DOCUMENTOS SIC
Nº 36
JUNIO 2022

STORMSHIELD

# Tecnologías de ciberseguridad ‘Made in EU’ para construir soberanía digital

- Especialización, innovación, cualificación y certificación de productos y servicios
- Protección avanzada, multicapa y proactiva para *endpoints*, redes y datos
- Un socio cercano de seguridad IT-OT en los procesos de transformación digital

ENTREVISTA

**Borja Pérez**
Country Manager de Stormshield Iberia

STORMSHIELD

## Subsidiaria del Grupo Airbus, se erige como uno de los referentes en protección

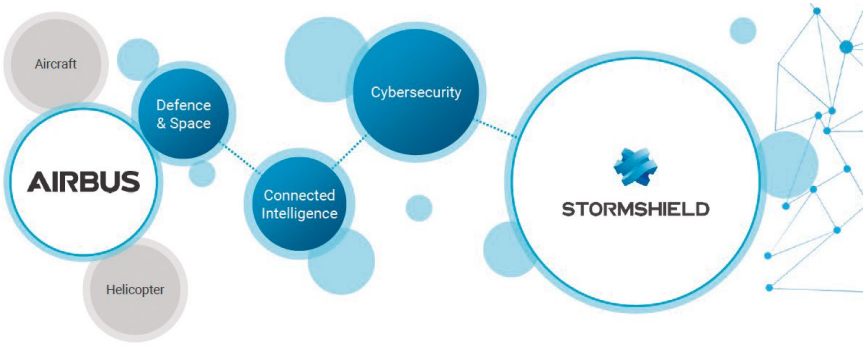
# Stormshield: ciberseguridad robusta y certificada para construir la soberanía digital europea

Fundada hace menos de una década, Stormshield tiene, sin embargo, más de 20 años de experiencia a sus espaldas. Actor destacado dentro del negocio de ciberseguridad de uno de los grupos industriales más importantes en Europa, Airbus, la compañía no ha parado de crecer apostando por una estrategia basada en la innovación, certificación y cualificación de productos y servicios, así como con alianzas con los referentes en diferentes ámbitos de la ciberprotección. Fruto de su buen hacer, en 2021, registró en Iberia sus mejores resultados. Entre sus grandes valores diferenciales destaca su gran especialización en IT y OT, la robustez de sus soluciones y la proximidad al cliente.

Pocas empresas representan tanto y tan bien la aspiración europea de contar con soberanía digital, también en ciberseguridad, como **Stormshield**. La multinacional, propiedad del **Grupo Airbus,** y a la que le gusta definirse como "socio europeo de confianza", se ha consolidado en menos de una década como uno de los referentes en protección de infraestructuras críticas, datos sensibles y entornos operativos, tanto en IT como en OT. "A medida que nuestra sociedad se digitaliza, las consideraciones geopolíticas se convierten en criterios para elegir proveedores de soluciones de ciberseguridad. Y Europa, por tanto, tiene un papel esencial que desempeñar: el de ofrecer soluciones fiables y transparentes", recuerdan desde la compañía.
Tras comenzar a vender sus primeras soluciones en 2014, fruto de la fusión de dos compañías galas, **Arkoon** y **Netasq**, actualmente está presente en sectores como el de Defensa, Salud, Administraciones Públicas, Industria o en el sector hídrico, entre otros, en más de 40 países. Además, cuenta con equipos dedicados e instalaciones en Francia, España, Alemania, Italia, Oriente Medio y Polonia, una expansión internacional a la que ha contribuido, de forma notable, la calidad de sus productos y servicios, fruto de su constante apuesta por la innovación.
Y es que Stormshield basa su propuesta en la oferta de capacidades con la cercanía al cliente y con la seguridad más avanzada, tanto para infraestructura de red, como para punto final y protección de datos. Así, su valor diferencial es una solución global que cumple con los requisitos de los diferentes entornos que deben protegerse, avalados por las certificaciones más globales (CC), las de más alto nivel en los estados de la UE y las de la OTAN, entre otras.
A su tecnología de última generación se suma una plantilla de alrededor de 400 especialistas, que comparten una cultura basada en tres pilares que marcan el trabajo en el día a día: tener siempre al 'cliente en el centro', apostar por un trabajo 'colaborativo de éxito' y hacerlo para 'generar confianza'. Algo muy importante teniendo en cuenta el crecimiento de la Industria 4.0, y la convergencia e hiperconexión de los entornos IT y OT, hechos que incrementan las superficies de ataque.
Esto es especialmente preocupante en servicios esenciales, donde los riesgos no ponen en peligro únicamente a los datos y a los dispositivos informáticos sino que, además, hacen peligrar la seguridad de activos y personas e, incluso, pueden llegar a afectar la estabilidad de las instituciones y las economías.
Por ello, Stormshield ha centrado su foco de negocio en los sectores más sensibles (redes críticas), a través de una oferta integral que combina tecnología de protección (punto final, redes, datos y seguridad industrial), así como servicios de integración y experiencia sectorial, con lo que busca ser un "socio perfecto para diseñar un plan maestro de desarrollo en la ciberseguridad de las compañías".

### Apuesta por la ciberserenidad

Stormshield quiere destacar por su compromiso con la excelencia en ciberprotección, que también se plasma en su apuesta por un proceso continuo de certificación y cualificación de sus productos y servicios. Este marco de trabajo incluye, en particular, una auditoría de sus códigos fuente y sus entornos de desarrollo para ofrecer transparencia real y máxima confianza.
A esta estrategia se suma su foco en responder a las inquietudes del cliente a través de la "comprensión de sus necesidades, una relación de cercanía y la capacidad para responder" en el momento y con la "excelencia" en lo que se precise. "Nuestra ambición no



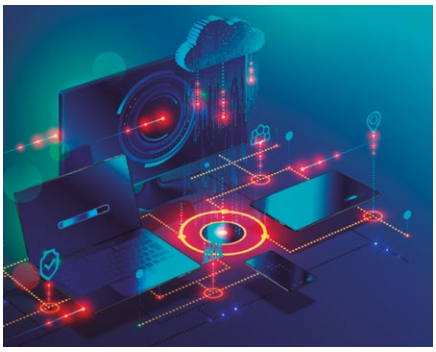

**A su tecnología certificada y de última generación se suma una plantilla de más de 400 especialistas que comparten una cultura basada en tres pilares: tener siempre al 'cliente en el centro', apostar por un trabajo 'colaborativo de éxito' y hacerlo para "generar confianza".**

es convertirnos en una criatura legendaria de un solo cuerno –explican con cierta ironía–, sino llevar, cada vez más, la 'ciberserenidad' a nuestros clientes" y permitir que sus colaboradores crezcan y puedan ayudar a desarrollar el 'ecosistema Stormshield'.

### Inteligencia de calidad y fuertes alianzas

"En el complejo, heterogéneo y multifacético entorno actual de las ciberamenazas, la información es un elemento crucial de la ciberdefensa. A través de nuestras soluciones UTM y EPP/EDR, participamos activamente en el ecosistema de protección", explica el responsable Técnico de Stormshield Iberia, **Antonio Martínez**, quien también destaca la reciente creación del 'Portal de Seguridad de Stormshield' para "informar mejor a socios y clientes sobre el nivel de cobertura que ofrecen sus productos ante una determinada ciberamenaza".

En la empresa resaltan que "compartir y cooperar son armas esenciales en la lucha contra el cibercrimen", que ya ha creado una 'economía paralela', según destaca el Director de Producto de Seguridad de Stormshield, **Sébastien Viou,** alertando de que este negocio delictivo ya mueve más de 1.400 millones de euros al año, una amenaza para la que es más necesaria que nunca la cooperación entre los diferentes actores del ecosistema de ciberseguridad, aspecto que la compañía tiene muy claro al apostar por la suma de fuerzas con otros actores destacados para desarrollar soluciones conjuntas, compartir información sobre amenazas, mejorar colectivamente las defensas de sus clientes y avanzar en el estado del arte para, además, "incorporar componentes de alto valor en productos y soluciones".



Así, a sus sinergias lógicas con **Airbus CyberSecurity,** el área de ciberprotección del gigante europeo, con casi 1.000 profesionales y muy presente en Defensa y Seguridad, se suman alianzas significativas con grandes referentes, como **Schneider Electric, Google, Nozomi Networks, TheGreenBow** o **LogPoint**, entre otras. Estos acuerdos permiten a la compañía cubrir las distintas y crecientes necesidades de los sistemas de información (incluidos los de misión crítica) de las empresas más destacadas en cada sector.

### Un canal de calidad

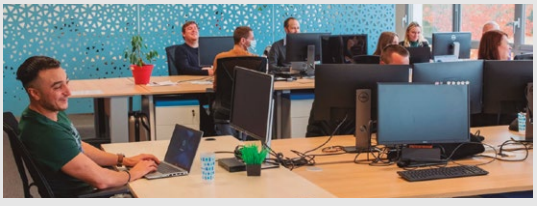
Para llegar al cliente, Stormshield también cuenta a nivel mundial con una amplia red de cerca de un millar de *partners* certificados, con el reto de "trabajar juntos para desarrollar ofertas de seguridad más sencillas y fiables". Y es que parte de su éxito es fruto de su enfoque "basado en las relaciones cercanas", destaca su CEO, **Pierre-Yves Hentzen**, quien recuerda que las iniciativas que se llevan a cabo a través de los *partners* "dan vida a nuestro lema: Piensa globalmente, actúa localmente".

Buena prueba de ello es su estrategia en Iberia donde la compañía registró en 2021 un notable crecimiento, consolidando uno de los mejores ejercicios de su historia. Un éxito al que también ha contribuido su programa Partner Connect, con un centenar de socios entre ellos destacados mayoristas como **Tech Data,** una compañía de **TD Synnex,** e **Ireo** –adquirida en 2021 por **Also**–, donde "prima la calidad más que la cantidad", explica el Country Manager para Iberia de Stormshield, **Borja Pérez.**

En el último año, su buena salud se ha basado en el crecimiento de la demanda de todas las líneas de productos, principalmente de las herramientas de seguridad perimetral y de red, así como de sus soluciones de seguridad para aquellas organizaciones con infraestructuras sensibles y que ha permitido a la filial española acometer, además, proyectos de muy alto valor. ●

## Un camino de éxito marcado por la innovación

La innovación ha marcado la estrategia de la compañía con numerosos equipos dedicados a la I+D+i en constante crecimiento. Arkoon**,** fundada en 1998, creó el primer cortafuegos con IPS integrado y Netasq, la primera solución UTM tras implementar una solución de anti*malware* en sus cajas de *firewall*. A estas capacidades se sumaron las de cifrado de archivos –tras adquirir **MSI** en 2006– dando lugar a lo



que es hoy Stormshield Data Security, y la de protección de servidores y estaciones de trabajo tras comprar, en 2009, **SkyRecon Systems,** plasmándose en lo que actualmente es Stormshield Endpoint Security. Así, actualmente, más de la mitad de los empleados de la compañía, en torno a 250 de casi 400, están dedicados a I+D+i en sus instalaciones de Paris, Lyon y Lille. Con ello se pretende "mejorar y facilitar la gestión de la seguridad de las infraestructuras IT y OT utilizando nuevos paradigmas y marcos".

## La certificación y cualificación, una constante en la compañía

La confianza en las soluciones de protección y seguridad de los sistemas de información es uno de los grandes valores diferenciales de Stormshield. Para ello, la multinacional lleva más de 20 años apostando por la certificación y cualificación desde que los primeros productos de Arkoon y Netasq recibieron la certificación Common Criteria por la **Agencia de Ciberseguridad de Francia** (ANSSI). Se trata de una estrategia en la que prima el "proceso continuo de cualificación y certificación de seguridad con las autoridades europeas competentes". Así, actualmente el portafolio de la compañía dispone de certificaciones como 'OTAN Restricted', 'EU Restricted', 'Common Criteria', en niveles EAL3 y EAL4+, así como el sello 'Made in Europe', de la **ECSO.** Además, en España ha obtenido la calificación 'Producto **CCN** Aprobado' y 'Producto CCN Cualificado' para sus soluciones Stormshield Network Security. A ello se suma que, en Francia, también ha obtenido las denominadas 'Visas de Sécurité', creadas en 2018 por la ANSSI.

# Borja Pérez,

## Country Manager de Stormshield Iberia

**Desde su llegada a Stormshield Iberia, hace un lustro, Borja Pérez ha consolidado la compañía en un mercado en el que, en 2021, ha vuelto a lograr sus mejores resultados. Gran conocedor del panorama español de ciberseguridad, desvela en esta entrevista los retos y las novedades que marcarán el corto y medio plazo de la compañía, en busca de convertirse en la gran alternativa europea para la protección de los servicios esenciales y los entornos críticos, bajo el aval del Grupo Airbus. De hecho, también aspira ser un agente destacado en la Red Nacional de SOC.**

# "Queremos que el mercado nos perciba como la alternativa tecnológica europea para los proyectos de ciberseguridad"

**– ¿Qué define a Stormshield Iberia y cuáles son sus grandes retos de negocio a corto plazo?**

– Stormshield posee en Iberia un equipo muy experto, con un gran conocimiento de todos los aspectos del mercado de ciberseguridad. Hemos tenido un crecimiento continuo desde que la compañía empezara a operar bajo esa marca, aunque no comenzamos de cero, sino que ya había actividad a través de una de las empresas que se adquirieron para la creación Stormshield. Nuestro principal reto es que el mercado piense en nosotros como la alternativa europea en cualquier proyecto de ciberseguridad.

**– Su portafolio se divide en tres grandes áreas de protección: para redes, datos y *endpoints*. ¿Qué marca la diferencia? Y, ¿qué propuesta posee para mitigar ataques cada vez más sofisticados y peligrosos?**

– Stormshield hace especial hincapié en la certificación por organismos internacionales de todas sus soluciones. El proceso que se sigue cada vez que se lanza un nuevo producto o versión del mismo es obtener las de Common Criteria, para después conseguir certificaciones nacionales, como las del ANSSI en Francia, el CCN en España, o internacionales, como NATO Restricted o EU Restricted. En este punto cabe destacar que, a fecha de hoy, el único *firewall* con el sello de producto aprobado por el CCN es el de Stormshield.

Otro aspecto clave para nosotros es la seguridad de nuestro propio producto. Primamos la robustez de cada componente del mismo sobre la incorporación de nuevas funcionalidades que no tengan una demanda clara. En ese sentido, es importante saber que el código fuente de nuestros productos ha sido auditado por terceros para garantizar que no existen vulnerabilidades como puertas traseras.

**– Además de las certificaciones obtenidas, ¿tienen previsto acometer más y en qué soluciones?**

– Nuestro objetivo es mantener todas las líneas de producto con el máximo nivel de certificaciones del mercado y estamos intentando, por todos los medios, conseguir que se valoren estas certificaciones. Todavía vemos muchos pliegos de concursos públicos en los que no se requieren certificaciones del CCN y sí otro tipo de calificaciones de analistas que en muchos casos no miden capacidades técnicas.

**– ¿Cuál es la aproximación de la compañía al mercado ibérico?**

– Como muchos fabricantes de TI, seguimos un modelo de negocio 100% canal. Contamos con un número limitado de *partners* de distintos tamaños y coberturas geográficas, pero todos ellos con una gran especialización en ciberseguridad. Desde grandes integradores, como Indra o GMV, que acometen proyectos en Defensa o en el sector Aeroespacial, hasta *partners* locales que conocen perfectamente el negocio regional y actúan de facto como el departamento de ciberseguridad de sus clientes.

**– La compañía destaca también por su gran especialización en entornos industriales, ICs y servicios esenciales…**

– Sí. De hecho, hemos codesarrollado parte del *firmware* de nuestros equipos junto a Schneider. Esto nos ha aportado dos grandes ventajas. Por un lado, un conocimiento profundo de los protocolos industriales, siendo capaces de realizar DPI (Deep Protocol Inspection) de un gran número de ellos. Y, por otro, nos permite presentarnos ante responsables de redes OT con el aval de un fabricante de equipamiento industrial referente a nivel mundial, lo que elimina alguna reticencia a la hora de incluir

equipamiento desconocido para ellos en su red.

**– Stormshield forma parte de Airbus, uno de los mayores grupos industriales europeos con una notable área de negocio de ciberseguridad. ¿Qué comparten ambas y qué aporta su relación a los clientes?**

– Efectivamente, Airbus Cybersecurity es dueña del 100% de Stormshield, por lo que podríamos decir que compartimos todo. No obstante, somos una empresa autónoma en cuanto a estrategia de mercado, lo que quiere decir que ni desarrollamos específicamente para el grupo, ni tenemos que ser obligatoriamente proveedor del grupo en cada proyecto. Por poner un par de ejemplos, nosotros utilizamos los *cyber range* de Airbus CyberSecurity para nuestra formación y la de nuestros *partners*, y nuestras soluciones de *sandboxing* (Breach Fighter) y ciberinteligencia, emplean *feeds* de Airbus CyberSecurity. A su vez, Airbus CyberSecurity adopta nuestras soluciones en sus SOCs, actuando como integrador de las mismas en proyectos en instituciones europeas; y Airbus Defence and Space monta *firewalls* de Stormshield en algunos modelos.

El grupo Connected Intelligence, de Airbus, en el que estamos junto a otras empresas como Airbus SLC (redes Tetra), está ganando peso dentro del grupo porque todo lo relacionado con la ciberseguridad y la ciberdefensa va adquiriendo una importancia vital para cualquier país.

**– En concreto, ¿qué propuesta hace la compañía en Defensa y Administración Pública, sectores donde es un referente en países como Francia?**

– Son nuestros principales mercados a nivel global y también empiezan a crecer en España. Hay dos valores fundamentales para esos dos mercados: soberanía y certificaciones. En muchas de las líneas de producto somos los únicos o de los pocos actores europeos del mercado. Cualquier organismo preocupado por cuestiones geopolíticas entiende que esto es clave. Y si hablamos, por ejemplo, de doble barrera de *firewall*, como requiere el ENS en su nivel alto, es muy buena idea colocar una de ellas de origen europeo.

En cuanto a las certificaciones, ya he comentado anteriormente su importancia para Stormshield. De hecho, además de obtener las certificaciones nacionales, colaboramos con ENISA, siendo uno de los dos únicos fabricantes en la elaboración de los nuevos estándares de certificación europeos.

**– ¿Qué opina sobre el desarrollo del Esquema de Certificación europeo de productos y servicios y procesos TIC?**

– Creo que es muy importante que en un futuro podamos certificar un producto de ciberseguridad, por ejemplo, en el CCN, y que esa certificación sea válida en toda Europa. Aunque es cierto que el trabajo que se realiza para certificar un producto en un país es reutilizable en otro proceso similar, no deja de suponer tener que realizar múltiples certificaciones nacionales, lo que conlleva numerosas horas de trabajo de muchas personas.

**– Stormshield posee una potente área de I+D+i. ¿Cómo se plasma en su propuesta tecnológica?**

– Más de la mitad de la plantilla de Stormshield trabaja en I+D+i. Y aunque somos una compañía relativamente pequeña en número de empleados, ese porcentaje de ingenieros nos permite realizar desarrollos muy punteros. Se hace especial foco en la robustez y la seguridad de los productos, lo que los convierte en idóneos para redes y datos críticos de cualquier cliente.

**– Nuestro país está trabajando para contar con una Red Nacional de SOC (RNS) en la que será decisiva la colaboración público-privada. ¿Qué opinión le merece?**

– Queremos apoyarla, además de con nuestra tecnología, con nuestra experiencia con otros CERT y SOC, tanto de instituciones públicas como de organizaciones privadas, o del propio Grupo Airbus. Como ejemplo de colaboración con la comunidad de ciberseguridad, tenemos nuestro nuevo portal de seguridad en el que compartimos información sobre CVE o reputación de redes IP, por mencionar dos tipos.

**– ¿Qué define su política de alianzas con los fabricantes de tecnología?**

– Entendemos que es fundamental mantener una política de alianzas y de integraciones con otros fabricantes para poder ofrecer los máximos niveles de seguridad. Y estamos en constante búsqueda de componentes de alto valor que complementen nuestras soluciones. Por el origen de la compañía, es más fácil que exploremos alianzas con compañías europeas, como es el caso de LogPoint (SIEM) o The Green Bow (clientes VPN con las máximas certificaciones de seguridad); pero nos integramos con todo tipo de soluciones, como QRadar de IBM, Nozomi o la ya mencionada Schneider.

**– ¿Cuáles son los proyectos más destacados en los que participa Stormshield en España ya sea por su alcance o por su singularidad?**

– Un buen ejemplo de los proyectos en los que participa Stormshield es el programa Galileo de la ESA, en el que trabajamos con GMV proporcionando *firewalls* para las estaciones de control y seguimiento. Otra referencia muy importante para nosotros es Acciona, donde protegemos puestos de trabajo de empleados en todo el mundo y a la que hemos protegido frente a ataques de *ransomware* que sí han afectado a otras empresas de su entorno o tamaño. Y un tercero, que ha sido muy interesante, porque de él, y a petición del cliente, ha salido un nuevo producto. Se trata de un operador español que buscaba un *feed* de ciberinteligencia europeo y nos pidió su desarrollo. Basándonos en Breach Fighter, nuestra solución de *sandboxing* en la nube, hemos generado una solución que está siendo utilizada por clientes en todo el mundo. ●

**“La seguridad es un aspecto clave para Stormshield en el desarrollo de productos: siempre primamos la robustez del conjunto y de cada componente sobre la incorporación de nuevas funcionalidades sin demanda clara”**

## Tecnología de ciberprotección avanzada, multicapa y confiable

# Seguridad de red, puntos finales y cifrado de extremo a extremo para entornos IT, OT y convergentes

Desde sus orígenes, la especialización en la protección de los sectores que manejan datos sensibles ha sido el eje vertebrador del desarrollo de las soluciones que ofrece Stormshield. Junto a ello, la integridad de sus productos, auditados de forma regular, y el respaldo de calificaciones, certificaciones y cualificaciones de organismos internacionales, también están presentes en su apuesta por crear un fuerte vínculo de 'ciberconfianza' con sus clientes.

El incremento del número y virulencia de los ataques está poniendo a prueba las defensas, especialmente las de los proveedores de servicios esenciales y las cadenas de suministro. Sólo en el último año, los incidentes por *phishing* han aumentado un 30%, según el informe 'Phishing Attack Landscape' y, en el caso del *ransomware,* la situación es aún más preocupante. En este frente, España ocupa la tercera posición mundial de países con mayores pérdidas por esta razón –casi 500 millones de euros–, sólo por detrás de Estados Unidos y Francia, según datos de Emsisoft.

La orientación al desarrollo de soluciones robustas de seguridad digital (IT/OT/IoT), que guían la estrategia de Stormshield, alcanza hoy una especial relevancia porque en el contexto geopolítico actual, cualquier organización puede ser objetivo: estados, administraciones públicas, servicios esenciales, empresas estratégicas y cadena de suministro.

Para mitigar el riesgo, Stormshield dispone de un conjunto de soluciones orientadas en IT a la protección de redes, datos y puntos finales. A ellas se suma la dedicada específicamente a protección OT para ayudar a preservar la integridad y privacidad de los flujos de información, con una visión completa de su seguridad, la identificación y el mapeo de activos sensibles, la segmentación (o, incluso, microsegmentación para el IIoT) al objeto de controlar la propagación de ataques, además de asegurar PLCs y estaciones de control.

### Protección de red a medida

La compañía es uno de los principales proveedores de tecnologías de protección de red de alto rendimiento con su familia de soluciones *firewall* y UTM (Gestión Unificada de Amenazas), que reúne bajo el paraguas de su línea **Stormshield Network Security** (SNS). Además de su desarrollo estándar (cortafuego hardware, virtuales y como servicio *cloud*), permite diseñar soluciones a medida para entornos de operación específicos. En las tres modalidades, la compañía ofrece "el mismo nivel de seguridad", con una amplia gama de funciones, como la protección en tiempo real (con un potente sistema de inspección y prevención de intrusiones –IPS y DPI–, control de aplicaciones, anti*malware*, etc.), control y supervisión (filtrado de URL, geolocalización de IP, detección de vulnerabilidades, etc.), filtrado de contenidos (anti*spam*, anti*spyware*, anti*phishing*, etc.), así como comunicaciones seguras (a través de VPN IPSec, VPN SSL).

La familia de cortafuegos físicos incluye una gama de entrada, para pequeñas organizaciones, que empieza con el SN160; una media, a la que se añadirán en verano equipos con doble fuente, y, por supuesto, una alta, con su SN1100, entre otros, para empresas *multisite* con infraestructuras complejas y necesidades de una mayor densidad de puertos. Además cuenta con una oferta dirigida a entornos restringidos, industriales y críticos con altas exigencias operativas. Aquí destaca el nuevo SNxr1200, destinado a cubrir los requisitos de seguridad de entornos tan sensibles como los aeronáuticos, marítimos y militares.


### Visibilidad y sencillez de gestión

La familia SNS brinda una notable facilidad de uso a través de un mismo *firmware*, así como con herramientas unificadas de gestión: **Stormshield Management Center**, para la supervisión y el acceso, así como la ejecución de comandos en múltiples dispositivos; y **Stormshield Log Supervisor**, herramienta SIEM desarrollada con **LogPoint**, para gestionar registros y ofrecer una vista unificada de los eventos de seguridad generados por toda la línea de productos.

### Enfoque diferencial en puntos finales

En lo que se refiere a la seguridad en el *endpoint* la multinacional tiene un elevado protagonismo en España, a través de su gama

**Stormshield es hoy un destacado proveedor europeo de ciberseguridad para organizaciones de sectores esenciales y estratégicos, públicos y privados y, en general, para negocios donde la garantía de integridad, disponibilidad y confidencialidad de los datos sensibles no es negociable.**


**Stormshield Endpoint Security** (SES). Su apuesta pasa por desmarcarse de los enfoques tradicionales, que considera insuficientes para asegurar terminales y servidores -sobre todo, en entornos críticos- para adoptar un enfoque que va más allá del de detección y respuesta, combinando funciones de prevención de punto final (EPP) y detección (EDR), no solo para bloquear proactivamente ataques sofisticados, sino, también para proporcionar información para su posterior análisis.

Estas soluciones aúnan "la protección del comportamiento y el control de dispositivos para ajustar el nivel de protección en respuesta al entorno de la estación de trabajo que está protegiendo", añaden desde la compañía, lo que incluye la protección del vector de entrada, ya sea a través de internet, como de USB, discos externos o cualquier equipo portátil. Y al mismo tiempo, permite capacidades de análisis y el acceso a las aplicaciones y recursos de la empresa en función de la ubicación del puesto de trabajo, así como protección de día cero y ante *ransomware*, entre otras características.

### Seguridad de datos

Fruto de su apuesta por una protección multicapa, Stormshield también ofrece una línea de soluciones de seguridad de datos, destinada a preservar la integridad y confidencialidad de los mismos. Bajo el paraguas de **Stormshield Data Security** (SDS), incorpora cifrado de extremo a extremo, poniéndolo a disposición solo de las personas autorizadas. "La información solo es legible por el remitente y el destinatario, independientemente del método de transferencia específico (correo electrónico, llave USB, etc.) o dispositivo (estación de trabajo, tableta, móvil) utilizado", afirman desde la compañía, que recuerda que, además, garantiza que "las claves pertenecen a la empresa".

La propuesta pasa por diferenciar la gestión de la protección de datos de su almacenamiento. Por ello, el administrador del sistema gestiona las soluciones y el almacenamiento y solo los usuarios autorizados pueden acceder a los datos sensibles. Asimismo, y para almacenamiento externalizado, como por ejemplo en la nube, la organización cliente sigue siendo propietaria de las claves de protección.

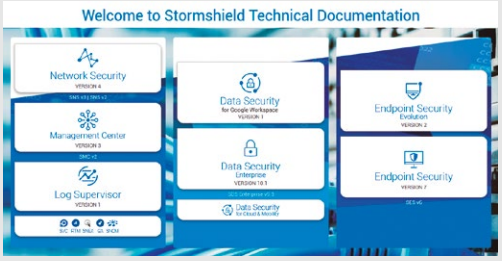
Esta línea, que también están disponible en versiones Enterprise o Cloud & Mobility, además, dispone de una funcionalidad de geolocalización, que permite el bloqueo de la aplicación en función del riesgo relacionado con el país en que se ubica el usuario, pudiéndose impedir la consulta de documentos confidenciales.

Cabe destacar que, con sus propuestas, Stormshield se adhiere a los requerimientos europeos de soberanía de datos y al cumplimiento legal efectivo en materia de datos personales. ●

## Un ecosistema digital de información

Stormshield dispone de un ecosistema digital de webs para consultar información sobre los productos y soluciones, además de disponer de datos de inteligencia y documentos de interés.

- **Portal de ciberseguridad.** En esta web se pueden conocer los datos más destacados del equipo de inteligencia de la empresa –'Customer Security Lab'– y el nivel de cobertura que se obtiene con sus soluciones y propuestas. Además, ofrece su servicio gratuito 'Breach Fighter' para analizar ficheros y archivos en busca de *malware*.
- **Plataforma de gestión documental.** Información técnica, manuales de usuario y guías para facilitar el despliegue y uso de sus tecnologías.




- **MyStormshield.** Entendido como un "espacio de confianza", se puede encontrar documentación de productos y gestionar licencias desde el área de cliente y contactar con el soporte técnico.
- **Stormshield Advisories.** Web abierta a clientes y no clientes. En ella se pueden conocer todos sus avisos de seguridad, publicados desde julio de 2014, para ayudar a "analizar todas las vulnerabilidades potenciales y comprobadas de atacantes identificados".
- **Colaboratorio.** Plataforma de información para compartir información, opiniones y comentarios sobre seguridad de redes y productos.
- **Plataforma de certificación de personas.** Una de las más punteras de la empresa, con apoyo personalizado para los que comienzan en la compañía o a tener relación con sus productos, ya que facilita la realización del examen de certificación en ellos, además de disponer de recursos de enseñanza del **Stormshield Institute.**

## La apuesta por el cifrado

Fruto de la importancia que da a la protección de datos, entre otras iniciativas, la marca cerró en 2001 una alianza con **Google**, dando lugar a SDS for Google Workspace, una solución específica para el cifrado del lado del cliente (CSE). Gracias a ella las compañías que utilizan Google Workspace pueden cifrar sus espacios de trabajo de forma independiente, manteniendo la experiencia nativa del usuario. Se facilita así el cumplimiento normativo (general y sectorial) de las empresas.

También destaca por permitir el uso de claves independientes para cifrar los datos en el lado del cliente antes de enviarlos a los servidores de Google. De este modo, las organizaciones mantienen control sobre la confidencialidad de sus datos. La propia Airbus ya está utilizando el cifrado del lado del cliente de Google Workspace para proteger sus datos más importantes.

STORMSHIELD

La opción europea de ciberseguridad

Su socio de confianza

para acompañarle

en su

**transformación digital**

**www.stormshield.com**