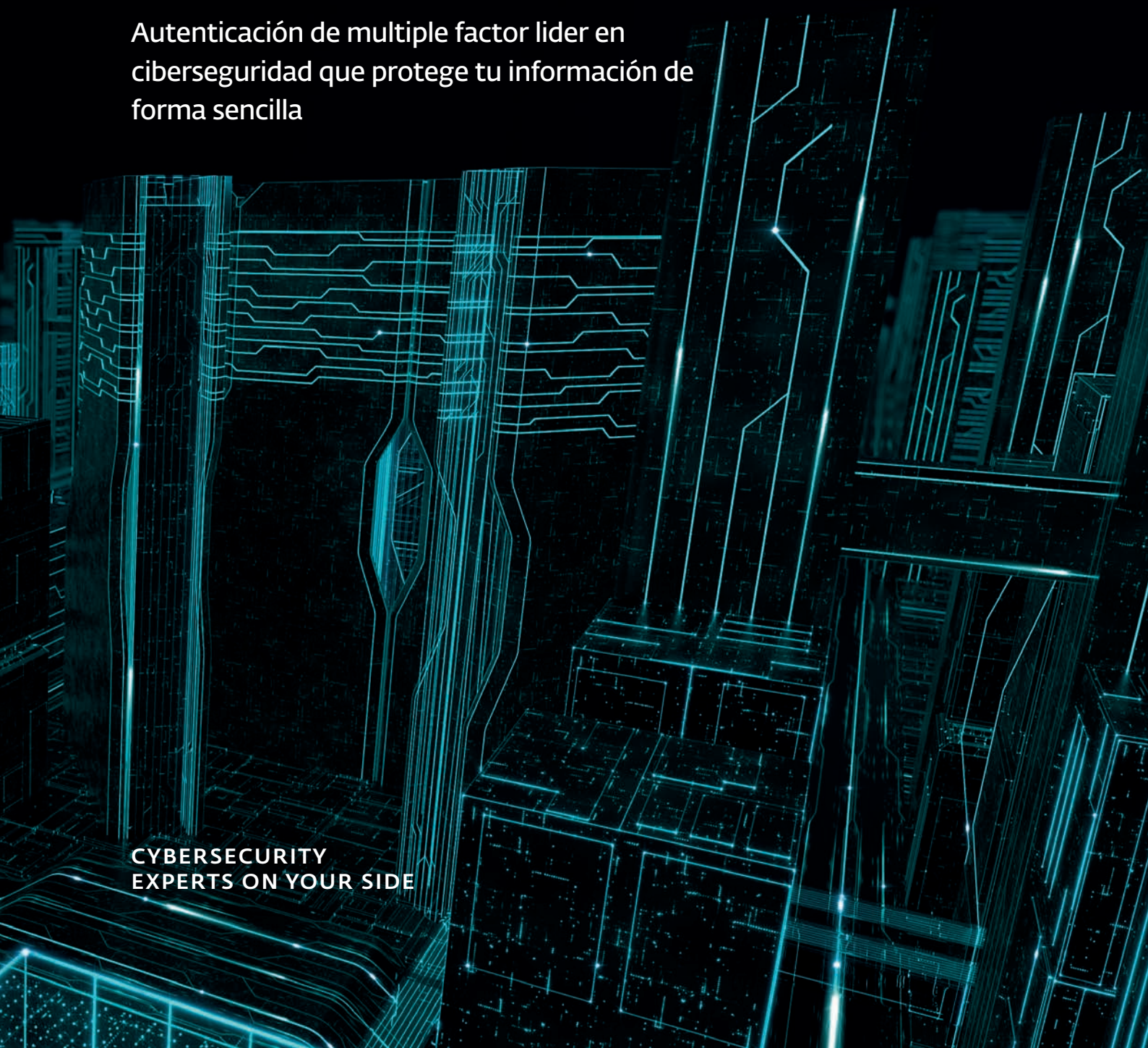
SECURE AUTHENTICATION

Autenticación de multiple factor lider en ciberseguridad que protege tu información de forma sencilla



¿Qué es la **Autenticación con múltiple factor?**

Es un método de autenticación que requiere dos piezas independientes de información para comprobar la identidad del usuario. La 2FA es mucho más fuerte que la autenticación con contraseña estática o PIN. Si complementamos la autenticación tradicional con un segundo factor dinámico, reduce eficazmente el riesgo de fugas de información provocado por contraseñas débiles o inseguras.

ESET Secure Authentication proporciona una solución sencilla para que las empresas de cualquier tamaño implementen MFA en sus sistemas más usados como VPNs, Escritorio Remoto, Microsoft 365, Outlook Web Access, el inicio de sesión del sistema operativo y mucho más.

¿Por qué elegir la **Autenticación con múltiple factor?**

Los empleados, además de usar la misma contraseña en varias páginas web y aplicaciones, a veces comparten libremente sus contraseñas con amigos, familia y compañeros de trabajo.

CONTRASEÑAS DÉBILES

Siempre se dice que "los empleados son el eslabón más débil" porque normalmente los empleados pueden poner a la empresa en riesgo de muchas formas. Uno de los más comunes es el uso de contraseñas débiles. Los empleados, además de usar la misma contraseña en varias páginas web y aplicaciones, a veces comparten libremente sus contraseñas con amigos, familia y compañeros de trabajo. Por si fuera poco, cuando las empresas implementan políticas de contraseñas, normalmente provoca que los empleados usen variantes de su anterior contraseña o que apunten las contraseñas en notas.

Una solución de autenticación con múltiple factor protege a las empresas contra la mala práctica de las contraseñas débiles implementando aparte de la contraseña normal una contraseña adicional, por ejemplo generándola en el teléfono del empleado. Teniendo esta solución implementada, evita que los atacantes obtengan acceso a tus equipos adivinando una contraseña débil.

FUGAS DE INFORMACIÓN

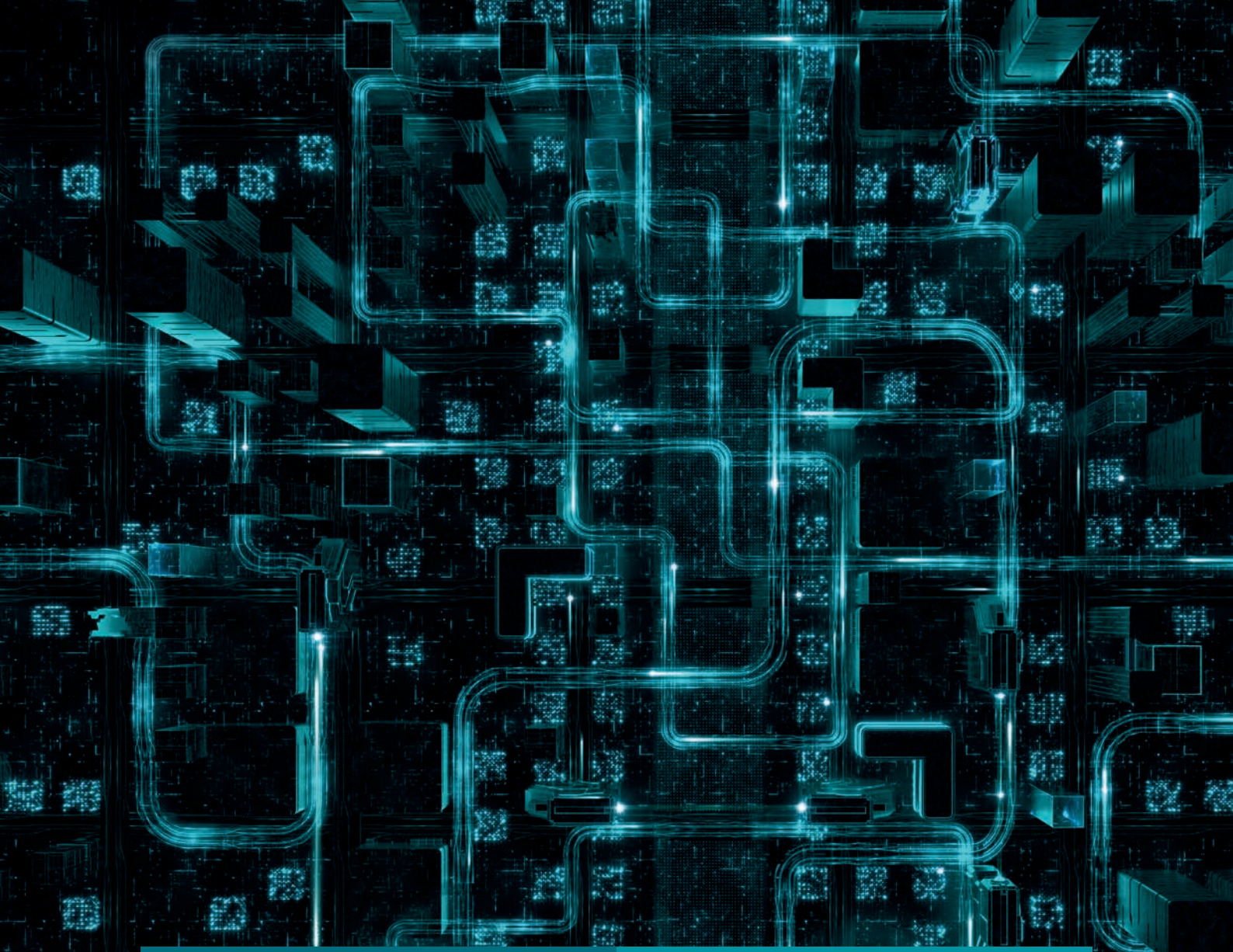
El panorama actual de la ciberseguridad cuenta un número creciente de fugas de información a diario. Una de las formas más comunes en la que los cibercriminales obtienen acceso a la información de las empresas es a través de contraseñas débiles o robadas. Únicamente protegiendo el inicio de sesión de los usuarios en servicios importantes, las empresas pueden implementar autenticación con múltiple factor en todas las escaladas de privilegios para evitar accesos no autorizados.

Añadiendo una solución con múltiple factor, las empresas consiguen que sea mucho más difícil para los cibercriminales obtener acceso a sus equipos y ponerlos en riesgo. Los sectores más vulnerables en cuanto a fugas de información son aquellos que tienen información importante como datos financieros, de ventas, sanidad y del sector público. Sin embargo, eso no significa que los demás sectores estén seguros, tan solo que los cibercriminales normalmente sopesan el esfuerzo necesario frente al posible beneficio.

CUMPLIMIENTO DE REGLAMENTOS

Cuando se trata de reglamentaciones, la mayoría de empresas necesitan primero evaluar si deben cumplirlas o no. Después, deben evaluar qué requisitos se recomiendan y cuáles se les obliga a implementar en la empresa. En el caso de la autenticación con múltiple factor, diversas directivas obligan a que se implementen, como PCI-DSS y GLBA, y la mayoría de reglamentos en general ponen el foco en la necesidad de una autenticación más fuerte, entre ellas la GDPR y la HIPAA.

La autenticación con múltiple factor ya no es una solución opcional para la mayoría de empresas que manejan tarjetas de crédito o transacciones financieras, sino que son un requisito obligatorio. Todas las empresas deberían investigar y evaluar si necesitan adaptarse para cumplir ciertos reglamentos.



Una de las formas más comunes en la que los cibercriminales obtienen acceso a la información de tu empresa es a través de contraseñas débiles o robadas.

Implementa esta solución y evita que los atacantes obtengan acceso a tus equipos adivinando una contraseña débil.

Autentícate con solo pulsar un botón, sin necesidad de reescribir la contraseña de un solo uso.

ESET marca la diferencia

ELIGE FÁCILMENTE TU MÉTODO DE INTEGRACIÓN

ESET Secure Authentication se ha diseñado para funcionar como solución independiente, gestionado desde una consola web. En un dominio de Windows, puedes elegir integrarlo con Active Directory. Esto hace que la configuración sea rápida y fácil, y elimina la necesidad de preparación adicional para implementar la 2FA en tu empresa.

SIN NECESIDAD DE HARDWARE DEDICADO

Todos los costes de ESET Secure Authentication están integrados porque no necesita ningún hardware adicional. Simplemente instala la aplicación de 10MB en cualquier servidor y empieza a proteger el acceso.

FUNCIONA CON LA MAYORÍA DE SMARTPHONES

Sin necesidad de tokens especiales o dispositivos para los empleados. ESET Secure Authentication funciona en todos los smartphones macOS y Android.

PUESTA A PUNTO EN 10 MINUTOS

Se han invertido muchas horas de desarrollo en la creación de ESET Secure Authentication para garantizar que la configuración sea lo más fácil posible. Hemos creado esta solución para que una empresa pequeña sin departamento de sistemas la pueda instalar y configurar. Tanto si una empresa tiene 5 usuarios o 100.000, ESET Secure Authentication, gracias a su capacidad para abastecer a múltiples usuarios a la vez, mantiene el tiempo de configuración lo más rápido posible.

SDK Y API COMPLETA INCLUIDAS

Para las empresas y grandes corporaciones que quieren sacar el máximo partido a ESET Secure Authentication, incluimos una SDK y API que las empresas pueden usar para ampliar su funcionalidad para adaptarse a sus necesidades.

AUTENTICACIÓN CON UNA PULSACIÓN

Permite autenticarte con una única pulsación, sin necesidad de reescribir la contraseña de un solo uso. Funciona con smartphones macOS y Android.

"Con una sola instalación en el servidor, una fácil configuración, la integración con Active Directory y una de sus mayores ventajas: una aplicación que podemos proporcionar a nuestros empleados para evitar la necesidad de envío de SMS constantemente. Además de esto, el hecho de que se integre perfectamente con VPNs nos hizo muy felices porque no tuvimos que cambiar la configuración de nuestra VPN para adaptarnos al producto."

Tom Wright, IT Service Officer, Gardners Books

Casos de uso

Prevenir fugas de información

Las empresas deben notificar públicamente a sus clientes que han sufrido una fuga de información, en caso de que ocurra.

SOLUCIÓN

- ✓ Protege comunicaciones vulnerables como Escritorio Remoto añadiendo autenticación con múltiple factor.
- ✓ Añade autenticación con múltiple factor a todas las VPNs en uso.
- ✓ Exige autenticación con múltiple factor para iniciar sesión en dispositivos que contienen información sensible.
- ✓ Protege tu información sensible con ESET Endpoint Encryption.

PRODUCTOS ESET

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Comprobar el proceso de inicio de sesión de los usuarios

Las empresas usan equipos compartidos y requieren la verificación de todos los usuarios que inician sesión a lo largo de la jornada laboral.

SOLUCIÓN

- ✓ Implementación de la autenticación con múltiple factor para iniciar sesión en equipos de escritorio en todos los espacios de trabajo compartidos.

PRODUCTOS ESET

- ✓ ESET Secure Authentication

Fortalecer la protección con contraseña

Los usuarios usan las mismas contraseñas en varias aplicaciones y servicios web poniendo en riesgo a las empresas.

SOLUCIÓN

- ✓ Restringir el acceso a los recursos de la empresa habilitando la autenticación con múltiple factor.
- ✓ Solicitar la autenticación con múltiple factor reduce la preocupación asociada a contraseñas compartidas o robadas solicitando una contraseña de un solo uso (OTP) además de la contraseña.

PRODUCTOS ESET

- ✓ ESET Secure Authentication

Características técnicas y plataformas que protege

AUTENTICACIÓN CON UNA PULSACIÓN

Autenticación con una única pulsación para todos los smartphones macOS y Android.

OTRAS FORMAS DE AUTENTICACIÓN

ESET Secure Authentication es compatible con aplicaciones móviles, envío de notificaciones, tokens hardware y los SMS para el envío de la OTP, así como otros métodos personalizados.

ADMINISTRACIÓN REMOTA

A través de la consola web de ESET Secure Authentication. Se integra con Active Directory para una fácil gestión, o funciona de forma independiente en empresas sin un dominio de Windows.

AMPLIA COMPATIBILIDAD

Redes privadas virtuales (VPN), Protocolos de Escritorio remoto (RDP), Outlook Web Access (OWA), VMware Horizon View y los servicios basados en Radius son totalmente compatibles con ESET Secure Authentication.

PROTECCIÓN ADICIONAL DEL SISTEMA OPERATIVO

Autenticación adicional para iniciar sesión en escritorio y escaladas de privilegios, también están protegidos con la autenticación con múltiple factor.

Es compatible con Windows y también con macOS y Linux.

COMPATIBLE CON LA NUBE

Además de aplicaciones en local, ESET Secure Authentication también es compatible con servicios web o en la nube como las aplicaciones de Google Apps, Microsoft 365, Dropbox y muchos otros.

COMPATIBLE CON TOKENS FÍSICOS

Aunque no son necesarios tokens físicos, son compatibles todos los tokens HOTP basados en eventos que pertenecen al tipo OATH.

VPNS COMPATIBLES

VMware Horizon View, Barracuda, Cisco ASA, Citrix XenApp,Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

Soporte para la integración personalizada de cualquier VPN basada en RADIUS.

Acerca de ESET

ESET, pieza clave en la seguridad de la información, ha sido nombrado el único Challenger en el Cuadrante mágico Gartner para plataformas de protección de equipos*

Durante más de 30 años, ESET ha desarrollado programas de seguridad informática y servicios líderes en el sector, que proporcionan una protección exhaustiva al instante contra las amenazas a la seguridad informática en constante evolución para empresas y consumidores en todo el mundo.

ESET es una empresa privada. Sin deudas ni préstamos, tenemos la libertad de hacer lo necesario para la máxima protección de todos nuestros clientes.

ESET EN NÚMEROS

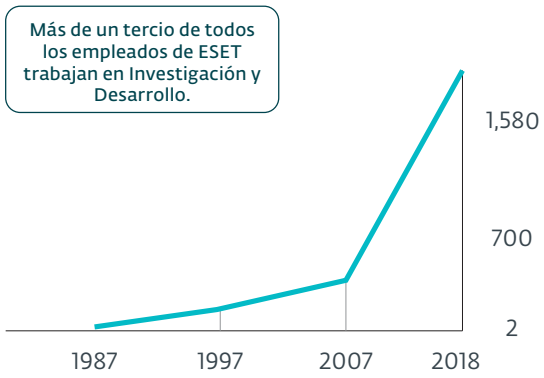
+110M
usuarios en todo el mundo

+400k
clientes empresa

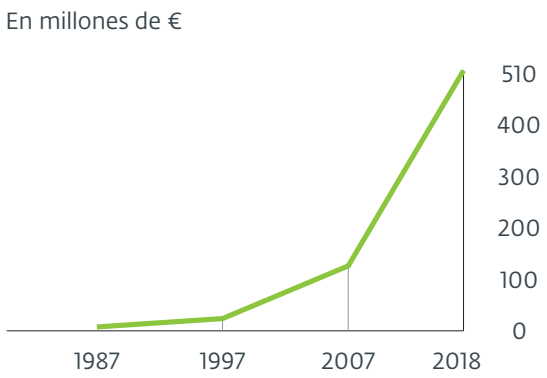
+200
países y territorios

13
centros globales de I+D

EMPLEADOS DE ESET



FACTURACIÓN DE ESET



*Gartner no promociona a ningún fabricante, producto o servicio que aparezca en sus artículos de investigación. Los artículos de investigación de Gartner representan la opinión de la empresa de investigación Gartner y no deberían interpretarse como exposición de hechos. Gartner niega cualquier responsabilidad, expresa o implícita, respecto a esta investigación, incluyendo toda garantía de comercialización o idoneidad para un objetivo determinado.

ALGUNOS DE NUESTROS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

protegido por ESET desde 2017,
más de 14.000 equipos

Canon
Canon Marketing Japan Group

protegido por ESET desde 2016,
más de 9.000 equipos

Allianz Suisse

protegido por ESET desde 2016,
más de 40.000 buzones de correo

Distribuidor ISP desde 2008.
2 millones de clientes base

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES

"Dadas las buenas características tanto en anti-malware y manejabilidad, como el alcance global en el soporte de clientes, ESET debe estar preseleccionada para su consideración en las RFPs para las soluciones anti-malware."

KupppingerCole Leadership Compass Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER TECHNOLOGY™