POLICÍA NACIONAL

sealpath

1824 · 2024

Ransomware al acecho: *Toc Toc, ¡Tengo tus datos!*

IV EDICIÓN CONGRESO SEGURIDAD DIGITAL Y CIBERINTELIGENCIA

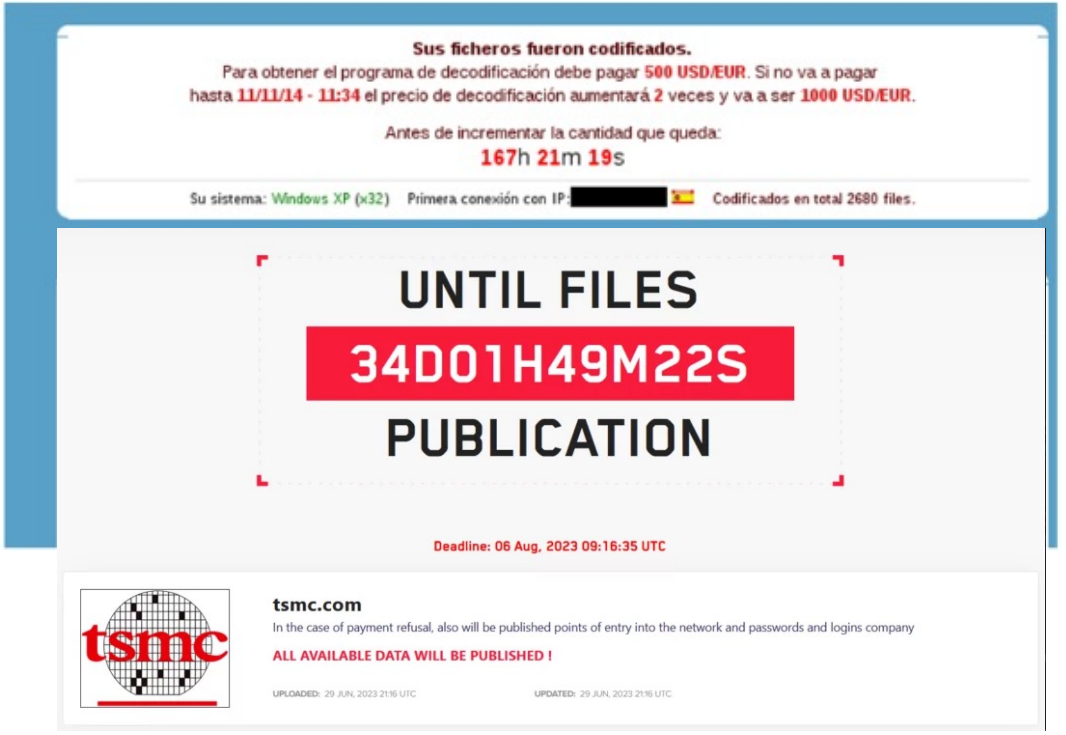
Y si un día…

SU RED HA SIDO COMPROMETIDA.

Este enlace y su clave expirarán en 14 dias tras la infección de sus sistemas.
Compartir este enlace o email le llevará a la irreversible destrucción de sus claves de descifrado.

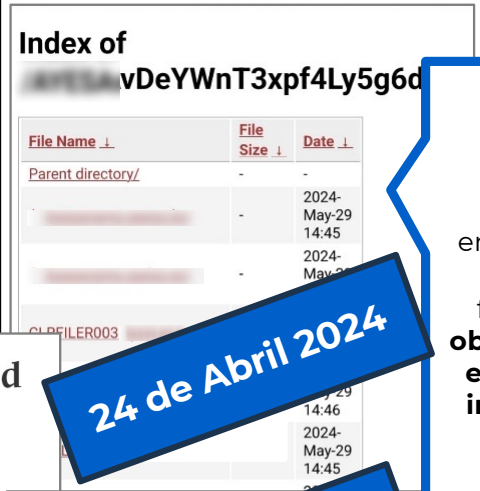
NO SE DA MAS TIEMPO a precio especial.

Todos los archivos en cada host de la red han sido encriptados con un fuerte algoritmo.
No existe ningún software de descifrado disponible en otras fuentes.
No renombre los archivos infectados o de informacion de texto. No mueva los archivos infectados ni de información de texto.
Esto podría llevarle a la imposibilidad de recuperar ciertos archivos.
Tambien hemos recopilado toda su información sensible.
Así que, si decide no pagar la haremos pública.
Podría dañar la reputación de su negocio.



POLICÍA NACIONAL

30 de Mayo 2024

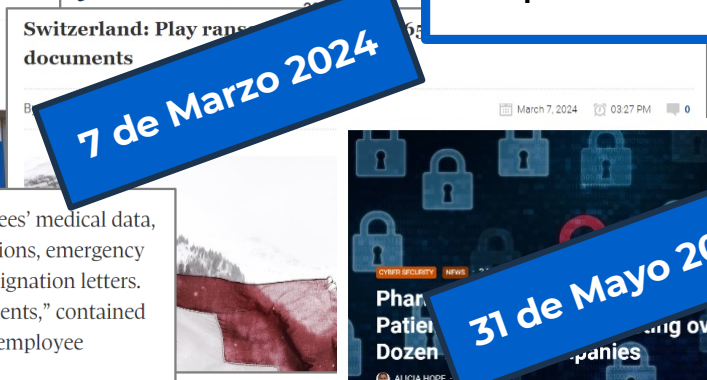


24 de Abril 2024

Al igual que recibimos ciberataques a nivel personal para intentar sacarnos dinero, las empresas reciben ataques continuos para robar ficheros, documentos, y **obtener dinero a través de extorsiones que pueden impactar en reputación, costes legales, operacionales, etc**.

30 de Mayo 2024

23 de Mayo 2024



7 de Marzo 2024

31 de Mayo 2024

La amenaza no para de crecer

8º

+ atacado

del mundo

*Threat Landscape Report de S21sec

1.133

x semana en Iberia

*Security Report Iberia 2024 de Check Point

20% de

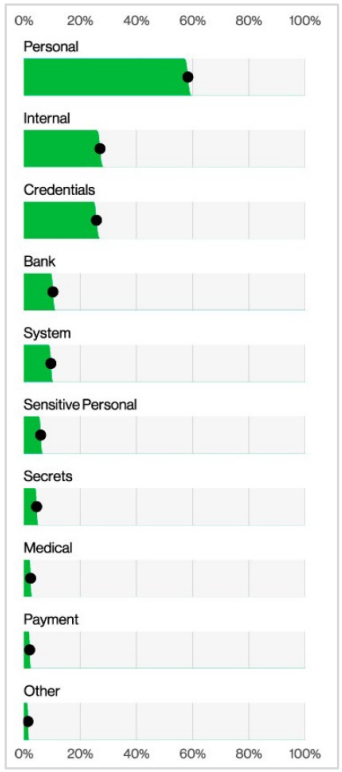
empresas

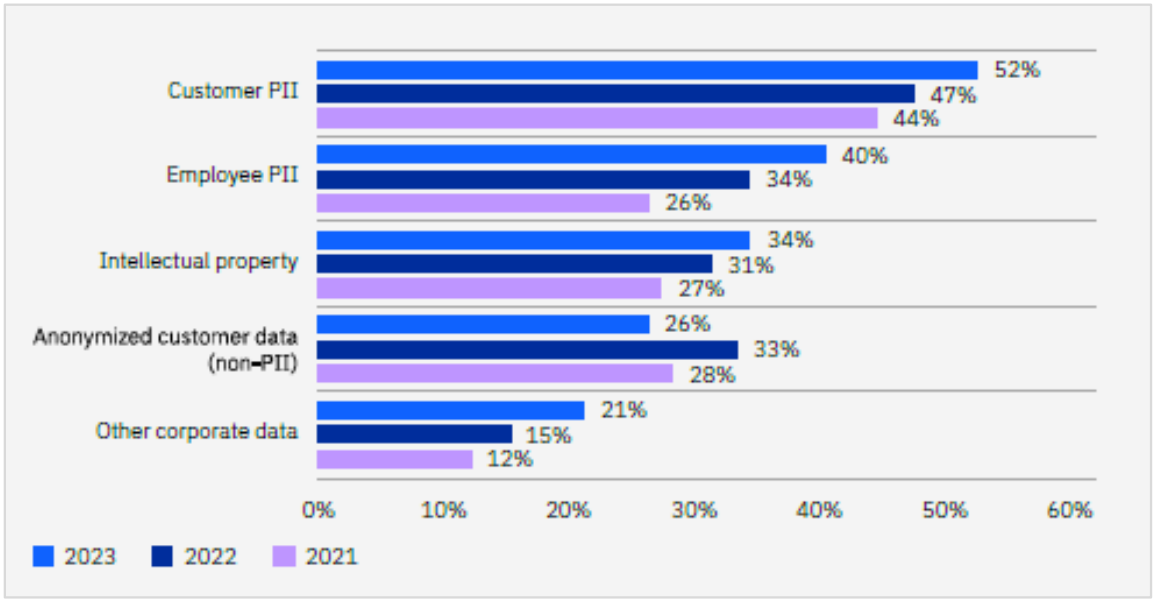
en España

*Informe de Ciberpreparación 2023 de Hiscox

sealpath

Tipos de Datos





Top Información extraída

Datos personales de clientes

Siguiéndole datos personales de empleados, y propiedad intelectual.

sealpath

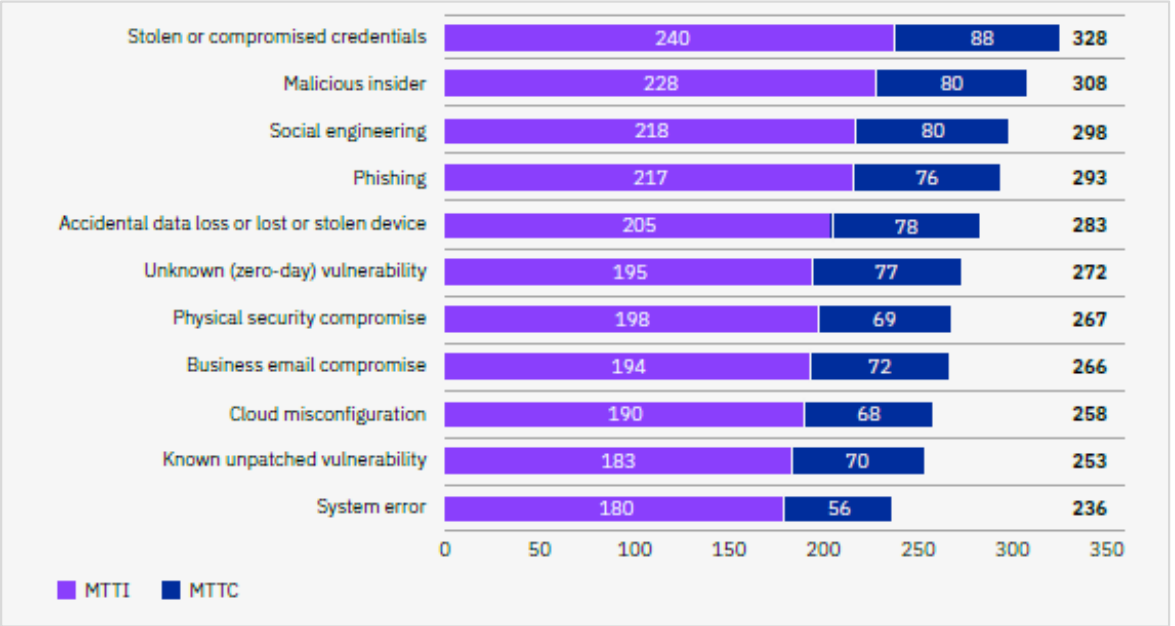
***IBM Cost of a data breach report 2023**
*** Verizon Data Breach Investigations Report 2024**

Reaccionamos tarde

Tiempo para contener la fuga

Desde los 180 días a los 240 para identificar una fuga.

Y desde 56 días hasta 88 para contenerla.



*IBM Cost of a data breach report 2023
* Verizon Data Breach Investigations Report 2024

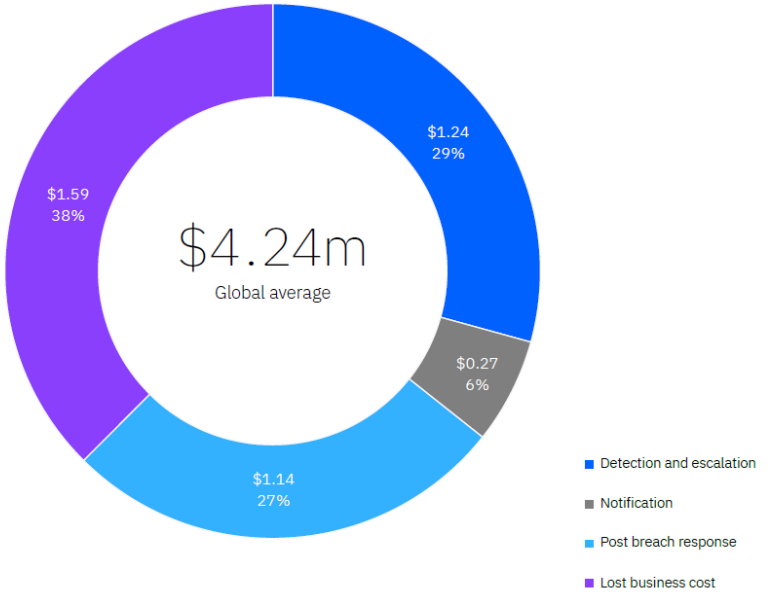
El coste e impacto

1. Costes de detección y escalado
- Actividades forenses y de investigación
- Auditoría, gestión de crisis, comunicación ejecutivos.

2. Costes de notificación
- emails, cartas, etc. a afectados.
- Comunicación con reguladores, involucración expertos.

3. Costes de respuesta tras la fuga
- Soporte a afectados y comunicación.
- Expedientes legales, descuentos. Multas.

4. Costes por pérdida de negocio
- Pérdidas por interrupción del negocio, caídas, etc.
- Pérdida de clientes y reputación.



***IBM Cost of a data breach report 2023**
*** Verizon Data Breach Investigations Report 2024**

Evolución del Ransomware Moderno

2013 Cryptolocker

Cifrado de archivos a baja escala, a individuos.

2018 Wannacry

Dirigidos, caza mayor de organizaciones, restaurar operativa.

2019 Maze

La doble extorsión, filtración pública.

sealpath

Ransomware en la Actualidad

RansomOps

Diversos actores, entramado más complejo.

IAB

Initial Access Brokers

RaaS

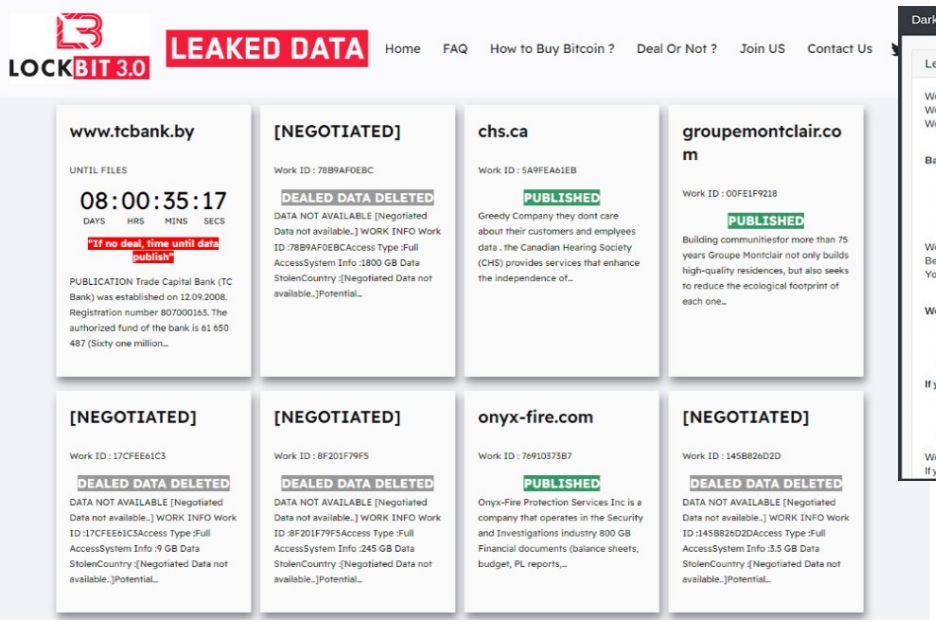
Ransomware-as-a-Service

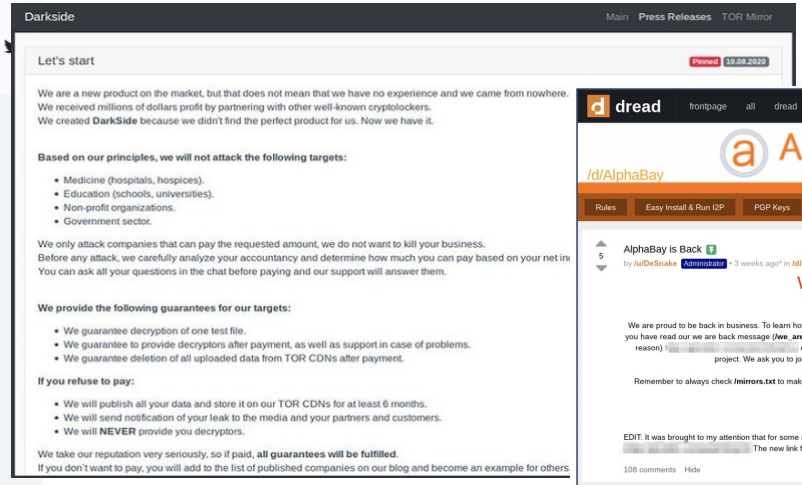
Presas más valiosas

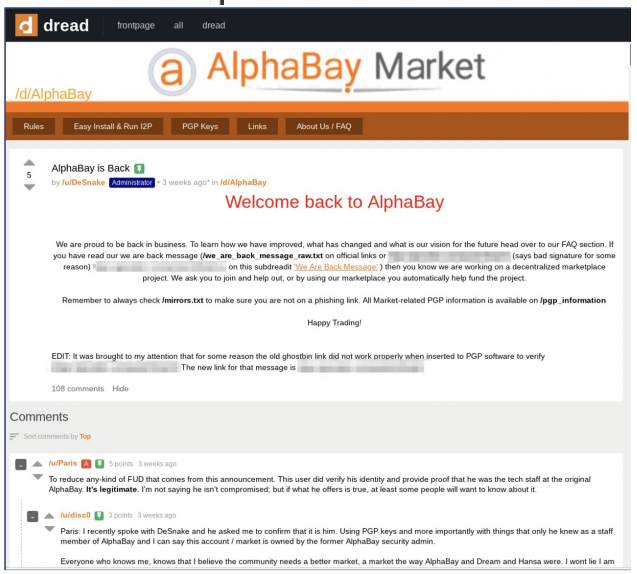
Botines más grandes

sealpath

Su infraestructura en la dark web

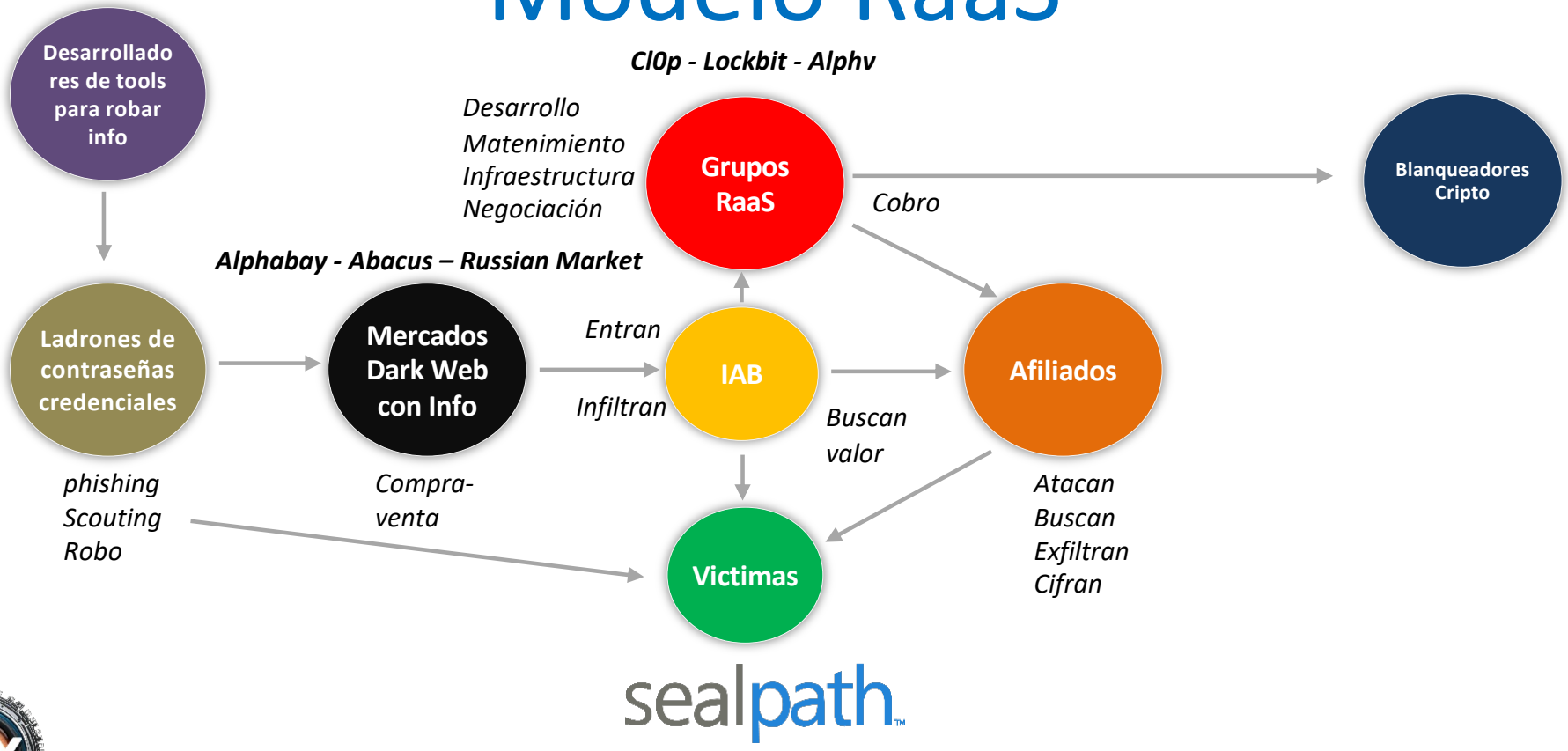






sealpath

Modelo RaaS



sealpath

¿Cómo seleccionan organizaciones?

Ingresos

Organizaciones con capacidad para hacer frente a un pago alto por extorsión.

Sectores

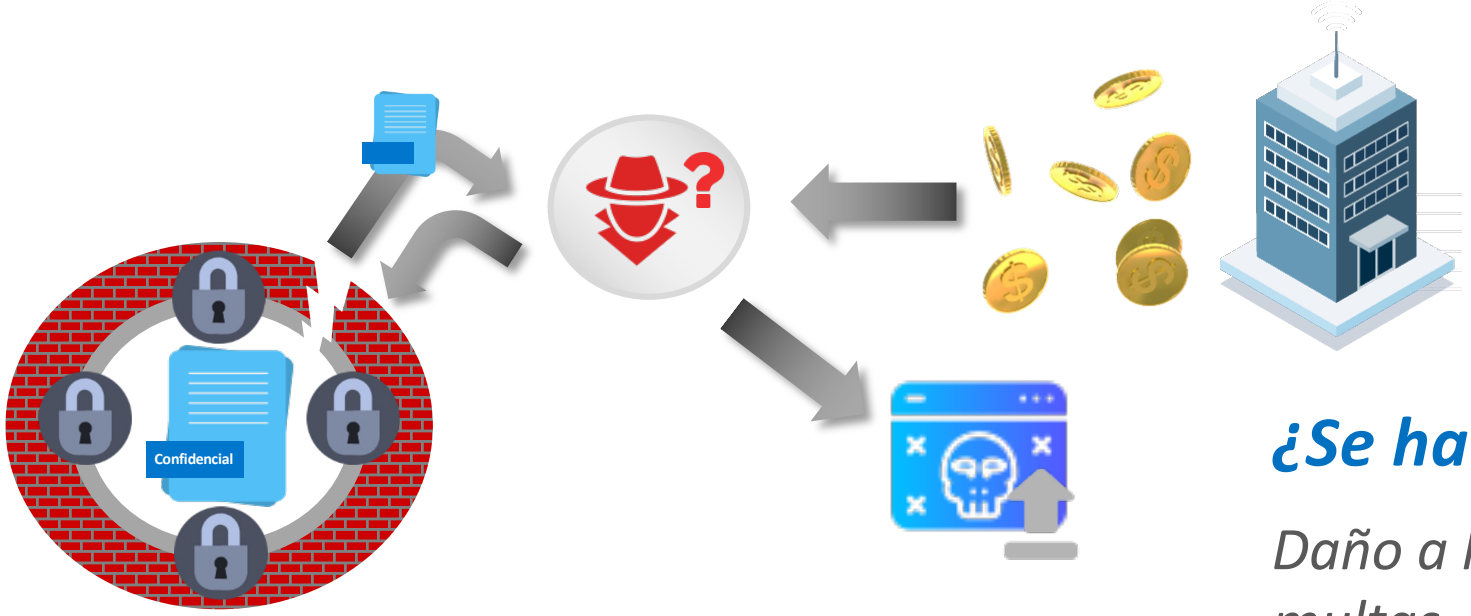
Priorizan los menos maduros en ciberseguridad-

Acceso

Compran cualquier tipo de acceso que les provean, comenzando por RDP y VPN.

sealpath

La doble Extorsión

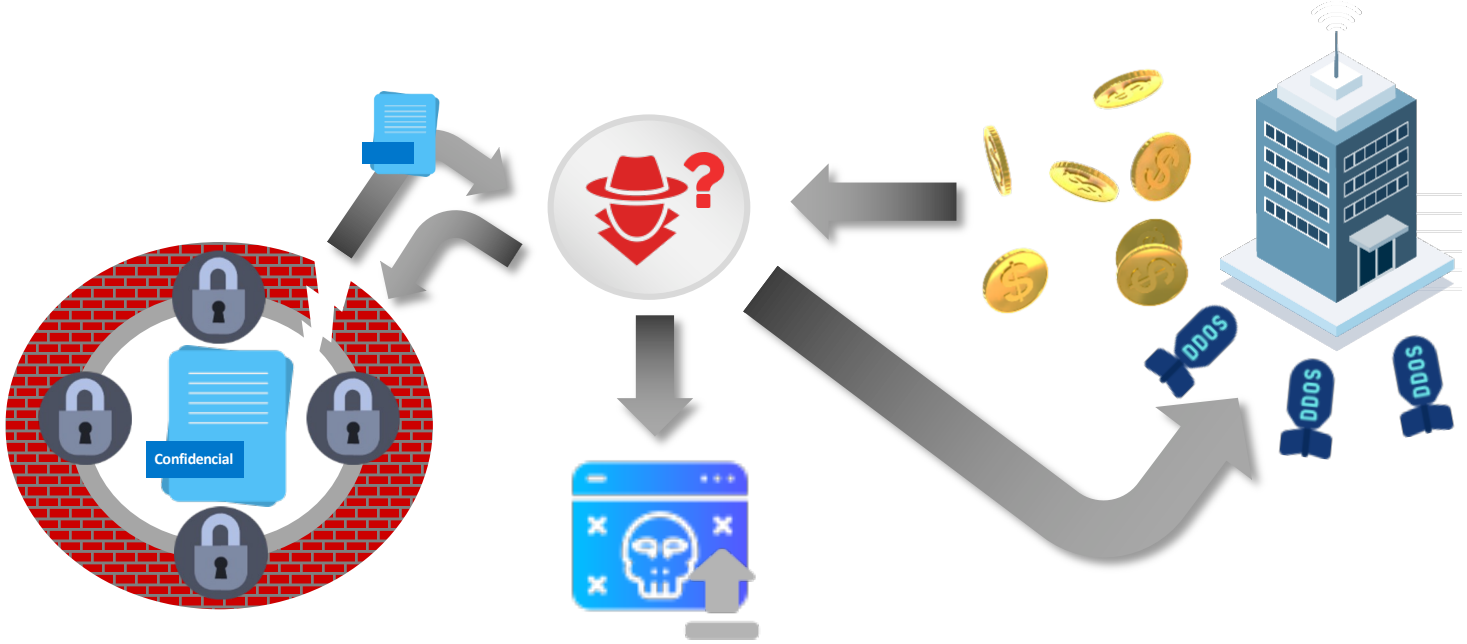


¿Se hace público?

Daño a la reputación, multas, pérdidas económicas…

sealpath

Incluso triple Extorsión



¿Te hago más daño?

-Ataques DDoS

-Ataques a terceros: Clientes, socios, proveedores…

sealpath

Y cuádruple

¿Te añado presión social?

Contactan con terceros asociados notificando que se niegan a pagar y los daños van a ser catastróficos para todos.

sealpath

Los Mega-ataques

Dirigidos a Proveedores de servicios Cloud

Aprovechan Vulnerabilidades Zero-day

1 ataque, cientos de empresas afectadas

Anatomía de un ataque

1. Acceso Inicial

Phishing y vulnerabilidades. Algunas conocidas otras compran en la dark web, ZeroDay.

2. Escalado de Privilegios

AD, Políticas de Grupo

*Mimikatz

3. Infiltración

Creación de cuentas, credenciales

*Cobalt Strike

4. Movimiento Lateral

phishing más interno

*IPScannner, Splashtop, Anydesk

5. Evaden las Defensas

Limpian los logs, desactivan EDRs y herramientas.

6. Recopilan los datos, extraen y despliegan

Crean paquetes de datos y los mandan fuera para luego cifrar.

*Rclone, Mega Upload

POLICÍA NACIONAL

Medidas para protegerse

enisa European Network and Information Security Agency

Cifrado

Evitas la extorsión por filtración.

Formación

Usuarios concienciados contra el phishing.

Backups

Completos y aislados para restaurar datos.

Patching

Tapar agujeros de acceso.

Controlar Accesos

Principio del Mínimo privilegio.

Monitorizar

Supervisión constante.

Detectar

Ser proactivos.

Plan IR

Establecer procedimientos.

Medidas para protegerse

Segmentación

Aislando contra la propagación.

End-points

Protección antimalware.

MFA

Una barrera más a la entrada.

Whitelisting

Para prevenir ejecución de apps no conocidas

Antiphising

Controles y herramientas.

Políticas

Políticas de Control y uso.

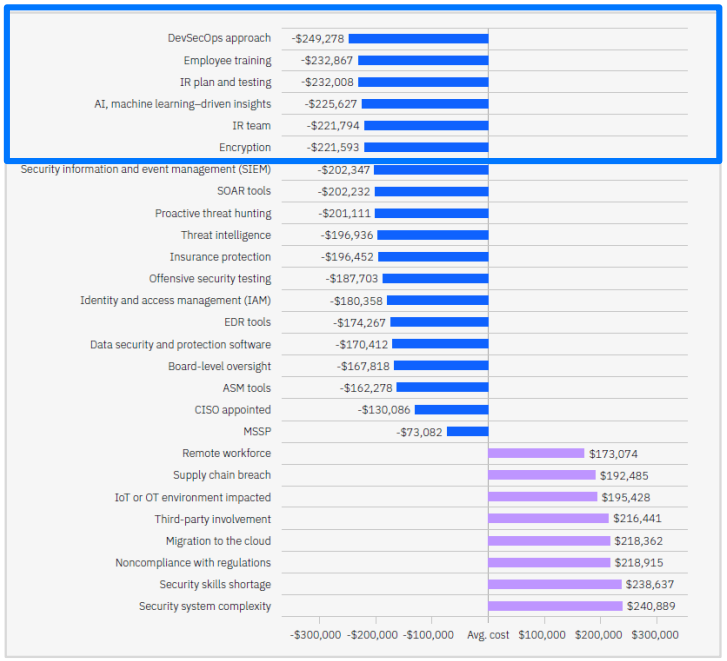
Email Security

Proteger emails y adjuntos.

Contraseñas

Fuertes y gestión segura.

¿Cómo mitigar el impacto?



Factores que mitigan el impacto

Formación de empleados, plan de respuesta a incidentes, uso de IA para detección, y uso del cifrado..

Plan IR

Formación

Cifrado

DevSecOps

IA

Equipo IR

...

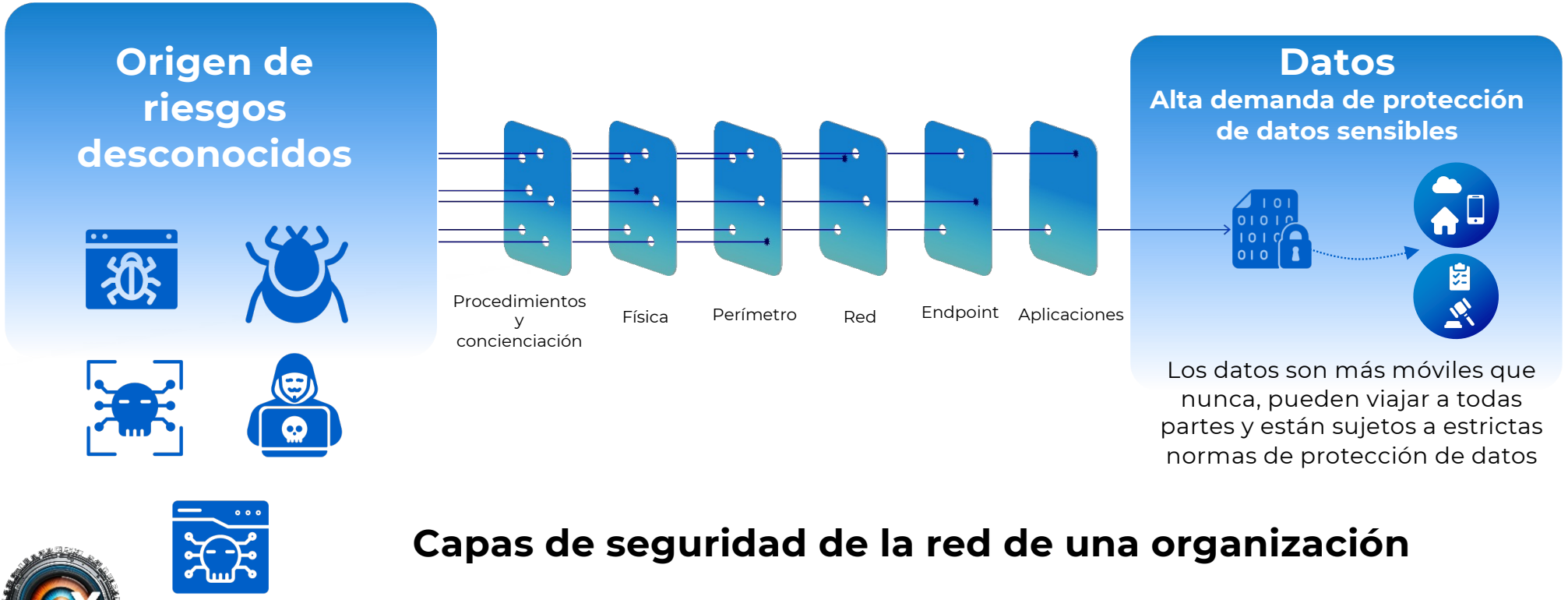
sealpath

El dato es lo más valioso

Su protección debe ser un pilar desde el que extender nuestras defensas

sealpath

Cuando atraviesan cada capa…



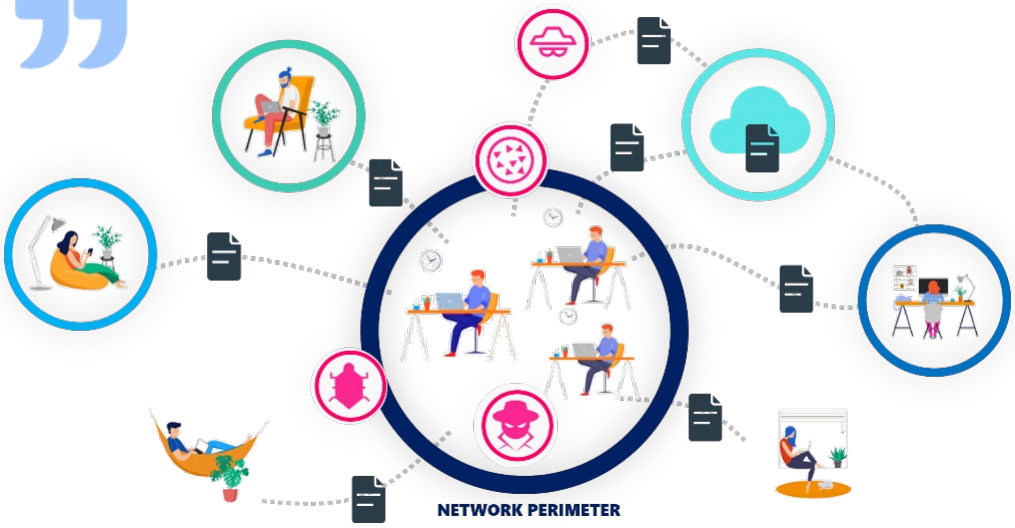
Capas de seguridad de la red de una organización

El papel de la protección del dato

No confíes en nadie, verifícalo todo
El perímetro de seguridad ya no existe.

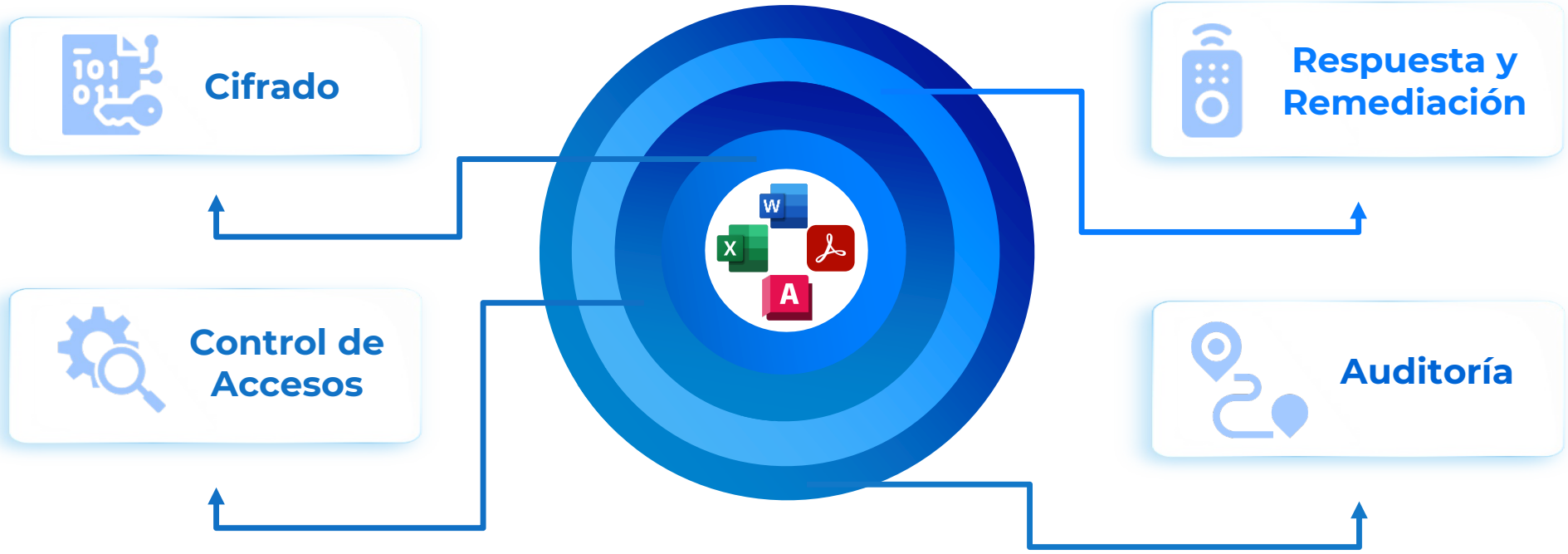
Principio del menor privilegio
Autenticación y autorización rigurosa antes de otorgar acceso a los recursos, independientemente de la ubicación.

Protección Persistente
Es necesario proteger el dato en sí, independientemente de la forma con la que se infiltren o accedan.



sealpath

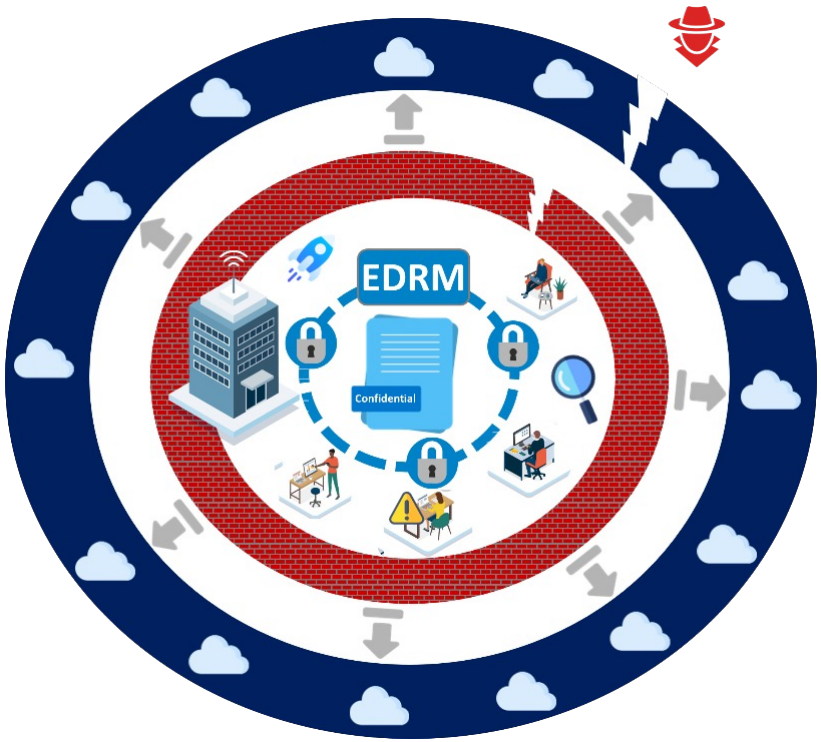
¿Cómo blindar el dato con IRM?



Protección centrada en el dato

Proteger dentro y fuera

No importa dónde viaje o se ubique el dato, la protección es persistente.



Auditar los accesos

Debemos mantener el control en todo momento para decidir quién accede.

Identificar a los usuarios

Todas las personas accediendo a los datos deben identificarse.

Responder y Revocar

Es necesario poder responder con rapidez y medidas correctoras para frenar el daño.

Protección del Dato VS Ransomware

Evita la Extorsión
Nadie puede acceder a la información aunque la publiquen.

Ayuda a detectar acciones sospechosas
La trazabilidad otorga visibilidad en tiempo real para respuesta temprana

Evita daños desde terceros
Ya sea un proveedor o un socio el que es atacado, tu información se mantiene a salvo.

Otorga capacidad de respuesta
Reaccionar ante eventos anómalos con rapidez minimiza el impacto.

Ejemplo real

Multinacional Europea Sector Metalúrgico
Ataque de Ransomware

1. Contacto

Contactan a la empresa para hacer saber que han cifrado información sensible y que paguen rescate por descifrarla.

2. Extorsión

Tenían backup y al decir que no pagan, amenazan con publicarla abiertamente.

3. Pruebas

Mandan una muestra para corroborar que tienen los datos en su poder y la criticidad de estos.

4. Validación

En las muestra de los datos que habían robado **vieron que estaba protegida y por tanto era inaccesible.**

Daño Mitigado

> **Prevenir el acceso no autorizado a los datos es crucial**
> Que no haya pasado no significa que estés a salvo

POLICÍA NACIONAL

+10 años ayudando a proteger la información de las organizaciones

Seguridad del Dato Avanzada
www.sealpath.com

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023
CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023
CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

Mejor empresa de Seguridad de Datos y Producto de Europa 2023

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

La mejor solución E-DRM 2022

2021 Computing Security Awards

Finalistas en 3 categorías 2022

Gartner

Nombrados en 2 ciclos hype y 1 investigación de Octubre 2022

kuppingercole ANALYSTS

Uno de los líderes de la colaboración segura por su informe de mercado

POLICÍA NACIONAL

200 1824 - 2024

CIBER WALL

sealpath™

CYBER X MIÉRCOLES