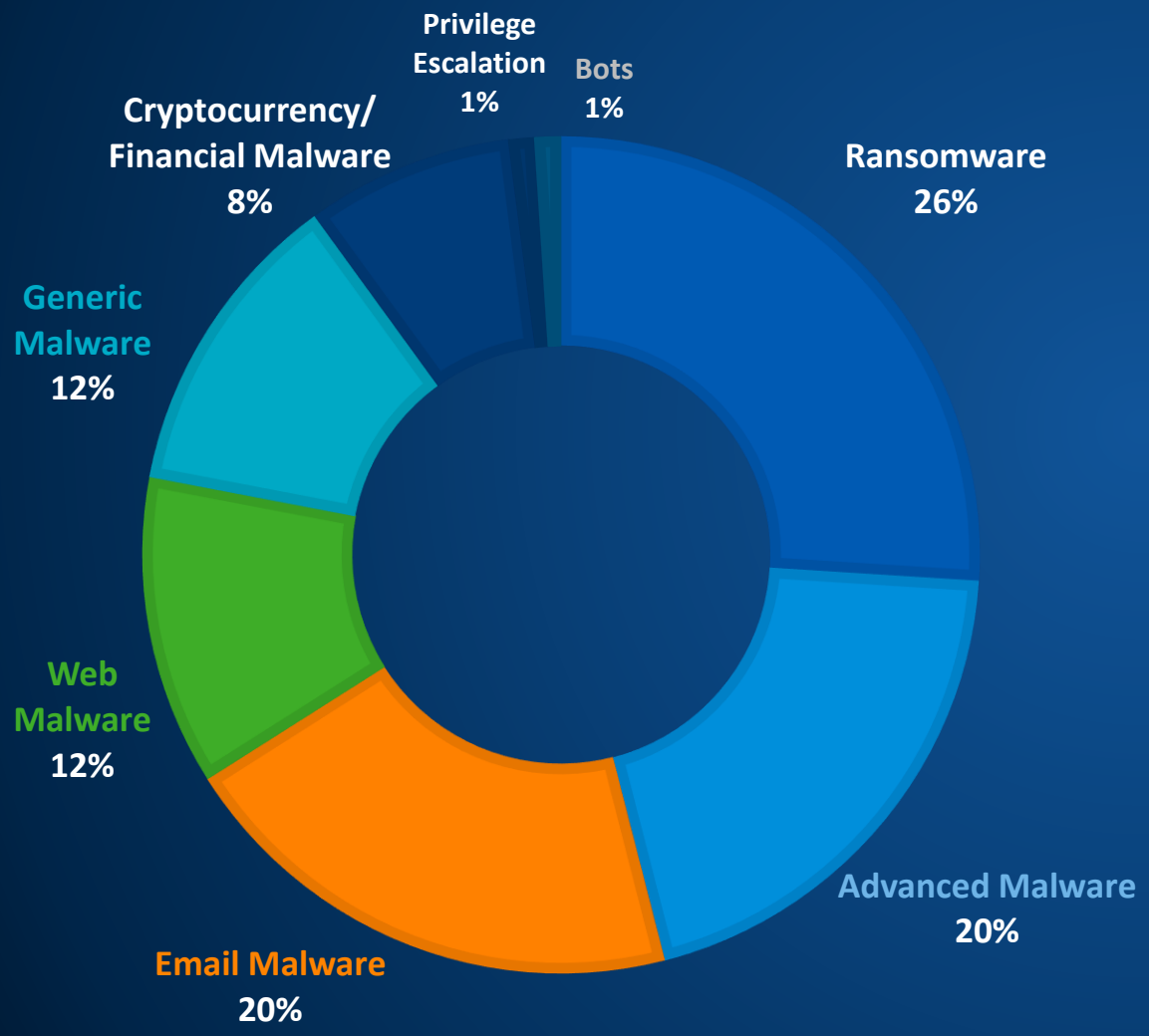
Detenga las amenazas desconocidas con Sophos Intercept X

Distribuidor Platinum Sophos

SOPHOS

El panorama de amenazas ha cambiado



Ransomware

El 54 % de las empresas fueron atacadas dos veces promedio en 2017^

Amenazas avanzadas

El 83 % de las empresas coincide en que cada vez es más difícil detener las amenazas ^

Exploits

La mayoría de empresas no disponen de prevención de exploits^

SOPHOS

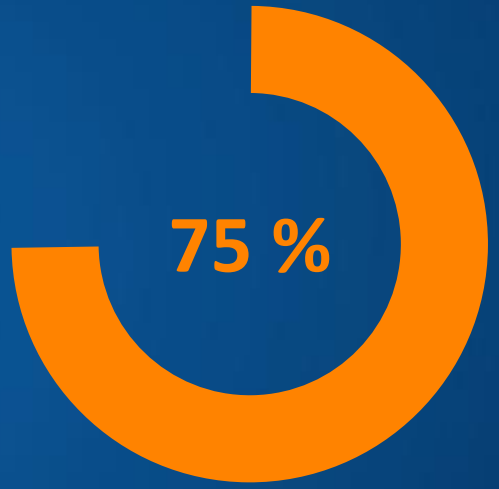
Fuente: SophosLabs

^Fuente: Encuesta sobre el estado actual de la seguridad para endpoints

Las amenazas son desconocidas, lo que dificulta su detección

400 000

Cada día, SophosLabs recibe y procesa 400 000 muestras de malware desconocidas hasta la fecha.



El 75 % de los archivos maliciosos que detecta SophosLabs solo se hallan dentro de una única empresa.

SOPHOS

Fuente: SophosLabs


SOPHOS
INTERCEPT X
SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

La protección para endpoints más completa

PROTÉJASE CONTRA LO DESCONOCIDO

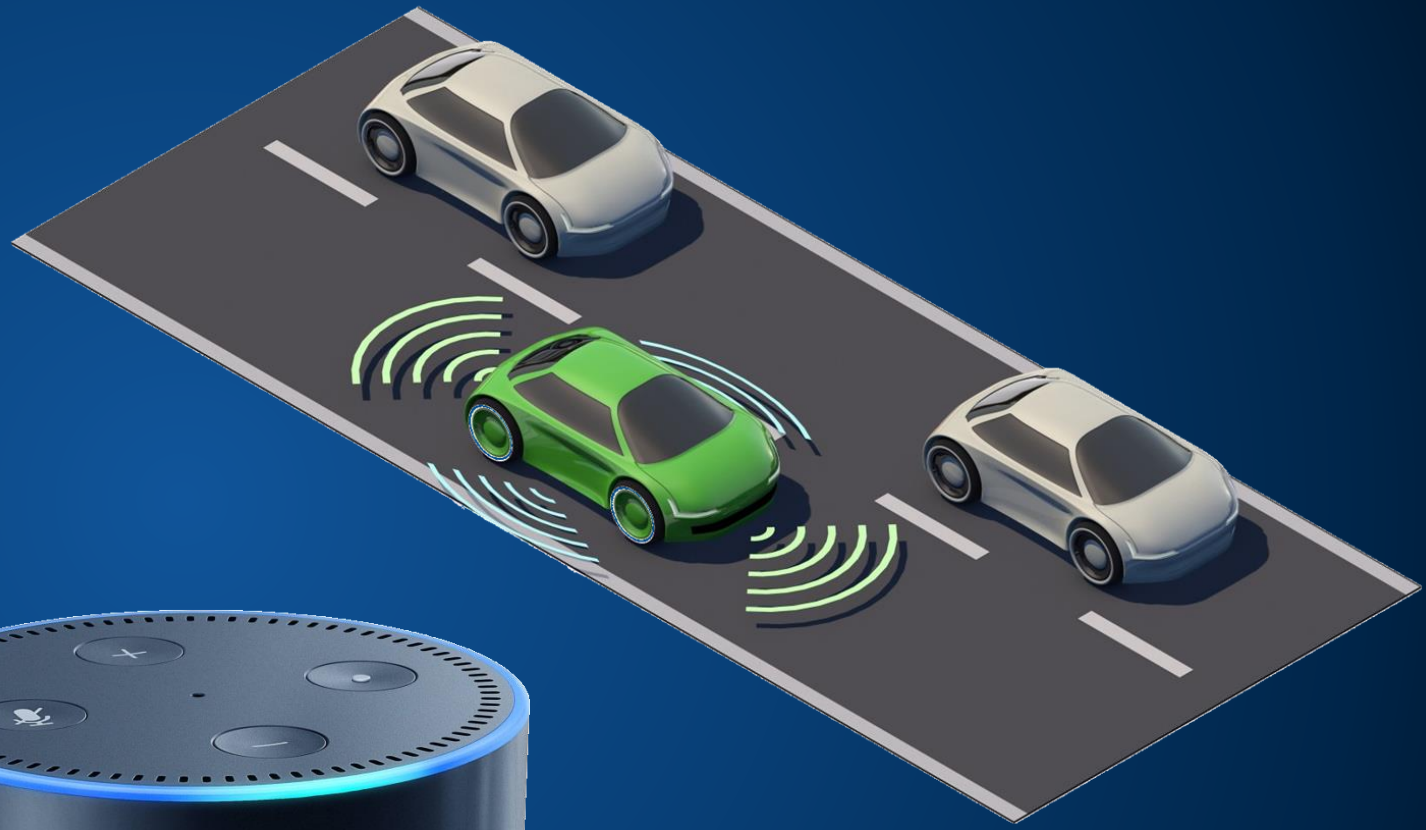
DETENGA EL RANSOMWARE

REPELA AL ATACANTE

Seguridad predictiva

SOPHOS

El Deep Learning nos rodea



Deep Learning aplicado a la ciberseguridad

FRENTE A

BENIGNWARE

MALWARE

Funciones de la detección de malware con Deep Learning de Sophos

- Evita el malware conocido y nunca antes visto
- Bloquea el malware antes de que se ejecute
- No depende de firmas
- Clasifica los archivos como maliciosos, aplicaciones no deseadas o benignas
- Ocupa muy poco espacio (menos de 20 MB) y solo requiere actualizaciones ocasionales
- Detecta malware en aproximadamente 20 milisegundos
- Protege incluso cuando el host está desconectado
- Funciona directamente sin entrenamiento adicional

SOPHOS

El Deep Learning frente a otros tipos de Machine Learning

Modelo más inteligente

Mayor escalabilidad

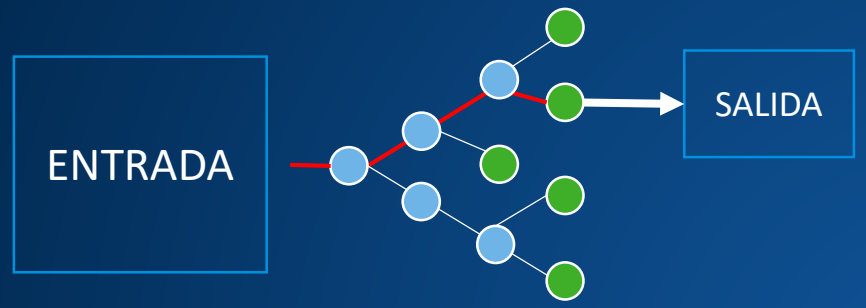
Menor consumo de recursos

"Intercept X utiliza una red neuronal de Deep Learning que funciona como el cerebro humano… El resultado en un elevado índice de precisión tanto para programas maliciosos existentes como de día cero, así como un índice menor de falsos positivos."

- Informe de ESG Lab, diciembre de 2017

Machine Learning frente a Deep Learning

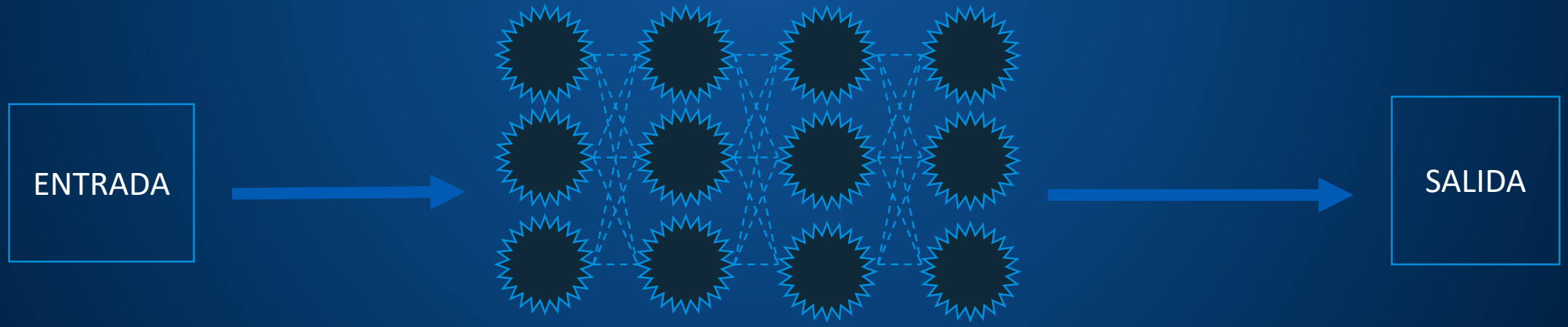
MACHINE LEARNING



Árbol de decisión

Bosque aleatorio

DEEP LEARNING



Capas interconectadas de neuronas;
cada una identifica funciones más complejas

SOPHOS

Ventajas del Deep Learning de Sophos

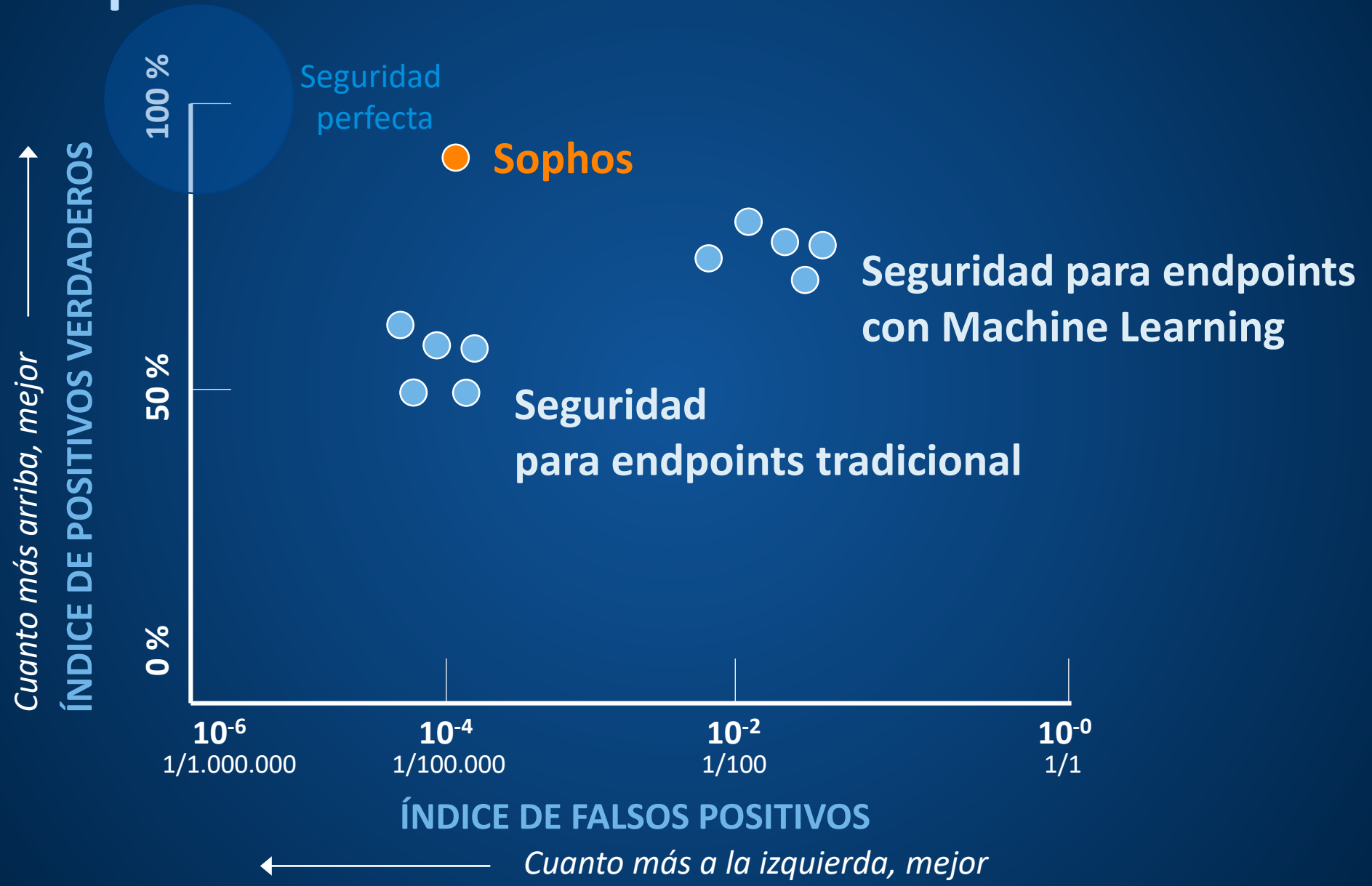
- Probado
  - Tasa de detección de malware nº 1 en la industria
  - Probado en VirusTotal desde agosto de 2016; validado por terceros
- Rendimiento
  - Detiene el malware desconocido sin firmas
  - Detecta y bloquea amenazas en 20 milisegundos
- Experiencia
  - En desarrollo desde 2010
  - Creado por científicos de datos de SophosLabs con tecnología de la DARPA
- SophosLabs: Se entrena con cientos de millones de muestras

> “Una de las ***mejores puntuaciones de rendimiento*** que hemos visto en nuestras pruebas”
>
> *Maik Morgenstern, director tecnológico, AV-TEST*

VIRUS TOTAL NSS LABS AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS

SOPHOS

Seguridad predictiva: detección de malware desconocido



SOPHOS

Resultados de las pruebas: aumento de las detecciones de malware desconocido por parte de Sophos frente a otra seguridad para endpoints

Período de prueba	Tamaño de de la muestra	% aumento de las detecciones frente a la seguridad para endpoints tradicional	% aumento de las detecciones frente a la seguridad para endpoints con Machine Learning
Semana 1	132	171 %	39 %
Semana 2	176	235 %	51 %
Semana 3	251	137 %	18 %
Semana 4	381	159 %	26 %
Semana 5	353	213 %	12 %
Semana 6	14	426 %	60 %
Total	**1307**	**183 %**	**26 %**

Fuente: Análisis de SophosLabs de malware en circulación; porcentaje superior a la media de los enfoques de la competencia

Detenga el ransomware

SOPHOS

Vivimos a la sombra del ransomware

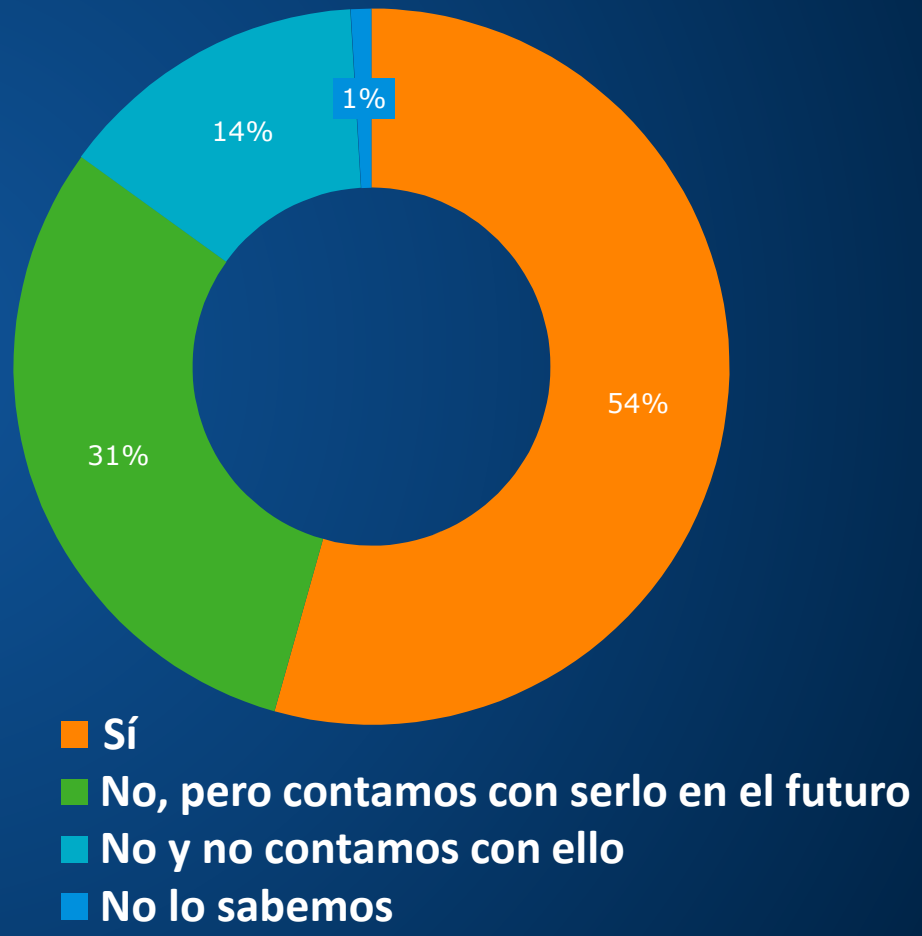
El 54 %

de las empresas sufrió un ataque de ransomware el año pasado

El 85 %

de las empresas se ha visto afectada por el ransomware o espera serlo

¿Se ha visto afectada su empresa por el ransomware?



Fuente: Encuesta sobre el estado actual de la seguridad para endpoints

SOPHOS

Datos básicos del ransomware

2

Promedio de ataques de ransomware entre los afectados^

El 77 %

de las víctimas de ransomware contaba con una protección para endpoints actualizada ^

2500 $

de rescate se pagaron de media*

133 000 $

Coste medio de un ataque de ransomware^ *(USD)*

^Fuente: Encuesta sobre el estado actual de la seguridad para endpoints

*Fuente: Instituto Ponemon

Impacto de NotPetya

+ 310 M $ MERCK

+ 400 M $ FedEx

100 M $ Reckitt Benckiser

300 M $ MAERSK

Protección contra el comportamiento del ransomware

CryptoGuard – Protección de archivos

- Usa la caché de archivos en tiempo de ejecución
- Identifica el comportamiento del cifrado malicioso de archivos
- Aísla los procesos maliciosos
- Revierte automáticamente los cambios en los archivos afectados

WipeGuard – Protección de disco y registro de arranque

- Evita la manipulación maliciosa de áreas de sistema del disco
- Detiene los procesos maliciosos
- Se ha demostrado su eficacia durante el ataque de NotPetya

Ventajas anti-ransomware de Intercept X

Muy eficaz

- Condena basada en el comportamiento
- Detiene el cifrado malicioso
- Detiene el ransomware que ataca archivos, el disco y el sector de arranque
- Preparado para el futuro contra nuevas variantes

Recuperación automatizada

- Revierte los archivos al estado conocido
- Tecnología de instantáneas exclusiva
- Garantiza la productividad y seguridad de los usuarios

Análisis de la cadena de ataque

- Identifica el punto de origen
- Reproducción visual de nivel forense
- Captura todos los archivos que se han tocado

“Desde que lo desplegamos, ha detenido 400 nuevos ataques de ransomware y no hemos sufrido ninguna infección de ransomware.”

- Emily Vandewater, analista de seguridad informática, Flexible Systems

Repela al atacante

SOPHOS

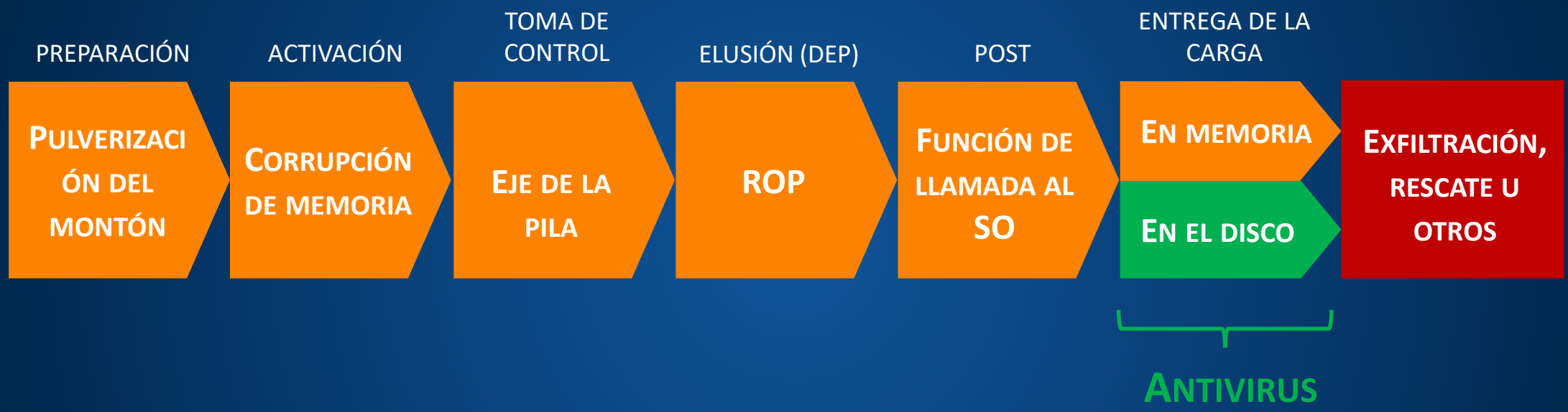
Detener los exploits y ataques sin archivos es fundamental

- Las funciones antiexploits de Intercept X detienen los ataques antes de que descarguen ejecutables maliciosos y los ataques que nunca introducen malware
- Los ejecutables maliciosos solo representan el 41 % del malware que se distribuye a un endpoint^
- Muchas técnicas no se sirven de un archivo para alcanzar el almacenamiento de un equipo
- El 26 % de los ataques basados en malware usaba archivos de Office armados con programas maliciosos

^Basado en las muestras enviadas a VirusTotal (31/12/17 – 6/1/18)

* Informe de investigación sobre filtraciones de datos de Verizon del 2017

La cadena de ataque



- La mayoría de ataques basados en exploits constan de 2 o más técnicas
- Las técnicas de explotación no cambian y son obligatorias para explotar vulnerabilidades de software actuales y futuras
- Detener el exploit es detener el ataque

Técnicas de piratería de Active Adversary

OBJETIVOS

Reconocimiento
Activo y pasivo
Investigación social
Phishing

SONDEO

Sondeo antes del ataque
Barridos de redes
Escaneado de puertos
Prueba de vulnerabilidad

ACCESO

Exploits
Denegación de servicio
Robo de credenciales
Instalador de malware

PERSISTENCIA

Rootkits para mantener una presencia
Inyección de código
Escalado de procesos

BORRADO DE HUELLAS

Tunelización
Movimiento lateral
Purgar registros
Eliminar herramientas

Algunas de las técnicas de explotación y de Active Adversary que detiene Intercept X

Aplicación de la prevención de ejecución de datos	Selección aleatoria del diseño del espacio de direcciones obligatoria	ASLR de abajo a arriba	Desreferencia página NULL	Asignación de pulverización del montón	Pulverización dinámica del montón	Eje de la pila y ejecución de la pila (protección de memoria)
Mitigaciones de ROP basadas en pilas (autor de llamada)	Sobrescritura del controlador de excepciones estructurado (SEHOP)	Filtrado de tabla de direcciones de importación (IAF)	Carga de bibliotecas	Inyección de DLL reflectiva	Código shell malicioso	Modo Dios de VBScript
WOW64	Syscall	Vaciado de procesos	Secuestro de DLL	Omisión de AppLocker Squiblydoo	Protección de APC (Double Pulsar / AtomBombing)	Aumento de privilegios de procesos
	Protección contra robos de credenciales	Mitigación de cuevas de código	Protección contra Man-in-the-Browser (Safe Browsing)	Detección de tráfico malicioso	Detección de shell Meterpreter	

SOPHOS

“Intercept X detuvo el 100 % de las técnicas de explotación que escaparon a la aplicación antivirus tradicional.”

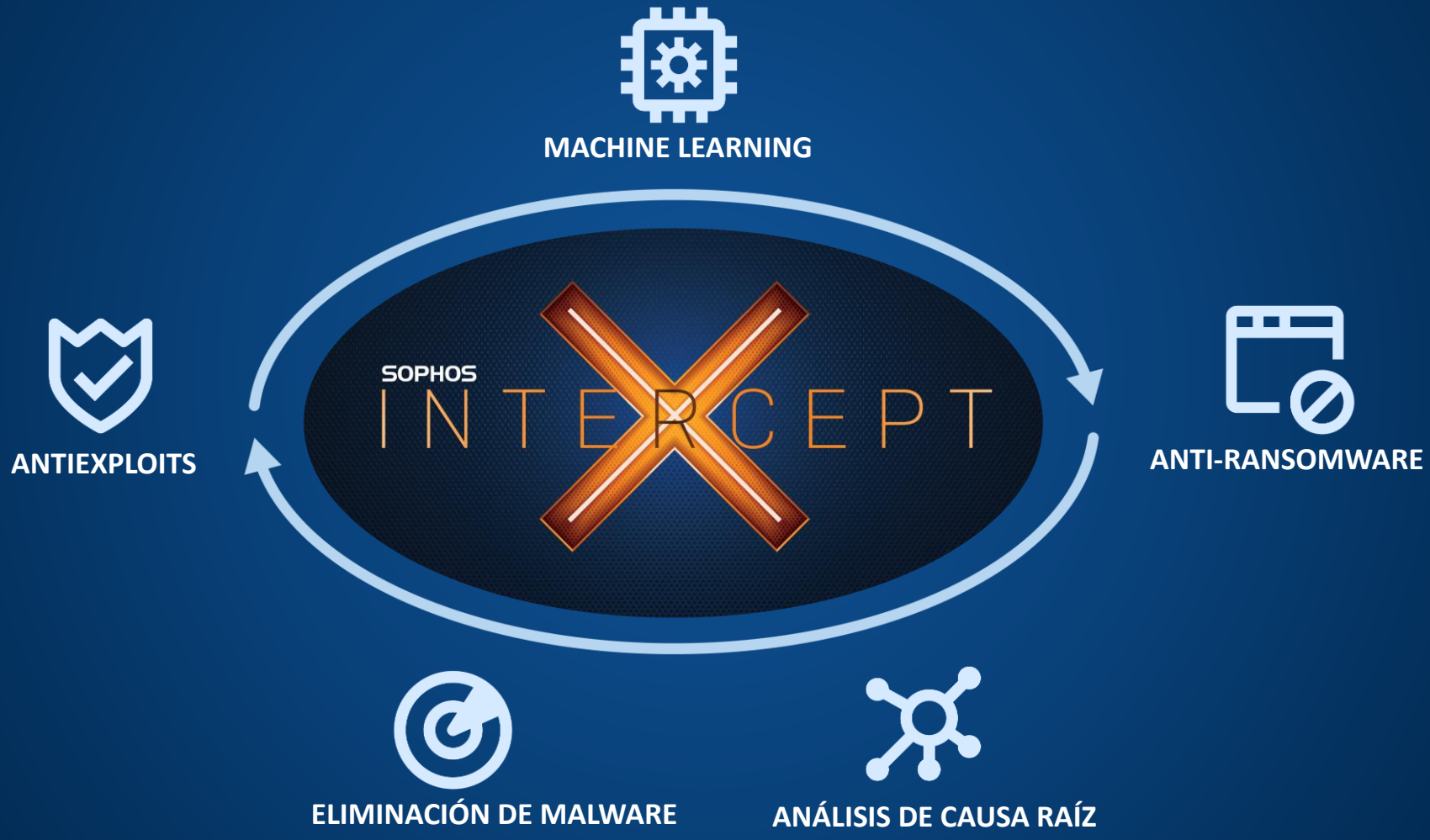
- ESG Labs, *Un nuevo enfoque de la seguridad de endpoints para las amenazas actuales*, Enero de 2018

SOPHOS

Y hay más…

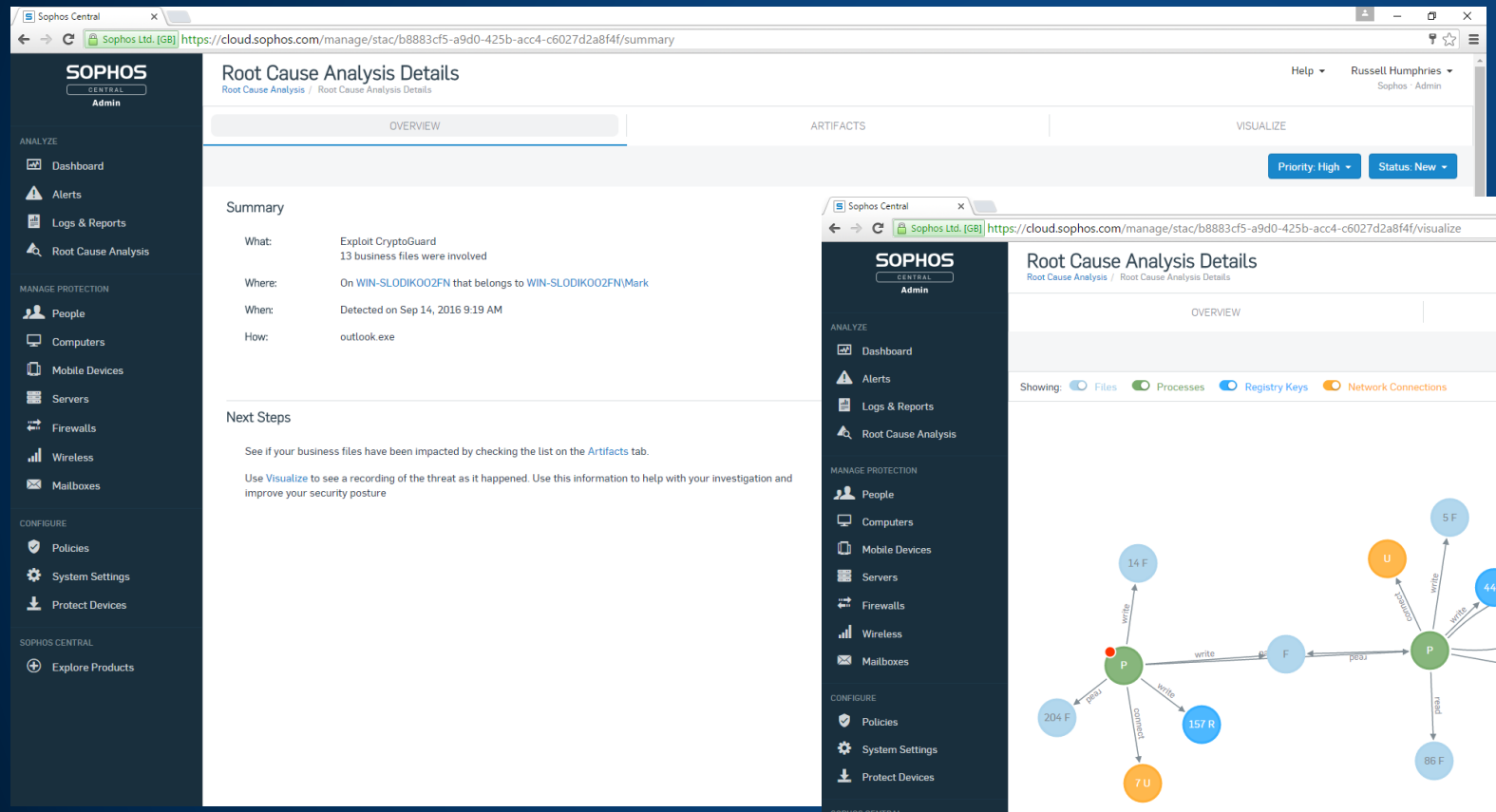
SOPHOS

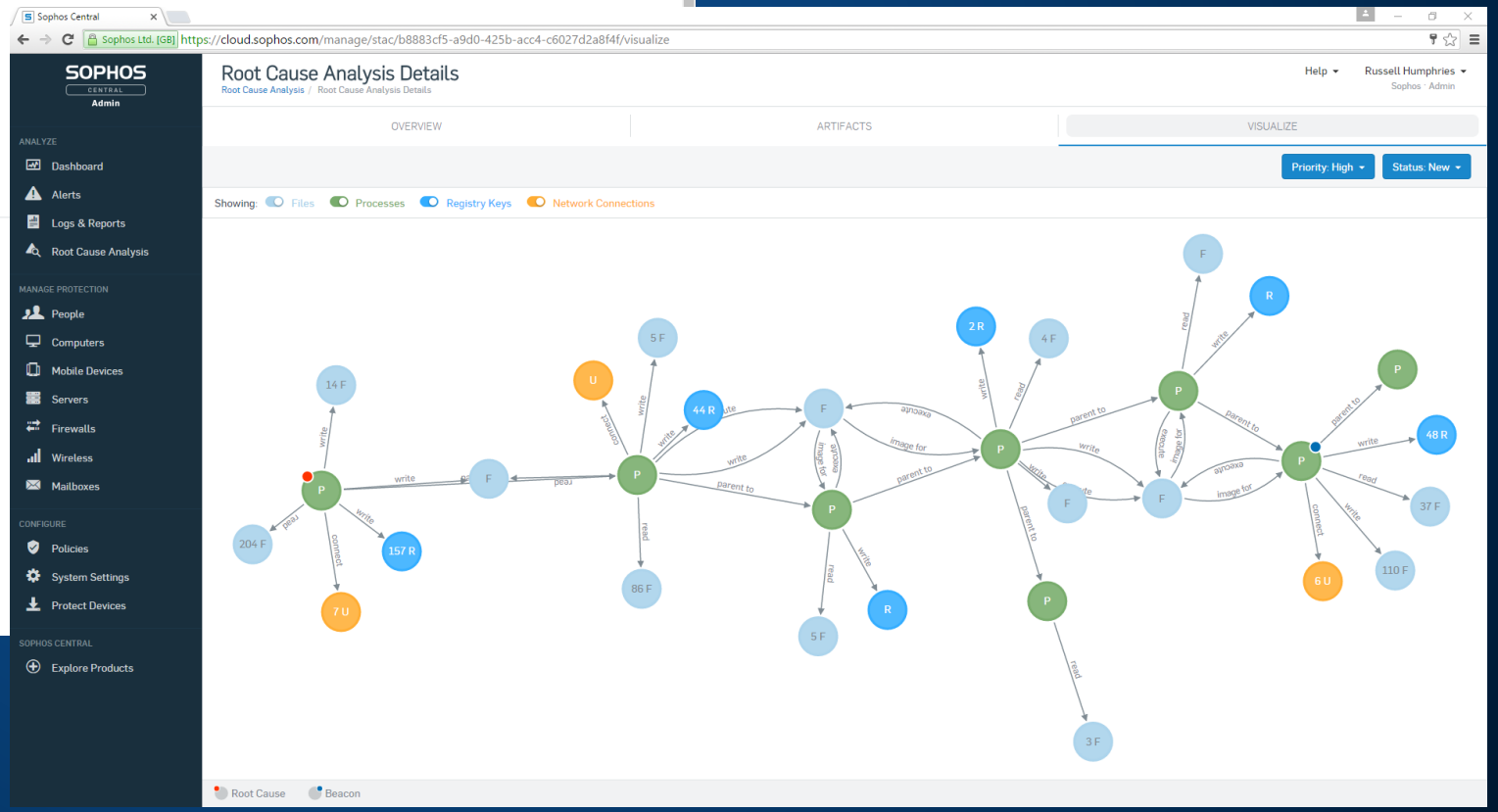
Protección completa para endpoints de Intercept X



Análisis de causa raíz

Comprender quién, qué, cuándo, dónde, por qué y cómo





SOPHOS

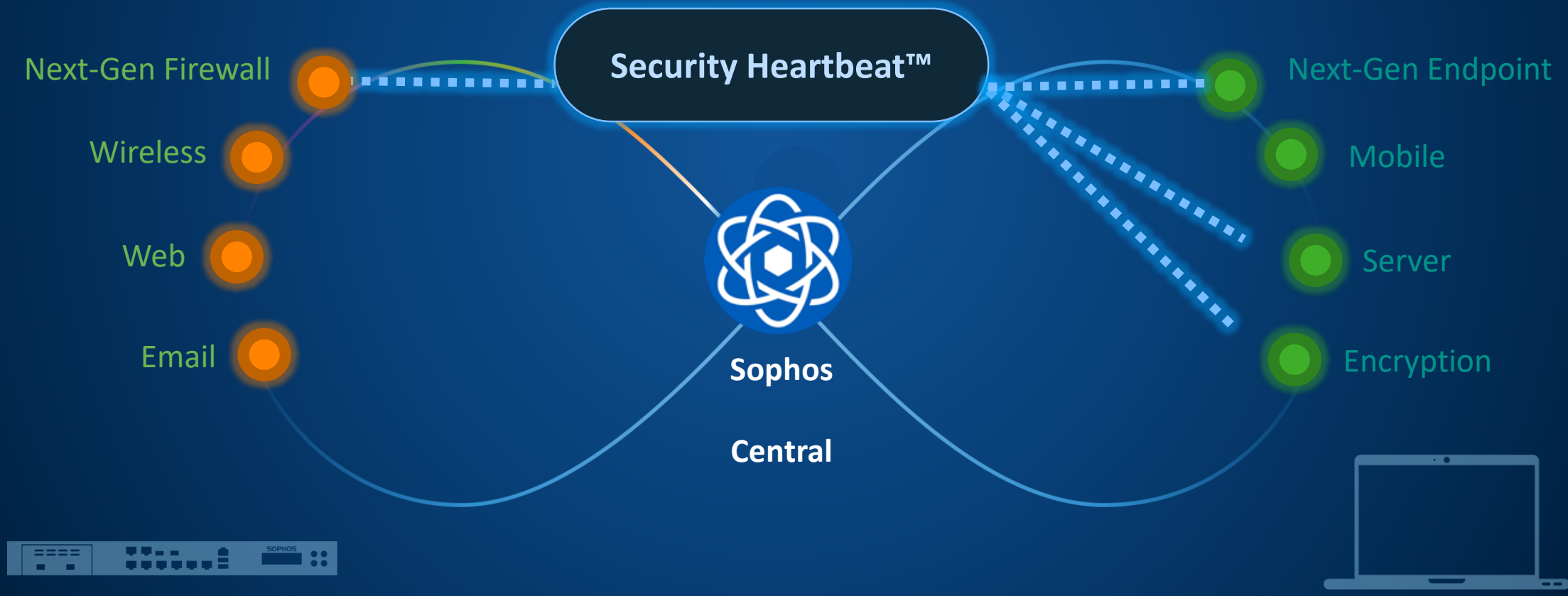
Eliminación de malware Sophos Clean

Limpieza de malware automatizada

Elimina claves de registro maliciosas

Erradica el código malicioso

Seguridad Sincronizada de Sophos



SOPHOS

Seguridad Sincronizada de Sophos

Información en tiempo real compartida entre sus endpoints y su firewall

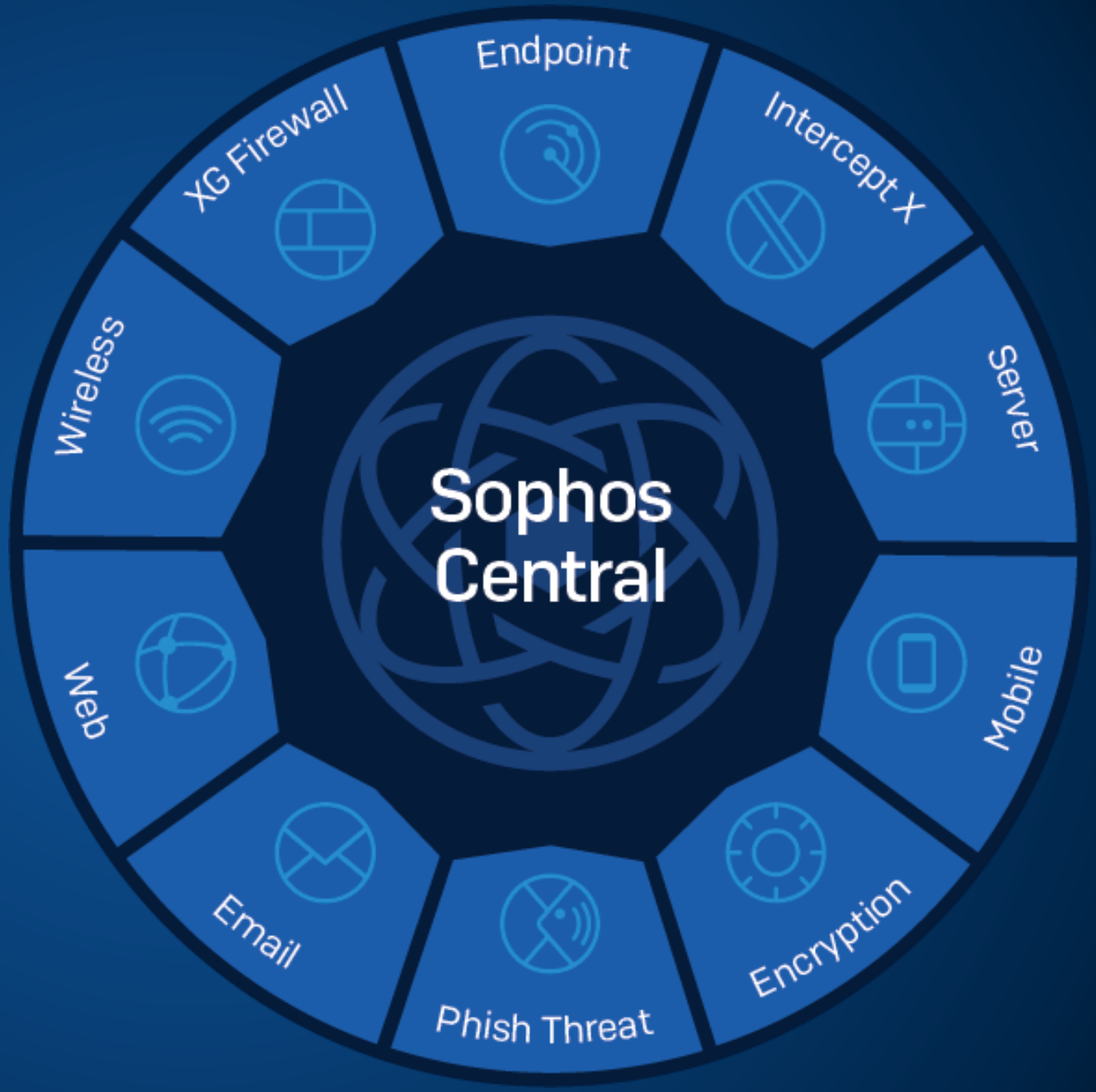
> “**Ninguna empresa** está cerca de proporcionar este tipo de comunicación entre productos de seguridad de **endpoints y redes**.”

Chris Christianson, vicepresidente de programas de seguridad, **IDC**

SOPHOS

Sophos Central

Administre múltiples productos de Sophos desde un único panel de control



¿Qué hace único a Intercept X?

SOPHOS

SOPHOS INTERCEPT X: EL PODER DEL MÁS

AMENAZAS CONOCIDAS

RANSOMWARE

EJECUTABLES DESCONOCIDOS

EXPLOITS Y SIN ARCHIVOS

BASE

CRYPTOGUARD

DEEP LEARNING

FUNCIONES ANTIEXPLOITS

La mejor protección para endpoints del mundo

Detenga las amenazas desconocidas con el Deep Learning

Detecta malware nuevo y desconocido utilizando Machine Learning avanzado

> "Una de las ***mejores puntuaciones de rendimiento*** que hemos visto en nuestras pruebas."
>
> *Maik Morgenstern, director tecnológico, AV-TEST*

Evite el ransomware con CryptoGuard

Bloquea el ransomware y revierte los archivos a un estado seguro

> "Intercept X ***detuvo todos los ataques de ransomware*** con que lo probamos en segundos."
>
> *ESG Labs*

Repela al atacante con la prevención de exploits

Bloquea las técnicas de explotación que utilizan los hackers para llevar a cabo sus ataques

> "Intercept X detuvo cada uno de los ataques complejos avanzados con que lo retamos."
>
> *ESG Labs*

Múltiples capas de defensa: el ejemplo del ransomware

1. Distribución

Evita que el ransomware se instale

Antiexploits

2. Ejecución

Pone el ransomware en cuarentena antes de que se ejecute

Deep Learning

3. Cifrado

Detiene el cifrado malicioso y revierte los cambios

CryptoGuard

"Instalar Sophos Intercept X junto con la protección para endpoints existente es sencillo y eficaz. Hemos notado que bloquea las amenazas de manera más rápida y ofrece un análisis sencillo e integral de un ataque".

- Bob Appleby, Partner, Asistente personal, Computer Connections

SOPHOS

SOPHOS

Security made simple.