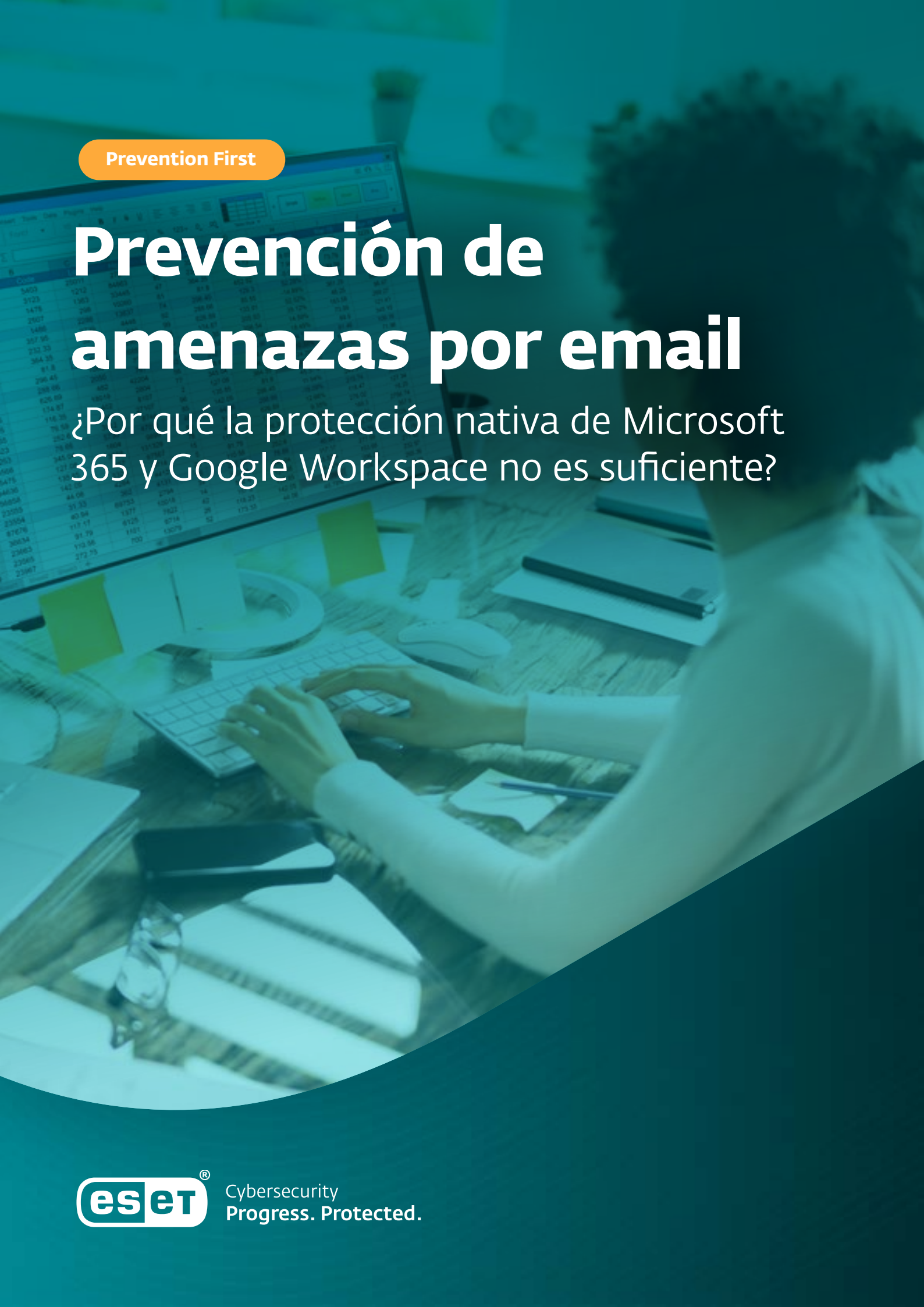

Prevention First

Prevención de amenazas por email

¿Por qué la protección nativa de Microsoft 365 y Google Workspace no es suficiente?

Cybersecurity
Progress. Protected.

Brechas de seguridad

Es seguro que las organizaciones forman parte de los 3,000 millones de usuarios de Google Workspace (que incluyen 1,800 millones de usuarios activos de Gmail), los 400 millones de usuarios de Outlook o los 320 millones de usuarios de la aplicación de colaboración Microsoft Teams; todas ellas, herramientas de negocios digitales esenciales

Tras su despliegue exitoso y la configuración de algunas reglas de seguridad, en un mundo ideal, los equipos corporativos podrían centrarse en tareas críticas para el negocio mientras trabajan en entornos de colaboración seguros

Ese no es necesariamente el caso. Existen **numerosos actores de amenazas que abusan de aplicaciones legítimas en la nube**, pero este problema tiene solución. Los responsables de TI deben implementar capas adicionales de seguridad.

Con las herramientas adecuadas, los administradores pueden minimizar la superficie de ataque que se propaga desde sus servicios en la nube, adoptando un enfoque centrado en la prevención que protege las aplicaciones de colaboración corporativa y el correo electrónico frente a las amenazas antes de que se ejecuten.

Entre los mayores desafíos que enfrentan las empresas en el ámbito de la seguridad de las aplicaciones en la nube, se encuentran, principalmente, las amenazas relacionadas con el correo electrónico:

PHISHING AND SPEAR-PHISHING

Los atacantes utilizan métodos innovadores, como el uso de códigos QR o de homógrafos, para engañar a las personas y lograr que escaneen o hagan clic en enlaces que parecen legítimos.

SUPLANTACIÓN DE IDENTIDAD E EMAIL SPOOFING

Los correos electrónicos que intentan engañar a las personas para que crean que se están comunicando con un remitente legítimo son cada día mejores, especialmente con el uso creciente de tecnologías de IA.

FACTOR HUMANO

Los empleados cometen errores, lo que hace que las puertas de enlace de correo electrónico sean especialmente atractivas para los atacantes. Las capacitaciones en ciberseguridad siguen siendo relevantes, ya que el factor humano continúa siendo el eslabón más débil de la cadena y ninguna tecnología puede funcionar al 100% si no se utiliza correctamente.

AMENAZAS ZERO-DAY

La IA también está facilitando que los adversarios creen amenazas nuevas o nunca antes vistas.

Email: el blanco ideal de los cibercriminales

El correo electrónico sigue siendo el principal vector de ciberamenazas. Durante los últimos años, ESET ha detectado y bloqueado millones de amenazas que lograron evadir la protección nativa tanto de Microsoft 365 como de la suite de oficina en la nube Google Workspace.

La mayoría de esas amenazas bloqueadas fueron mensajes de phishing y spam. Según Verizon, el tiempo medio que tardan los usuarios en caer en correos de phishing es de menos de 60 segundos. Su Informe de Investigaciones de Filtraciones de Datos (DBIR) de 2024 afirma que el '*Pretexting*' es una de las técnicas de ataque más utilizadas. Sus cifras casi se duplicaron entre 2022 y 2023, y actualmente el '*Pretexting*' está involucrado en alrededor del 20% de todos los ataques con fines financieros. La mayoría de los incidentes de '*Pretexting*' derivaron en el Compromiso del Correo Electrónico Empresarial (BEC), con un monto de transacción promedio de alrededor de $50,000 dólares, según el conjunto de datos del IC3 del FBI. Los datos más recientes muestran que esta tendencia no parece tener fin.

Según el Informe de Amenazas de ESET H2 2024, la detección de spam aumentó un 19 por ciento, y los archivos HTML maliciosos que redirigen a las víctimas a sitios web de phishing (el troyano HTML/Phishing.Agent) siguen siendo, por mucho, la amenaza de correo electrónico más frecuente. En conjunto, **estos ataques por correo electrónico representan casi una cuarta parte (23.8 por ciento) de todas las ciberamenazas** detectadas por ESET. Otras amenazas en la nube detectadas por la telemetría de ESET incluyen diversos tipos de malware, como puertas traseras (backdoors), programas espía (spyware), ladrones de información (infostealers) y descargadores (downloaders).

No tan seguro como crees

Aunque tanto Microsoft como Google han incorporado seguridad de alta tecnología directamente en sus aplicaciones en la nube, las cuales están protegidas y se actualizan con regularidad, esto no significa que sean inmunes a todas y cada una de

las amenazas que existen.

Ejemplos de la vida real demuestran que las aplicaciones y servicios legítimos en la nube pueden ser utilizados de forma indebida para distribuir malware, ocultar procesos maliciosos y permitir el acceso remoto a dispositivos corporativos:

- **Investigadores de ESET** detectaron en años recientes nuevas campañas de correos de phishing, realizadas por un actor de amenazas desconocido, dirigidas a empresas en países europeos. Los correos contenían archivos adjuntos maliciosos potenciados por AceCryptor, un malware del tipo 'cryptor-as-a-service' diseñado para ocultar a otros códigos maliciosos de las herramientas de ciberseguridad. De tener éxito, los atacantes podrían desplegar la herramienta de acceso remoto Rescoms (también conocida como Remcos) y espiar a su víctima..
- En la segunda mitad de 2024, Formbook, un ladrón de información (infostealer) descubierto por primera vez en 2016, experimentó un resurgimiento significativo, con un aumento en las detecciones de más del 200%. Este malware recopila, entre otras cosas, datos del portapapeles, pulsaciones de teclas (keystrokes), capturas de pantalla y datos almacenados en la caché del navegador. Se trata de una solución de 'malware-as-a-service' (MaaS), vendida en foros clandestinos, que se propaga a través de archivos adjuntos maliciosos en correos electrónicos de phishing. Los productos de ESET protegieron a casi 34,000 usuarios de este malware, principalmente en Europa Central y del Este, así como en Japón, Canadá y España.

920,000
amenazas detectadas en emails

813,000
emails de phishing bloqueados

110,000
amenazas de correo no provenientes de OneDrive, SharePoint, y Google Drive

75,820,000
spam de email capturado

*datos de 2024

¿Cómo mejorar la defensa *cloud*?

Está claro que la seguridad nativa de las aplicaciones en la nube no es suficiente por sí sola. Para minimizar esta creciente superficie de ataque, y para prevenir y mitigar las agresiones antes de que puedan causar daño, las empresas deberían considerar reforzar los controles integrados de Microsoft o Google con **capas adicionales de protección:**

Filtrado de Spam

Los mensajes de spam representaron más del 46,8 por ciento de los 362.000 millones de correos electrónicos enviados y recibidos diariamente en todo el mundo durante 2024. Con la solución de filtrado adecuada, las empresas pueden ahorrar una cantidad significativa de tiempo de sus empleados y evitar problemas con el spam malicioso.

Anti-phishing

En 2024, el phishing fue identificado como el vector de ataque inicial en el 22% de los ciberataques sufridos por empresas estadounidenses. Contar con una herramienta automatizada que reconozca los enlaces de phishing adjuntos a los correos electrónicos es absolutamente crítico.

Escaneo Anti-malware

Una buena solución de seguridad en la nube debería escanear automáticamente cualquier archivo nuevo o modificado en el almacenamiento compartido, con el fin de evitar que el malware se ejecute o se propague.

Análisis de comportamiento y entorno de sandbox

Dado que constantemente surgen nuevas amenazas, las herramientas de ciberseguridad automatizadas deben estar preparadas para ataques nunca antes vistos. Esto puede lograrse mediante un análisis de comportamiento profundo de muestras sospechosas en un entorno de sandbox aislado y seguro.

Anti-spoofing y motores de reglas

Los correos electrónicos adversos que ocultan su propia identidad y suplantan a un remitente legítimo deben ser detenidos. Con este control, solo los correos que parecen provenir de fuentes confiables son realmente legítimos y permitidos.

Protección contra homógrafos

Los atacantes utilizan caracteres visualmente similares para crear direcciones de correo electrónico o dominios engañosos que parecen legítimos. Detectar y bloquear estos ataques de homógrafos ayuda a prevenir el spear-phishing (phishing dirigido) y otras actividades maliciosas, garantizando que las comunicaciones de su organización permanezcan seguras.

¿Cómo ayuda ESET?

Tener tantas herramientas a disposición y gestionar un sistema de seguridad robusto puede parecer un desafío más; sin embargo, implementar seguridad adicional no tiene por qué aumentar necesariamente la complejidad del trabajo de un administrador de TI.

ESET Cloud Office Security brinda protección preventiva avanzada para las aplicaciones de Microsoft 365 y Google Workspace con todas las funciones mencionadas anteriormente. Mejora la postura de seguridad de una organización con protección avanzada contra amenazas, así como visibilidad y control del correo electrónico basado en la nube, el intercambio de archivos y las herramientas tanto de datos como de colaboración. Además de agilizar las operaciones y mejorar la seguridad, ESET Cloud Office Security contribuye a reducir la complejidad mediante la centralización y automatización de procesos rutinarios tales como

- Los nuevos usuarios dentro del entorno empresarial no necesitan ser añadidos manualmente por un administrador de TI en una consola, sino que quedan protegidos automáticamente tras la creación de su cuenta.
- Los administradores de TI pueden configurar intervalos de notificación para evitar la fatiga por alertas, garantizando al mismo tiempo que reciban las advertencias más importantes.
- Los archivos sospechosos pueden gestionarse fácilmente desde una cuarentena centralizada, con la posibilidad de liberarlos, eliminarlos o investigarlos por separado

con mayor detalle si fuera necesario.

- La solución permite una gestión multi-usuario (multi-tenant) para decenas de miles de usuarios, cubriendo cuentas creadas dentro de las dos plataformas más utilizadas: Microsoft 365 y Google Workspace.

Con un enfoque en la prevención y en la protección de los usuarios finales y sus dispositivos, **ESET Cloud Office Security** garantiza niveles más altos de protección contra amenazas para la organización al minimizar las superficies de ataque relacionadas con la nube, aliviando así la carga de trabajo de los administradores de TI mediante una consola de gestión en la nube fácil de usar.

INTEGRACIÓN

Por último, ESET Cloud Office Security cuenta con integración gratuita con **ESET LiveGuard Advanced**, una tecnología basada en la nube que utiliza escaneo avanzado, IA de última generación, *sandboxing* en la nube y análisis de comportamiento profundo para prevenir ataques dirigidos, así como amenazas nuevas o desconocidas, incluido el *ransomware*.

Como solución independiente o como parte de la plataforma ESET PROTECT, ESET Cloud Office Security ayuda a proteger a las organizaciones contra infecciones, minimiza las interrupciones laborales debidas a mensajes no deseados y contribuye a prevenir ataques dirigidos, así como tipos de amenazas nunca antes vistas, especialmente el ransomware.

Somos ESET

Defensa proactiva. Nuestra misión es minimizar la superficie de ataque.

Manténte un paso por delante de las ciberamenazas conocidas y emergentes con nuestro **enfoque basado en la prevención, impulsado por la IA y la experiencia humana**.

Disfruta de la mejor protección gracias a nuestra **inteligencia global sobre ciberamenazas propia**, recopilada y analizada durante más de 30 años, que impulsa nuestra amplia red de I+D liderada por **investigadores aclamados en la industria**. ESET protege su empresa para que pueda liberar todo el potencial de la tecnología.

EXPLORAR

Multicapa, con foco en prevención

IA de última generación se une a la experiencia humana

Inteligencia sobre amenazas de renombre mundial

Soporte personalizado e hiperlocal

eset
Cybersecurity
Progress. Protected.