SOPHOS

EVOLVE

Sophos Day Madrid

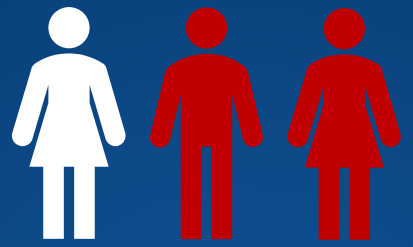
Ricardo Maté
Director General Sophos Iberia
@ricardomatesal

https://events.sophos.com/sophosday2019madrid

El rompecabezas imposible de la Ciberseguridad

Resultados de la encuesta independiente patrocinada por Sophos
a 3.100 Directores de TI y realizada por Vanson Bourne

SOPHOS
EVOLVE



2 de cada 3 organizaciones fueron victimas de un ciberataque en 2018

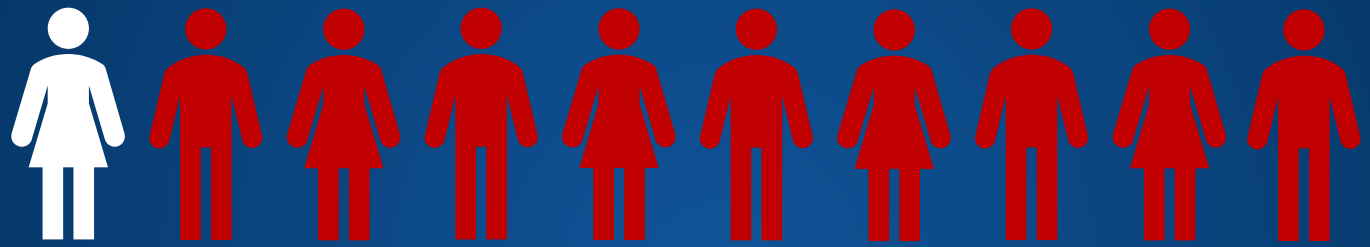
2

Dos ataques con éxito de media

10%

Sufrieron cuatro o más ataques que sobrepasaron sus defensas.

Las soluciones tradicionales de Cibersecuridad no son suficientes



9 de cada 10 tenían sus soluciones de ciberseguridad actualizadas en el momento en que sufrieron su ataque de más impacto

Los Ciberataques generan diferentes areas de preocupación

Perdida de Datos

- #1 preocupación para el 31% de los managers de TI
- Entre las tres primeras preocupaciones del 68% de los managers de TI

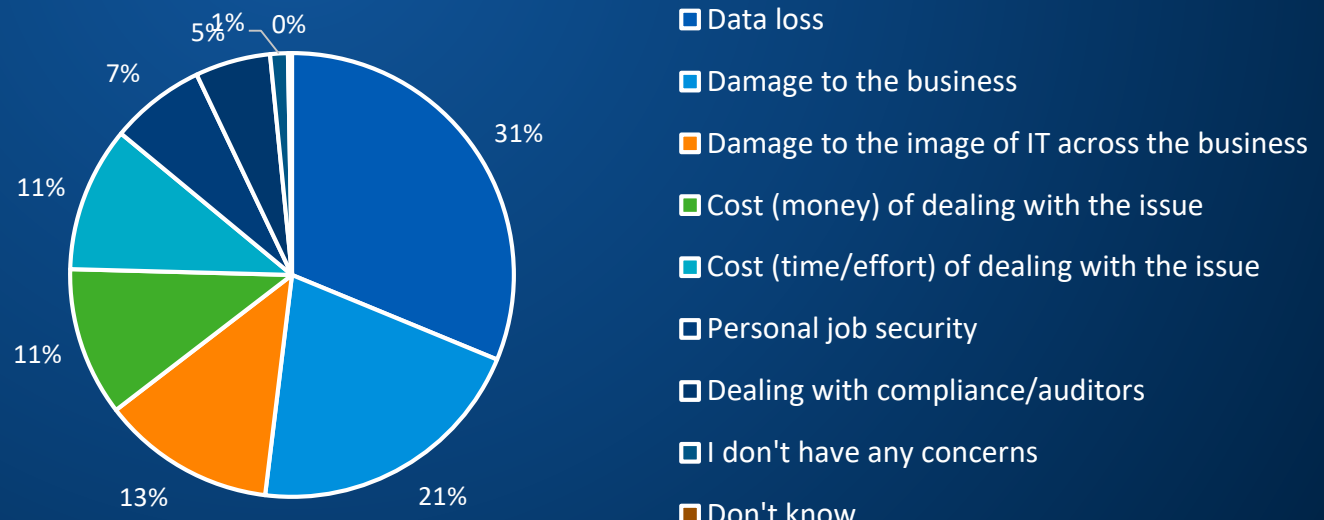
Impacto al Negocio

- #1 preocupación para el 21% de los managers de TI
- Entre las tres primeras preocupaciones del 56% de los managers de TI

Coste (tiempo y dinero)

- #1 preocupación para el 22% de los managers de TI
- Foco por igual entre tiempo y dinero (11% cada uno)

¿Cuales son las principales procupaciones de que su organización se vea afectada por un ciberataque?
La primera respuesta.



¿Por qué las empresas son incapaces de reducir el riesgo en ciberseguridad?

#1

Los ataques proceden de multiples direcciones

¿Cómo entraron los ataques más significativos?

Email

- Vehículo en 1 de cada 3 ataques (33%)

Web

- Usado en 3 de cada 10 ataques

20%

No lo saben

Vulnerabilidades Software

- Vector en el 23% de los ataques

USB / External Device

- Vector en el 14% de los ataques

#2
Los Ciberataques son coordinados, mixtos y constan de varias fases

Los ataques mixtos son la norma

53%
E-mail con Phishing

41%
Brecha de Seguridad

35%
Código malicioso

35%
Vulnerabilidad en el Software

30%
Ransomware

21%
Robo de credenciales

Una nueva brecha de seguridad revela información sensible de 1.200 millones de personas

23 noviembre, 2019 Por Francisco Salido — Deja un comentario

La fuga de información más grande hasta la fecha contiene nombres, direcciones de correo, números de teléfono e información sobre los perfiles de LinkedIn y Facebook de **más de 1.200 millones de personas**. Esta información parece tener origen en **dos compañías diferentes dedicadas al enriquecimiento de datos**.

Edenre

By Sergiu G

Marriott Faces $

July 09, 2019 Wang Wei

Google Is Fined
Europe's Data

4TH APRIL 2019 4:05PM CYBERSECURITY

Newham Council fin
breach

Payment s
undisclose
the infecti

Edenred o
employees

In 2018, th
representi
and online

poses
ta Leak

a

vered a **data breach**

En España hay ***al mes***

Since 25th of May to

After SamSam, Ryuk shows targeted ransomware is still evolving

18 DEC 2018 2

Ransomware, Security threats

portaltic / software / seguridad

INCIBE investiga el ciberataque de 'ransomware' que afecta a varias empresas españolas

Actualizado 04/11/2019 18:53:12 CET

Ransomware, ciberataque, virus, ciberamenaza - PIXABAY - Archivo

Últimas noticias / Portaltic »

- Google anuncia nuevas herramientas y funciones de seguridad para Cloud Platform
- Un error en la Cámara de Google permitía que hackers espiaran a través de los dispositivos Android

#3
La tecnología, el talento y el tiempo escasean

Gestionar la Ciberseguridad lleva a los equipos de TI una semana cada mes

26%

del tiempo del equipo de TI se dedica a gestionar la ciberseguridad

La mayoria

no tienen el ratio adecuado

Atraer talento es uno de los mayores retos

86%

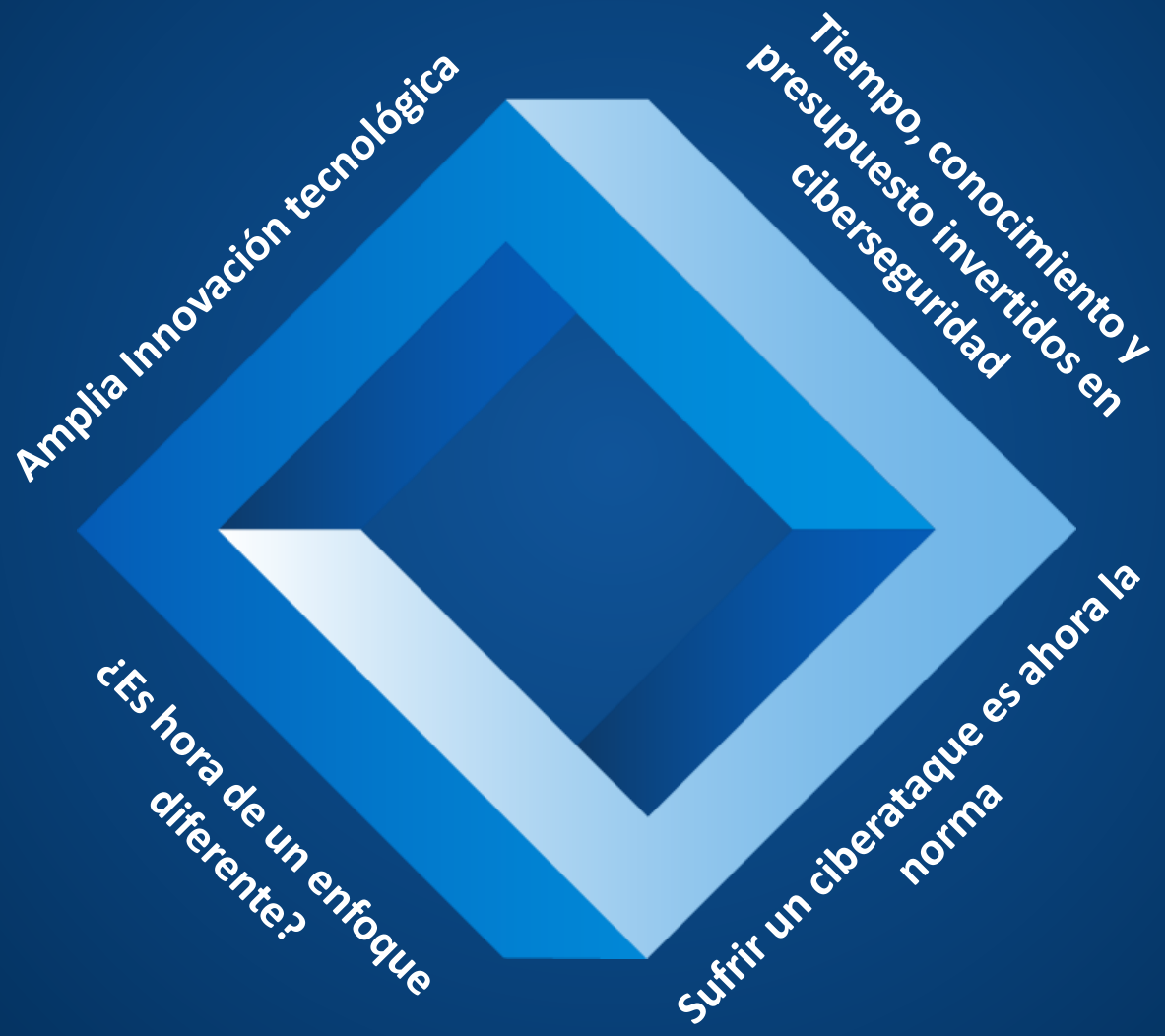
necesitan más conocimiento en ciberseguridad

8 de cada 10

no son capaces de contratar los recursos necesarios

% respondents who agree that recruiting people with the cybersecurity skills they need is a challenge

El rompecabezas imposible de la Ciberseguridad



ATAQUE INICIAL

Phishing

URL maliciosos

Command & Control

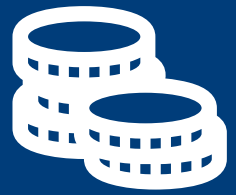
SEGUNDO ATAQUE

Robo de credenciales

Escalado de privilegios

Ejecutables maliciosos

OBJETIVO FINAL



Robo de Datos

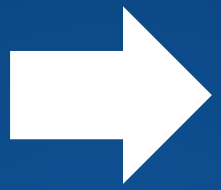
Ransomware

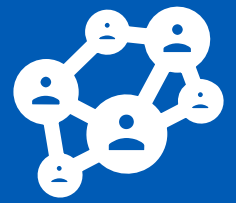
Ataque a los Servidores

Es tiempo de "*Cybersecurity EVOLVED*"

Productos de Seguridad

- Trabajando aislados
- Sin compartir información
- Varias consolas de gestión
- Diseñados por separado



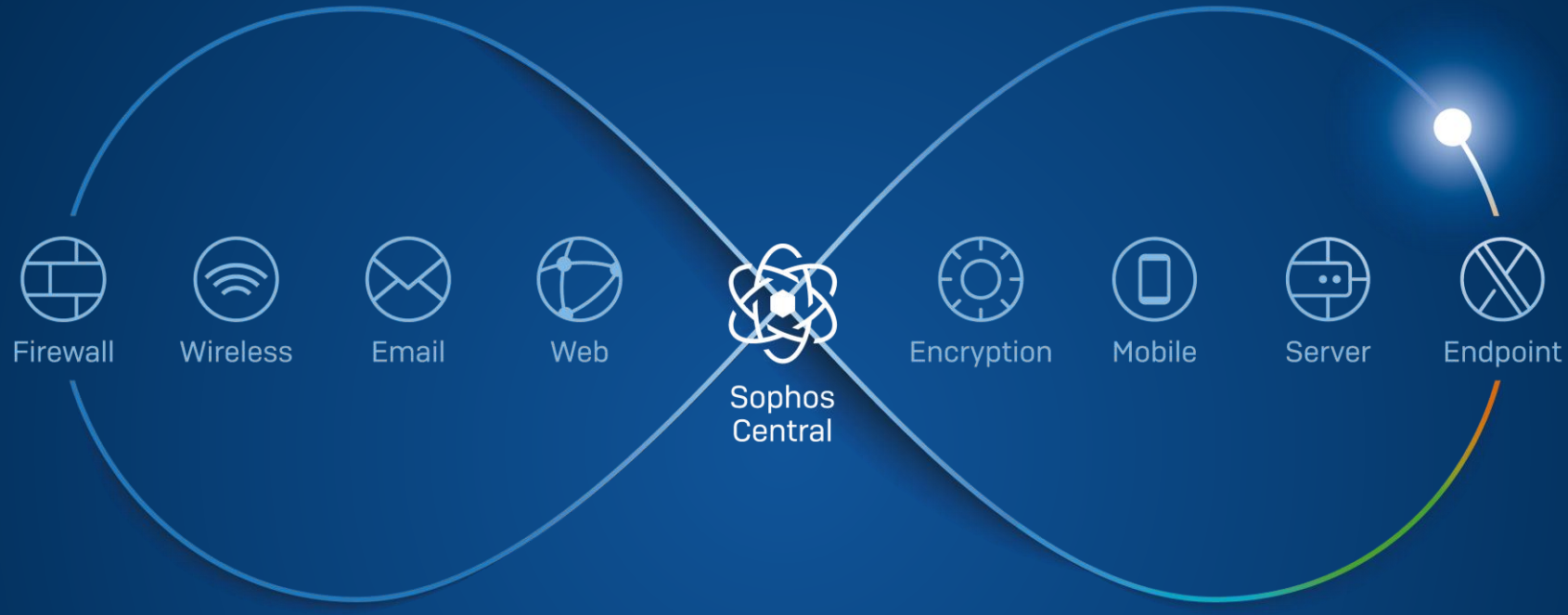


Cibersecuridad como Sistema

- Trabajando unidos
- Compartiendo información constantemente
- Gestión centralizada
- Compatibles por diseño

Estrategia Tecnológica de Sophos

Securidad Sincronizada



PROTECCIÓN SIN IGUAL

- Elimina los gaps de seguridad
- Reduce la exp. a amenazas
- Elimina el movimiento de los hackers

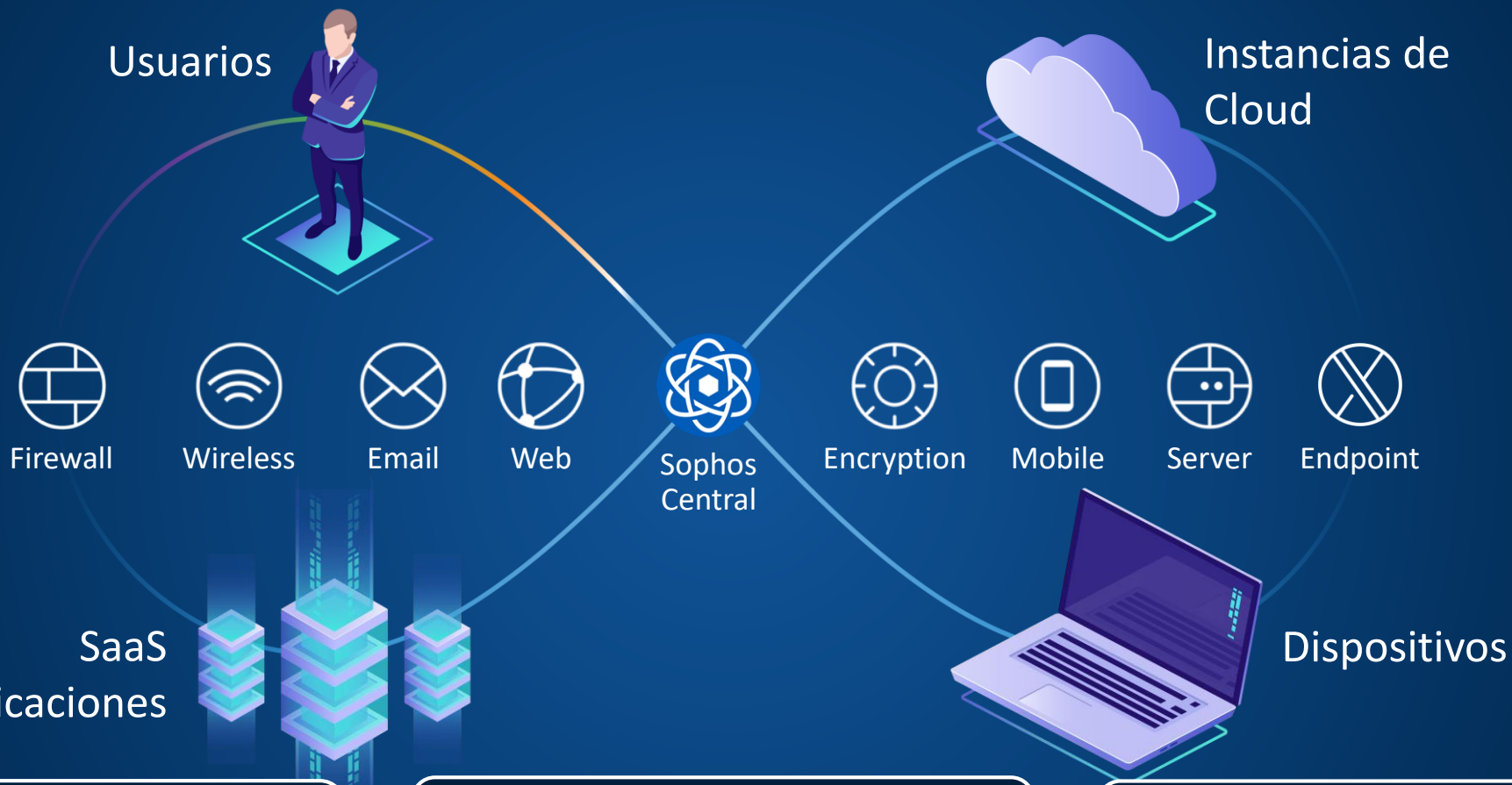
VISIBILIDAD EXTREMA

- Detección de amenazas
- Identifica riesgos apps y usuarios
- Identifica el 100% tráfico de red

MÁXIMA ESCALABILIDAD

- Descubrimiento automático de dispositivos
- Respuesta automática incidentes
- Limpieza automática de malware

EVOLUCIÓN de la Seguridad Sincronizada



ANALIZAR

- Descubrir usuarios, apps, dispositivos, y datos – on-prem, y en la nube
- Identificar y autenticar en tiempo real

ADAPTAR

- Politicas dinámicas de securidad basadas en detección de amenazas, comportamiento de usuarios, análisis de tráfico, y cumplimiento de normativa

AUTOMATIZAR

- Control de acceso a la Red y a la Wi-Fi
- Aislamiento automático de dispositivos
- Optimización del ancho de banda

SOPHOS
EVOLVE

FORRESTER®

SE Labs AAA APR-JUN 2018 ENTERPRISE ENDPOINT PROTECTION

Synchronized Security

NSS LABS RECOMMENDED

Gartner®

SOPHOS

Cloud Optix

See everything. Secure everything

SOPHOS

Sophos Cloud Optix
La Respuesta

Visibilidad

Si no puedes verlo no puedes protegerlo

- Visibilidad continua
- Visualización de la Topología
- Detección de las anomalías

Compliance

Entorno auto-escalable en constante cambio

- Compliance continuo
- Customización del Compliance
- Colaboración del Compliance
- DevOps Seguro

Respuesta

Ataques complejos, pero recursos limitados

- Detección de Desviaciones
- Guardarailes y Remediación
- Escaneado de plantillas proactivo


Intercept X

Intercept X la mejor solución de EPP/EDR del mercado

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

100 %
de protección contra ataques

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

N.º 1
en protección contra exploits

SE Labs AAA
ENTERPRISE ENDPOINT PROTECTION

Calificación AAA
en protección para grandes empresas

SE Labs
BEST Small Business Endpoint
WINNER 2019

Mejor producto
de protección de endpoints para pymes

AV comparatives

N.º 1
en índice de protección antimalware

NSS LABS RECOMMENDED

N.º 1
en eficacia de la seguridad y coste total de propiedad

Gartner

LÍDER

FORRESTER®

LÍDER

SC MAGAZINE
BEST BUY

AV-TEST
av-test.org
AWARD
BEST ANDROID SECURITY
Sophos Mobile Security

SC 2019 awards EUROPE
Winner


INTERCEPT X
NOW WITH EDR
THE BEST JUST GOT BETTER

Managed Threat Response

La mejor Protección

Managed Threat Response

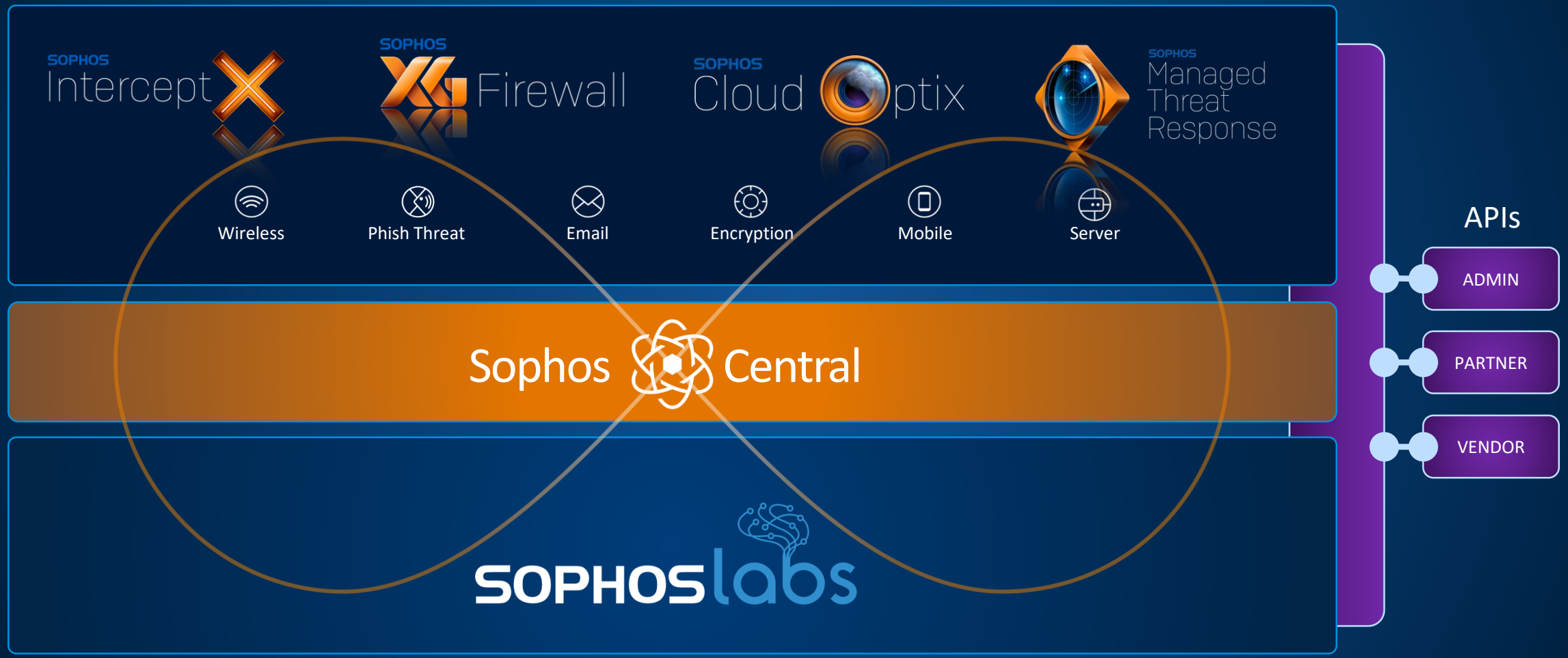
Threat hunting, detección, y respuesta 24x7, proporcionado como servicio gestionado, por un equipo de expertos

"Clients with successful SOCs put the premium on people rather than process and technology. People and process overshadow technology as predictors for SOC success or failure."

-- Gartner, "How to Plan, Design, Operate and Evolve a SOC" (2018)

XG Firewall

Securidad Sincronizada



¿Por qué Sophos?

1. Compañía fiable:
   - 35 años de historia, 3.600 empleados. Market cap 3.900M$
   - Revenue 372M$ & Cash Flow 94M$ (H1-FY20). 60% Next Gen Security (+40% YoY)
   - >400.000 Clientes & >9.000 en Iberia
2. El Mejor equipo de Ciberseguridad
3. Solución Completa de Nueva Generación en Ciberseguridad:
   - Innovadora, Eficiente y Sencilla de gestionar
   - Seguridad Sincronizada y Proactiva (Deep learning)
   - Consola unificada: Sophos Central
4. La mejor Solución de Endpoint Detection & Response según todos los analistas (Intercept X EDR) y Servicios Gestionados de Threat Hunting (MTR)
5. Sophos Labs
6. Comprometidos con los mejores Partners del Mercado
7. Soporte Local

SOPHOS

Cybersecurity made simple.