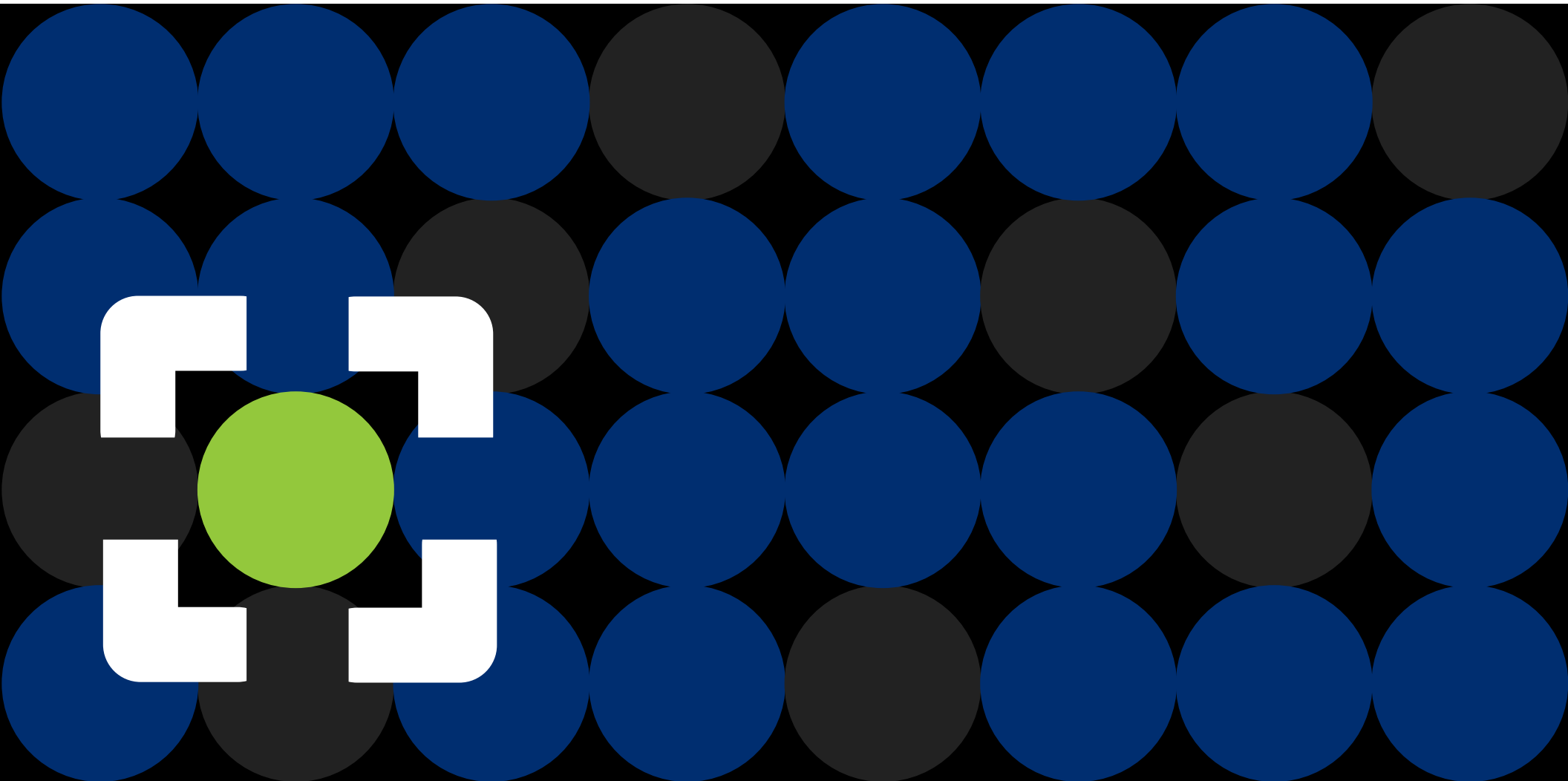
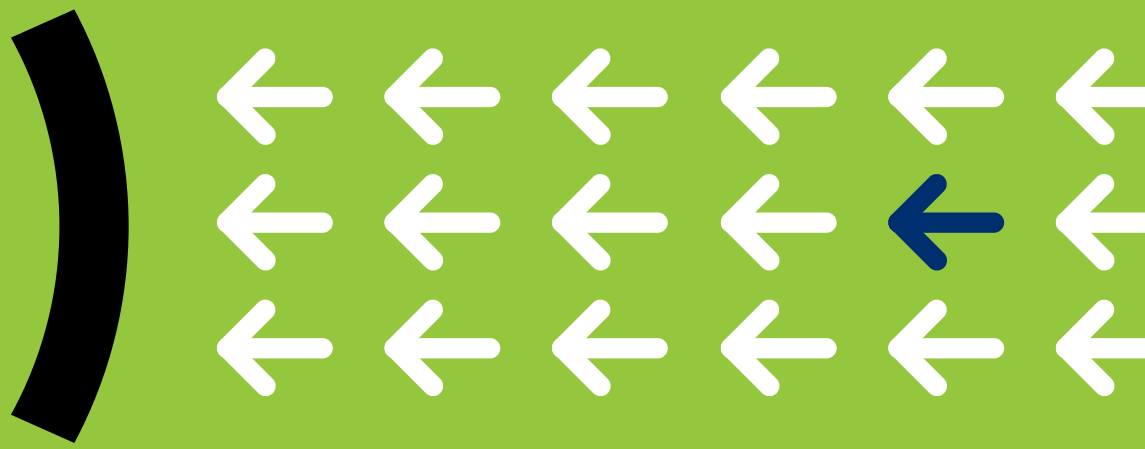
FORESCOUT
Active Defense for the Enterprise of Things™

Cómo proteger el Enterprise of Things
Cinco retos de la seguridad



ÍNDICE



INTRODUCCIÓN

Los dispositivos de las empresas actuales representan un reto de seguridad muy importante para cualquier organización. Tanto en términos de cifras (miles de millones) como en lo referente a tipos (IT, OT, IoT, BYOD), están en plena expansión. Algunos están gestionados y son conocidos, pero otros son desconocidos y pasan desapercibidos. Los usuarios de estos dispositivos están literalmente distribuidos por todo el mundo. Todos (empleados, proveedores, contratistas, partners y clientes) pueden conectarse a datacenters o a la nube desde cualquier lugar, tanto si es seguro como si no lo es, y esto añade complejidad a los entornos de red.

Todo esto *complica* los entornos de red: una verdadera empresa de las cosas o **Enterprise of Things (EoT)** necesita una planificación detallada, junto con medidas que se lleven a cabo de forma automática para proteger los dispositivos y a la propia empresa.

A continuación se incluyen los cinco retos de EoT principales para los CISO actuales y otros jefes de operaciones, y se ofrecen recomendaciones prácticas para superar estos retos.

RETO 1

¿Cómo inventariar y gestionar el incremento de dispositivos no gestionados?

> **Según los expertos, solo durante 2020, se han instalado 31 000 mil lones de dispositivos IoT en todo el mundo.**
>
> ***SECURITY TODAY, 13 DE ENERO, 2020[1]***
>
> **“Según el 62 % de los encuestados, la capacidad de su empresa para conseguir un estado de la seguridad más maduro dependerá cada vez más de la convergencia entre los sistemas de IT y OT”.**
>
> **PONEMON INSTITUTE, FEBRERO DE 2019[2]**

El número de dispositivos gestionados con agentes de seguridad incorporados, como los PC, portátiles y smartphones de las empresas disminuye cuando se compara con los miles de millones de dispositivos IoT y OT sin agente que se conectan a las redes. Al mismo tiempo, se está produciendo una convergencia entre las redes de IT y OT, lo que incrementa la productividad y facilita el trabajo de administración de la red, si bien es cierto que, al mismo tiempo, añade riesgos. Conocer verdaderamente las superficies de ataque en las redes heterogéneas actuales es más difícil que nunca.

Recomendaciones:

- Determinar qué herramientas ofrecen un 100 % de visibilidad de los dispositivos, sin ángulos muertos.
- Concretar el proceso de selección para incluir únicamente las soluciones que proporcionen evaluación del estado de los dispositivos en tiempo real y sin agentes.
- Proporcionar al personal informático y de operaciones de seguridad opciones de inventario de activos en tiempo real.

RETO 2

En el entorno empresarial actual, ¿dónde reside el riesgo?

> **"Los edificios y dispositivos médicos inteligentes, los equipos de con exión a red y los teléfonos VoIP conforman los grupos de dispositivos IoT de mayor riesgo".**
>
> **FORESCOUT RESEARCH, MAYO 2020[3]**

> **"Las tecnologías de dispositivos IoT y de conexión a redes han intro ducido un riesgo potencial en redes y empresas... Los equipos encargados de la seguridad deben aislar, proteger y controlar cada uno de los dispositivos de las redes, continuamente".**
>
> **FORRESTER RESEARCH, JUNIO 2020[4]**

El concepto del análisis de riesgos está cambiando y se amplía, al igual que la superficie de ataque. Según un reciente análisis del "EoT" realizado por Forescout, el mayor riesgo procede de los dispositivos IoT. "Estos dispositivos no solo son difíciles de supervisar y controlar, sino que, además, generan vulnerabilidades, ya que conectan la capa de lo cibernético con la de lo físico, que hasta ahora estaban separada. Los dispositivos IoT pueden ser puertas de entrada a las redes y objetivos prioritarios del malware especializado[3]".

Recomendaciones:

- Emplear análisis de riesgos de varios factores para conocer su superficie de ataque.
- Adoptar una estrategia de defensa activa que incorpore un modelo Zero Trust (de confianza cero).
- Acelerar la respuesta a las amenazas priorizando las alertas según su nivel de riesgo.
- Y, de nuevo, la visibilidad total de los dispositivos es clave.

RETO 3

El perímetro de la red ha desaparecido. ¿Y ahora qué?

> **“Se deben aplicar nuevas mejores prácticas para proteger los perímet ros de la red de la empresa”.**
>
> **GARTNER, MAYO 2020[5]**

¿Abiertas y, al mismo tiempo, seguras? ¿Cómo es posible, con redes distribuidas en campus, datacenters, la nube y entornos OT? Ahora que las redes corporativas se extienden por todo el mundo hasta dondequiera que se encuentren las cargas de trabajo y los empleados, ya no existe un perímetro alrededor de la organización que pueda protegerse. Hemos llegado a un punto en el que los perímetros deben rodear a cada uno de los dispositivos y cargas de trabajo conectadas. La seguridad empieza por el perímetro de cada activo.

Recomendaciones:

- Limitar el acceso a los activos corporativos mediante un modelo que limite al máximo los privilegios, como el de confianza cero, Zero Trust.
- Descubrir y evaluar continuamente todos los dispositivos que acceden a la red, con independencia de su ubicación.
- Garantizar el cumplimiento estricto de las normativas en todos los activos, ya sean locales, BYOD o remotos.

RETO 4

La segmentación de la red es imprescindible, pero ¿cómo hacerla bien, sin afectar a las operaciones empresariales?

> **"Calculamos que el 90 % de las empresas con las que hemos hablado han incluido proyectos de segmentación en sus planes este año. Todo el mundo está interesado, pero no siempre está claro por dónde comenzar, cuáles son los riesgos o si vale la pena el dinero y el esfuer zo que requieren estos proyectos".**
>
> **FORESCOUT RESEARCH, ENERO DE 2019[6]**

La segmentación de la red tiene mala reputación desde hace años. Hasta hace poco tiempo, las herramientas de segmentación disponibles eran difíciles de desplegar y no admitían varios dominios de red, lo que provocaba interrupciones en la actividad empresarial y creaba un entorno fragmentado. Cuando las organizaciones incorporaron nuevos dispositivos y ampliaron aún más sus redes, los problemas aumentaron. Sin embargo, hoy día existen soluciones de segmentación de gran eficacia. Ya no tiene sentido seguir utilizando redes planas vulnerables.

Recomendaciones:

- Mostrar la segmentación y realizar una simulación de las directivas antes del despliegue, con el fin de evitar interrupciones innecesarias.
- Verificar si su solución principal puede simplificar la segmentación Zero Trust de los dispositivos en cualquier lugar (incluidos los dispositivos IT, IoT y OT).
- Acelerar la implementación Zero Trust en todo el entorno corporativo.
- Elegir una plataforma de NAC moderna que se haya desarrollado con el objetivo de facilitar la segmentación de la red.

RETO 5

¿Cómo afrontar la paradoja “hacer más con menos”?

> **“Las empresas están progresando en la reducción de los grupos frag mentados de herramientas de administración de la red. Sin embargo, el 64 % aún utilizan de 4 a 10 herramientas para supervisar las redes y resolver sus problemas”.**
>
> **NETWORK MANAGEMENT MEGATRENDS 2020, ABRIL DE 2020[7]**

> **“El interés en la seguridad y la gestión de riesgos alcanza cotas nunca vistas a nivel de directivos”.**
>
> **GARTNER RESEARCH, JULIO DE 2019[8]**

Es difícil defender que su departamento de operaciones de seguridad es un prodigio de eficiencia y una fuente de ahorro de costes cuando para la administración de la seguridad y la red de su empresa emplea un batiburrillo de herramientas inconexas, cada una de ellas adecuada para un fin concreto. Dicho esto, hasta los planes de transformación mejor trazados pueden sufrir problemas; concretamente, despliegues lentos, rentabilidad de la inversión tardía, curvas de aprendizaje pronunciadas y una satisfacción limitada con las soluciones elegidas. Por suerte, si selecciona la plataforma adecuada puede contentar a todas las partes implicadas, incluido el director financiero.

Recomendaciones:

Elegir una plataforma que permita organizar las herramientas que posee y que cumpla estos criterios:

- Despliegue rápido, flexible y sin interrupciones
- Rápida creación de valor y rentabilidad
- Sin dependencia de proveedores concretos; permite utilizar su infraestructura actual
- Sin necesidad de actualizaciones de software ni hardware
- Integraciones con los principales productos de seguridad e IT
- Descubrimiento de dispositivos y evaluación del estado y de riesgos, sin agentes
- Sin las complicaciones, los retrasos por el despliegue y los costes asociados a 802.1X
- Ajuste el crecimiento a la escalabilidad de la empresa
- Aumente la productividad de las operaciones de seguridad
- Visibilidad, control y segmentación sin agentes, y Zero Trust

El mayor reto detrás de estos cinco retos

Si bien, cada uno de los retos que se han expuesto pueden ser abrumadores, de no resolverse, podrían conducir al reto por excelencia: un ciberataque que provoque problemas operativos, robo de datos, daños a la reputación de la marca, multas cuantiosas, problemas de seguridad pública... y la lista continúa.

La clave es la prevención, lo que implica que para ser eficaz, una solución debe ofrecer una visibilidad total de los dispositivos sin necesidad del uso de agentes, una supervisión continua y una respuesta automática a las amenazas.

*Notas

1. *The IoT Rundown for 2020: Stats, Risks, and Solutions* (Resumen de IoT para 2020: Estadísticas, riesgos y soluciones), Security Today, 13 de enero de 2020
2. *Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT* (Seguridad, protección y privacidad en un mundo de IT, OT y IIoT interconectado), Informe de investigación del Ponemon Institute, febrero de 2019.
3. *The Enterprise of Things Security Report, The State of IoT Security in 2020* (Informe de seguridad del Enterprise of Things, el estado de la seguridad de IoT en 2020), Forescout Research Labs, mayo de 2020
4. *Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles and Techniques* (Mitigación del ransomware con Zero Trust: fortalezca sus defensas con principios y técnicas Zero Trust), 8 de junio de 2020, Forrester Research
5. *Securing the Enterprise's New Perimeters* (Protección de los nuevos perímetros de la empresa), Gartner, 27 de marzo de 2020
6. *Network Segmentation* (Segmentación de red), Blog de Forescout, enero de 2019
7. *Network Management Megatrends 2020* (Megatendencias de administración de red 2020), Informe de investigación de Enterprise Management Associates, abril de 2020
8. *Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer* (Cinco preguntas que los líderes de la seguridad y los riesgos tienen que estar preparados a responder), Gartner Research, julio de 2019

No se conforme con verlo. Protéjalo.

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

ACERCA DE FORESCOUT

Forescout es el líder en seguridad del Enterprise of Things y ofrece una plataforma holística que identifica, segmenta y aplica el cumplimiento de normativas en todo lo que haya conectado a una red heterogénea. La plataforma Forescout es la solución de categoría empresarial más ampliamente desplegada y más escalable para la visibilidad y el control de dispositivos sin agentes. Se despliega rápidamente en su infraestructura actual, sin necesidad de agentes, actualizaciones de sistemas o autenticación 802.1X. Empresas del Fortune 1000 y organismos oficiales confían en Forescout para reducir el riesgo de interrupciones de la actividad empresarial por incidentes de seguridad o fugas de datos, garantizar y demostrar el cumplimiento de normativas en materia de seguridad y aumentar la productividad de las operaciones de seguridad.

forescout.com/platform/eyeSight

info-espana@forescout.com

Tel. (internacional) +1-408-213-3191

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