FICHA DE PRODUCTO

# SECURE AUTHENTICATION

Potente autenticación multifactor
para un acceso seguro a redes y datos

Progress. Protected.

# ¿Qué es la **autenticación multifactor?**

**La autenticación multifactor (MFA, por sus siglas en inglés), también conocida como autenticación en dos factores (2FA), requiere dos elementos independientes para verificar la identidad de un usuario. La MFA es mucho más segura que el uso de una contraseña o un PIN estático tradicional. Al complementar la autenticación tradicional con un segundo factor dinámico, reduce de manera efectiva el riesgo de filtraciones de datos causadas por contraseñas débiles o comprometidas.**

ESET Secure Authentication ofrece una forma sencilla para que empresas de todos los tamaños implementen la autenticación multifactor (MFA) en sistemas comúnmente utilizados, como VPNs, Protocolo de Escritorio Remoto (RDP), Outlook Web Access, inicio de sesión en sistemas operativos y más.


Digital Security
Progress. Protected.

# Prevén las filtraciones de datos y protege los activos de tu empresa

La autenticación multifactor puede ayudar a mitigar los riesgos del 'credential stuffing' (un ataque que utiliza información comprometida de los empleados). Este riesgo se debe a quienes:

- Usan la misma contraseña en varias aplicaciones y sitios
- Comparten sus contraseñas con otras personas
- Hacen solo cambios mínimos al actualizar sus contraseñas

## CONTRASEÑAS DÉBILES

Los datos son uno de los activos más importantes de tu empresa. Sin embargo, tú y tus empleados podéis ponerlos en riesgo de muchas maneras. Uno de los mayores peligros es la mala higiene de las contraseñas. No solo reutilizáis la misma contraseña en varios sitios web y aplicaciones, sino que, a veces, las compartís libremente con amigos, familiares y compañeros de trabajo. Si esto no fuera suficiente, cuando las empresas imponen políticas de contraseñas, suele provocar que los empleados utilicen variantes de sus contraseñas anteriores o las apunten en notas adhesivas.

Una solución de autenticación multifactor protege a la empresa contra la mala higiene de las contraseñas al añadir, además de la contraseña habitual, un factor adicional de autenticación, como generarlo en el teléfono del empleado.

Al implementar esta solución, ayudas a prevenir que los atacantes accedan a tus sistemas adivinando contraseñas débiles o explotando credenciales de empleados comprometidas.

## FUGA DE DATOS

En el panorama actual de ciberseguridad, cada día ocurren un mayor número de filtraciones de datos. Una de las formas más comunes en que los hackers pueden acceder a los datos de tu empresa es a través de contraseñas débiles o robadas, obtenidas mediante bots automatizados, phishing o ataques dirigidos. Además de proteger el acceso de los usuarios normales a servicios críticos, las empresas pueden implementar la autenticación multifactor (MFA) en todas las escaladas de privilegios para evitar accesos administrativos no autorizados.

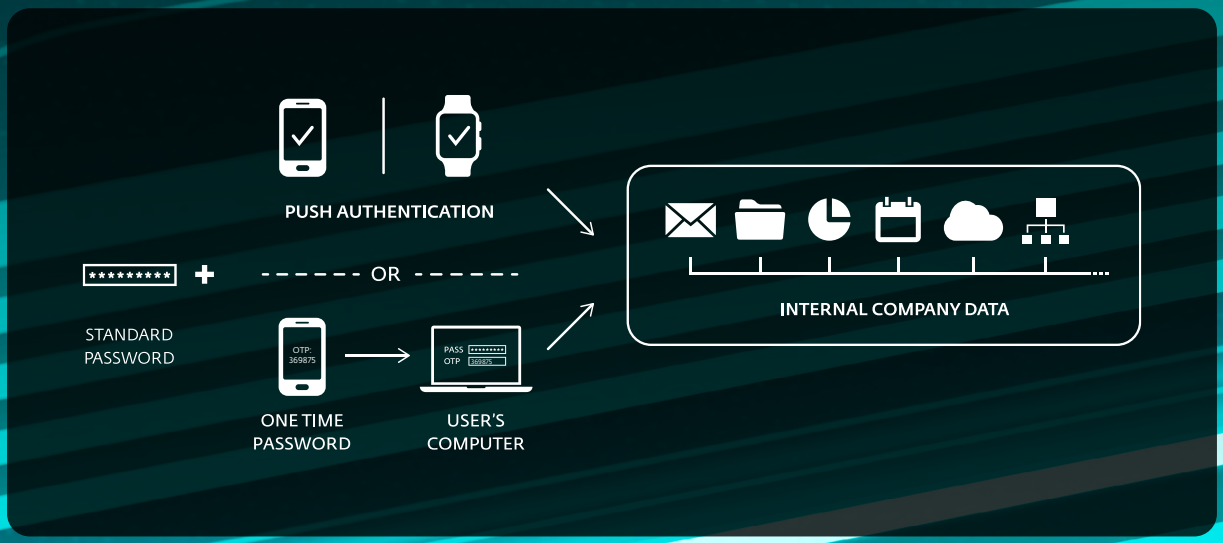
Al añadir una solución de autenticación multifactor, harás que sea mucho más difícil para los hackers acceder a tus sistemas y, en última instancia, comprometértelos. Las principales industrias afectadas por las filtraciones de datos suelen ser las que manejan datos valiosos, como las financieras, el comercio minorista, la sanidad y el sector público. Sin embargo, eso no significa que otras industrias estén a salvo, sino que los hackers suelen evaluar el esfuerzo necesario frente al beneficio obtenido.

## CUMPLIMIENTO

Cuando se trata de cumplimiento, la mayoría de las empresas primero necesitan entender si tienen que cumplir con algún objetivo de cumplimiento o no. Después, deben revisar qué medidas y recomendaciones debe implementar tu empresa para cumplir con ello. En cuanto a la autenticación multifactor, varias normativas, como PCI-DSS y GLBA, exigen que se implemente, y muchas leyes, incluyendo el RGPD y HIPAA, hacen hincapié en la necesidad de una autenticación más fuerte.

La autenticación multifactor ya no es solo una opción para la mayoría de las empresas que gestionan tarjetas de crédito o transacciones financieras, sino una solución obligatoria. Todas las empresas deben examinar qué leyes y normativas se aplican a ellas y asegurarse de cumplir con sus requisitos.

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



# ESET marca la diferencia

## AUTENTICACIÓN PUSH

Te permite autenticarte con un solo toque, sin necesidad de volver a escribir la contraseña de un solo uso. Funciona con teléfonos inteligentes iOS y Android.

## PROTEGE TUS APLICACIONES EN LA NUBE

Añade MFA para reforzar el acceso a servicios como Google Apps, Dropbox y muchos otros. ESET admite la integración a través del protocolo de autenticación SAML-2 utilizado por los principales proveedores de identidad.

## CONFIGURACIÓN EN 10 MINUTOS

Hemos trabajado duro para que no tengas que hacerlo tú. Nuestro objetivo era crear una solución que incluso una pequeña empresa sin personal de IT pudiera configurar e instalar. Ya sea que tu empresa tenga decenas o miles de usuarios, ESET Secure Authentication, gracias a su capacidad para provisionar múltiples usuarios al mismo tiempo, mantiene el tiempo de configuración al mínimo.

## MÚLTIPLES FORMAS DE AUTENTICAR

No es necesario utilizar tokens o dispositivos especiales para los empleados. ESET Secure Authentication funciona de manera fluida en teléfonos inteligentes, tiene su propio PIN para mayor seguridad y puede integrarse con las biometrías de los dispositivos (Touch ID, Face ID, huella dactilar en Android) para una mayor seguridad y una mejor experiencia de usuario. Cuando es necesario, también admite tokens de hardware o claves de seguridad FIDO.

## NO NECESITA HARDWARE DEDICADO

Los requisitos de recursos de ESET Secure Authentication son mínimos: puedes utilizar la versión en la nube, por lo que no necesitarás un servidor dedicado. Al mismo tiempo, la solución también ofrece una alternativa de implementación local.

## INTEGRACIÓN SIN INTERRUPCIONES

La solución ofrece dos modos de integración: integración con Active Directory para empresas que usan un dominio de Windows, o modo independiente, adecuado para aquellas que no tienen uno. De cualquier manera, la instalación y configuración son rápidas y fáciles, todo gestionado de manera fluida a través de una consola en la nube.

## MULTIUSUARIO

La versión en la nube de ESET Secure Authentication ha sido diseñada con capacidad de gestión multiusuario para que los Proveedores de Servicios Gestionados (MSP) puedan administrar múltiples empresas o sitios, ofreciendo la flexibilidad de definir configuraciones específicas para grupos individuales de usuarios.

## VDI Y VPN COMPATIBLES

Son compatibles VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet, FortiGate, Juniper, Palo Alto y SonicWall. También se ofrece soporte para la integración personalizada con cualquier VPN basada en RADIUS.

## API Y SDK COMPLETOS INCLUIDOS

Para las empresas que desean llevar la autenticación multifactor más allá, hemos incluido una API y un SDK completos que los clientes pueden utilizar para extender la autenticación multifactor (MFA) a las aplicaciones o plataformas que utilizan, incluso sin un complemento dedicado.

# Casos de uso

## Protege múltiples puestos

### PROBLEMA

Una empresa MSP necesita gestionar varias sucursales o empresas con una variedad de políticas de seguridad y configuraciones.

### SOLUCIÓN

- ✓ Crea cada empresa como un sitio en el portal de ESET PROTECT Hub y asigna a cada uno una cierta proporción de la licencia de ESET Secure Authentication. Al volver a iniciar sesión en la consola, verás la opción de Menú "Empresas".
- ✓ La versión multiusuario en la nube, que no requiere ningún hardware local, permite gestionar la autenticación multifactor para diferentes empresas o sucursales desde una única instancia.

## Previene fugas de información

### PROBLEMA

Las empresas aparecen en las noticias todos los días para alertar a sus clientes de que ha ocurrido una fuga de datos.

### SOLUCIÓN

- ✓ Protege las comunicaciones vulnerables, como el Protocolo de Escritorio Remoto, añadiendo autenticación multifactor.
- ✓ Añade autenticación multifactor a todas las VPN que se utilicen.
- ✓ Requiere autenticación multifactor para iniciar sesión en dispositivos que contengan datos sensibles.

## Fortalece la protección de contraseñas

### PROBLEMA

Los usuarios tienden a utilizar las mismas contraseñas en varias aplicaciones y servicios web, lo que pone a las empresas en riesgo.

### SOLUCIÓN

- ✓ Restringe el acceso a los recursos de la empresa aprovechando la autenticación multifactor.
- ✓ La autenticación multifactor reduce la preocupación y el peligro asociado con contraseñas compartidas o robadas al requerir un factor adicional de autenticación, como la aprobación mediante mensaje push.

## Previene fugas de información

### PROBLEMA

Las empresas utilizan ordenadores compartidos en espacios de trabajo compartidos y requieren verificación de todas las partes que inician sesión a lo largo de la jornada laboral.

### SOLUCIÓN

- ✓ Implementa autenticación multifactor para los inicios de sesión en escritorios en todos los dispositivos en espacios de trabajo compartidos.

# Características técnicas y plataformas protegidas

| CARACTERÍSTICAS | DESCRIPCIÓN | |
|---|---|---|
| **MULTIUSUARIO**<br>Disponible solo para MSPs con la versión en la nube. | Varios puestos/empresas | ✓ |
| **PROTECCIÓN DE INICIO DE SESIÓN** | Inicio de sesión en Windows | ✓ |
| **PROTECCIÓN DE INICIO EN SESIÓN REMOTA** | Servidor RADIUS para protección VPN | ✓ |
| | Escritorio remoto | ✓ |
| **PROTECCIÓN DE APLICACIONES WEB** | Servidor Microsoft Exchange | ✓ |
| | Servidor Microsoft SharePoint | ✓ |
| | Acceso web al escritorio remoto | ✓ |
| | Microsoft Dynamics CRM | ✓ |
| | Acceso web remoto | ✓ |
| **PROTECCIÓN DE SERVICIOS DE FEDERACIÓN DE ACTIVE DIRECTORY (AD FS)** | | ✓ |
| **CONECTOR DE PROVEEDOR DE IDENTIDAD (SAML)** | | ✓ |
| **PROXY** | | ✓ |
| **API** | | ✓ |
| **LISTADO BLANCO DE IPS** | Listado blanco de IPs global | ✓ |
| | Listado blanco de IPs por función | ✓ |
| **PROVISIONAMIENTO** | OTPs basados en SMS | ✓ |
| | OTP de aplicación móvil | ✓ |
| | Notificación push de aplicación móvil | ✓ |
| | Token físico | ✓ |
| | FIDO | ✓ |
| **NOTIFICACIONES** | Problema | ✓ |
| | Inicio de sesión en la consola web | ✓ |
| | Usuario bloqueado | ✓ |
| | Usuario desbloqueado | ✓ |
| | Licencias | ✓ |
| **LIMITACIÓN DE VELOCIDAD** | Limitación de velocidad basada en el tiempo | ✓ |
| **REGISTROS DE AUDITORIAS E INFORMES** | Informe | ✓ |
| | Filtro | ✓ |
| | Exportar | ✓ |

# Esto es ESET

## Defensa proactiva. Minimiza los riesgos con la prevención.

Ve un paso por delante de las ciberamenazas conocidas y emergentes con nuestro enfoque basado en la IA y centrado en la prevención. Combinamos el poder de la IA y la experiencia humana para que la protección sea fácil y eficaz.

Experimenta la mejor protección de su clase gracias a nuestra información interna sobre ciberamenazas globales, compilada y examinada durante más de 30 años, que impulsa nuestra amplia red de I+D dirigida por investigadores reconocidos en la industria.

ESET PROTECT, nuestra plataforma de ciberseguridad XDR pionera en la nube, combina capacidades de prevención, detección y detección proactiva de amenazas de última generación con una amplia variedad de servicios de seguridad, incluida la detección y respuesta gestionadas.

Nuestras soluciones altamente personalizables incluyen asistencia local y tienen un impacto mínimo en el rendimiento, identifican y neutralizan las amenazas conocidas y emergentes antes de que puedan ejecutarse, respaldan la continuidad de la actividad de las empresas y reducen el coste de implementación y gestión.

ESET protege tu negocio para que puedas liberar todo el potencial de la tecnología.

## ESET EN CIFRAS

**+1000M**
de usuarios protegidos en todo el mundo

**+400k**
clientes de empresa

**200**
países y territorios

**12**
centros de I +D en el mundo

## ALGUNOS DE NUESTROS CLIENTES

MITSUBISHI MOTORS
Drive your Ambition

protegido por ESET desde 2017, más de 9.000 equipos

Allianz Suisse

protegido por ESET desde 2016, más de 4.000 buzones

Canon
Canon Marketing Japan Group

protegido por ESET desde 2016, más de 32.000 equipos

distribuidor ISP desde 2008, 2 millones de clientes base

## RECONOCIMIENTO

AV comparatives APPROVED Business Security DEC 2023

ESET es un líder **constante en las pruebas independientes** de AV-Comparatives y logra las mejores tasas de detección con cero o mínimos falsos positivos.

G2 Leader SPRING 2024

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**.

kuppingercole ANALYSTS

ESET es **reconocida como líder del mercado** y líder general en MDR según el Leadership Compass 2023 de KuppingerCole.