



# Ciberseguridad como Servicio

## La mejor solución para sus clientes

Fernando Casares

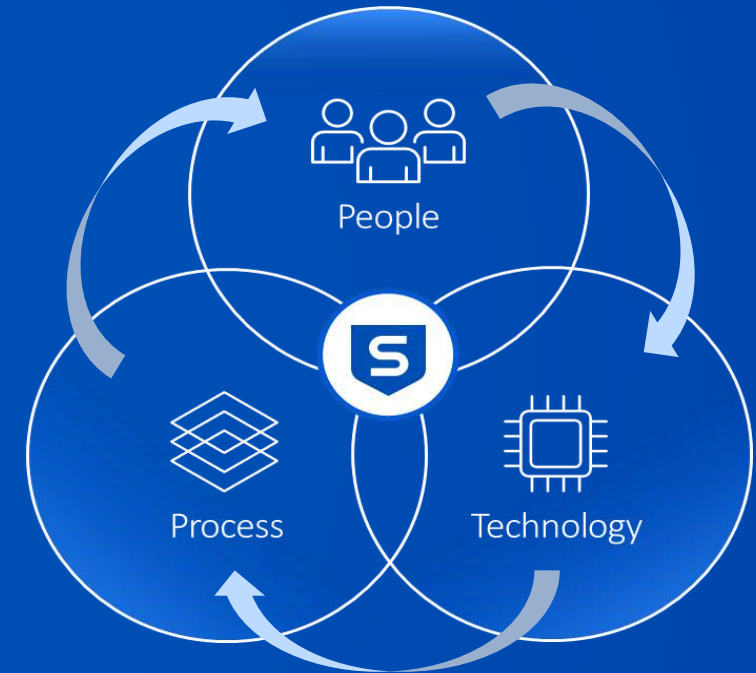
Distributor and MSP Manager

Sophos Iberia

**SOPHOS**

# Escenario actual

La ciberseguridad se ha vuelto demasiado compleja como para que la mayoría de organizaciones la gestionen de forma efectiva.



**Tecnología**

**Un ciberataque a Iberdrola expone 1,3 millones de clientes**

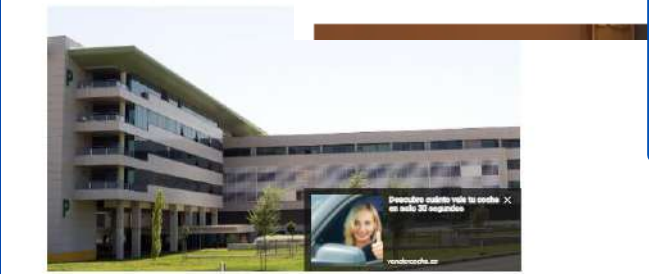
La compañía niega que se hayan comprometido datos de los usuarios, aunque reconoce que si reveló su nombre y teléfono



**Los hackers de Sevilla aterrorizan a la policía local, acusados de un ataque a la red municipal**

**El IB-Salut sufre una nueva historia de Balears: médicos personal**

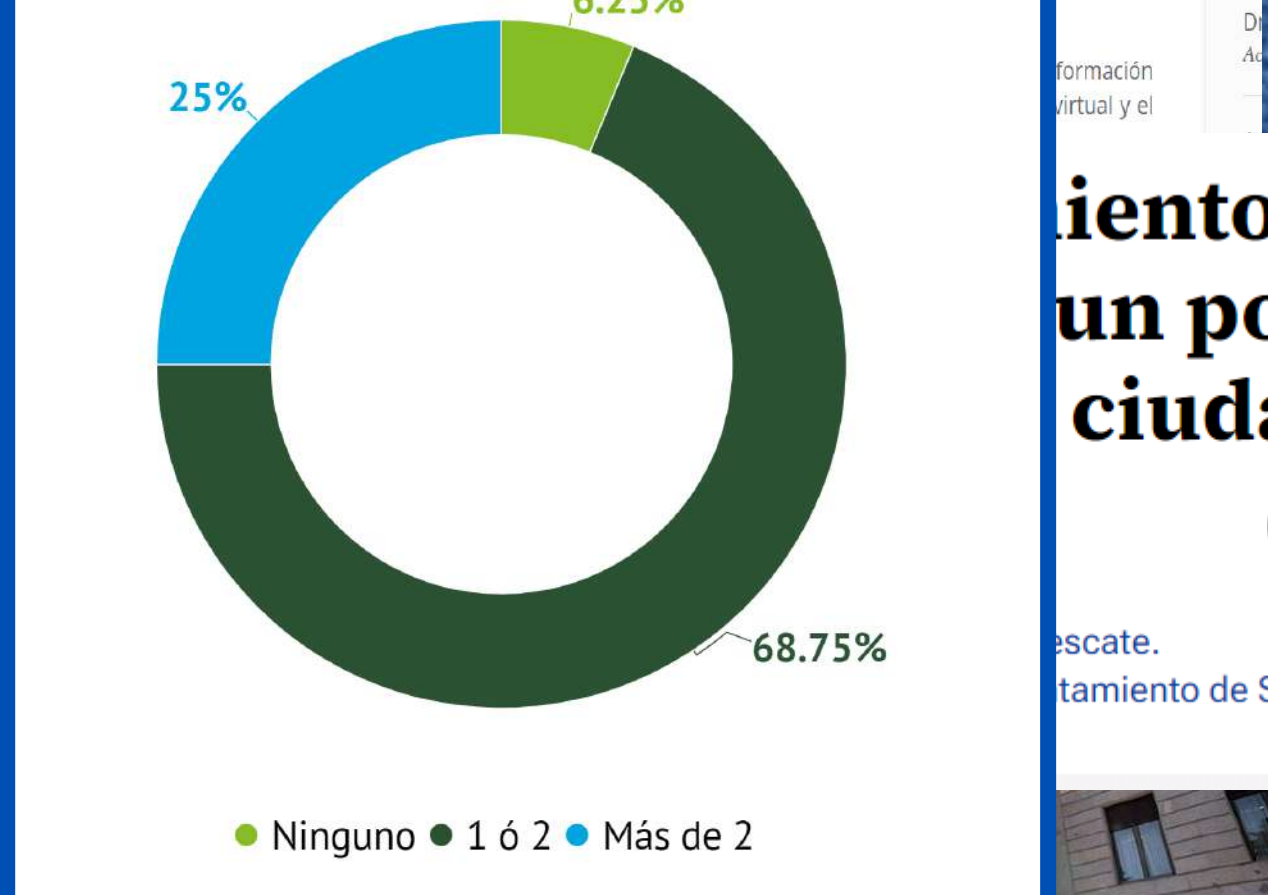
La rápida detección de la infiltración en los centros de salud llevan desde finales de agosto a ciudadanos afectados para volver a utilizar sus servicios



**España**

**Un ataque informático afecta a 179 entidades**

La empresa pública de agua de Madrid sufrió un asalto procedente de un grupo de hackers



**Un ciberataque a Glovo expone datos de clientes y repartidores**

El ciberdelincuente los ha puesto a la venta en Internet, aunque la empresa asegura que no se han filtrado datos relacionados con tarjetas de crédito.

ataque informático

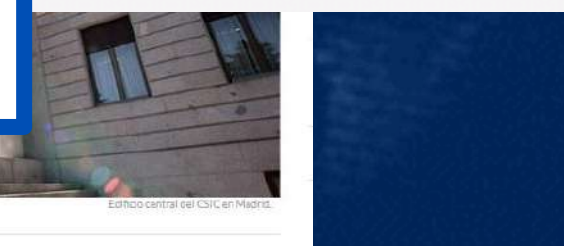
Un ataque informático afecta a 179 entidades

**Un ataque informático afecta a 179 entidades**

La empresa pública de agua de Madrid sufrió un asalto procedente de un grupo de hackers

**Un ataque informático afecta a 179 entidades**

La empresa pública de agua de Madrid sufrió un asalto procedente de un grupo de hackers



**¿De verdad creéis que no eligieron el «Mejor Producto» para sus necesidades?**



**Complejidad**



**Conocimientos**

**Cybersecurity as a Service combina eficientemente servicios, tecnologías, conocimientos y herramientas líderes en el mundo en una única solución holística.**

# Cybersecurity as a Service



**Centro de operaciones de seguridad instantáneo:** que puede ser administrado por usted, nosotros o ambos.



**Defensas de ciberseguridad** integradas de primera clase que funcionan con los productos que ya tiene.



**Un equipo de expertos** en ciberseguridad.



Gestión a través de una **intuitiva plataforma de seguridad basada en la nube.**

# Cybersecurity as a Service



**OPTIMICE LA  
PREVENCIÓN**



**MINIMICE LOS  
TIEMPOS DE  
DETECCIÓN Y  
RESPUESTA**

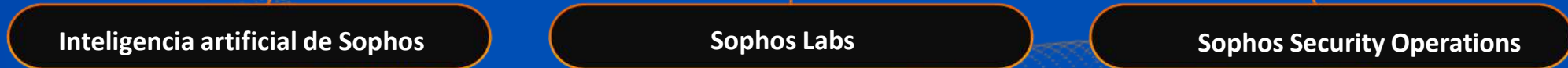
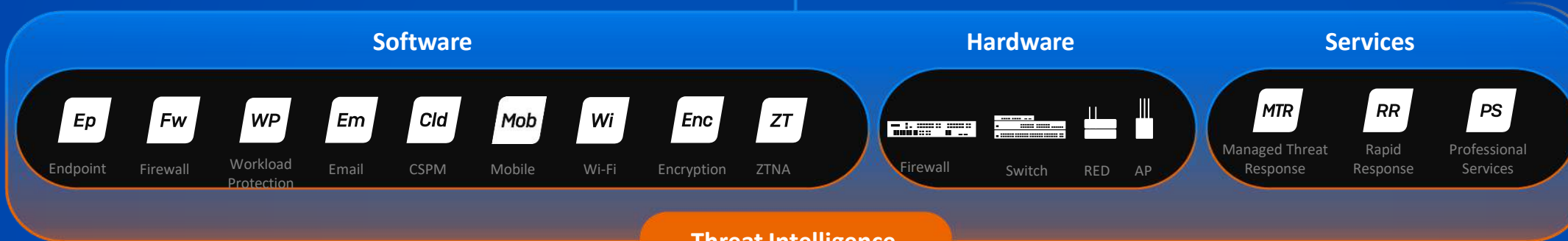
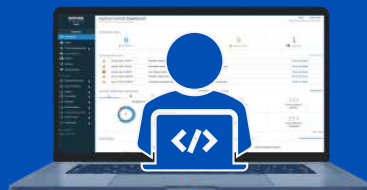


**AUTOMATICHE CON  
LA COLABORACIÓN  
HUMANO-MÁQUINA**



# Estrategia Tecnológica

# Ecosistema de ciberseguridad adaptativa



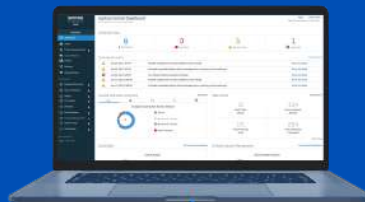
- SOAR/SIEM**
  - RAPID7
  - splunk>
  - LogRhythm
  - CORTEX XSOAR
  - sumo logic
- BI/IT/DP/DOC**
  - BrightGauge
  - liongard
  - concertium
  - aruba
  - CIGENT
- RMM**
  - servereye
  - ConnectWise
  - Kaseya
  - N-ABLE
- PSA**
  - ConnectWise
  - datto | AUTOTASK

\* Subset of all integrations

# Consola única de Gestión

Overview

- Dashboard
- Alerts
- Threat Analysis Center
- Logs & Reports
- People
- Devices
- Global Settings
- Third-party Integrations
- Protect Devices
- Account Health Check



**Sophos Central**  
Security Management  
Security Operations (XDR)

## Software

- FW (Firewall)
- WP (Workload Protection)
- Em (Email)
- Cld (CSPM)
- Mob (Mobile)
- Wi (WiFi)
- Enc (Encryption)
- ZT (ZTNA)

## Hardware

- Firewall
- Switch
- RED
- AP

## Services

- MTR (Managed Threat Response)
- RR (Rapid Response)
- PS (Professional Services)

Threat Intelligence

Sophos Artificial Intelligence

Sophos Labs

Sophos Security Operations

Data Lake

# Como construimos la cartera de negocio.

¿He sido Vulnerado?

▼

**Sophos Compromise Assessment**

**El medio más rápido y eficaz para identificar la actividad de los atacantes en curso o pasada en su entorno**

Me han vulnerado, ¿Que hago ahora?

▼

**Sophos Rapid Response**

**Respuesta a incidentes de emergencia para eliminar rápidamente las amenazas activas y monitorear la recurrencia**

No quiere que me vulneren (otra vez) ¿Como puedo ser proactivo?

▼

**Sophos MDR**

**Búsqueda de amenazas, investigación y respuesta 24/7 entregada por un equipo de expertos como un servicio totalmente administrado**



# Gartner®

Para el año 2025, el 50% de las organizaciones usarán Servicios MDR para monitorización de amenazas, y funciones de detección y respuesta que ofrezcan contención de amenazas y capacidad de mitigación

# Sophos X-Ops impulsa MDR

**31 mil millones de eventos de seguridad diarios**

De 600K+ clientes de Sophos



**150 analistas MDR SecOps**

Monitoreo de cuentas de clientes 18K +



**21 científicos de datos de IA**

18 Artículos publicados



Sophos X-Ops



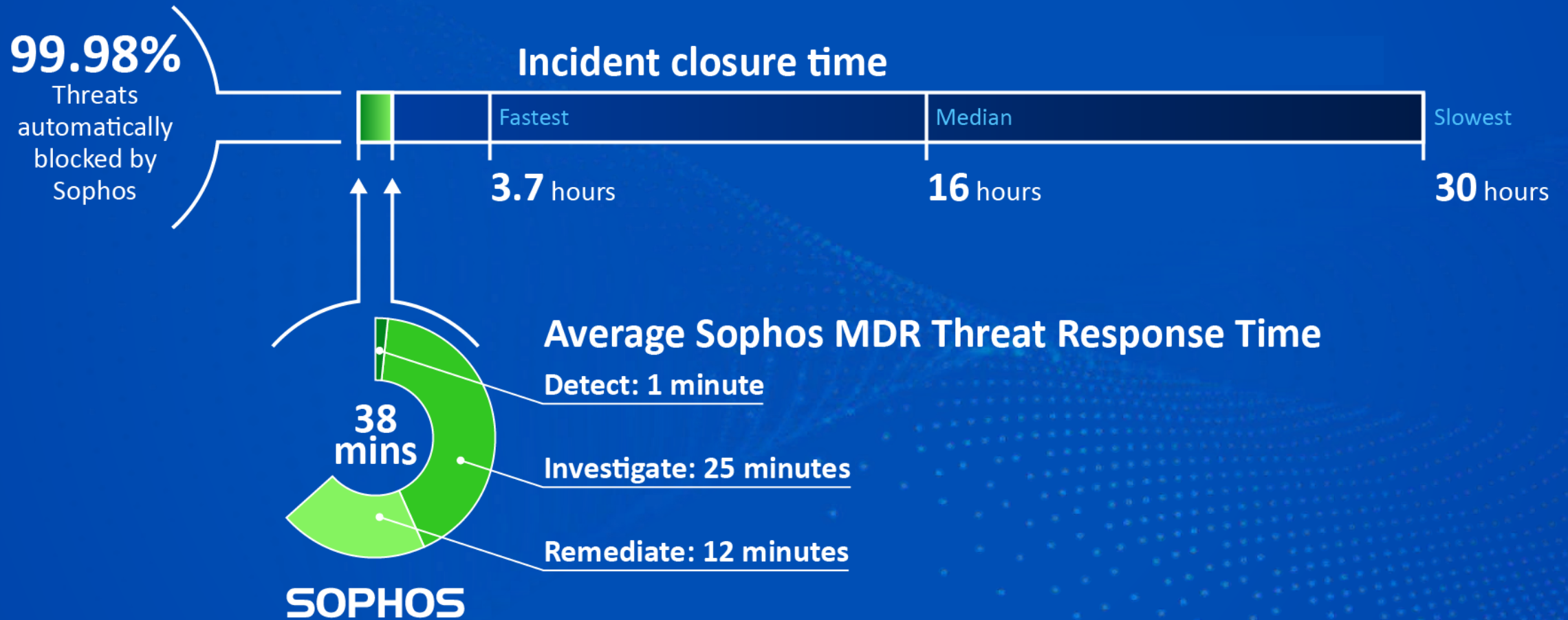
**6 Global SOCs**



**120 investigadores de Sophos Labs**

Análisis de amenazas

# Leading Detection and Response Times



# Sophos MDR Service Tiers

Cualquier solución de endpoint [CIXA]

Necesita Sophos Endpoint

Sophos MDR Essentials

Sophos MDR Complete

<b>Monitoreo y respuesta a amenazas 24/7 dirigido por expertos</b>	✓	✓
<b>Compatible con productos de seguridad que no son de Sophos</b>	✓	✓
<b>Informes semanales y mensuales</b>	✓	✓
<b>Sesión informativa mensual de inteligencia: "Sophos MDR ThreatCast"</b>	✓	✓
<b>Comprobación del estado de la cuenta de Sophos</b>	✓	✓
<b>Búsqueda de amenazas dirigida por expertos</b>	✓	✓
<b>Respuesta a amenazas: los ataques activos se detienen y se contienen</b> <small>Utiliza el agente completo de Sophos XDR (protección, detección y respuesta) o el sensor Sophos XDR (detección y respuesta)</small>	✓	✓
<b>Soporte de llamadas directas durante incidentes activos</b>	✓	✓
<b>Análisis de causa raíz: realizado para prevenir recurrencias futuras</b>		✓
<b>Respuesta a incidentes a gran escala: las amenazas se eliminan por completo</b> <small>Requiere un sensor Sophos XDR completo (protección, detección y respuesta)</small>		✓
<b>Líder de respuesta a incidentes dedicado</b>		✓
<b>Garantía de protección contra infracciones de Sophos</b>		✓



# MDR que te encuentra donde estás

## Gente

Necesito un equipo experto para...

Gestione completamente la respuesta a las amenazas

Co-gestionar la respuesta a las amenazas con mi equipo

## Proceso

Las amenazas confirmadas requieren...

Respuesta a incidentes a gran escala: se elimina la amenaza

Contención para que mi equipo pueda eliminarlos

## Tecnología

Quiero usar...

Sophos: mejor protección, detección y respuesta

Una combinación de herramientas de Sophos y de otros lugares

## Visibilidad

Detecte amenazas utilizando datos de...

Endpoint

Firewall

Email

Identity

Public Cloud

Network

Soluciones de Sophos integradas sin coste adicional

 Sophos XDR

 Sophos Firewall

 Sophos Email

 Sophos Endpoint

 Sophos Cloud

Soluciones que no son de Sophos integradas sin coste adicional



Cualquier plataforma de protección de endpoints, incluido Windows Defender

Integraciones complementarias disponibles para su compra:



Prácticamente cualquier herramienta de seguridad que genere datos de detección de amenazas

# Sophos MDR: apertura y flexibilidad líderes del sector

## MDR Sophos MDR

### Compatible con su entorno

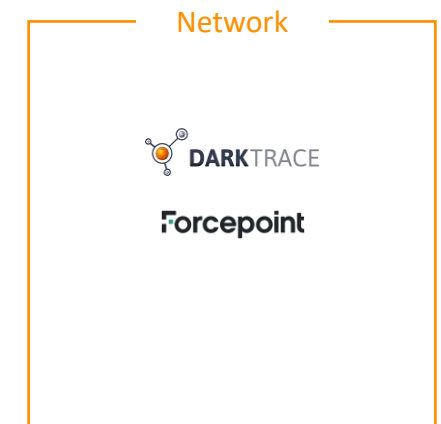
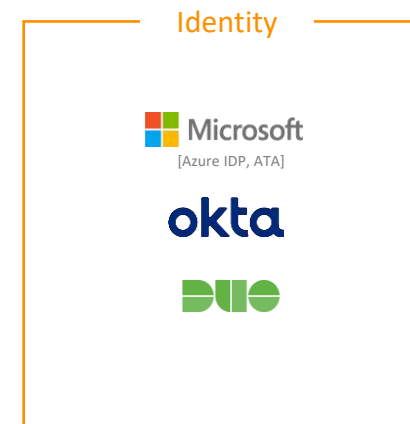
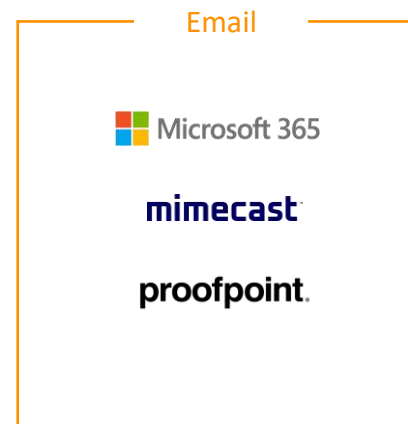
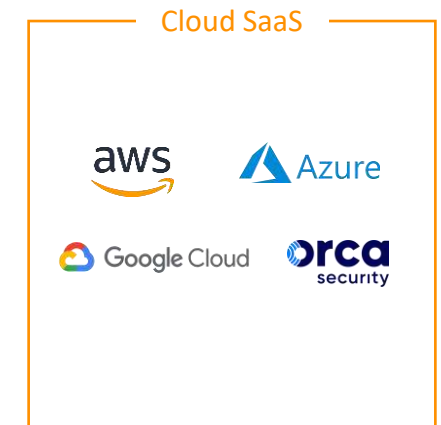
Podemos usar nuestras herramientas, las herramientas de otro proveedor o cualquier combinación de las dos.

### Compatible con sus necesidades

Si necesita respuesta a incidentes a gran escala o asistencia para tomar decisiones más precisas

### Compatible con tu negocio

Nuestro equipo tiene una amplia experiencia en la búsqueda de amenazas dirigidas a organizaciones de todas las industrias.



# Sophos NDR: Cinco motores de detección de amenazas en tiempo real



# Sophos Breach Protection Warranty



En Sophos, hacemos de su ciberseguridad nuestra responsabilidad. La garantía de protección contra infracciones de Sophos se incluye sin cargo adicional con nuestra suscripción a Sophos MDR Complete. Cubre hasta \$ 1 millón en gastos de respuesta para clientes calificados.

## Protección confiable para una total tranquilidad Includo con Sophos MDR Complete

Más organizaciones confían en Sophos MDR que en cualquier otro proveedor de seguridad. Con la garantía de protección contra infracciones de Sophos, los clientes de Sophos MDR Complete disfrutan de la tranquilidad y la tranquilidad que conlleva tener cobertura financiera en caso de infracción.

## Cobertura clara y completa

- Proporcionado automáticamente: no es necesario presentar una solicitud
- Includo con suscripciones de uno, dos y tres años
- Includo con las compras de licencias nuevas y de renovación
- Cubre puntos finales, servidores y dispositivos que ejecutan Windows y macOS
- Sin niveles de garantía que restrinjan la cobertura
- No hay requisitos adicionales de compra de licencias

La garantía se incluye automáticamente y sin cargo adicional con nuevas compras o renovaciones de suscripciones anuales de Sophos MDR Complete. No hay niveles de garantía, términos mínimos de contrato o requisitos de compra adicionales.

## Hasta \$1 millón en Gastos de Respuesta

La garantía cubre los gastos de respuesta tras un incidente de ransomware en un entorno protegido por Sophos MDR Complete:

- Hasta \$1,000 por máquina violada
- Hasta \$1 millón en gastos totales de respuesta
- Pago de rescate de hasta \$100,000 (como parte del límite por dispositivo)

Reflejando la realidad de los entornos operativos actuales, las máquinas violadas incluyen puntos finales, servidores y dispositivos Windows y macOS. La garantía cubre una amplia gama de gastos incurridos, incluida la notificación de violación de datos, relaciones públicas, legal y cumplimiento.

## Warranty Overview

- Hasta \$1 millón en gastos totales de respuesta
- Hasta \$100,000 para el pago del rescate (como parte del límite por dispositivo)
- Hasta \$1,000 por máquina violada
- Cubre una variedad de gastos incurridos, incluida la notificación de violación de datos, relaciones públicas, legal y cumplimiento

Para ver los términos y condiciones completos de la garantía, visite [www.sophos.com/legal](http://www.sophos.com/legal)

# Probado. De confianza.

## Crecimiento de los clientes

Uno de los proveedores de servicios MDR más grandes y de mayor crecimiento

**+ 630 000 clientes**  
+ 100 millones de dispositivos protegidos

**+ 55 000 partners de canal**  
+ 8000 MSP

**+ 18 000 clientes de MDR**  
Miles de investigaciones

## Analistas del sector

13 veces líder del Cuadrante Mágico de Gartner

**Líder: Plataformas de protección de endpoints**  
Cuadrante mágico de Gartner

**Mejor solución de endpoints para grandes empresas**  
SE Labs

**Puntuación de protección y usabilidad del 100 %**  
AV-Test

## Pruebas de terceros

Productos y servicios galardonados

**Ganador: Mejores servicios de seguridad administrada**  
Premios Channel Partner Insight

**“One of the TOP performing Security services vendor”**  
MITRE Engenuity ATT&CK Evaluation

**Customers' Choice para FW, EPP y MDR**  
Gartner Peer Insights

# Logre resultados superiores en ciberseguridad

MENOS RIESGO

MAYOR EFICIENCIA

MENOR COSTE

**85%** Reducción en incidentes que requieran investigación

**2X** Mayor eficiencia en los equipos de IT

**5X** Más barato que manejado "in-house"



**Empresa Diseño Industrial**  
700 usuarios

"El lunes tengo más de 1.000 alarmas para revisar, ¿a cuál hago caso?"



**Ayuntamiento**  
300 usuarios, 50.000 habitantes

"Desde que tenemos el Servicio de MDR he ganado más de 1 hora de sueño al día"



**Empresa Logistica**  
1.300 empleados

"Cuándo me explicasteis el Servicio pensé ... ¿Dónde habéis estado todo este tiempo?"



**Universidad**  
2.000 usuarios, 60.000 estudiantes

"Lo que buscamos es un Servicio de Ciberseguridad que nos permita dormir tranquilos".



**Empresa de Consultoria**  
800 usuarios

"El departamento de IT somos los que ves, no teníamos tiempo y tiempo es lo que hemos comprado"



**Empresa de Retail**  
200 empleados

"El equipo de Rapid Response? Parecían sacados de una película de Hackers"

# ALSO Cloud MARKETPLACE

- Plataforma para automatizar el negocio Cloud de los proveedores MSP



► Ventajas únicas

# VENTAJAS DEL ALSO CLOUD MARKETPLACE

- Gestión centralizada del negocio MSP
- Ventas instantáneas
- Facturación Sencilla
- Soporte Técnico
- Aprovisionamiento automático de clientes en SOPHOS CENTRAL
- Complementa el ecosistema de ciberseguridad de Sophos con servicios añadidos
- Business Intelligence
- Visibilidad a los clientes




# Licencias acumulativas



100 User  
25 Server  
2 Devices

Customer A




150 User  
5 Server

Customer B



300 User  
10 Server  
15 Devices  
5 DR

Customer C



250 User  
5 Server  
14 Devices  
1 Cloud

Customer D

Uso acumulado por categoría de producto

=



800 User  
45 Server  
31 Devices  
1 Cloud  
5 Device Reporting

# Cálculo global por familia de productos

User Licenses: <i>Endpoint Intercept X, EDR,MDR, Mobile, Web, Disk, Phish Threat, Conectores</i>
1 -99 user licenses
100-499 user licenses
500-999 user licenses
1,000-4,999 user licenses
5,000-9,999 user licenses
10,000+ user licenses

Device : <i>XG Firewall and Virtual XG as a Service</i>
1-24 devices
25-99 devices
100-199 devices
200 -499 devices
500-999 devices
1,000 + devices

800 User  
45 Server  
31 Devices  
1 Cloud  
5 Device Rep.

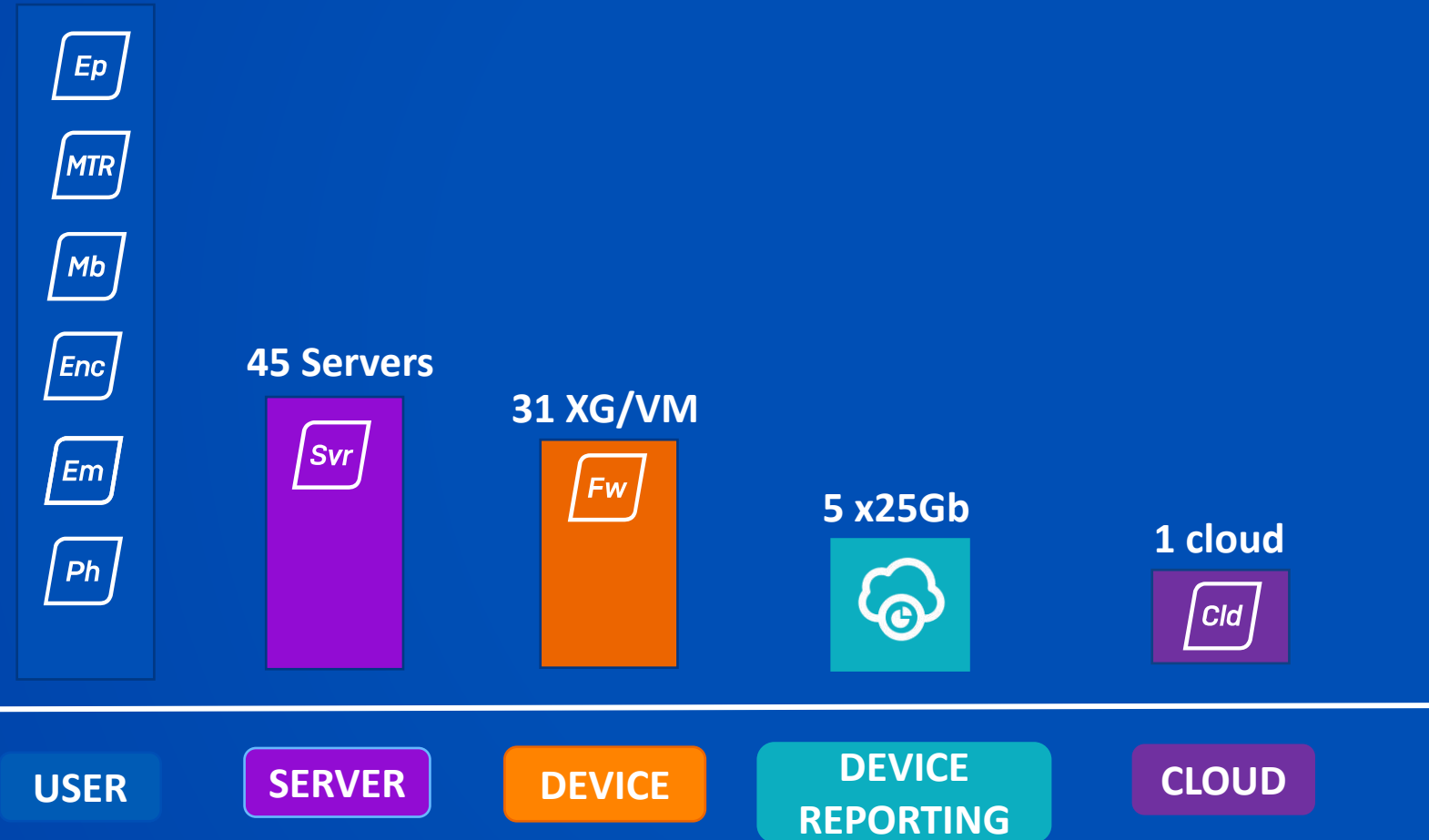
Server Licenses: <i>Standard,Advanced Intercept X, EDR, MDR</i>
1 -24 server licenses
25-99 server licenses
100-249 server licenses
250-499 server licenses
500-999 server licenses
1,000 + server licenses

Device Reporting Licenses: Per 25GB Per Month
1+ 25GB licenses

Cloud: Cloud Optix
1-24 devices
25-99 devices
100-199 devices
200 -499 devices
500-999 devices
1,000 + devices

# Programa Sophos MSP Connect Flex + Volumen = Más margen

800 Users



Todas las licencias implementadas para sus clientes se suman

Banda de **precio decreciente** según el volumen

**Una factura** por mes a través de su mayorista

Archivo de **uso en tiempo real**

# TODAVIA NECESITAIS UN EMPUJON?



30%  
DESCUENTO  
TODOS SKU  
MDR\*

\* SOLO EN ACMP

*Sophos Day*

# EXPERIENCE



*Tour*



**Museo Reina Sofía, Madrid**



**15 de noviembre 2023**



**¡Regístrese ahora!**

**SOPHOS**  
Cybersecurity delivered.