



Digital Security
Progress. Protected.





Número uno en ciberseguridad para empresas de la Unión Europea

Comprometidos con los más altos estándares de la industria



ESET cumple con la norma ISO/IEC 27001:2013, una norma de seguridad reconocida internacionalmente en la implementación y gestión de la seguridad de la información.

PACKS DE SOLUCIONES PARA EMPRESA

Nombre de la solución	ESET PROTECT ENTRY Avanzada protección multicapa de los equipos con un sólido machine learning y una gestión fácil de usar	ESET PROTECT ADVANCED La mejor protección de los equipos contra el ransomware y las amenazas de día cero, complementada por una potente seguridad de los datos	ESET PROTECT COMPLETE Protección completa y multicapa para equipos, aplicaciones en la nube y correo electrónico, el vector de amenazas número 1	ESET PROTECT ENTERPRISE Detección y respuesta ampliada (XDR) que ofrece nivel de visibilidad para empresa, detección de amenazas y opciones de respuesta
Gestión de la seguridad (ESET PROTECT)	✓	✓	✓	✓
Antivirus para equipos (ESET Enpoint Antivirus)	✓	✓	✓	✓
Protección avanzada EPP (ESET Endpoint Security + ESET Server Security)	✓	✓	✓	✓
Defensa contra amenazas avanzadas (ESET LiveGuard Advanced)	-	✓	✓	✓
Cifrado de disco completo (ESET Full Disk Encryption)	-	✓	✓	✓
Seguridad para el correo electrónico (ESET Mail Security)	-	-	✓	-
Protección para aplicaciones en la nube (Microsoft365) (ESET Cloud Office Security)	-	-	✓	-
Detección y respuesta (XDR) (ESET Inspect)	-	-	-	✓

TECNOLOGÍA ESET

Tecnología ESET	ESET PROTECT ENTRY	ESET PROTECT ADVANCED	ESET PROTECT COMPLETE	ESET PROTECT ENTERPRISE
Machine Learning	P	P	P	P
Detección por comportamiento y bloqueo de HIPS	P	P	P	P
Detecciones ADN	P	P	P	P
Análisis avanzado de memoria	P	P	P	P
Protección contra Botnets	P	P	P	P
Protección contra ataques de red	P	P	P	P
Escudo contra ransomware	P	P	P	P
Antispam	P	P	P	P
Control Web	P	P	P	P
Firewall	P	P	P	P
Sandbox o EDR automatizado	-	P	P	P
Protección de correo a nivel de servidor o Microsoft 365	-	-	P	-
XDR avanzado	-	-	-	P



PRE EJECUCIÓN
EJECUCIÓN
POST EJECUCIÓN



Reputación
y caché



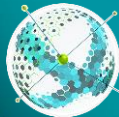
Detecciones
de ADN



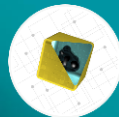
Análisis
UEFI



Control del
dispositivo



Protección
contra ataques
de red



Sandbox
en la
nube



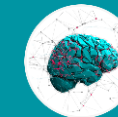
Escudo anti
ransomware



Escáner
avanzado
de memoria



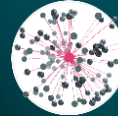
Detección por
comportamiento
y bloqueo de HIPS



Aprendizaje
automático avanzado



Protección
LiveGrid



Protección
contra botnets



Script
Scanner
& AMSI



Bloqueo
de exploits

Tecnología ESET

Mejoramos continuamente nuestra tecnología de detección a través de nuestros laboratorios de investigación en todo el mundo

Machine Learning ESET

ESET ha desarrollado su propio motor de Machine Learning, denominado ESET Augur. Utiliza la potencia combinada de las redes neuronales (como el aprendizaje profundo y la memoria a corto plazo) y un grupo seleccionado de seis algoritmos de clasificación. Esto le permite generar un resultado consolidado y ayudar a etiquetar correctamente la muestra entrante como "no infectada", "potencialmente no deseada" o "maliciosa".

Detección por comportamiento y bloqueo de Hips

El Sistema de prevención de intrusiones basado en el host (HIPS) suministrado por ESET supervisa la actividad del sistema y emplea un conjunto predefinido de reglas para reconocer el comportamiento sospechoso del sistema. Cuando se identifica una actividad sospechosa, el mecanismo de autodefensa del sistema HIPS evita que el programa o proceso lleve a cabo actividades potencialmente dañinas.

Detecciones ADN

Los tipos de detecciones varían desde el uso de hashes sumamente específicos hasta las Detecciones de ADN de ESET, que son definiciones bastante complejas de la conducta maliciosa y de las características del malware.

Si bien es fácil para los atacantes modificar u ofuscar el código malicioso, no pueden cambiar el comportamiento de los objetos con tanta facilidad. Las Detecciones de ADN de ESET están especialmente diseñadas para aprovechar este principio.

Tecnología ESET

Mejoramos continuamente nuestra tecnología de detección a través de nuestros laboratorios de investigación en todo el mundo

Análisis Avanzado de memoria

La Exploración avanzada de memoria es una tecnología exclusiva de ESET que aborda con eficacia un problema importante del malware moderno: el uso intensivo de técnicas de ofuscación y cifrado. Para afrontar estos problemas, la Exploración avanzada de memoria monitorea el comportamiento del proceso malicioso y lo explora cuando se muestra en la memoria.

Protección contra Botnets

La Protección ante botnets suministrada por ESET detecta las comunicaciones maliciosas que utilizan las botnets y al mismo tiempo identifica los procesos ofensivos. Bloquea todas las comunicaciones maliciosas detectadas y le informa al usuario.

Protección contra ataques de red

La Protección contra ataques de red es una extensión de la tecnología del firewall y mejora la detección de las vulnerabilidades conocidas en el nivel de la red. Constituye otra importante capa de seguridad ante la propagación del malware, los ataques que circulan por la red y el aprovechamiento de vulnerabilidades para las cuales aún no se lanzó al público o no se desplegó la revisión correspondiente.

Tecnología ESET

Mejoramos continuamente nuestra tecnología de detección a través de nuestros laboratorios de investigación en todo el mundo

Escudo Ransomware

ESET Ransomware Shield es una capa adicional que protege a los usuarios ante el ransomware. Esta tecnología monitorea y evalúa todas las aplicaciones ejecutadas en función de su comportamiento y reputación. Se diseñó para detectar y bloquear procesos cuya conducta es similar a la del ransomware.

Antispam

El correo electrónico no solicitado (llamado spam) es uno de los problemas más importantes de la comunicación electrónica. El spam representa hasta 50% de todas las comunicaciones por correo electrónico. La protección antispam sirve para proteger de este problema. Mediante la combinación de varios principios de seguridad del correo electrónico, el módulo antispam proporciona un filtrado superior para mantener su buzón de entrada desinfectado.

Firewall

El Firewall personal de ESET actúa como un filtro del tráfico de la red que regula la comunicación con la red local o Internet. Utilizando reglas predefinidas, el Firewall personal analiza la comunicación de la red y decide permitirla o no. Usted puede configurarlo para generar excepciones para ciertas aplicaciones.

Tecnología ESET

Mejoramos continuamente nuestra tecnología de detección a través de nuestros laboratorios de investigación en todo el mundo

Control Web

La sección Control Web permite configurar las opciones que protegen a su empresa del riesgo de responsabilidad legal. El Control Web puede regular el acceso a sitios Web que violan los derechos de propiedad intelectual. El objetivo es prevenir que los empleados accedan a páginas con contenido inapropiado o perjudicial o páginas que puedan tener un impacto negativo en la productividad.

El Control Web permite bloquear páginas Web que puedan contener material potencialmente ofensivo. Además, los empleadores y los administradores de sistemas pueden prohibir el acceso a más de 27 categorías de sitios Web predefinidos y a más de 140 subcategorías.

Sandbox o EDR automatizado

La Sandbox en la nube es un entorno virtual en los laboratorios de ESET. Cualquier muestra que entre en el equipo y sea potencialmente peligrosa, es enviada a la Sandbox para su ejecución. En función de las acciones realizadas en el entorno virtualizado se determina si es una amenaza y se elimina evitando que entre en los sistemas cliente.

Especialmente útil para ataques de día cero y ransomware. Esta capa de protección se basa en comportamiento y Machine Learning.

XDR Avanzado

Proporciona visibilidad de todos los procesos que están en funcionamiento en todos los equipos de la red y genera alertas por comportamientos sospechosos.

Una persona de IT debe revisar las alertas y actuar en consecuencia.



Digital Security
Progress. Protected.