto e información automatizados provenientes de Vedere Labs de Forescout, para suministrar las clasificaciones más precisas basadas en más de 150 atributos.

Información práctica de la mayor base de datos de dispositivos en la nube del mundo

La Nube de Dispositivos de Forescout se mejora con aprendizaje automático avanzado para ofrecer perspectivas procesables y conocimiento en tiempo real de los millones de activos bajo gestión de Forescout. Vedere Labs, el equipo de inteligencia de amenazas e investigación de Forescout, también aprovecha la Nube de Dispositivos para obtener inteligencia avanzada y alertar a los clientes y a la comunidad de seguridad en general sobre riesgos emergentes.

Características

Descubrimiento del 100% de activos: Inventario de todos los ciberactivos conectados con un enfoque rentable y de bajo impacto, sin agentes ni disrupciones.

Clasificación precisa: Información contextual recopilada a partir de más de 150 atributos para crear políticas de control con confianza.

Única fuente de verdad: Sincronización continua con su CMDB para mejorar su valor.

Acabe con el ruido mediante una corrección autopriorizada

Forescout Continuum incluye un servicio de evaluación de riesgos multifactor basado en la nube que muestra una lista contextualizada de amenazas priorizadas en función de su impacto probable. El servicio analiza el riesgo de cada activo de la red a través de indicadores como vulnerabilidades, superficies expuestas, puertos abiertos, nivel de Purdue, etc., y calcula una única evaluación agregada para cada uno. En lugar de buscar entre 10 000 alertas, ve las 10 alertas que necesitan atención ahora. Al correlacionar las evaluaciones de riesgo con los flujos de tráfico entre dispositivos, Forescout Continuum también evalúa el radio de explosión de los activos críticos.

Evalúe continuamente el cumplimiento y la higiene de riesgos de ciberactivos.

Dada la amplia gama de tipos de activos en cada organización, evaluar el cumplimiento requiere diversas técnicas de descubrimiento pasivo y exploración activa o integración. Los equipos de seguridad suelen depender de docenas de productos de evaluación de riesgos para adaptarse a cada necesidad. Pero, ¿quién vigila a los vigilantes?

Forescout Continuum es la única plataforma que identifica y mitiga continuamente el riesgo en todos los ciberactivos de su terreno digital. La plataforma mejora su inversión en herramientas de seguridad al ayudar a garantizar que estén implementadas, configuradas y funcionando correctamente, y al organizar la comunicación entre ellas.

Con el cumplimiento de los activos de ciberseguridad, no basta con garantizar que sus sistemas y procesos funcionan de acuerdo con los marcos y normativas de seguridad. Sigue estando sujeto a auditorías fallidas y sanciones a menos que pueda demostrar el cumplimiento. Con la evaluación automatizada de dispositivos y la aplicación de políticas, satisfacer los requisitos de auditoría e informes es un subproducto de las operaciones de seguridad de cumplimiento continuo.

Características

Corrección proactiva: Validación en conexión y sin agentes del estado de los ciberactivos frente a los marcos de seguridad para garantizar que las inversiones en seguridad están desplegadas y en funcionamiento

Identificación y priorización de riesgos: Análisis y mitigación de riesgos multifacéticos y en tiempo real para todos los ciberactivos conectados, basándose en las tendencias de los activos y las fuentes de amenazas

Agrupación de activos y mapeo de flujos de tráfico: Agrupación dinámica de ciberactivos por tipo y función para mapear los flujos de tráfico y la comunicación cruzada entre grupos

Una base sólida para Zero Trust

Zero Trust es un enfoque de diseño de seguridad, no una solución única o tecnología que se pueda adquirir a través de un solo proveedor. Forescout Continuum prepara el terreno para la seguridad de Zero Trust automatizando la aplicación de políticas de acceso con mínimos privilegios basadas en el usuario, el dispositivo, la conexión, la postura y el cumplimiento para todos los ciberactivos, con o sin 802.1X, y sin actualizaciones ni cambios en la infraestructura. Un punto centralizado de gestión y decisión de políticas (PDP) para su arquitectura de Zero Trust en toda la empresa refleja toda la información disponible necesaria para ejecutar las acciones correctas a través de puntos heterogéneos de aplicación de políticas (PEP).

Controle los ciberactivos de forma proactiva para minimizar la superficie de ataque y el impacto de las infracciones de forma continua.

El control requiere una serie de opciones para mitigar o corregir rápidamente y saber qué opción utilizar basándose en toda la inteligencia disponible. Incluyen la corrección automatizada, el control de acceso a la red, la segmentación, las actualizaciones de la CMDB y la organización entre productos. Forescout Continuum automatiza los flujos de trabajo de respuesta para aplicar las políticas de seguridad de forma nativa y a través de otras herramientas de seguridad mediante módulos de integración preconstruidos. Las acciones se basan en información compartida sobre dispositivos, usuarios y contextos para todos los ciberactivos, administrados y no administrados. Toda la información necesaria para crear políticas de aplicación granular está al alcance de su mano.

La disrupción del negocio es la forma más rápida de sabotear su proyecto de seguridad. Forescout Continuum aplica acciones de mitigación flexibles, desde medidas modestas hasta rigurosas, para proteger dispositivos vulnerables, de alto riesgo y comprometidos, al mismo tiempo que mantiene en línea los activos críticos para la misión. La plataforma también le permite simular políticas y supervisar los flujos de tráfico antes de activarlas, para que pueda detectar infracciones que podrían tener consecuencias inesperadas en toda la red y hacer cambios con seguridad.

Características

Corrección proactiva: Las configuraciones erróneas se corrigen en el momento de la evaluación para garantizar el cumplimiento sin necesidad de un análisis exhaustivo.

Respuesta rápida: La aplicación de políticas y acciones de respuesta a incidentes a la velocidad de la máquina para contener las amenazas, minimizar la propagación y mitigar los riesgos.

Flujos de trabajo automatizados: El cumplimiento de los dispositivos se aplica de forma nativa y mediante la organización con otras herramientas de seguridad.

Forescout Continuum se basa en más de 20 años de innovaciones de Forescout que protegen a muchas de las empresas más grandes del mundo y a las organizaciones más confiables en finanzas, gobierno, salud, manufactura y más.

La plataforma:

- Se basa en una solución comprobada ampliamente implementada en miles de empresas y organizaciones gubernamentales, incluyendo el 27% de las G2K, para asegurar los entornos más complejos a gran escala.
- Se integra perfectamente en la infraestructura de red existente mediante una arquitectura flexible que se adapta a las redes periféricas para identificar todos los ciberactivos en entornos heterogéneos de múltiples proveedores.
- Combina las innovaciones existentes de Forescout en seguridad sin agentes ni disrupciones con el nuevo aprendizaje automático, el análisis de riesgos a escala de la nube y la arquitectura administrada de sensores en la nube.

Visite www.forescout.com/platform/ para conocer la Plataforma Forescout Continuum

FORESCOUT

Forescout Technologies, Inc.

Llamada gratuita (EE.UU.) 1-866-377-8771
Tel (Internacional) +1-408-213-3191
Asistencia +1-708-237-6591

Más información en Forescout.com