Especificaciones de rendimiento
365 Extended Email Protection

365 Extended Email Protection proporciona una capa adicional de seguridad para proteger el tráfico de correo electrónico de los clientes de Microsoft 365 a través de su enfoque Integrated Cloud Email Security. Los filtros antispam y antimalware impulsados por Inteligencia Artificial de Hornetsecurity analizan en tiempo real el tráfico de correo electrónico entrante en busca de ciberamenazas avanzadas y eliminan de forma fiable el spam y los correos maliciosos de las bandejas de entrada de los usuarios en cuestión de segundos. La integración totalmente automatizada y sin fisuras del servicio con la plataforma Microsoft 365 permite una supervisión continua de todos los buzones y se basa en la inteligencia sobre amenazas 24/7 de Hornetsecurity para garantizar la protección más actualizada.

El requisito previo para utilizar el servicio es el uso de licencias de Microsoft Cloud con funcionalidad Exchange habilitada por Microsoft.

Los siguientes servicios están incluidos en el producto 365 Extended Email Protection:

1. Fácil onboarding
    a. La configuración de 365 Extended Email Protection está automatizada. Todos los dominios, buzones y grupos del cliente se transfieren directamente desde Microsoft 365 al Panel de Control de Hornetsecurity.
    b. El prerrequisito para usar Hornetsecurity Services para Microsoft 365 implica la habilitación del Hornetsecurity App ID para el tenant de Microsoft 365 por parte de un usuario administrativo del cliente. Esto se hace una única vez durante el proceso de onboarding.
    c. No es necesario cambiar los registros MX para utilizar el servicio, ya que 365 Extended Email Protection se integra perfectamente con la plataforma 365 a través de la interfaz API. Todos los correos entrantes del cliente se copian y se filtran mediante los filtros avanzados de correo electrónico de Hornetsecurity.
    d. El onboarding puede realizarse directamente en el Panel de control o a través de un enlace externo de onboarding.

2. Inicio de sesión único
    a. Todos los usuarios con acceso administrativo pueden autenticarse en Hornetsecurity utilizando sus credenciales administrativas de usuario de Microsoft 365.
    b. Si los usuarios ya han iniciado sesión en Microsoft 365, no necesitan autenticarse de nuevo en Hornetsecurity.

3. Amenazas detectadas

a. Los correos electrónicos detectados como amenazas se muestran a los usuarios y se eliminan de los buzones en una vista general configurable y filtrable individualmente. Además, se muestra información detallada sobre cada correo electrónico.

b. Los correos electrónicos del cliente que se reciben son analizados por Hornetsecurity en busca de contenido malicioso (por ejemplo, virus) y publicidad no deseada (por ejemplo, spam). Los correos maliciosos y la publicidad no deseada se eliminan automáticamente de los buzones del cliente final.

c. Los usuarios pueden recuperar correos electrónicos de la vista general y entregarlos al destinatario.

d. Los correos eliminados se almacenan en cuarentena durante tres meses para que los usuarios puedan consultarlos y recuperarlos.

e. La tasa de detección de spam y amenazas es como mínimo del 99,9% de media mensual, basada en el número de todos los correos electrónicos que llegan a los sistemas de Hornetsecurity para dominios del cliente en el periodo de tiempo medido.

f. La tasa de falsos positivos es inferior a 0,00015 de media mensual, basada en el número de todos los correos limpios que llegan a los sistemas de Hornetsecurity para dominios del cliente en el periodo de tiempo medido.

4. Cuadro de mandos

El cuadro de mandos ofrece al usuario una visión general de los servicios de Hornetsecurity contratados.

5. Informes y conformidad

a. El cliente recibe amplia información y estadísticas sobre su estado actual de seguridad.

b. Esto incluye estadísticas de correo electrónico y estadísticas de amenazas avanzadas:

- Suma total de correos electrónicos escaneados
- Suma total de amenazas detectadas
- Correos electrónicos clasificados por amenaza a lo largo del tiempo
- Los 100 buzones más atacados
- Ataques a lo largo del tiempo
- Amenazas por tipo y vector de ataque
- Vectores de ataque a lo largo del tiempo

c. Las actividades realizadas por los usuarios del Panel de Control se registran en un Registro de Actividades, por ejemplo, la recuperación de un correo electrónico o la configuración correcta de otro servicio.

6. Política de Uso Razonable

a. El ancho de banda, almacenamiento, infraestructura y recursos necesarios para emplear nuestra solución se reparte a tal fin entre todos nuestros clientes. En consecuencia, tenemos derecho a tomar medidas para garantizar que todos los clientes empleen la solución de un modo razonable y justo, de un modo que no interfiera con o impida el rendimiento normal del servicio para otros clientes.

b. Hemos decidido no definir valores de referencia respecto a lo que constituye un uso excesivo o poco razonable, ya que, a nuestra discreción, podemos decidir mantener nuestros niveles de servicio normales reasignando recursos reservados a otros usuarios que no los estén utilizando en ese momento concreto, o ampliar los recursos de algún otro modo. Le informamos de que, en caso de que decidamos no hacer cumplir nuestra política de uso razonable, esto no implicará que hayamos renunciado a nuestro derecho a hacerlo, ni que hayamos dado nuestro consentimiento a que usted continúe utilizando nuestros servicios al mismo nivel en todo momento.

c. Para poder disfrutar de nuestros servicios, es necesario que adquiera unidades de facturación. El número de unidades de facturación que necesita dependerá de varios criterios, tales como el tamaño de su organización, la cantidad de usuarios y el tamaño de almacenamiento de los recursos en concreto, etc. Puede determinar el número de unidades de facturación que necesita siguiendo nuestros documentos de orientación, que hemos subido a nuestra página de tarifas y facturación con la asistencia de nuestro equipo de ventas.

d. Independientemente de la cantidad de unidades de facturación que haya adquirido, debe emplear nuestros servicios de modo razonable y, en concreto, de un modo que no nos obligue a reasignar recursos en número desproporcionado. Para determinarlo, compararemos su uso de nuestros recursos (por ejemplo, requisitos de memoria, número de conexiones paralelas) con el del cliente medio. Para determinar el cliente medio ignoramos el 5% de los clientes con mayor uso y el 5% de los clientes con menor uso del recurso en cuestión y hacemos una media de las cantidades entre todos nuestros clientes activos.

e. Las características específicas relacionadas con el sector en el que usted opera no se tendrán en cuenta a la hora de determinar si su uso puede considerarse razonable.

f. Si, actuando de modo razonable y de buena fe, consideramos que su uso de nuestra solución no sea razonable o atente contra esta directiva, tomaremos alguna de las siguientes medidas a nuestra exclusiva discreción:

   i. Permitirle continuar el uso de nuestras soluciones, pero a condición del pago de importes adicionales y en cumplimiento de condiciones que consideremos razonables en función de las circunstancias.

   ii. Notificarle el cierre de su cuenta en un plazo razonable establecido a nuestra discreción. Durante este tiempo, todos los servicios y/o operaciones se suspenderán.

g. Si ejercemos nuestro derecho a cerrar su cuenta del modo mencionado, ocurrirá lo siguiente:
   i. Todos los datos (metadatos, datos de copia de seguridad u otros) se eliminarán al término de un plazo definido en la notificación enviada a este respecto, sin perjuicio de lo establecido en las condiciones generales de contratación.
   ii. Se le realizará una devolución de los importes pagados por adelantado por los días restantes de su periodo de suscripción.