vmware

REALIZE WHAT'S POSSIBLE.™

Por qué (solo) perseguir amenazas es una estrategia de seguridad errónea

La situación de la ciberseguridad es cada vez peor

Limitarse a perseguir amenazas es una tarea imposible, además de reactiva

230 000

nuevos casos de programas maliciosos al día.[1]

Los programas maliciosos suelen pasar desapercibidos en entornos donde se aprovechan de las vulnerabilidades

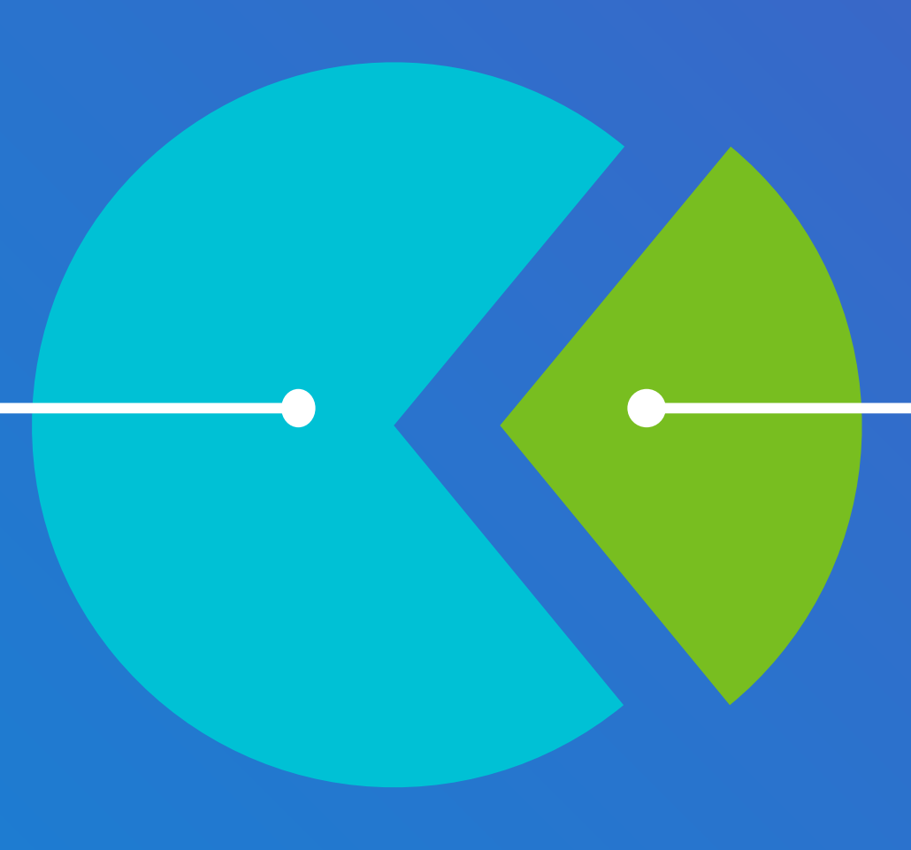
197 DÍAS

es el tiempo medio de identificación de vulneraciones de datos.[2]

Los mecanismos de defensa tradicionales no funcionan porque se concentran demasiado en perseguir amenazas

EL 84 % **de las organizaciones afirma que las soluciones de seguridad tradicionales no funcionan.**[3]

Las inversiones en seguridad se centran excesivamente en perseguir amenazas



EL 72 % **se centra en identificar amenazas y reaccionar ante ellas.**

EL 28 % **se centra en reducir la superficie de ataque.**[4]

11 400 MILLONES $ **se invirtieron en empresas de ciberseguridad en 2017-2018.**[5]

Perseguir amenazas Y reducir la superficie de ataque proporciona una seguridad más eficaz

Perseguir amenazas +

- PREVENCIÓN CONTRA PROGRAMAS MALICIOSOS
- ANÁLISIS DE AMENAZAS
- GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
- SEGURIDAD DE LOS DISPOSITIVOS MÓVILES
- PREVENCIÓN DE VULNERABILIDADES

Reducir la superficie de ataque

- ✓ LISTA BLANCA
- ✓ MICROSEGMENTACIÓN
- ✓ REFUERZO DEL SISTEMA
- ✓ APLICACIÓN DE PARCHES
- ✓ CIBEREDUCACIÓN

Al aplicar el **comportamiento correcto** se reduce la superficie de ataque

Es preciso tener un buen conocimiento de las aplicaciones y SOLO permitir las funciones que deben realizar.

Qué necesita para aplicar una estrategia de **comportamiento correcto**

Conocimiento profundo de las aplicaciones

El reconocimiento de aplicaciones va más allá del puerto y el protocolo. Es preciso que conozca a fondo sus aplicaciones: la topología, los procesos, qué estados son aceptables, quienes las utilizan y desde qué dispositivos, y la forma en que todo esto cambia con el tiempo.

Automatización inteligente

Las aplicaciones y sus políticas cambian con frecuencia. Necesita una automatización inteligente para definir, implementar, cambiar y corregir adecuadamente las políticas basadas en sus aplicaciones dinámicas.

Seguridad intrínseca

Obtener información sobre el estado correcto no es tarea fácil. Obtenerla sin añadir agentes y productos de seguridad cada vez más complejos resulta aún más complicado. Es necesario utilizar un sistema de seguridad que se integre en la infraestructura que ya tiene.

Incline la balanza a favor de los defensores en vez de a los atacantes

VMware convierte la seguridad en un elemento intrínseco al incorporarla en su infraestructura, lo que le proporciona una visibilidad y una protección de las aplicaciones sin precedentes, desde los terminales a la cloud. La información certera es la ventaja que le damos para que pueda aplicar una estrategia de comportamiento correcto.

Más información sobre las soluciones de seguridad de VMware

VMWARE.COM/ES/SECURITY

Síganos:

---

[1] Panda Security: https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/

[2] «2018 Cost of a Data Breach Study», Ponemon Institute, 2018

[3] «2017 Cloud Security Report», Cybersecurity Insiders, 2018

[4] «2018 Cyber Defenders», CB Insights, 2019

[5] «2016 Cyber Defenders», CB Insights, 2017; «2017 Cyber Defenders», CB Insights, 2018