excelia

Vigilancia Digital

Ciberseguridad potenciada por IA al alcance de todas las empresas

Según el World Economic Forum, el 77% de las organizaciones está percibiendo un aumento del fraude digital y el phishing. Las empresas se enfrentan a amenazas cada vez más sofisticadas, pero no siempre disponen de los recursos, las herramientas o el personal especializado necesarios para vigilarlas de forma permanente.

El servicio de Vigilancia Digital de Excelia acerca **capacidades avanzadas de ciberseguridad** a las empresas mediante un modelo gestionado, inteligente, flexible y adaptado a sus necesidades. Monitorizamos sus activos digitales, detectamos posibles amenazas y facilitamos recomendaciones claras para reducir riesgos antes de que se conviertan en incidentes.

Monitorización, análisis y respuesta adaptadas a tu negocio

La dispersión de herramientas, la falta de especialistas y el coste de las soluciones tradicionales dificultan que muchas empresas puedan mantener una vigilancia continua de su entorno digital.

Con el servicio de Vigilancia Digital, el equipo de Excelia centraliza la supervisión de los principales activos de la empresa y transforma la información técnica en alertas priorizadas y acciones comprensibles, gracias a una plataforma centralizada propia potenciada por Inteligencia Artificial que integra monitorización web, inteligencia de amenazas, vigilancia de filtraciones y análisis de vulnerabilidades.

De esta forma, tu empresa puede acceder a capacidades propias de organizaciones de mayor tamaño sin asumir la complejidad operativa ni la inversión necesaria para crear una estructura interna de ciberseguridad.

¿Qué protegemos?

Sitios web y activos públicos

Supervisamos la disponibilidad, los tiempos de respuesta, los certificados SSL, las cabeceras de seguridad y posibles modificaciones no autorizadas en los sitios web de la empresa.

Identidad y reputación digital

Analizamos fuentes de inteligencia de amenazas para detectar dominios, direcciones IP o activos que puedan haber sido identificados como maliciosos, comprometidos o vulnerables.

Información expuesta

Buscamos posibles menciones de la empresa en filtraciones conocidas, repositorios públicos, fuentes OSINT y espacios asociados a la deep y dark web.

Vulnerabilidades técnicas

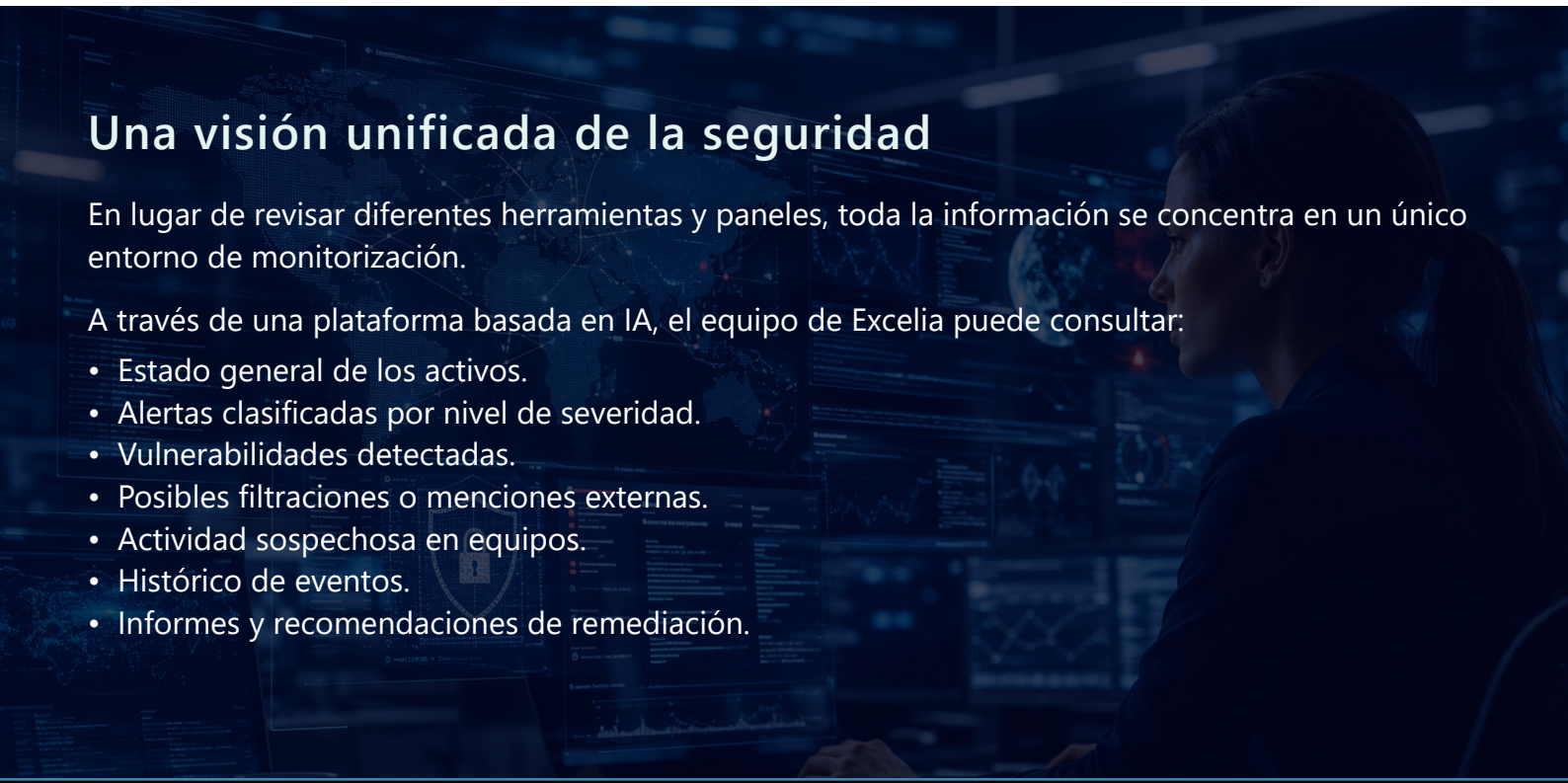
Identificamos tecnologías desactualizadas, configuraciones inseguras, rutas sensibles, archivos expuestos y vulnerabilidades conocidas, acompañadas de recomendaciones para su corrección.

Riesgo de ransomware

Contrastamos los activos de la organización con fuentes públicas relacionadas con campañas y grupos de ransomware para detectar posibles exposiciones de forma temprana.

Datos sensibles

Controlamos cómo se utilizan, comparten y transfieren los datos críticos de tu empresa para prevenir filtraciones, accesos no autorizados y pérdidas de información.



Una visión unificada de la seguridad

En lugar de revisar diferentes herramientas y paneles, toda la información se concentra en un único entorno de monitorización.

A través de una plataforma basada en IA, el equipo de Excelia puede consultar:

- Estado general de los activos.
- Alertas clasificadas por nivel de severidad.
- Vulnerabilidades detectadas.
- Posibles filtraciones o menciones externas.
- Actividad sospechosa en equipos.
- Histórico de eventos.
- Informes y recomendaciones de remediación.

Funcionalidades

► Monitorización de activos digitales

Supervisión continua de sitios web, dominios y servidores para controlar su disponibilidad, tiempos de respuesta, certificados SSL, cabeceras de seguridad y posibles cambios no autorizados.

► Escaneo de vulnerabilidades

Detección de tecnologías desactualizadas, configuraciones inseguras, rutas sensibles, archivos expuestos y vulnerabilidades conocidas, con recomendaciones para facilitar su corrección.

► Prevención de pérdida de datos

Capacidades DLP para supervisar cómo se utilizan, copian, comparten y transfieren los datos sensibles, reduciendo el riesgo de filtraciones, accesos no autorizados y exposición de información confidencial.

► Vigilancia de la dark web y fuentes OSINT

Búsqueda de menciones de la empresa, dominios, credenciales o información sensible en filtraciones conocidas, repositorios públicos, pastes y otras fuentes abiertas.

► Inteligencia de amenazas en tiempo real

Monitorización del panorama global de ciberseguridad para anticiparse a nuevas amenazas, contextualizar eventos y mejorar la capacidad de prevención, respuesta y recuperación.

► Vigilancia de ransomware

Contraste automático con fuentes públicas relacionadas con grupos y víctimas de ransomware para detectar posibles exposiciones o menciones de la organización.

► Análisis de reputación digital

Consulta automática de fuentes externas para identificar dominios, direcciones IP o URLs marcados como maliciosos, sospechosos o vulnerables.

Funcionalidades

► SOC - Centro de Operaciones de Seguridad

Gestión centralizada de incidentes con priorización por criticidad, asignación de analista, tiempos de respuesta definidos y trazabilidad completa de cada actuación. Incluye protocolos predefinidos para responder ante amenazas como ransomware, phishing, malware o accesos no autorizados.

► Pentesting automatizado con IA

Ejecución de pruebas sobre dominios, direcciones IP o URLs mediante herramientas de auditoría profesional, interpretación de resultados con IA y generación de informes con evidencias, nivel de severidad y recomendaciones.

► Asistente de Inteligencia Artificial

Analista virtual integrado en la plataforma que consulta los datos del entorno, relaciona eventos y ayuda a agilizar el análisis inicial de las alertas. Determinadas acciones operativas requieren confirmación previa del analista.

► Gestión centralizada e informes

Visualización unificada de activos, alertas, vulnerabilidades, eventos e incidentes, con histórico, clasificación por severidad e informes orientados a facilitar la toma de decisiones.

Cómo funciona el servicio

1 Identificamos los activos

Definimos junto a tu empresa qué sitios web, dominios, identidades y activos deben incorporarse al servicio.

2 Activamos la vigilancia

Configuramos los controles y fuentes de información necesarios para supervisar continuamente los activos seleccionados.

3 Detectamos y priorizamos

La plataforma analiza eventos, vulnerabilidades y posibles indicadores de amenaza, clasificándolos según su gravedad.

4 Te ayudamos a actuar

El equipo de Excelia revisa los hallazgos y facilita recomendaciones concretas para corregir vulnerabilidades, limitar la exposición y responder ante posibles incidentes.

5 Informamos de la evolución

Generamos informes periódicos que permiten conocer el estado de seguridad, las incidencias detectadas y las acciones recomendadas.

excelia

Tecnología e Inteligencia Artificial al servicio del analista

El servicio de Vigilancia Digital se apoya en una plataforma centralizada que incorpora un asistente de Inteligencia Artificial capaz de ayudar al equipo de Excelia a consultar información, relacionar eventos y agilizar el análisis inicial de las alertas.

También integra capacidades de pentesting automatizado que permiten realizar tareas de reconocimiento, detectar posibles vulnerabilidades y generar hallazgos con evidencias y recomendaciones.

Estas funciones apoyan el trabajo de los especialistas, reducen las tareas repetitivas y permiten dedicar más tiempo a interpretar los riesgos y acompañar al cliente en su resolución. El pentesting automatizado no sustituye las pruebas manuales avanzadas realizadas por especialistas cuando el alcance o la complejidad lo requieren, sino que lo complementa.

excelia

Beneficios para tu empresa

Detección temprana

Identifica posibles amenazas, filtraciones, vulnerabilidades y comportamientos sospechosos antes de que provoquen un impacto mayor.

Menor complejidad

Accede a diferentes capacidades de seguridad a través de un único servicio gestionado por Excelia.

Coste adaptado a todos los tamaños

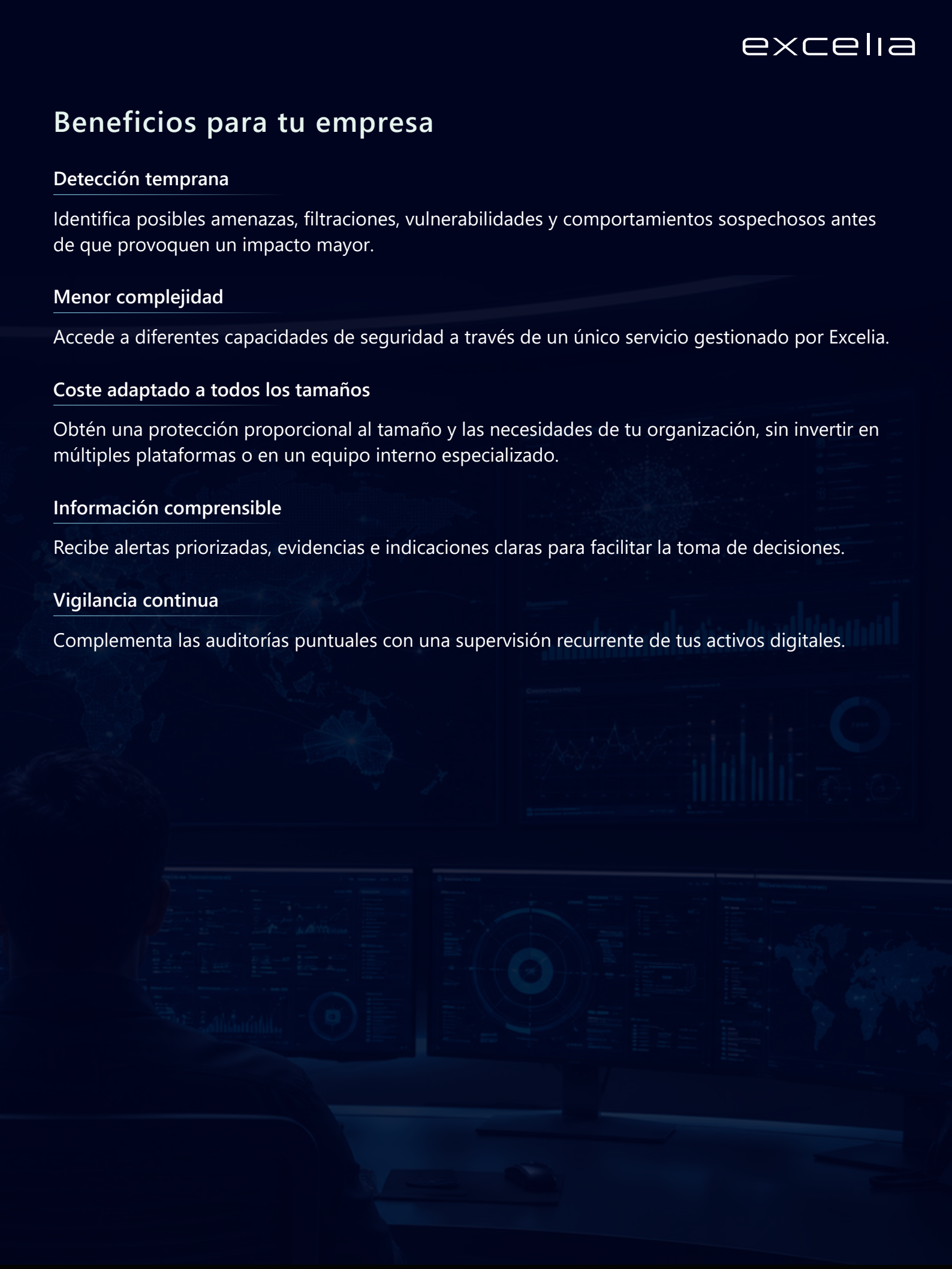
Obtén una protección proporcional al tamaño y las necesidades de tu organización, sin invertir en múltiples plataformas o en un equipo interno especializado.

Información comprensible

Recibe alertas priorizadas, evidencias e indicaciones claras para facilitar la toma de decisiones.

Vigilancia continua

Complementa las auditorías puntuales con una supervisión recurrente de tus activos digitales.



Planes adaptados a tus necesidades

PLAN BÁSICO

Servicio de vigilancia que incluye:

- Monitorización de sitios web y activos digitales.
- Control de disponibilidad, tiempos de respuesta y certificados SSL.
- Detección de cambios no autorizados y configuraciones inseguras.
- Vigilancia de vulnerabilidades y posibles exposiciones.
- Inteligencia de amenazas y análisis de reputación.
- Búsqueda de menciones en filtraciones, fuentes OSINT y dark web.
- Vigilancia frente a ransomware.
- Alertas priorizadas e informes con recomendaciones de actuación.
- Protección DLP.

PLAN BUSINESS

Incluye todo lo contemplado en el **Plan Básico,** más:

- Vigilancia digital de **3 perfiles VIP.**
  - > Monitorización de la exposición online de directivos o perfiles estratégicos.
  - > Detección de posibles filtraciones de credenciales, suplantaciones o menciones de riesgo.
  - > Seguimiento específico de amenazas dirigidas a las personas seleccionadas.

PLAN PREMIUM

Incluye todo lo contemplado en el **Plan Business,** más:

- Un pentesting avanzado por trimestre, combinando análisis automatizado y validación manual por especialistas.
  - > Análisis en profundidad de la superficie de ataque y detección de posibles vectores de entrada.
  - > Identificación y validación manual de vulnerabilidades para reducir falsos positivos.
  - > Pruebas exhaustivas de explotación controlada para comprobar el impacto real.
  - > Revisión manual del encadenamiento de vulnerabilidades para identificar riesgos de mayor impacto.
  - > Informe técnico y ejecutivo en profundidad con evidencias y recomendaciones priorizadas.
  - > Retest de las vulnerabilidades críticas tras su corrección.

excelia

¿Por qué Excelia?

Porque combinamos tecnología propia, conocimiento especializado en Inteligencia Artificial, experiencia en ciberseguridad y un modelo de servicio pensado para acercar capacidades avanzadas de protección a las empresas.

Nuestro equipo configura la vigilancia, supervisa los activos, interpreta las alertas y ayuda a priorizar las acciones necesarias para reducir la exposición al riesgo.

Con Excelia, tu empresa obtiene:

- **Una visión centralizada,** con la información de webs, servidores, vulnerabilidades y posibles filtraciones en un único entorno.
- **Acompañamiento experto,** para convertir datos técnicos en recomendaciones claras y accionables.
- **Tecnología propia,** desarrollada para integrar monitorización, inteligencia de amenazas y pentesting automatizado desde una misma plataforma.
- **Un servicio escalable,** adaptable al número de activos, equipos y necesidades de cada pyme.
- **Mayor control sobre los datos,** gracias a una arquitectura diseñada para evitar el envío de información de clientes a proveedores externos de Inteligencia Artificial.
- **Capacidad de respuesta,** no solo de detección, ante determinados incidentes que requieren actuar con rapidez.

Así, las empresas pueden acceder a un nivel de vigilancia más avanzado sin asumir el coste ni la complejidad de contar con un SOC.