sealpath™

SMART PROTECTION FOR SENSITIVE DATA

Seguridad Centrada en los Datos en la Era de la Colaboración y el Teletrabajo

Luis Ángel del Valle
SealPath - CEO

¿Para qué invertimos en seguridad?

¿Para proteger la red?¿Equipos?

*Para proteger **nuestros datos**, en especial los más **sensibles***

¿Cómo perdemos nuestros datos más valiosos?

Algunos ejemplos reales

Empleado **ENFADADO EXTRAE COMO VENGANZA VARIOS TERAS** de información confidencial de la compañía.

- Se le había cambiado de puesto y estaba descontento.
- Información confidencial de I+D de la compañía.
- Datos de procesos de fabricación, datos financieros, etc.

¿Cómo perdemos nuestros datos más valiosos?

Algunos ejemplos reales

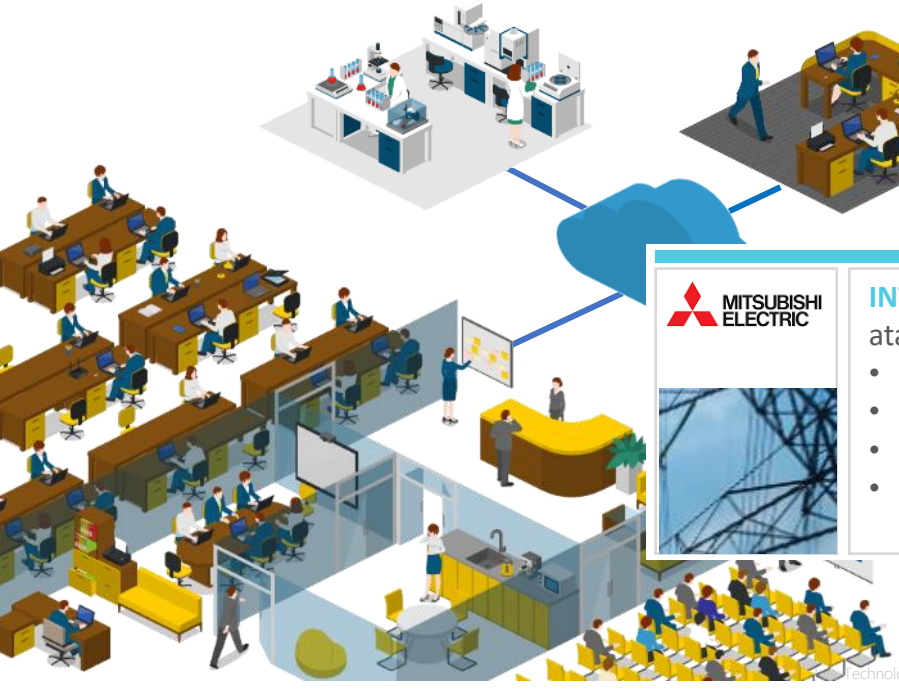
Anthem

Empleado de una **EMPRESA PARTNER EXTRAE INFORMACIÓN** con datos personales de pacientes:

- Anthem había hecho inversiones en seguridad por 230M$.
- Segunda empresa de seguros de salud en USA.
- La fuga tuvo origen en un partner con un nivel de seguridad débil.
- El empleado envió el fichero a su email personal.
- Impactó gravemente en LaunchPoint y en la reputación de Anthem.

¿Cómo perdemos nuestros datos más valiosos?

Algunos ejemplos reales



MITSUBISHI ELECTRIC

INTRUSIÓN QUE PASÓ DESAPERCIBIDA durante varios meses donde los atacantes extrajeron 200MB de ficheros confidenciales:

- Se comprometió la cuenta de un empleado.
- Los hackers ganaron acceso a las redes de 14 departamentos.
- Había ficheros con datos de 10 organizaciones de Gobierno.
- Información Técnica relevante de socios de negocio.

¿Cómo perdemos nuestros datos más valiosos?

Algunos ejemplos reales

Usuario **ENVIA POR ACCIDENTE UN EMAIL CON FICHERO CON DATOS SENSIBLES** a una lista de distribución errónea.

- Error humano sin intención maliciosa.
- Se expusieron datos de más de 21K personas.
- Números de la seguridad social, detalles bancarios, direcciones.
- Todo estaba incluido en adjuntos sin cifrar enviados en un email.

¿Cómo perdemos nuestros datos más valiosos?

Algunos ejemplos reales

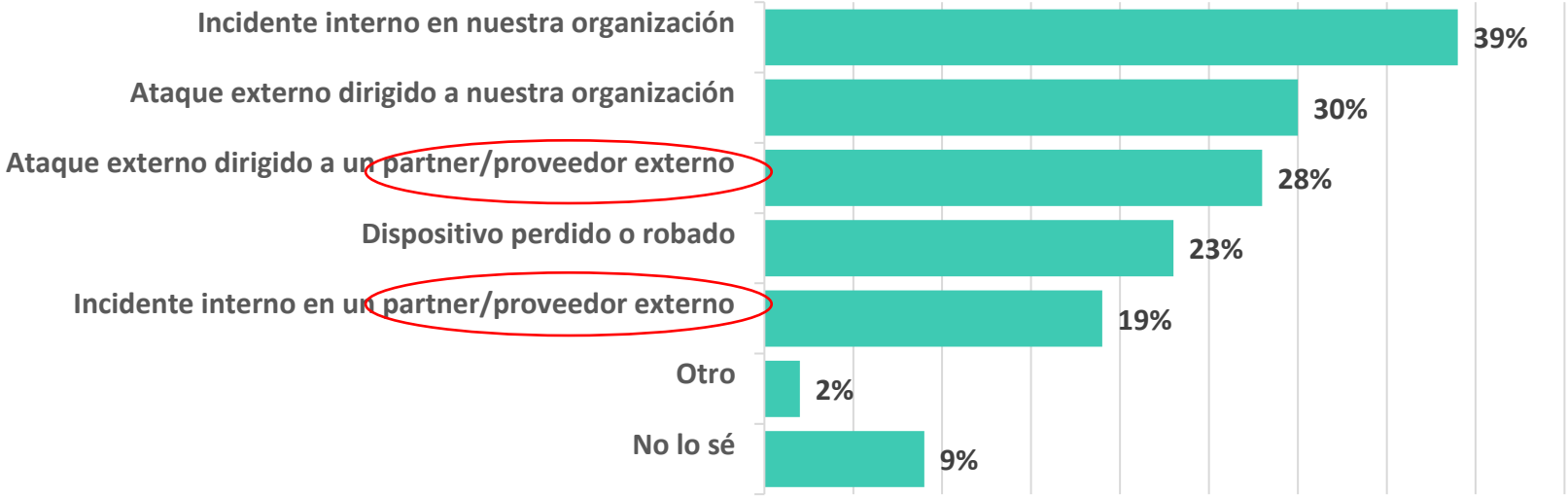
Empleado **DEJA LA EMPRESA Y SE LLEVA INFORMACIÓN** sobre tecnología de vehículos auto tripulados.

- Planos, PDFs confidenciales, videos, documentos.
- 14.000 ficheros descargados y copiados a disco externo.
- Funda empresa y la vende a Uber.
- Google había invertido 1,1 B$ en Waymo.

El coste se valoró en 245 M$

La fuga de datos puede darse en cualquier lugar

¿Cuál fue la forma común de fuga de información en los últimos 12 meses?



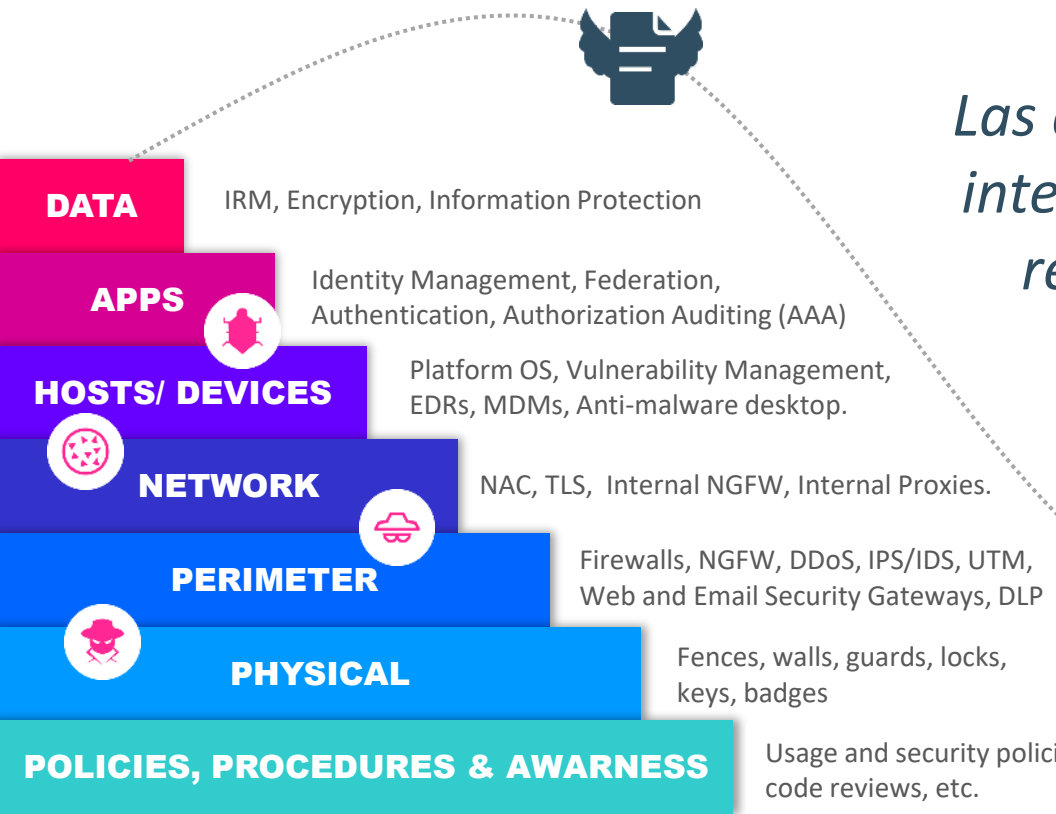
Fuente: Forrester's Global Business Technographics Security Survey

Base: 565 global network security decision-makers whose firms have had a security breach in the past 12 months

sealpath

Nos centramos en proteger las “capas”

Cuando lo importante son los datos… que son más móviles que nunca

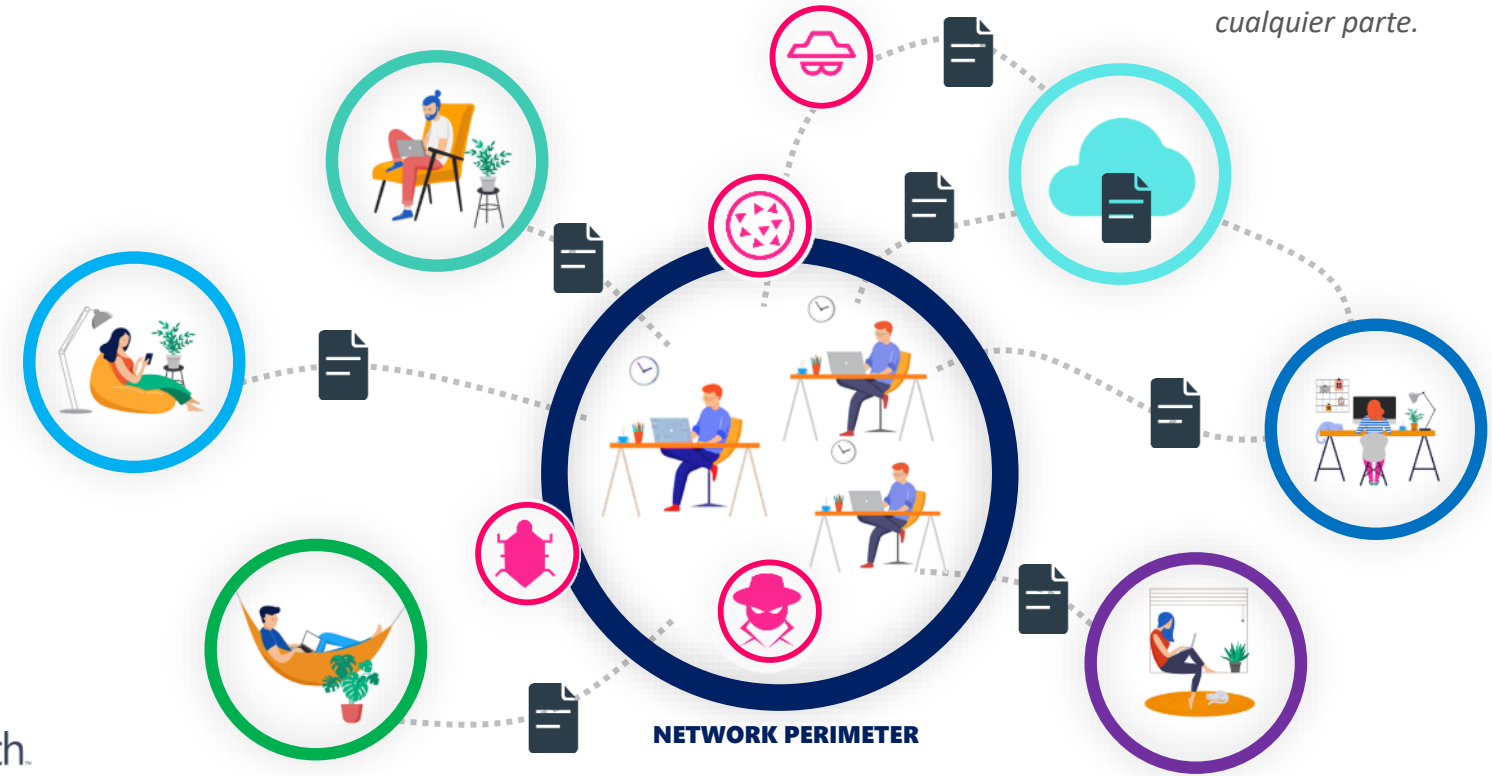


Las amenazas actúan ya desde el interior. ¿Y la nube y los usuarios remotos, proveedores, etc.?

¿Interno = Confiable y Externo = No Confiable?

El perímetro de la empresa ha desaparecido

*Explosión de la **colaboración Cloud Teletrabajo, BYOD**. Los datos en cualquier parte.*



sealpath

Extorsión por publicación de datos

El problema del ransomware

El ransomware ya no sólo cifra y pide rescate. Extrae datos no cifrados y extorsiona con hacerlos públicos.

"Solo en el 2.2% de las fugas de datos se utilizó el cifrado y los datos extraídos fueron ilegibles" (*)

BLEEPINGCOMPUTER

NEWS ▾ DOWNLOADS ▾ VIRUS REMOVAL GUIDES ▾ TUTORIALS ▾ DEALS ▾

Home > News > Security > New Jersey hospital paid ransomware gang $670K to prevent data leak

New Jersey hospital paid ransomware gang $670K to prevent data leak

By Lawrence Abrams — October 3, 2020 — 10:15 AM — 2

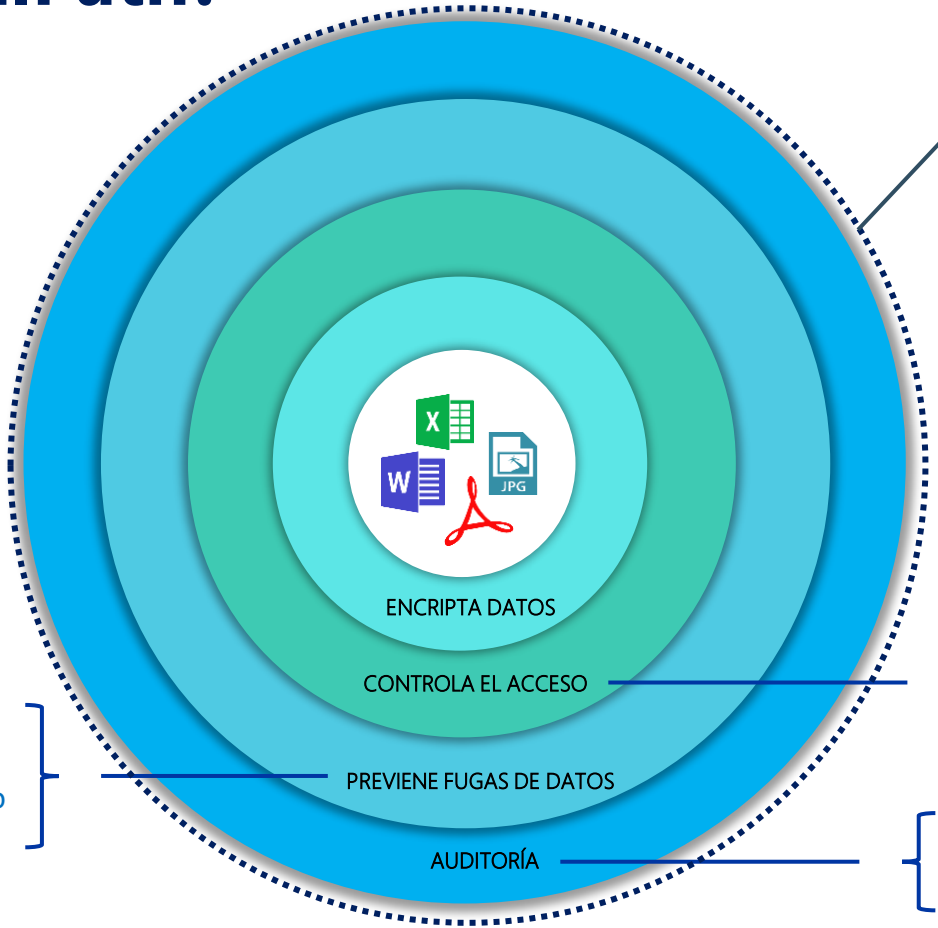
University Hospital New Jersey in Newark, New Jersey, paid a $670,000 ransomware demand this month to prevent the publishing of 240 GB of stolen data, including patient info.

The attack on the hospital occurred in early September by a ransomware operation known as SunCrypt, who infiltrates a network, steals unencrypted files, and then encrypts all of the data.

¿Qué es SealPath?

*SealPath **protege** tus documentos y te permite **controlarlos** en remoto*

¿Qué es SealPath?



Integridad de la comunicación

Quién accede
Con qué permisos (ver, editar, imprimir, etc.)

Se puede destruir el documento en remoto

Accesos, intentos de acceso bloqueados, etc.

sealpath

www.sealpath.com

Protección basada en Círculos de Confianza

Colaboración segura y controla dentro del Círculo de Confianza

sealpath

Colaboración Segura

Con protección que viaja con el fichero

TRANSFERENCIA SEGURA

Se evita el anonimato.
Se identifica al emisor.
Cifrado extremo a extremo

COMPARTICIÓN SEGURA

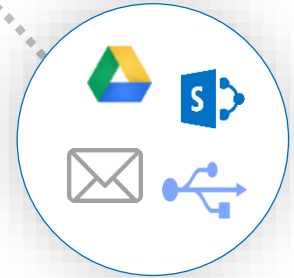
Permisos por usuario.
Tracking de accesos.
Posibilidad de revocación

EDICIÓN SEGURA

Posibilidad de Edición.
Nivel de Colaboración
controlado en tiempo real.

¿Cómo funciona?

1. Protege cualquier archivo



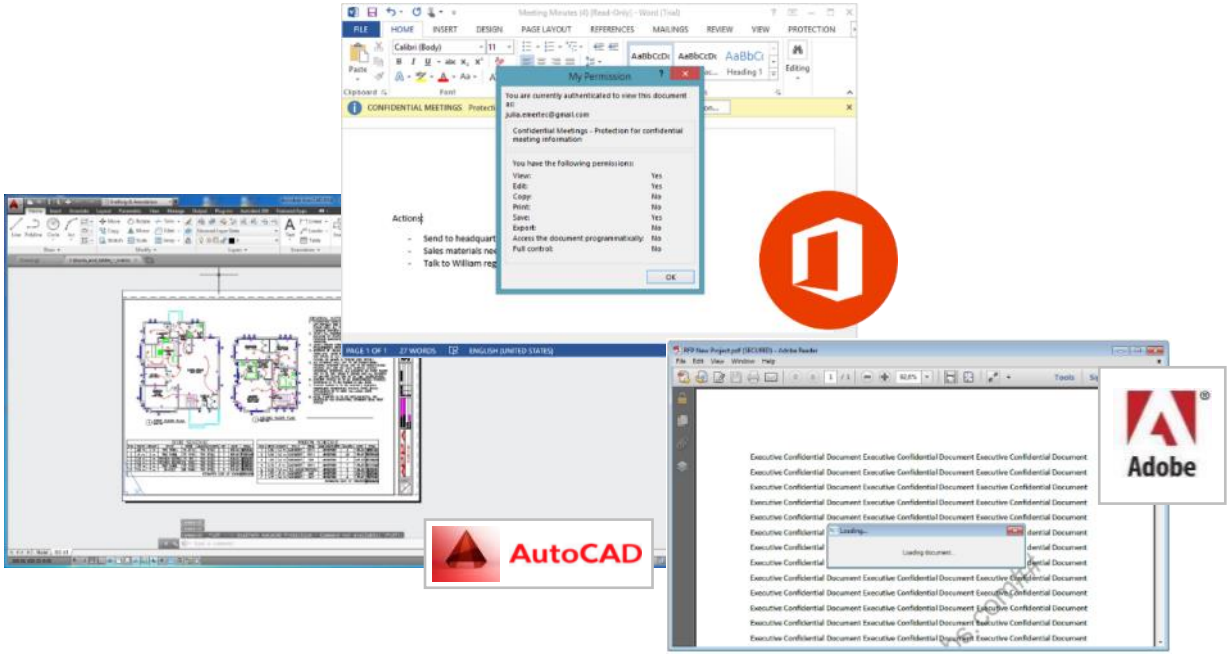
2. Compártelo como quieras

3. Usa tus herramientas habituales

4. Monitorización & Control

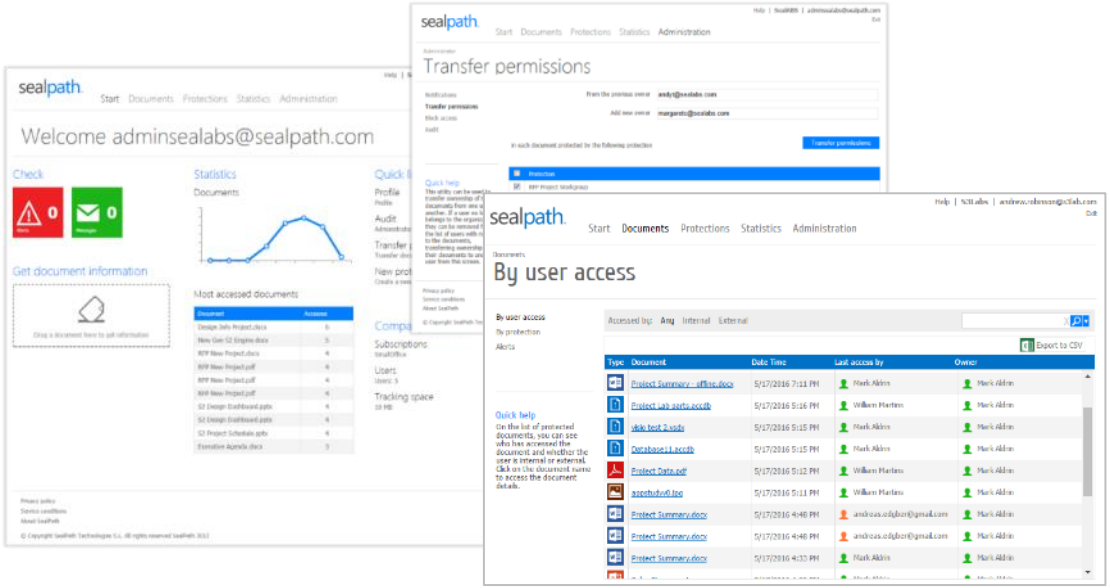
Facilidad de uso

Usa tus herramientas habituales, sin agentes



Facilidad de gestión

Políticas flexibles, control y auditoría



Despliegue

DOS OPCIONES

pueden ser instaladas

On-Premise

Cloud/SaaS

Ambas pueden ser integradas con AD/LDAP
Un cliente de protección es instalado en Desktop o en File Servers

SealPath no almacena documentos. Solo los protege

Automatización de la Protección

Ciclo de Gestión Segura de Información

Recomendación para trabajar con información

Extender una cultura de protección dentro de la organización.

Sobre SealPath

+20 Países *100% Orientación al Canal* *Fuerte Enfoque en I+D*

Algunos Clientes

SIEMENS Gamesa RENEWABLE ENERGY · ferrovial · Claro · Dietsmann Maintaining Energy · codere · PRODIEL · LOEWE · navarra.es

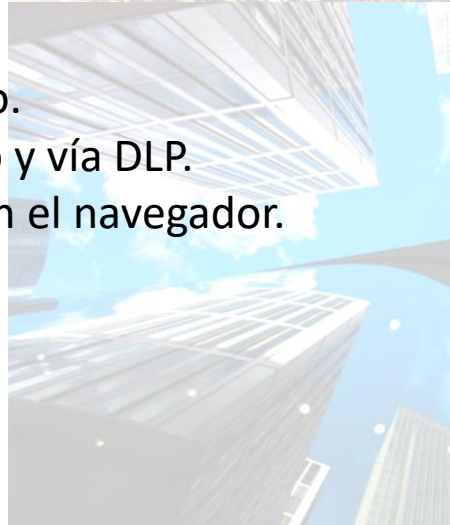
Allianzas Integraciones

FORCEPOINT · McAfee · Symantec. · boldonjames A QinetiQ Company · AUTODESK.

¿Cómo lo utilizan nuestros clientes?

MULTINACIONAL – SECTOR ENERGÍA

- Necesidad de proteger y controlar información técnica interna y de clientes.
- La información se protege de forma automática en repositorios de información.
- Se ha integrado SealPath con aplicaciones internas de ERP/RRHH.
- Disponen de una auditoría exhaustiva de accesos y posibilidad de revocar accesos.



BANCO INTERNACIONAL DE INVERSIÓN

- Necesidad de protección de información financiera y medios de pago.
- Protección automática vía email en función del contenido del fichero y vía DLP.
- Protección de información en SharePoint y posibilidad de apertura en el navegador.
- Los usuarios externos no necesitan instalar software en sus equipos.

Ver casos de éxito publicados en www.sealpath.com

sealpath

La estrategia de protección de SealPath

Protección y control para cualquier formato y aplicación, en cualquier lugar

Multi-plataforma, Sin agentes, Integración con servicios Cloud

Análisis de contexto y comportamiento, Detección de Nivel de Riesgo

sealpath

PROTECCIÓN INTELIGENTE PARA TUS DATOS
Y
COLABORACIÓN SEGURA

Gracias