GrayHats

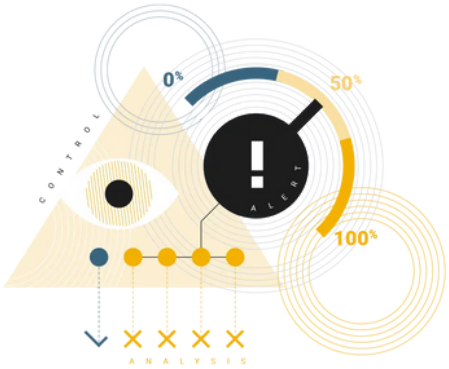
Ciberprotección

DATA SHEET

Descripción de la solución

Ciberprotección 24x7 para que tu negocio nunca se detenga

Protege tu empresa frente a ciberataques con un servicio gestionado, accesible y siempre activo. Tecnología de nivel multinacional al alcance de tu pyme.



Nuestro servicio combina la tecnología de grandes corporaciones con la cercanía de un aliado local, para que tu empresa esté siempre protegida, evite interrupciones críticas y pueda centrarse en crecer con tranquilidad.

Esta solución incluye:

Protección de Endpoints

- Protección de Pcs y Servidores
- Antimalware avanzado (EDR) con detección en tiempo real de amenazas.
- Firewall inteligente para bloquear accesos no autorizados.
- Control de aplicaciones vulnerables.
- Control de USB y dispositivos Bluetooth.
- Función de recuperación automática tras un incidente de ransomware.

Soportado por: SentinelOne

Protección E-mail

- Protección contra ataques BEC, EAC y suplantación de indentidad en correo.
- Filtros anti-phishing y anti-spam.
- Escaneo de archivos adjuntos para detectar malware y sandboxing de sospechosos.
- Protección contra URLs maliciosas.
- Cifrado automático de correo electrónico..
- DLP en correo electrónico.
- Cursos de concienciación y threat simulation

Soportado por: proofpoint.

Vigilancia & Control

- Vigilancia 24/7 para tu seguridad, permitiéndote enfocarte en tu negocio.
- Gestión de alertas: monitoreamos y analizamos alertas, avisando solo si hay anomalías.
- Respuesta a incidentes: nos encargamos de cualquier incidente que surja.
- Portal de soporte y teléfono disponible para dudas e incidencias urgentes.

Soportado por: GrayHats

Protección de Navegación

- Supervisión y bloqueo de sitios maliciosos en internet.
- Protección contra malware en descargas y phishing. Control DLP básico.
- Control sobre las aplicaciones SaaS utilizadas en la empresa.
- Mejora en la velocidad de acceso a Microsoft 365 y Google Workdocs.
- Reportes de navegación de empleados.

Soportado por: netskope

Esto es para tí, si...

- Tienes una empresa y usas habitualmente ordenadores.
- Manejas información confidencial de clientes.
- Te gustaría que tu personal pudiese trabajar de manera segura desde cualquier sitio.
- Realizas transferencias de dinero desde internet.

Principales ventajas

- Protege tu negocio de las principales ciber amenazas.
- Evita una interrupción de tu negocio debido a un incidente de ciberseguridad.
- Te ayuda a cumplir con la LOPD.
- Habilita y abarata el precio de un seguro de ciber riesgos para tu empresa.
- Evita que le roben a tus clientes.

GrayHats

Ciberprotección

DATA SHEET

¿Por qué esta es la solución que necesitas?

Cada empresa es diferente, por eso te ofrecemos tres niveles de protección adaptados a tus necesidades.
Sin complicaciones, sin sorpresas. Seguridad real para tu negocio.

Funcionalidad	🔰 Protección Básica *(24,95€/usuario/mes)*	🛡️ Protección Estándar *(29,95€/usuario/mes)*	🔥 Protección Avanzada *(39,95€/usuario/mes)*
Protección de Dispositivos, Correo y Navegación	✅	✅	✅
Vigilancia y Respuesta Automatizada (24x7)	✅	✅	✅
Gestión de alertas	7x5 (L-V)	12x5 (L-V)	24x7
Respuesta a Incidentes	Solo criticidad alta (2 días)	Media y alta (1 día)	Media y alta (inmediata)
Cursos de concienciación en ciberseguridad	✅	✅	✅
Simulacros de phishing	✅	✅	✅
Recomendaciones de seguridad vía email	✅	✅	✅
Revisiones periódicas de seguridad	❌	✅	✅
Desarrollo de políticas de seguridad	❌	✅	✅
Reportes Mensuales de Seguridad	❌	✅	✅
Asesoramiento especializado	❌	❌	✅
Cumplimiento normativo	❌	❌	✅

Protección Básica.

- Agentes para protección de dispositivos, email y navegación por internet.
- Vigilancia y Respuesta Automatizadas (24x7)
- Gestión de alertas (7x5)
- Respuesta a Incidentes de criticidad alta. 7x5 lunes a viernes. Respuesta en 2 días laborables. Portal de soporte.
- Cursos de concienciación en en mejores prácticas en ciberseguridad e identificación de amenazas
- Simulacros de phishing: Ejercicios prácticos para evaluar y mejorar la respuesta del personal ante intentos de suplantación de identidad.
- Recomendaciones de seguridad. Emails periódicos con recomendaciones y avisos de seguridad.

Protección Estándar.

- *Básica +*
- Respuesta a incidentes de criticidad media y alta. 12x5 de lunes a viernes. Respuesta en 1 día Laborable. Portal de soporte..
- Revisiones de seguridad: Evaluación periódica de políticas y prácticas de seguridad para asegurar su eficacia
- Desarrollo de políticas: Elaboración de políticas y procedimientos para fortalecer la postura de seguridad corporativa.
- Reportes Mensuales: Informe ejecutivo sobre el estado de la ciberseguridad en la organización.

Protección Avanzada.

- *Estándar +*
- Respuesta a incidentes de criticidad media y alta. 24x7 de lunes a domingo. Portal de soporte y Teléfono.
- Asesoramiento Especializado: Orientación en la implementación de soluciones de seguridad adaptadas a las necesidades específicas de la empresa.
- Servicio vCISO: Verificación de que la organización cumple con las regulaciones y estándares aplicables en materia de seguridad.

Preguntas frecuentes

GrayHats

¿Qué es un endpoint?

Es cualquier dispositivo en el cual comience o termine una conexión de datos. Por ejemplo, ordenadores personales, smartphones o servidores.

¿Por qué es fundamental proteger tus endpoints?

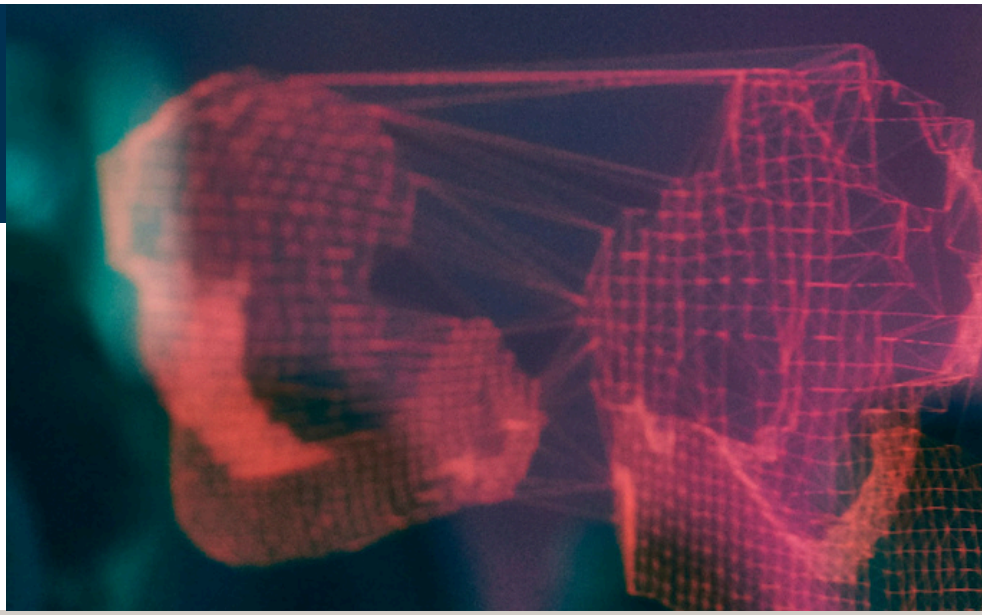
Porque son los destinos finales de los atacantes. Es el objetivo a infectar y permanecer oculto para llevar a cabo sus acciones. De manera continua, hay que asegurarse de que estos dispositivos están limpios allí donde estén.

¿Por qué es fundamental proteger el correo electrónico?

El correo electrónico es la principal puerta de entrada de malware a las empresas hoy día. Se estima que es responsable de más del 80% de las infecciones por malware y más del 98% de los ataques de Phishing.
También es el principal medio de exfiltración de datos e información confidencial de la empresa.

¿Cómo adaptais la solución a mi empresa?

Hacemos una evaluación inicial sin coste para la empresa y damos una serie de recomendaciones y un plan personalizado a la empresa.



¿Por qué es fundamental el entrenamiento básico de usuarios en ciberdefensa?

Los usuarios son, de manera inconsciente, el mejor aliado de los ciber delincuentes cuando son engañados para realizar ciertas acciones que allanen el camino de entrada. Por este motivo hay que hacerlos capaces de discernir los principales engaños y técnicas de ingeniería social las cuales van a ser usadas contra ellos.

¿Cómo me protege esta solución contra el malware o phishing provenientes del correo electrónico?

1. Controla a tiempo real una base de datos de millones de servidores de correo que activamente distribuyen malware y phishing y los bloquea.
2. Analiza el cuerpo y redacción del mensaje mediante inteligencia artificial para detectar si es un engaño.
3. Examina todos los archivos adjuntos del correo y los bloquea si contienen algún tipo de malware antes de que lleguen a la bandeja de entrada. Por otro lado, si hay algún enlace en el cuerpo del mensaje, lo pre ejecuta para ver si lleva a alguna web de descarga de malware o phishing.

¿Por qué es fundamental proteger la navegación?

Cualquier ataque, ya sea en su fase de infección, o en posteriores como la de persistencia o exfiltración de datos, va a realizar acciones de navegación por internet. Ya sea para descargarse un malware, para conectarse a un centro de control, o sacar información confidencial de la empresa. Estas acciones de navegación se pueden detectar y cortar, frustrando así ataques en cualquier fase que estos se encuentren.

¿Puedo controlar en qué tipo de páginas navegan mis usuarios?

Sí, existen bases de datos con millones de urls categorizadas sobre las que se pueden establecer políticas de acceso. Estas políticas pueden ser, permitir, denegar o "educar" que es permitir pero con un aviso al usuario de que se permite pero que se haga con un uso moderado de tiempo. También se pueden crear categorías personalizadas con las urls que decida el cliente.

¿Es capaz está solución de diferenciar entre instancias corporativas y no corporativas de aplicaciones SaaS como Microsoft 365?

Sí, es capaz de diferenciarlas.

Preguntas frecuentes

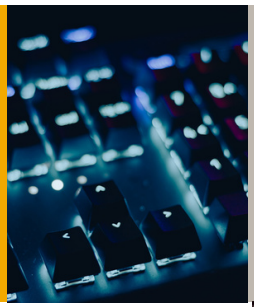
GrayHats

¿Puedo controlar en qué tipo de páginas navegan mis usuarios?

Sí, existen bases de datos con millones de urls categorizadas sobre las que se pueden establecer políticas de acceso. Estas políticas pueden ser, permitir, denegar o "educar" que es permitir pero con un aviso al usuario de que se permite pero que se haga con un uso moderado de tiempo. También se pueden crear categorías personalizadas con las urls que decida el cliente.

¿Es capaz está solución de diferenciar entre instancias corporativas y no corporativas de aplicaciones SaaS como Microsoft 365?

Sí, es capaz de diferenciarlas.



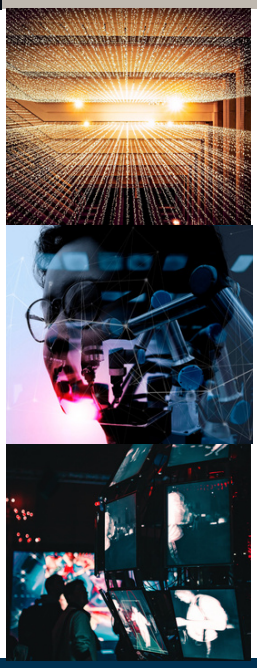
¿Es capaz de controlar puertos diferentes a los típicos de navegación web 80/443?

Sí, es capaz también de detectar protocolos como ssh, rdp, ftp o telnet entre otros muchos, independientemente del puerto por el que se ejecuten.

¿Cómo me ayuda esta solución a cumplir la Ley de Protección de Datos?

Dicha ley en su artículo 36 especifica que el responsable de los datos, el empresario, debe tomar las medidas necesarias y de acuerdo al estado del arte de la tecnología para asegurar, entre otras cosas, la confidencialidad de los datos en posesión de la empresa.

La solución ayuda a cumplir la Ley al implementar medidas tecnológicas avanzadas para garantizar la confidencialidad de la información, permitiendo solo el acceso autorizado a los datos, y evitando infecciones por malware que comprometan la confidencialidad.



La mayor parte de la navegación por internet está cifrada mediante el protocolo SSL.

¿Cómo puede esta solución ver donde navegan o qué se descargan los usuarios?

Somos capaces de desencriptar todo el tráfico de navegación web y buena parte del tráfico de aplicaciones que usan internet.

¿Qué son los servicios de ciberprotección de GrayHats?

Son nuestros servicios de vigilancia y respuesta. Las herramientas de ciberseguridad nos aportan visibilidad de lo que pasa en tus sistemas para así poder detectar y responder de manera temprana cualquier amenaza. Para esto necesitamos personas que monitoricen y operen estas herramientas de manera continua.

Sobre nosotros

QUIENES SOMOS

Somos una empresa de ciberseguridad especializada en proteger a empresas mediante servicios gestionados de última generación. Combinamos tecnología avanzada, experiencia, y un enfoque cercano para ofrecer soluciones de protección continua, adaptadas a las necesidades reales de las empresas

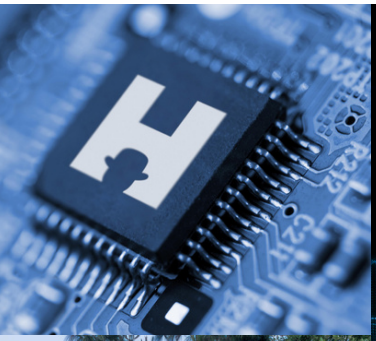
NUESTRA PROPUESTA DE VALOR

Ofrecemos a las pequeñas y medianas empresas la misma ciberseguridad de nivel multinacional que protege a los gigantes, sin necesidad de grandes inversiones ni equipos internos.

GrayHats

Te protegemos antes de que sea tarde

Hazte tu propio presupuesto en nuestra calculadora online.



PARTNERS WITH aws SentinelOne paloalto NETWORKS tenable netskope NASUNI

Grayhats S.L.
T: (+34) 957 858 977
Gran Capitán 46, Planta 1. Of. 1
14006- Córdoba

GrayHats