

# Proofpoint Collaboration Security Prime

Seguridad de la colaboración completa y continua para la era de la IA

## Características principales

- Bloquea la mayor variedad de amenazas con una eficacia del 99,999 %.
- Contiene el compromiso de cuentas en minutos, independientemente de si la amenaza se origina en el correo electrónico, en otros vectores o en un proveedor comprometido.
- Reduce en un 40 % los clics en enlaces maliciosos reales en los seis meses posteriores al despliegue.
- Detiene la suplantación de identidad y cierra los dominios parecidos antes de que lleguen a sus clientes.
- Reduce el coste total de propiedad en un 40 % mediante la consolidación de plataformas.

**Esta suite de soluciones forma parte de la plataforma integrada Human-Centric Security de Proofpoint, que protege a las personas y los datos en los entornos de trabajo ágenticos.**

## Descripción general

La IA ha transformado el panorama para todos. Los ciberdelincuentes recurren a ella para lanzar ataques más innovadores y personalizados, con mayor sofisticación y alcance. Las campañas como las de Business Email Compromise (BEC) han aumentado un 27 %, y el phishing generado mediante IA registra ahora una tasa de clics 4,5 veces mayor que el phishing tradicional. Los usuarios son cada vez más vulnerables al contenido generado mediante IA, mientras que los responsables de la defensa se ven desbordados por la clasificación de alertas y la fragmentación de las herramientas.

Las organizaciones necesitan un enfoque radicalmente diferente, diseñado para la era de los agentes, en la que las herramientas y los asistentes basados en IA pasan a formar parte de una plantilla ampliada a través del correo electrónico, la mensajería instantánea y las aplicaciones cloud, lo que amplía aún más la superficie de ataque que ya explotan los ciberdelincuentes.

Desafortunadamente, muchas organizaciones se ven obligadas a adoptar un enfoque de seguridad fragmentado, basado en soluciones aisladas. Pero esto crea más brechas en las defensas, aísla a los equipos y aumenta la complejidad operativa.

Frente a los ataques impulsados por IA multicanal y multifase, y para proteger las interacciones de confianza entre personas, IA y aplicaciones cloud, las organizaciones requieren un enfoque más integral. Proofpoint Collaboration Security Prime puede ayudarle. Proofpoint Prime unifica la detección y respuesta ante amenazas en todo el entorno de trabajo agéntico.

### Le ayuda a:

- Detectar antes nuevas amenazas generadas mediante IA y obtener mayor visibilidad de toda la superficie de ataque.
- Bloquear con mayor confianza gracias a una precisión líder del sector y a un bajo índice de falsos positivos.
- Ofrecer protección continua antes y después de la entrega, en el navegador y con cobertura agéntica.
- Proteger las comunicaciones empresariales dondequiera que se produzcan, en chats, aplicaciones y agentes.
- Contener el compromiso de cuentas en minutos, no en días.

## Detección más temprana de nuevas amenazas con mayor visibilidad

Los nuevos ataques generados mediante IA se propagan más rápido de lo que las defensas tradicionales pueden detectarlos. Como resultado, están sorteando los filtros tradicionales y llegando a los usuarios a través del correo electrónico, las plataformas de colaboración y las aplicaciones cloud.

Proofpoint Collaboration Security Prime subsana esta vulnerabilidad mediante una protección continua que abarca todo el ciclo de vida de las amenazas, antes y después del envío del correo electrónico, desde el momento en que se hace clic hasta el inicio de sesión y en todos los canales que utilizan los empleados.

Proofpoint Prime protege frente a una amplia gama de amenazas:

- Phishing avanzado, incluido el de credenciales y el de devolución de llamadas
- BEC y suplantación de la identidad del CEO
- Distribución del malware
- Ataques con códigos QR
- Ataque por teléfono (TOAD)
- Envío masivo de correo electrónico
- Ransomware
- Usurpación de cuentas
- Abuso de servicios legítimos
- Ataques generados por IA y técnicas de explotación de la IA, como la inyección de prompts

La base de esta protección es Proofpoint Nexus® AI, el motor de detección más avanzado del sector. Entrenado con uno de los conjuntos de datos más grandes del sector, Nexus AI evalúa más de 1000 atributos por mensaje. Combina cinco tipos de modelos: modelos de lenguaje, gráficos de relaciones, aprendizaje automático, inteligencia sobre amenazas y visión artificial, que trabajan conjuntamente y aprenden continuamente de cada veredicto.

El resultado es una eficacia de detección del 99,999 % y la tasa de falsos positivos más baja del sector, lo que permite detener las amenazas reales sin saturar a los equipos con ruido innecesario.

## Protección frente al compromiso de cuentas

El compromiso de cuentas no se limita al phishing por correo electrónico. La IA está facilitando a los ciberdelincuentes llevar los ataques contra las credenciales mucho más allá de la bandeja de entrada, desde la creación de páginas de inicio de sesión convincentes que imitan a las legítimas hasta la elusión de la autenticación multifactor mediante el bombardeo automatizado de prompts.

En un entorno de trabajo impulsado por la colaboración y asistido por agentes, es fundamental detener estas amenazas en todas las etapas: antes, durante y después del compromiso.

Proofpoint Collaboration Security Prime ayuda a prevenir los compromisos antes de que se produzcan. SSO Password Guard de Proofpoint Prime detecta cuándo los empleados reutilizan su contraseña de

empresa en sitios web ajenos al trabajo, lo que elimina uno de los puntos de entrada más habituales para los ataques basados en credenciales y extiende la protección más allá del correo electrónico hasta el propio navegador.

Cuando la prevención no es suficiente, Proofpoint Prime detecta los compromisos de cuentas a medida que se producen. Correlaciona las señales de identidad y las posteriores al inicio de sesión en Microsoft 365, Google Workspace y Okta para identificar indicios de compromiso en las cuentas.

Una vez detectado un compromiso, Proofpoint Prime le ayuda a analizarlo y contenerlo en cuestión de minutos, en lugar de días, lo que limita su impacto antes de que el atacante pueda seguir avanzando por el entorno.

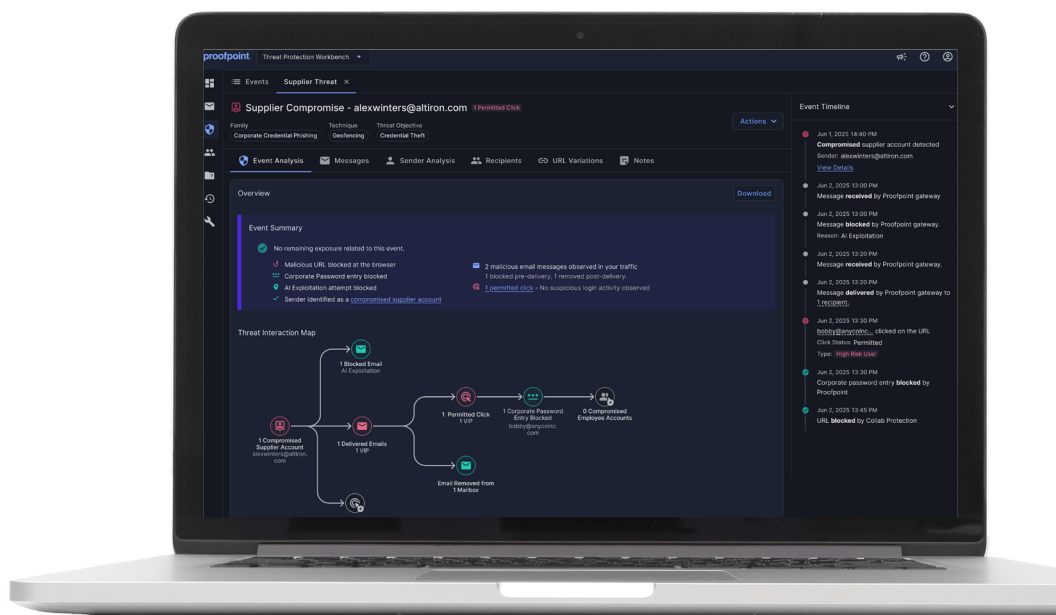


**Figura 1.** Proofpoint Collaboration Security Prime detiene y correlaciona las amenazas en el correo electrónico, las herramientas de mensajería y colaboración, la nube y los proveedores.

Los modelos Nexus® AI se entrenan con uno de los conjuntos de datos más amplios y diversos del sector de la ciberseguridad.

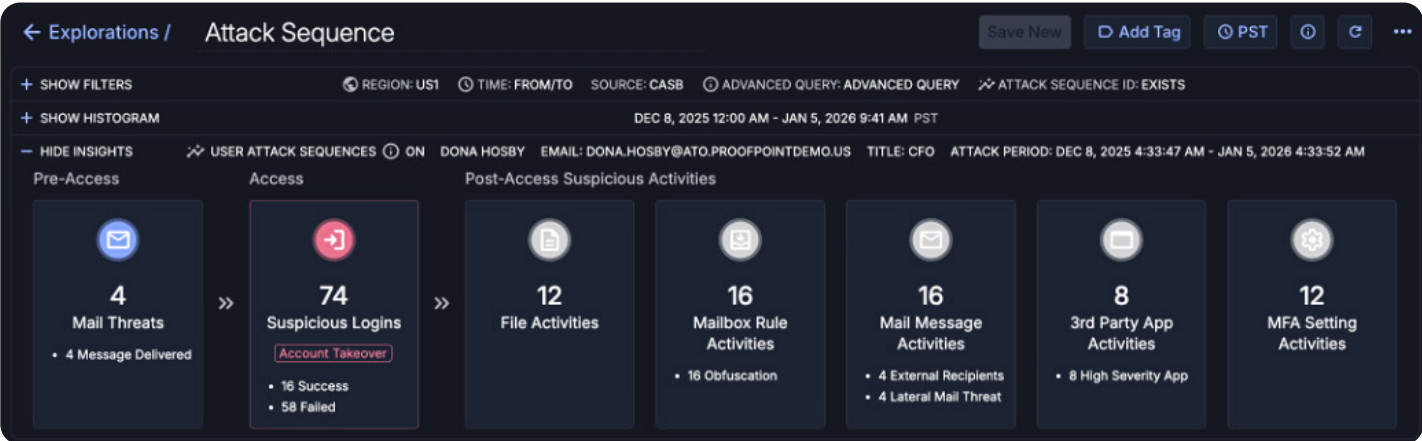


Figura 2. Proofpoint Collaboration Security Prime ofrece visibilidad sobre las secuencias de ataque y automatiza la contención.

## Protección de sus comunicaciones empresariales de confianza

Los ciberdelincuentes suelen recurrir a tácticas de suplantación de identidad para infiltrarse en comunicaciones empresariales de confianza, ya sea mediante la falsificación directa de dominios, el uso de dominios parecidos o cuentas de proveedores comprometidas. Cuando su organización o sus partners son víctimas de suplantación de identidad o de un compromiso, sus empleados y clientes quedan expuestos a riesgos, y su marca puede sufrir graves daños.

Proofpoint Collaboration Security Prime puede ayudarle a reducir estos riesgos de suplantación de la identidad de forma proactiva. Le ofrece una visibilidad completa de todos los correos electrónicos salientes enviados desde sus dominios de confianza, incluidos los de terceros. Tendrá acceso a potentes herramientas y a consultores expertos que le guiarán en cada paso del proceso de implementación de la autenticación del correo electrónico. Esto garantizará el cumplimiento de DMARC y evitará que los ciberdelincuentes suplanten sus dominios.

Nuestra protección se extiende más allá de los correos electrónicos generados por los usuarios para incluir un entorno seguro dedicado a retransmitir los mensajes generados por las aplicaciones, así como los correos electrónicos enviados por proveedores SaaS externos en su nombre.

En el caso de amenazas procedentes de proveedores, Proofpoint Prime protege a sus empleados contra el riesgo de explotación por parte de ciberdelincuentes que utilizan cuentas de terceros comprometidas. Detecta actividades sospechosas procedentes de cuentas de proveedores y aplica medidas de protección adaptativas, como indicadores de alerta y el aislamiento de URL, para reducir los riesgos sin interrumpir las comunicaciones empresariales legítimas.

Proofpoint Prime también ofrece funciones avanzadas para detectar dominios parecidos. Supervisa dinámicamente Internet para identificar dominios muy similares al suyo. Además, proporciona información detallada sobre su registro y sobre cualquier posible uso indebido.

No nos limitamos a la detección. Podemos desactivar las URL y los dominios maliciosos en su nombre gracias a las estrechas relaciones que mantenemos con los registradores, los proveedores de alojamiento web y los proveedores de dominios de nivel superior. Nuestros profesionales gestionan el proceso de principio a fin, para que sus equipos puedan centrarse en su actividad principal.

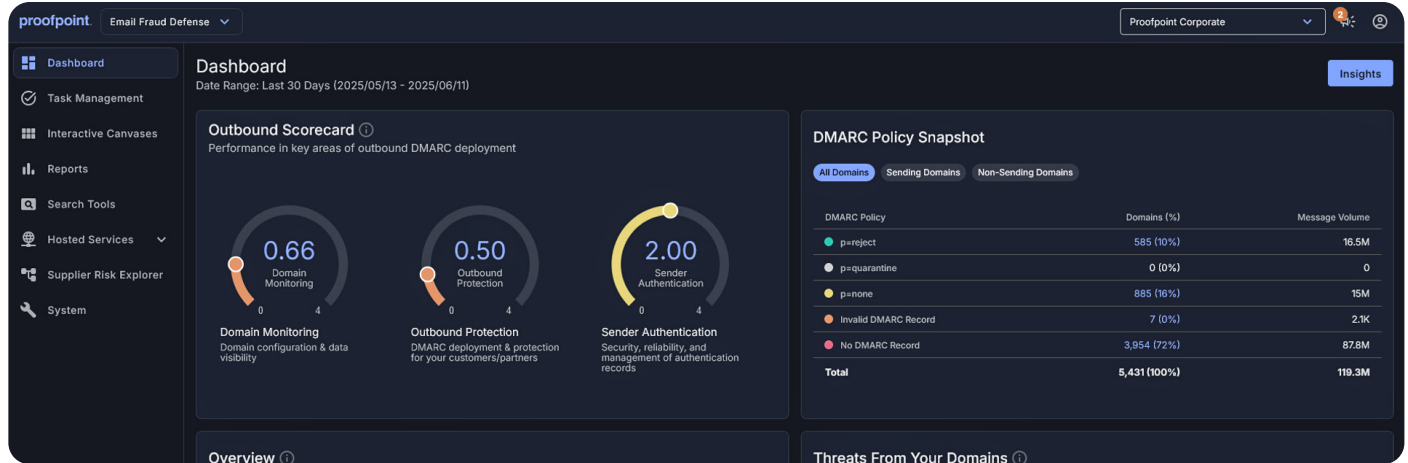


Figura 3. Proofpoint Collaboration Security Prime ofrece una visibilidad sobre las amenazas de suplantación de la identidad, como la suplantación de dominios y los dominios parecidos maliciosos.

## Refuerzo de la resiliencia de los usuarios mediante consejos basados en riesgos

A medida que el trabajo se vuelve más colaborativo y dinámico, es esencial que los empleados sean más resilientes frente a los ciberataques. Esto requiere ir más allá de una formación centrada en el cumplimiento normativo para abarcar la gestión de los riesgos relacionados con los usuarios, es decir, una formación en tiempo real que refleje la forma en que trabajan los usuarios y los riesgos reales a los que se enfrentan.

Proofpoint Collaboration Security Prime refuerza la resiliencia de los usuarios mediante un enfoque sistemático, no con una formación puntual, sino a través de un ciclo continuo vinculado a los riesgos reales.

Todo comienza con la identificación de los objetivos. Human Resilience Workbench recopila señales de comportamiento y riesgo de toda la plataforma e identifica automáticamente a los usuarios de alto riesgo, los nuevos empleados y los usuarios que hacen clic de forma recurrente, para que los equipos de seguridad puedan centrar su atención en lo que más importa.

A partir de ahí, Proofpoint Prime fomenta comportamientos más seguros cuando el riesgo es mayor. Con ThreatFlip, optimizado mediante IA, Proofpoint Prime transforma amenazas reales y activas en simulaciones instantáneas con un solo clic, para que los empleados puedan reconocer un ataque justo cuando se enfrentan a él, y no varias semanas después en un módulo de formación genérico.

Por último, Proofpoint Prime demuestra el impacto de estas medidas. Las puntuaciones de riesgo y los análisis comparativos ofrecen a los administradores una visión clara de dónde están mejorando los comportamientos y dónde siguen existiendo deficiencias. Las organizaciones que adoptan este enfoque registran un 40 % menos de clics en enlaces maliciosos reales durante los seis meses siguientes, lo que demuestra que la resiliencia, y no solo la concienciación, genera un cambio duradero.

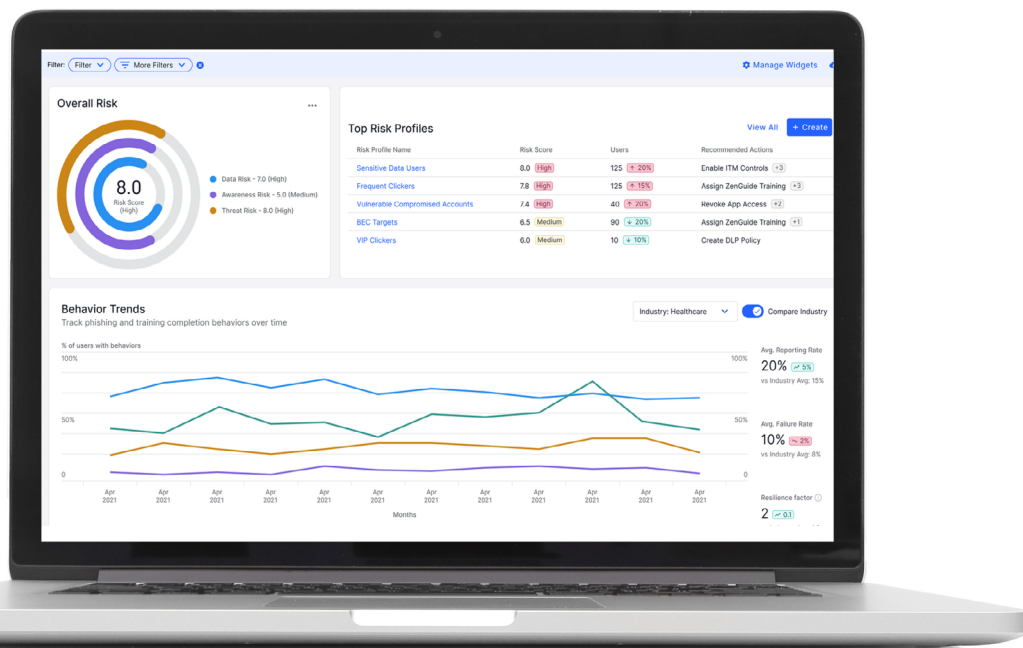


**Figura 4.** Proofpoint Collaboration Security Prime ofrece visibilidad sobre el comportamiento real de los usuarios, lo que permite ofrecer formación específica y basada en los riesgos.

## Simplificación de las operaciones de seguridad

A medida que las amenazas se expanden más allá del correo y alcanzan herramientas de colaboración, plataformas cloud y ecosistemas de proveedores, los equipos de seguridad deben hacer cada vez más con menos recursos. En este contexto, las soluciones puntuales y desconectadas no facilitan las cosas. No solo aumentan la complejidad, sino que también ralentizan los tiempos de respuesta y aumentan los costes operativos. Todo esto complica enormemente la reducción de riesgos a gran escala.

Proofpoint Collaboration Security Prime simplifica las operaciones de seguridad al unificar la detección y la investigación de amenazas, y al automatizar los flujos de trabajo y la respuesta. Gracias a las integraciones nativas, el Threat Protection Workbench puede recopilar información de detección y análisis detallados de ataques procedentes de plataformas de correo electrónico, mensajería instantánea y colaboración, cuentas cloud y ecosistemas de proveedores. De este modo, los equipos pueden investigar los incidentes y tomar medidas decisivas, todo ello desde un entorno de trabajo unificado para lograr la máxima eficacia.

Proofpoint Prime también ayuda a los equipos a establecer prioridades de manera eficaz. El Threat Interaction Map correlaciona las amenazas y los eventos de seguridad en todos los puntos de control, y proporciona un mapa visual de las vías de ataque. Esto permite a los analistas identificar rápidamente los incidentes más críticos. Al mismo tiempo, inspecciona automáticamente los mensajes denunciados por los usuarios, neutraliza el contenido malicioso y proporciona comentarios a los usuarios. Esto permite reducir las intervenciones manuales y reforzar los comportamientos seguros de los usuarios.

¿El resultado? Una respuesta más rápida y una menor complejidad operativa. Además, su equipo de seguridad puede hacer más con menos, sin sacrificar la protección.

## Elección del nivel adecuado de protección

Proofpoint Collaboration Security Prime está disponible en varios niveles, lo que le permite adaptar la protección al perfil de riesgo y las necesidades operativas de su organización. Cada nivel se basa en el anterior.

La cobertura abarca desde amenazas básicas por correo electrónico hasta canales de colaboración, pasando por el compromiso de cuentas, la reducción de riesgos relacionados con las personas y la protección avanzada de la marca.

Descubra las funciones disponibles en la página siguiente.



Más información en [proofpoint.com/es](https://proofpoint.com/es)

**Acerca de Proofpoint.** Inc. Proofpoint, Inc. es un líder mundial en ciberseguridad centrada en las personas y los agentes, que protege la forma en que las personas, los datos y los agentes de IA se conectan a través del correo electrónico, la nube y las herramientas de colaboración. Proofpoint es un partner de confianza para más de 80 de las empresas Fortune 100, más de 10 000 grandes empresas y millones de pequeñas organizaciones. Les ayuda a bloquear las amenazas, prevenir la pérdida de datos y reforzar la resiliencia de las personas y los flujos de trabajo de IA. La plataforma de colaboración y seguridad de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y responsabilizar a sus empleados, al tiempo que adoptan la IA de forma segura y con total confianza. Más información en [www.proofpoint.com/es](https://www.proofpoint.com/es)

Conecte con Proofpoint: [LinkedIn](#)

Proofpoint es una marca registrada o nombre comercial de Proofpoint, Inc. en Estados Unidos y/o en otros países. Todas las demás marcas comerciales contenidas en el presente son propiedad de sus respectivos propietarios.

**proofpoint**<sup>®</sup>

Todos los niveles de Proofpoint Collaboration Security están disponibles tanto para despliegues de SEG como para despliegues de API. La disponibilidad de las funciones puede variar en función del modelo de despliegue.

|                                                   | Funciones disponibles                                                                                                         | Proofpoint Core Email Protection | Proofpoint Collaboration Security Tier 2 | Proofpoint Collaboration Security Tier 3 | Proofpoint Collaboration Security Prime |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------------------|------------------------------------------|-----------------------------------------|
| Seguridad del correo electrónico                  | Protección contra ataques BEC, phishing, phishing de devolución de llamadas y malware                                         | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Pila de detección multicapa optimizada por Nexus AI                                                                           | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Datos sobre amenazas incomparables procedentes de más de 2,8 millones de clientes                                             | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Análisis en entorno aislado (sandbox) de archivos adjuntos y URL                                                              | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Reescritura de URL y análisis en entorno aislado (sandbox) al hacer clic                                                      | SEG                              | SEG                                      | SEG                                      | SEG                                     |
|                                                   | Aislamiento de clics sospechosos en URL reescritas                                                                            | VAP*                             | Todos los usuarios*                      | Todos los usuarios*                      | Todos los usuarios*                     |
|                                                   | Antispam y detección de correo gris                                                                                           | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Etiquetas de advertencias contextuales de correo electrónico                                                                  | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Herramientas adaptables de higiene de integridad de la mensajería con autoaprendizaje basado en el comportamiento del usuario | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Políticas de enrutamiento de correo electrónico configurables                                                                 | SEG                              | SEG                                      | SEG                                      | SEG                                     |
| Protección contra amenazas multicanal y multifase | Corrección automatizada de mensajes                                                                                           | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Automatización del buzón de correo malicioso                                                                                  | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Personas muy atacadas (VAP)™, ciberdelincuentes e inteligencia de amenazas global                                             | ✓                                | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Detección y corrección de cuentas cloud comprometidas                                                                         |                                  | ✓                                        | ✓                                        | ✓                                       |
| Resiliencia humana y concienciación en seguridad  | Bloqueo de URL maliciosas enviadas a través de aplicaciones de mensajería y colaboración                                      |                                  | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Detección del uso indebido de contraseñas corporativas en sitios web de riesgo o no autorizados                               |                                  | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Protección frente a cuentas de proveedores comprometidas                                                                      |                                  | ✓                                        | ✓                                        | ✓                                       |
|                                                   | Automatización de la formación basada en el nivel de riesgo                                                                   |                                  |                                          | ✓                                        | ✓                                       |
| Protección contra la suplantación de identidad    | Refuerzo de la concienciación de los empleados mediante simulaciones basadas en amenazas reales                               |                                  |                                          | ✓                                        | ✓                                       |
|                                                   | Conversión de amenazas activas en simulaciones seguras                                                                        |                                  |                                          | ✓                                        | ✓                                       |
|                                                   | Detección y priorización de usuarios en riesgo en función del comportamiento, la telemetría de amenazas y los roles           |                                  |                                          | ✓                                        | ✓                                       |
| Protección contra la suplantación de identidad    | Prevención del uso indebido de marcas mediante la autenticación de correos electrónicos                                       |                                  |                                          |                                          | ✓                                       |
|                                                   | Detección y corrección de dominios parecidos                                                                                  |                                  |                                          |                                          | ✓                                       |
|                                                   | Retransmisión segura de correos electrónicos generados por aplicaciones (250 GB)                                              |                                  |                                          |                                          | ✓                                       |

SEG = Despliegue de gateway de correo electrónico seguro únicamente \* = Disponible únicamente para los despliegues de SEG.