FORESCOUT
Active Defense for the Enterprise of Things.

Seguridad de IoT

Elija una estrategia Zero Trust flexible para proteger los dispositivos no tradicionales en la Empresa de las cosas

Los dispositivos del Internet de las cosas (IoT) a menudo son invisibles en las redes empresariales. A diferencia de los sistemas tradicionales, no son fáciles de localizar y rara vez admiten agentes de software. Estos dispositivos amplían la superficie de ataque y aumentan sobremanera el riesgo para las empresas, ya que pueden ser comprometidos y utilizarse como puntos de entrada a las redes vulnerables. Las empresas necesitan una solución de seguridad que pueda identificar, segmentar y garantizar el cumplimiento continuo de las normativas para todos los dispositivos IoT en redes heterogéneas.

Dispositivos IoT: ¿merece la pena correr el riesgo?

Los dispositivos IoT son activos empresariales fundamentales y a menudo de gran valor. Impulsan la productividad, mejoran la calidad de los productos y servicios, y permiten incrementar los ingresos. El 63 % de las empresas esperan conseguir en tres años la rentabilidad financiera de sus proyectos de IoT[2]. Hay ciberdelincuentes sofisticados y con una buena financiación que buscan continuamente en las empresas áreas de vulnerabilidad, como las lagunas de visibilidad de IoT y seguridad, que provocan tiempo de inactividad, riesgo para los datos, pérdida de propiedad intelectual y daños a la reputación. Tenga en cuenta lo siguiente:

- Casi 9 de cada 10 participantes en una encuesta reciente del Ponemon Instituye esperan que su empresa sufra un ciberataque o una fuga de datos a través de dispositivos IoT o aplicaciones no protegidos, en los dos próximos años[3].
- Para 2023, cada CIO, de media, será responsable de más del triple de endpoints que gestionaba en 2018[4].

DEFINICIÓN DE ZERO TRUST

El modelo de seguridad de la información de confianza cero, o Zero Trust, de Forrester es una estrategia conceptual y arquitectónica de la seguridad para empresas. Básicamente, el enfoque Zero Trust trata de generar confianza, ofreciendo la seguridad de tener un usuario fiable en un dispositivo fiable y con acceso en el que puede confiar. El acceso se limita exclusivamente a los activos que cada usuario necesita para hacer su trabajo. Según Forrester[1], para implementar políticas Zero Trust eficaces, es preciso:

- Rediseñar las redes y convertirlas en microperímetros seguros
- Fortalecer la seguridad de los datos mediante técnicas de ofuscación
- Limitar los riesgos asociados al exceso de privilegios y de acceso de los usuarios
- Mejorar drásticamente la detección y respuesta de seguridad con análisis y automatización

forescout.com/platform/IoT info-espana@forescout.com Tel (Intl) +1-408-213-3191

En la actualidad, en lo que se conoce como la Empresa de las cosas (EoT) se conectan e interaccionan innumerables dispositivos de IT, IoT y OT (tecnología operativa), por lo que las empresas necesitan una solución de seguridad que facilite la visibilidad y el control de los dispositivos IoT, y de todos los dispositivos conectados mediante IP, con un enfoque Zero Trust de conexión en red. De lo contrario, cualquier dispositivo puede ser atacado y explotado con fines maliciosos.

La estrategia Zero Trust de Forescout

Forescout considera que la seguridad del IoT debe basarse en una estrategia Zero Trust que combine visibilidad total de los dispositivos, segmentación preventiva de la red y un control del acceso basado en un mínimo de privilegios, para todos los activos digitales: dispositivos, usuarios, aplicaciones y cargas de trabajo. La plataforma Forescout le permite gestionar de forma eficaz los riesgos de ciberseguridad, operativos y de cumplimiento de normativas en todo su entorno EoT, gracias a que:

- Proporciona visibilidad total de los dispositivos IoT, IoMT (IoT de la salud) y OT no gestionados, así como de todos los sistemas conectados mediante IP.
- Evalúa e identifica los dispositivos IoT con credenciales de fábrica o débiles, y automatiza las medidas basadas en directivas para implementar contraseñas fuertes.
- Facilita información en tiempo real de las comunicaciones y los comportamientos de riesgo de los dispositivos IoT en todo el entorno ampliado.
- Segmenta los dispositivos en zonas seguras mediante la aplicación de un mínimo de privilegios de acceso, según la política Zero Trust.
- Automatiza la coordinación de directivas Zero Trust en entornos multiproveedor y varios dominios de red.
- Acaba con los silos de administración de la seguridad para acelerar la respuesta y maximizar el valor de sus inversiones en otras soluciones de seguridad.
- Ayuda a las organizaciones de prestación de servicios sanitarios a detectar y reducir de manera proactiva las vulnerabilidades/amenazas, aplicar la segmentación y las reglas de acceso a la red de manera granular y contener de forma inmediata las amenazas contra dispositivos médicos al tiempo que facilita la corrección mediante la integración con Medigate.

“Forescout es el proveedor de seguridad Zero Trust para dispositivos IoT/OT. La seguridad de los dispositivos IoT/OT es uno de los problemas más complicados en las empresas. Y es precisamente un punto fuerte de Forescout. Las funciones de la plataforma para la seguridad de IoT/OT destacan frente a la competencia”.

THE FORRESTER WAVE: ZERO TRUST EXTENDED ECOSYSTEM PLATFORM PROVIDERS, FORRESTER RESEARCH, OCTUBRE DE 2019

Figura 1: Forescout protege activamente todos los dispositivos de su Empresa de las cosas al identificar, segmentar y garantizar el cumplimiento de las normativas de todas las herramientas conectadas

Descubra y clasifique el 100 % de los dispositivos conectados mediante IP

Es fundamental conseguir visibilidad completa y datos del contexto de todos los endpoints IoT, OT y de infraestructura crítica de todo el entorno heterogéneo. La plataforma Forescout:

- Detecta continuamente todos los dispositivos conectados mediante IP, tanto físicos como virtuales, en el instante en el que se conectan a su red, sin necesidad de agentes de software.
- Ofrece una visibilidad profunda de todos los dispositivos utilizando una combinación de más de 20 técnicas activas y pasivas de detección, identificación de perfiles y clasificación.
- Aprovecha Forescout Device Cloud, el mayor lago de datos del mundo con inteligencia sobre dispositivos obtenida de manera colaborativa, que proporciona una única fuente de verdad intersectorial sobre huellas digitales, comportamientos y perfiles de riesgo de más de 12 millones de dispositivos.

Implemente segmentación dinámica de la red y automatice los controles

En los entornos de EoT heterogéneos actuales, una empresa que adopta el modelo Zero Trust debe ser capaz de realizar la segmentación de la red y organizar la respuesta ante incidentes en todos los dominios EoT. Con Forescout, puede:

- Correlacionar el acceso con las identidades de los usuarios (quién hace qué, dónde, cuándo y por qué).
- Aprovisionar dispositivos en segmentos de red dinámicos, en función de directivas y contexto en tiempo real.
- Definir los flujos de datos para diseñar directivas de segmentación y simularlas para realizar un despliegue sin complicaciones.
- Automatizar la segmentación para reducir el riesgo operativo y de ciberamenazas.

Organice la seguridad y el cumplimiento de normativas

La mayoría de las organizaciones están inundadas de soluciones de seguridad caras y que solo sirven para un fin, que son incapaces de compartir el conocimiento o coordinar la respuesta a incidentes. Forescout ofrece la solución para esta situación ineficaz. Los productos Forescout eyeExtend comparten contexto de dispositivos entre la plataforma Forescout y otros productos de seguridad e IT para la automatización de los flujos de trabajo y la aplicación de directivas en soluciones heterogéneas. Estas funciones de organización pueden ayudarle a:

- Aumentar la seguridad de IoT y el nivel de cumplimiento de normativas de los dispositivos en general.
- Reducir el tiempo medio de detección y respuesta.
- Aumentar la rentabilidad de las herramientas existentes.
- Automatizar el proceso de actualización de su base de datos de administración de configuraciones (CMDB), eliminando el inventario manual, laborioso y propenso a errores.

"Ahora sabemos lo que hay conectado a nuestra red, incluidos los dispositivos IoT, como impresoras, teléfonos VoIP y cámaras de seguridad. Forescout clasifica el dispositivo y lo sitúa en el segmento de VLAN adecuado".

– KEN COMPRES, INGENIERO SÉNIOR DE SEGURIDAD DE REDES E INTEGRACIÓN/CSO, HILLSBOROUGH COMMUNITY COLLEGE COLLEGE

1 Five Steps to a Zero Trust Network, (Informe Cinco pasos para una red Zero Trust), Forrester Research, octubre de 2018

2 A New Roadmap for Third Party IoT Risk Management (Una nueva hoja de ruta para la gestión de riesgos de IoT de terceros), estudio de referencia, Ponemon Institute, Sabine Zimmer, 3 de junio de 2020

3 Internet of Things: Unlocking True Business Potential (Internet de las cosas: cómo aprovechar todo el potencial de negocio), Gartner

4 Gartner Top Strategic IoT Trends and Technologies Through 2023 (Principales tendencias y tecnologías de IoT hasta 2023), septiembre de 2018

No se conforme con verlo. Protéjalo.

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

forescout.com/platform/IoT info-espana@forescout.com Tel (Intl) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things.

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

info-espana@forescout.com
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Más información en forescouttechnologies.es