



PROTECT

Plataforma de gestión de seguridad unificada que
proporciona una visibilidad superior de la red

Progress. Protected.



¿Qué es una consola de gestión de seguridad para endpoints?

ESET PROTECT es una consola UEM versátil, implementable en la nube o en local, que garantiza visibilidad en tiempo real de los equipos locales y externos, así como la elaboración de informes completos y gestión de la seguridad para todos los sistemas operativos.

Se trata de un panel único para todas las soluciones de seguridad de ESET implementadas en la red. Controla las capas de prevención, detección y respuesta de endpoints en todas las plataformas, incluyendo equipos de escritorio, servidores, máquinas virtuales e incluso dispositivos móviles gestionados.

¿Por qué la gestión de la seguridad de endpoints?

VISIBILIDAD

Vulnerabilidades de día cero, amenazas persistentes avanzadas, ataques dirigidos y redes de bots son preocupaciones para las industrias de todo el mundo. Tener visibilidad de estas amenazas en tiempo real es extremadamente importante para que el personal de IT pueda responder con prontitud y mitigar cualquier riesgo que pueda haber surgido. Debido al continuo hincapié de las empresas en añadir una fuerza de trabajo móvil, la visibilidad no solo es necesaria a nivel local, sino también externo.

ESET PROTECT proporciona información actualizada para comunicar al personal de IT sobre el estado de todos los endpoints, ya sean locales o externos. También proporciona visibilidad de todos los sistemas operativos que pueda tener una empresa. En la mayoría de casos, la visibilidad también se mejora para mostrar información a nivel de dispositivo, como inventarios de hardware o software, para garantizar un entendimiento completo de la situación.

COMUNICACIÓN

El panorama actual de la ciberseguridad evoluciona constantemente con nuevos métodos de ataque y amenazas nunca antes vistas. Cuando se produce un ataque o una filtración de datos, las empresas suelen sorprenderse de que sus defensas hayan estado en peligro o desconocen por completo que el ataque se haya producido. Una vez se descubre el ataque, las empresas pueden querer llevar a cabo tareas específicas en los dispositivos, como los análisis. Esto puede llevar a las empresas a cambiar completamente sus medidas de configuración para protegerse mejor contra un futuro ataque.

ESET PROTECT cuenta con políticas predefinidas potentes e inteligentes, y permite a las empresas ajustar las medidas o configuraciones de los productos de seguridad para endpoints en cualquier momento. Además, las tareas se pueden automatizar para ahorrar a los administradores de IT tiempo al no tener que ejecutarlas manualmente en cada ordenador.

REPORTING

Además de tener que cumplir con la normativa de protección de datos, la mayoría de las empresas tienen sus requisitos internos relacionados con la presentación de informes. Independientemente de la empresa, hay informes que se deben generar de forma planificada y proporcionarse a las partes pertinentes o guardarse para su futura utilización.

ESET PROTECT puede generar informes de forma planificada y guardarlos en carpetas específicas o enviarlos por correo electrónico directamente a quien los haya solicitado. Cuenta con una gran cantidad de plantillas de informes que pueden utilizarse de inmediato o personalizarse para proporcionar al solicitante lo que necesita. Este proceso es primordial para ahorrar tiempo a los administradores de IT en el intenso trabajo asociado a los informes continuos.

“La mayor ventaja de ESET es que dispones de todos los usuarios en una sola consola y que puedes gestionar y revisar adecuadamente su estado de seguridad.”

— Jos Savelkoiul, Jefe de equipo del departamento de TIC;
Hospital de Zuyderland, Holanda, más 10 000 puestos

Tener visibilidad de estas amenazas en tiempo real es extremadamente importante para permitir que el personal de IT dé respuesta de inmediato y mitigue cualquier riesgo que pueda haber surgido.

No importa el tipo de empresa, habrá informes que necesitarán ser generados a intervalos programados y proporcionarlos a partes relevantes o almacenarlos para su uso futuro.



ESET marca la diferencia

DE LA PREVENCIÓN A LA RESPUESTA

En una sola consola, ESET PROTECT combina la gestión de múltiples soluciones de seguridad de ESET. Desde la prevención de amenazas hasta la detección y la respuesta, cubren toda tu empresa de forma multicapa para obtener el mejor nivel de protección.

SOLUCIONES DE INCIDENTES CON UN SOLO CLIC

Desde el panel principal, un administrador de IT puede evaluar rápidamente la situación y responder a los problemas. Acciones como crear una exclusión, enviar archivos para su análisis o iniciar un análisis están disponibles con un solo clic. Las exclusiones se pueden hacer por nombre, URL, hash o combinación.

RBAC AVANZADOS

Comenzando con el acceso protegido por MFA, la consola está equipada con un sistema avanzado de control de acceso basado en roles (RBAC). Asigna a los administradores y usuarios de la consola a subredes, grupos de objetos y define conjuntos de permisos con un gran nivel de granularidad.

SISTEMA DE NOTIFICACIÓN TOTALMENTE PERSONALIZABLE

El sistema de notificaciones cuenta con un editor completo que representa cómo lo verás, con el que podrás configurar las notificaciones para que te avisen con la información exacta que deseas recibir.

INFORMES DINÁMICOS Y PERSONALIZADOS

ESET PROTECT proporciona más de 170 informes integrados y te permite crear informes personalizados a partir de más de 1000 puntos de datos. Esto permite a las empresas crear informes con el aspecto que deseen. Una vez creados, los informes pueden configurarse para ser generados y enviados por correo electrónico a intervalos programados.

MARCO DE AUTOMATIZACIÓN

Los grupos dinámicos pueden ordenar los ordenadores en función del estado actual del dispositivo o de los criterios de inclusión definidos. A continuación, se pueden configurar tareas para desencadenar acciones como análisis, cambios de políticas o instalaciones/desinstalaciones de software.

SOPORTE VDI TOTALMENTE AUTOMATIZADO

Se utiliza un algoritmo de detección de hardware completo para determinar la identidad de la máquina a partir de su hardware. Esto permite la creación automática de imágenes y la clonación de entornos de hardware no persistentes. Por lo tanto, el soporte VDI de ESET no requiere ninguna interacción manual y está totalmente automatizado.

PROBADO Y FIABLE

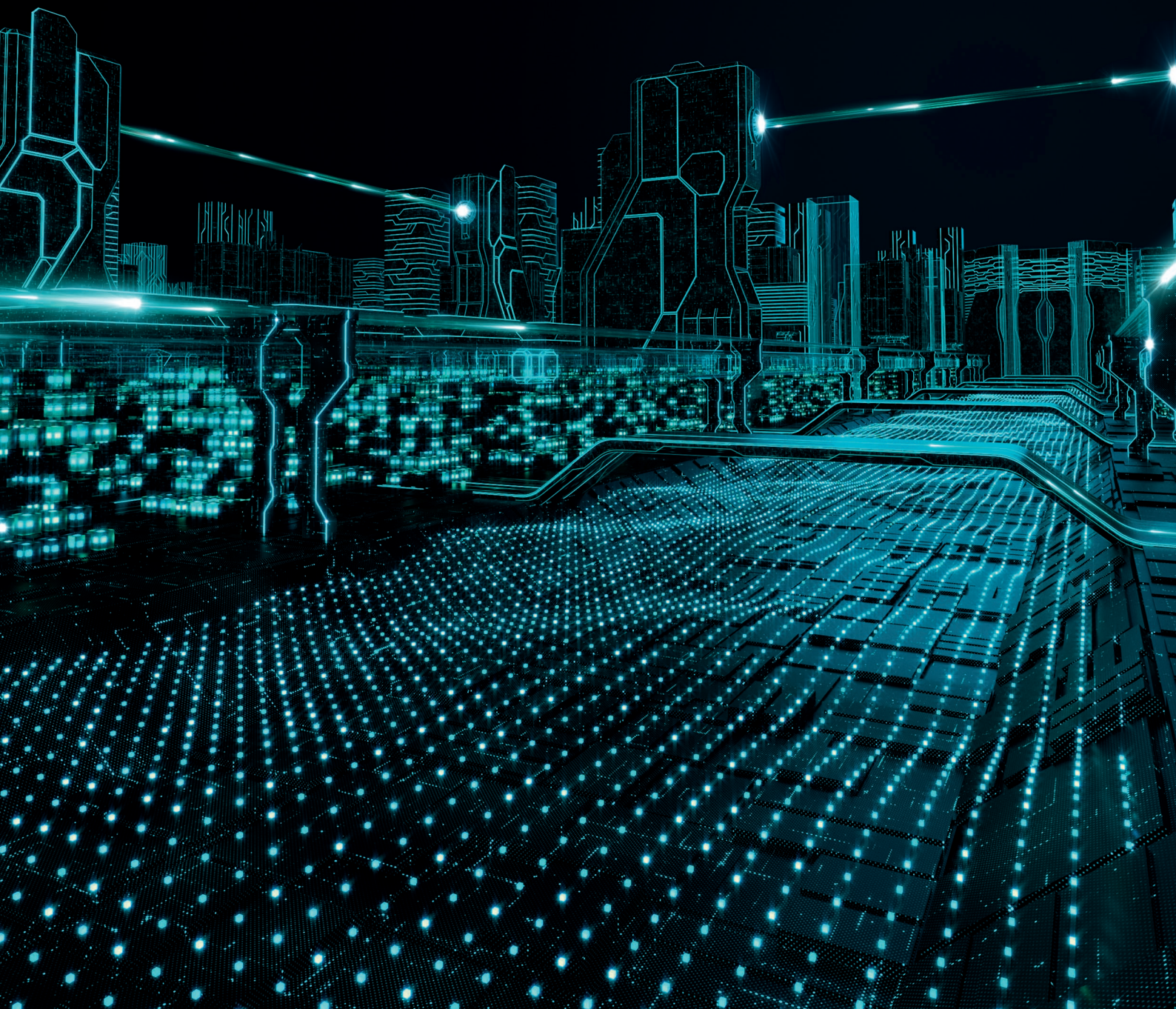
ESET lleva más de 30 años en el sector de la seguridad y seguimos desarrollando nuestra tecnología para estar un paso por delante de las amenazas más recientes. Esto nos ha llevado a contar con la confianza de más de 100 millones de usuarios en todo el mundo. Nuestra tecnología es analizada constantemente y aprobada por terceros que demuestran la eficacia de nuestra propuesta para detener las últimas amenazas.

MSP COMPETENTE

Si eres un proveedor de servicios gestionados (MSP) que se ocupa de las redes de sus clientes, apreciarás las capacidades de tenencia múltiple de ESET PROTECT. Las licencias MSP se detectan automáticamente y se sincronizan con el servidor de licencias, y la consola te permite realizar acciones avanzadas como instalar/eliminar cualquier aplicación de terceros, ejecutar scripts, comandos remotos, listar procesos en ejecución, configuraciones HW, etc.

“Una empresa excepcional, una asistencia técnica magnífica que proporciona una fuerte protección contra las amenazas y una gestión centralizada.”

— Dave, Director de IT, Deer Valley Unified School District,
más de 15 500 puestos



Use cases

Ransomware

Un usuario abre un correo electrónico malicioso que contiene un nuevo tipo de ransomware.

SOLUCIÓN

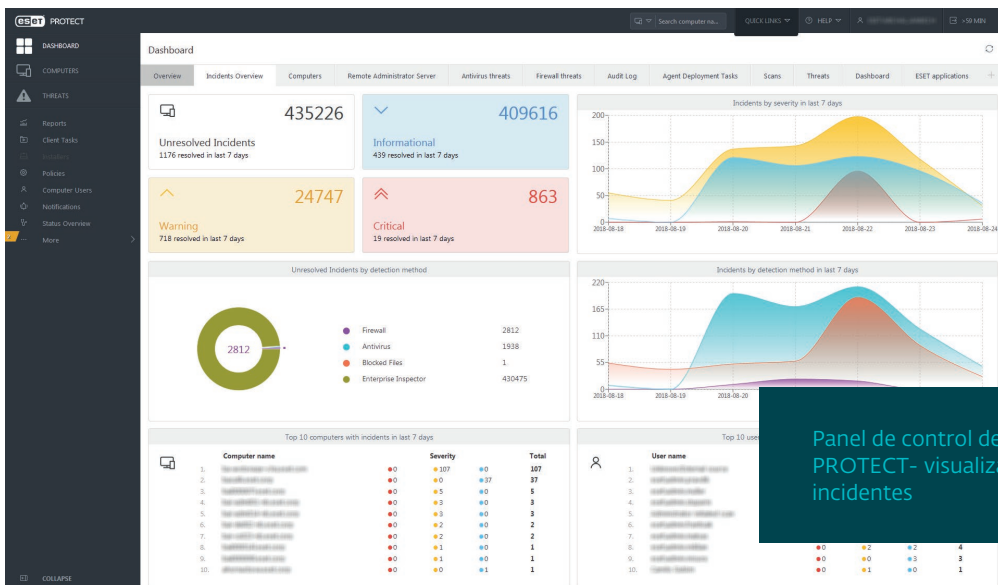
- ✓ El departamento de IT y su SIEM reciben una notificación por correo electrónico de que se ha detectado una nueva amenaza en un determinado ordenador.
- ✓ Se inicia un análisis con un solo clic en el equipo infectado.
- ✓ El archivo se envía a ESET LiveGuard Advanced con un nuevo clic.
- ✓ Después de confirmar que la amenaza ha sido controlada, las advertencias en la consola de ESET PROTECT se borran automáticamente.

Desarrolladores de código

Los programadores que trabajan con código en sus ordenadores de empresa podrían crear falsos positivos debido a la compilación de software.

SOLUCIÓN

- ✓ El departamento de IT y su SIEM reciben una notificación por correo electrónico de que se ha encontrado una nueva amenaza.
- ✓ La notificación muestra que la amenaza proviene del ordenador de un desarrollador.
- ✓ Con un clic, el archivo se envía a ESET LiveGuard Advanced para confirmar que el archivo no es malicioso.
- ✓ El departamento de IT, con un solo clic, pone una exclusión para evitar que se muestren futuros falsos positivos en esta carpeta.



Implementación de VDI

Los entornos de hardware no persistentes suelen requerir la interacción manual de un departamento de IT y crean problemas de informes y visibilidad.

SOLUCIÓN

- ✓ Después de implementar una imagen patrón en los equipos que ya están presentes en ESET PROTECT, los equipos seguirán informando a la instancia anterior a pesar de la nueva imagen completa del sistema.
- ✓ Los sistemas que vuelven a su estado inicial de un turno de trabajo no causarán duplicados, sino que se adjuntarán en un solo registro.
- ✓ En el momento de implementar imágenes no persistentes, puedes crear una imagen que incluya el dispositivo, de forma que cada vez que se cree un nuevo equipo con otra huella de hardware, se creen automáticamente nuevos registros en ESET PROTECT.

Registro de hardware y software

Las empresas necesitan saber qué software está instalado en cada ordenador y la antigüedad de cada uno de ellos.

SOLUCIÓN

- ✓ Puedes ver cada software instalado, incluida la versión, en el historial del ordenador.
- ✓ Consulta los detalles de hardware de cada ordenador, como por ejemplo dispositivo fabricante, modelo, número de serie, procesador, memoria RAM, espacio en el disco duro y mucho más.
- ✓ Ejecuta informes para ver una visión más holística de una empresa con el fin de tomar decisiones presupuestarias sobre las actualizaciones de hardware en los próximos años, basándose en marcas y modelos actuales.

Corrección de software

Las empresas necesitan saber cuándo se ha instalado un software no aprobado y poder corregirlo posteriormente.

SOLUCIÓN

- ✓ Configura un grupo dinámico en ESET PROTECT para buscar un software específico indeseado.
- ✓ Crea una notificación para avisar al departamento de IT cuando el ordenador cumpla los criterios.

- ✓ Configura una tarea de desinstalación de software en la consola de ESET PROTECT para que se ejecute automáticamente cuando un equipo cumpla con los criterios del grupo dinámico.
- ✓ Configura una notificación para el usuario que aparezca automáticamente en tu pantalla para indicar si has cometido una infracción en la instalación del software en cuestión.

ESET PROTECT puede funcionar como una consola en la nube, puede instalarse en Windows o Linux, o puede implementarse como un dispositivo virtual.

La compatibilidad con la multipropiedad y los inicios de sesión protegidos por 2FA permiten optimizar totalmente las responsabilidades en los equipos de las grandes empresas.

“La seguridad centralizada en los endpoints, servidores y dispositivos móviles fue una utilidad fundamental para nosotros.”

— Responsable de IT, Diamantis Masoutis S.A.,
Grecia, más de 6000 puestos

Características técnicas

UN ÚNICO PANEL DE CONTROL

Todos los productos endpoint de ESET pueden ser gestionados desde una única consola de ESET PROTECT. Esto incluye estaciones de trabajo, móviles, servidores, máquinas virtuales y los siguientes sistemas operativos: Windows, macOS, Linux y Android.

SOPORTE PARA XDR

Para mejorar aún más el conocimiento de la situación y proporcionar visibilidad a través de tu red, ESET PROTECT trabaja junto con ESET Inspect, el componente de la plataforma ESET PROTECT que permite el uso de XDR. ESET Inspect es multiplataforma (Windows, macOS y Linux), permite la detección y corrección avanzada de amenazas y puede integrarse perfectamente con tu Centro de Operaciones de Seguridad.

CIFRADO DE DISCO COMPLETO (FDE)

El cifrado de disco completo es propio de ESET PROTECT y gestiona el cifrado de datos en endpoints tanto de Windows como de macOS (FileVault), mejorando la seguridad de los datos y ayudando a las empresas a resolver el problema del cumplimiento de la normativa de datos.

DEFENSA CONTRA AMENAZAS AVANZADAS

La capacidad de defensa contra amenazas avanzadas mejora en gran medida la detección de amenazas de día cero, como el ransomware, al analizar rápidamente los archivos sospechosos en la potente sandbox en la nube de ESET. Además, ejecuta una serie de análisis de malware muy completos, incluida la detención en la nube.

INVENTARIO DE HARDWARE Y SOFTWARE

ESET PROTECT no solo informa sobre todos los programas de software instalados de una empresa, sino también sobre el hardware instalado.

COMPLETAMENTE MULTIUSUARIO

Se pueden crear múltiples usuarios y grupos de permisos para permitir el acceso a una parte limitada de la consola de ESET PROTECT. Esto permite racionalizar completamente las responsabilidades en los equipos de una gran empresa.

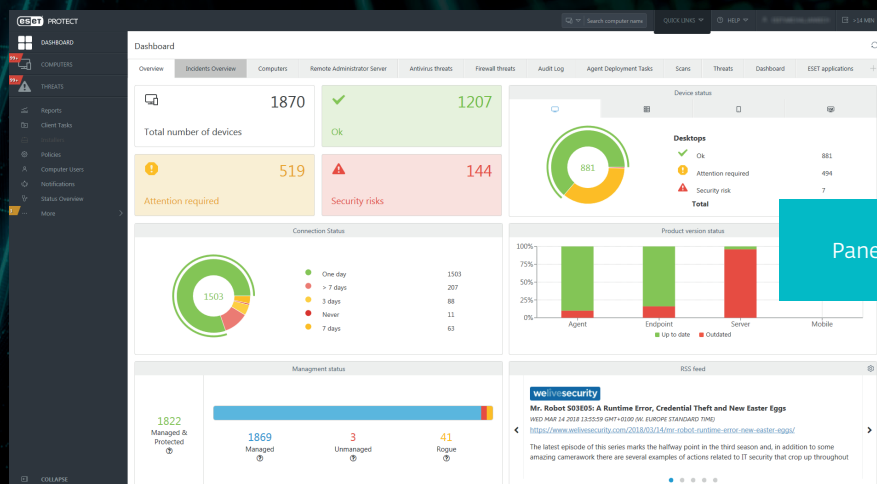
Esto hace posible hacer más desde una sola ubicación al agrupar dinámicamente los equipos en función de la marca, modelo, sistema operativo, procesador, memoria RAM, espacio en disco duro y muchos más elementos.

CONTROL DE POLÍTICA GRANULAR

Las empresas pueden asignar políticas múltiples al mismo equipo o grupo y anidarlas para los permisos heredados. Además, las empresas pueden configurar los ajustes de las políticas como configurables por el usuario, por lo que se puede bloquear a los usuarios finales la cantidad de ajustes que se desee.

SOPORTE TÉCNICO SIEM Y SOC

ESET PROTECT es totalmente compatible con las herramientas SIEM y puede emitir toda la información de registro en los fácilmente reconocibles formatos JSON o LEEF, lo que permite la conexión con los Centros de Operaciones de Seguridad (SOC).



Panel de control de ESET PROTECT



Pasos a seguir

Cómo comprar:

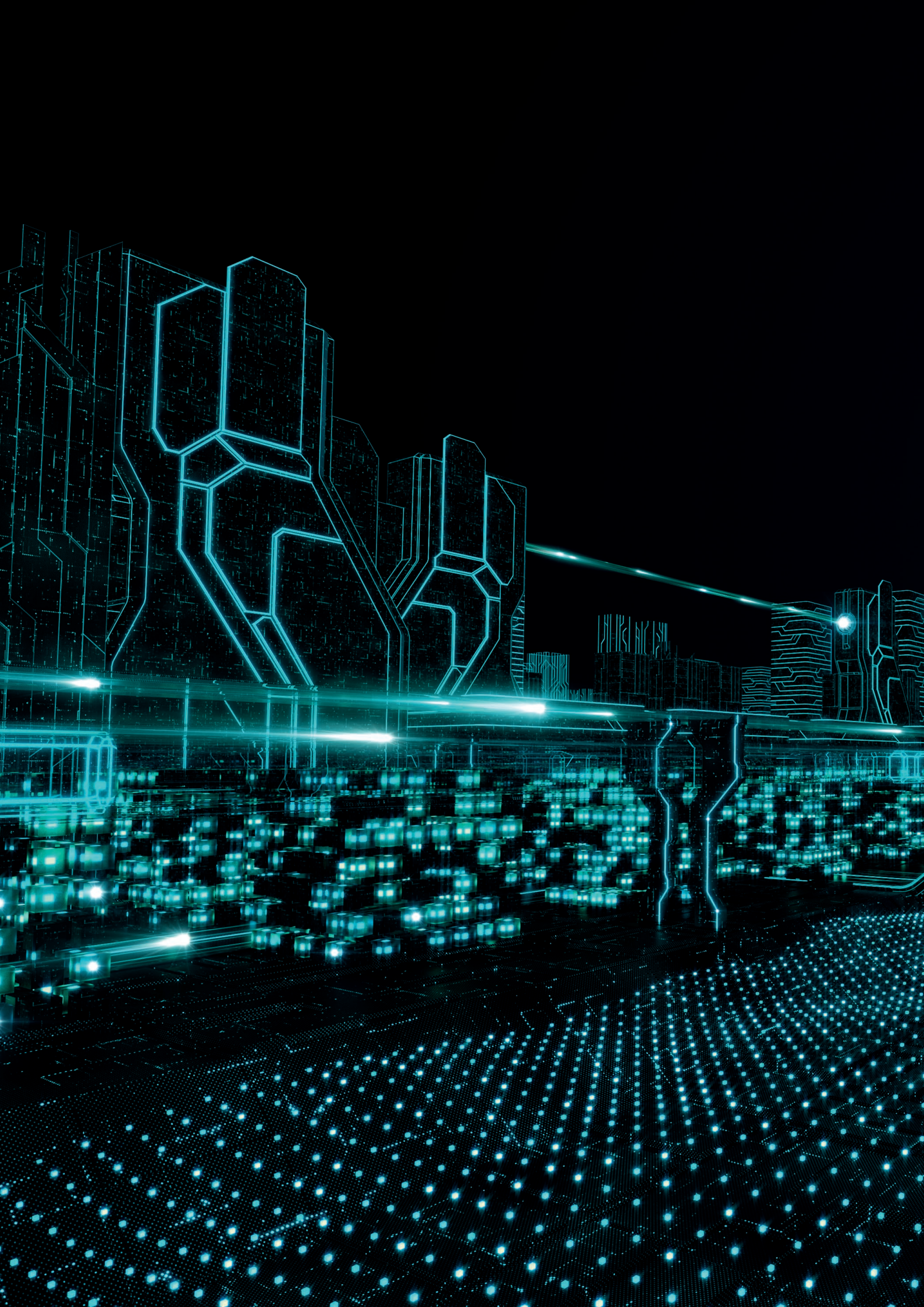
Solo tienes que adquirir cualquiera de las soluciones para empresas directamente en:
<https://www.eset.com/es/empresas/pymes/>

Inicia tu prueba de 30 días ahora

Desbloquea tu prueba gratuita de 30 días para probar la solución completamente equipada, incluyendo la protección de endpoints.

Migración desde una consola ESET local:

¿Ya utilizas una consola local de ESET?
Contacta con un representante de ESET de tu zona para que te ayude con la migración.
<https://www.eset.com/es/empresas/formulario-demo/>



Acerca de ESET

Durante más de 30 años, ESET® ha desarrollado software y servicios de seguridad informática líderes en el sector para ofrecer una protección completa y multicapa contra las ciberamenazas a empresas y consumidores de todo el mundo.

ESET es pionera en tecnologías de aprendizaje automático y en la nube que previenen, detectan y responden al malware. ESET es una empresa privada que promueve la investigación y el desarrollo científico en todo el mundo.

ESET EN CIFRAS

+100M

de usuarios seguros
en todo el mundo

+400k

clientes de
empresa

+200

países y
territorios

13

centros de I+D
en el mundo

ALGUNOS DE NUESTROS CLIENTES



Protegido por ESET desde 2017, con más de 9.000 endpoints



Protegido por ESET desde 2016, con más de 4.000 buzones de correo



Protegido por ESET desde 2016, con más de 32.000 endpoints



Colaborador de seguridad de ISP desde 2008, con una base de 2 millones de clientes

COMPROMETIDOS CON LOS MÁS ALTOS ESTÁNDARES DE LA INDUSTRIA



ESET recibió el premio Business Security APPROVED de AV-Comparatives en el Business Security Test en diciembre de 2021.



ESET consigue de manera consecutiva las mejores clasificaciones en la plataforma global de revisión de usuarios G2 y sus soluciones son apreciadas por clientes de todo el mundo.



Las soluciones de ESET son constantemente reconocidas por las principales firmas analistas, incluyendo en "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" como fabricante ejemplar.



Digital Security
Progress. Protected.

