Seguridad de Microsoft 365
Creencias y Realidades

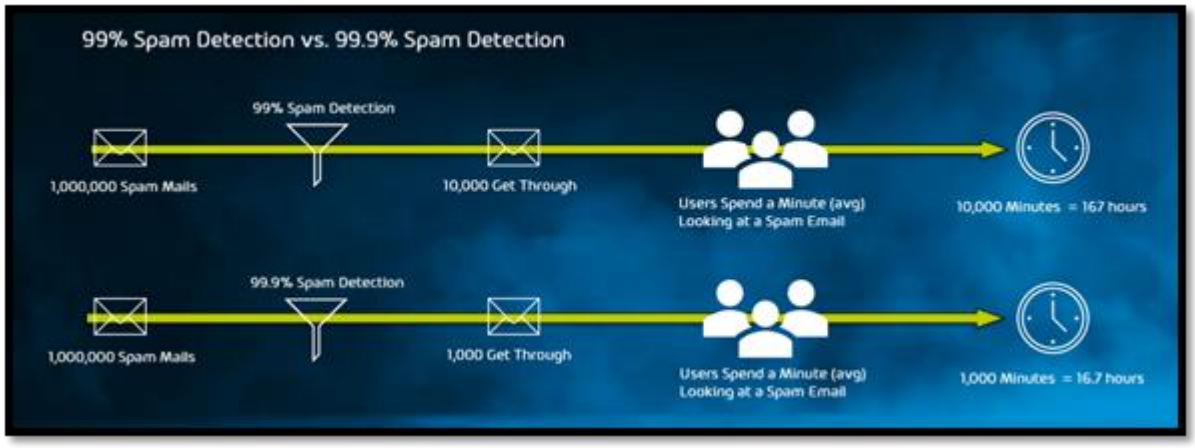
HORNETSECURITY

Lo entendemos, conformarse con lo predeterminado es agradable y fácil. Pero creer que la seguridad integrada de Microsoft 365 es lo suficientemente buena, está poniendo su negocio en peligro. Es hora de desmentir algunas creencias sobre la seguridad de M365 y mostrar algunas realidades.

CREENCIA

Los índices de detección de spam de Microsoft EOP son lo suficientemente altos

Mientras que los índices de detección de spam de Microsoft se sitúan en el 99%, el 1% restante deja mucho espacio a un gran número de amenazas para vulnerar su seguridad. Si tomamos 1.000.000 de correos electrónicos de spam, una tasa de detección del 99% dejará pasar 10.000 de ellos, haciendo que los usuarios pasen 167 horas viendo mensajes no deseados y potencialmente peligrosos. En comparación, la tasa de detección del 99,9% de Hornetsecurity reduce significativamente esas cifras, con sólo 1.000 correos electrónicos no deseados que pasan, y 16,7 horas dedicadas a revisarlos.



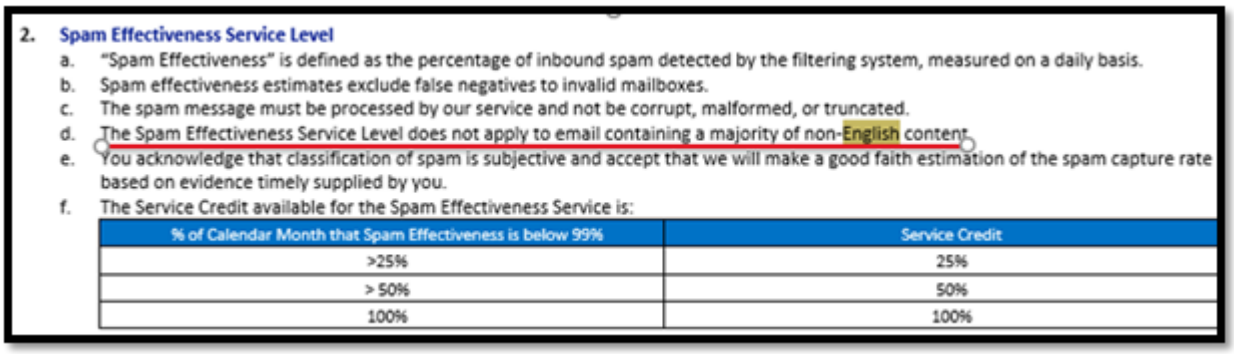
REALIDAD

Hornetsecurity ofrece los mayores índices de detección de virus y spam del mercado, con un 99,9% de detección de spam garantizada y un 99,99% de detección de virus, lo que disminuye en gran medida los correos electrónicos no deseados que llegan a las bandejas de entrada de los usuarios.

CREENCIA

Microsoft EOP reconoce el spam en todo tipo de correos electrónicos

La eficacia de los filtros de Microsoft NO se aplica a los correos electrónicos con contenido predominantemente no inglés, como se indica en sus propias condiciones de servicio. Por lo tanto, los correos electrónicos no deseados y peligrosos escritos en otros idiomas distintos del inglés se colarán entre las defensas de Microsoft. Y todos sabemos que las ciberamenazas no conocen barreras lingüísticas.



2. **Spam Effectiveness Service Level**
   a. "Spam Effectiveness" is defined as the percentage of inbound spam detected by the filtering system, measured on a daily basis.
   b. Spam effectiveness estimates exclude false negatives to invalid mailboxes.
   c. The spam message must be processed by our service and not be corrupt, malformed, or truncated.
   d. The Spam Effectiveness Service Level does not apply to email containing a majority of non-English content.
   e. You acknowledge that classification of spam is subjective and accept that we will make a good faith estimation of the spam capture rate based on evidence timely supplied by you.
   f. The Service Credit available for the Spam Effectiveness Service is:

% of Calendar Month that Spam Effectiveness is below 99%	Service Credit
>25%	25%
> 50%	50%
100%	100%

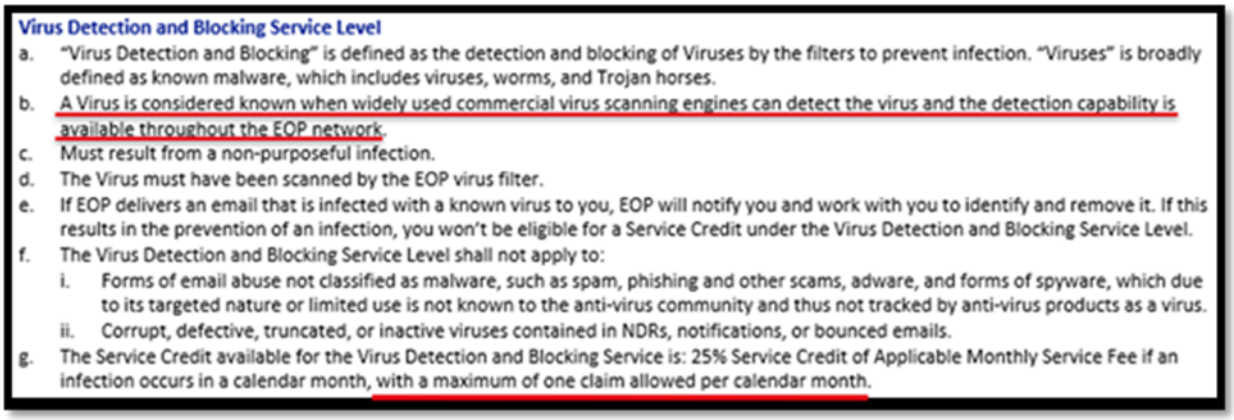
REALIDAD

Los filtros de Hornetsecurity no pierden eficacia por el contenido del correo electrónico que no está en inglés. Si las ciberamenazas no conocen barreras lingüísticas, Hornetsecurity tampoco.

CREENCIA

Microsoft EOP detecta todos los virus

Microsoft no ofrece ninguna garantía de protección contra virus desconocidos. Como se indica en sus condiciones de servicio, sólo se detectan los virus conocidos: se considera que un virus es conocido cuando los motores comerciales de escaneo de virus ampliamente utilizados pueden detectarlo. Para entonces, será demasiado tarde para su empresa si le ataca un nuevo virus desconocido.



Virus Detection and Blocking Service Level
   a. "Virus Detection and Blocking" is defined as the detection and blocking of Viruses by the filters to prevent infection. "Viruses" is broadly defined as known malware, which includes viruses, worms, and Trojan horses.
   b. A Virus is considered known when widely used commercial virus scanning engines can detect the virus and the detection capability is available throughout the EOP network.
   c. Must result from a non-purposeful infection.
   d. The Virus must have been scanned by the EOP virus filter.
   e. If EOP delivers an email that is infected with a known virus to you, EOP will notify you and work with you to identify and remove it. If this results in the prevention of an infection, you won't be eligible for a Service Credit under the Virus Detection and Blocking Service Level.
   f. The Virus Detection and Blocking Service Level shall not apply to:
      i. Forms of email abuse not classified as malware, such as spam, phishing and other scams, adware, and forms of spyware, which due to its targeted nature or limited use is not known to the anti-virus community and thus not tracked by anti-virus products as a virus.
      ii. Corrupt, defective, truncated, or inactive viruses contained in NDRs, notifications, or bounced emails.
   g. The Service Credit available for the Virus Detection and Blocking Service is: 25% Service Credit of Applicable Monthly Service Fee if an infection occurs in a calendar month, with a maximum of one claim allowed per calendar month.

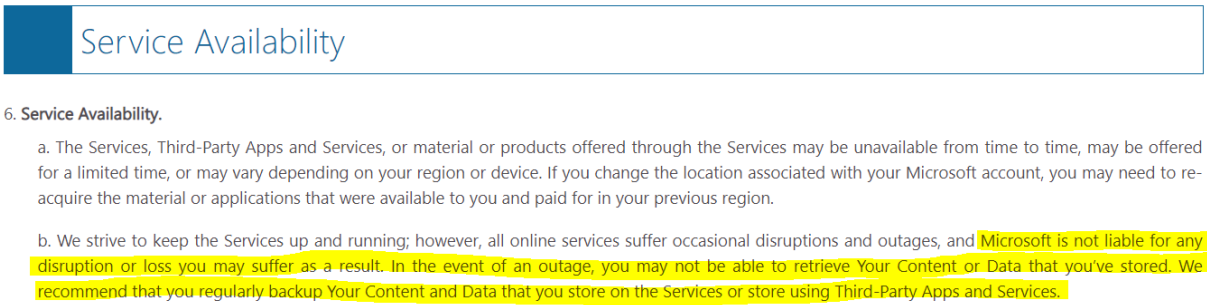
REALIDAD

Hornetsecurity detiene los virus nuevos y desconocidos con la detección temprana de virus, una característica fundamental de 365 Total Protection. Hornetsecurity no espera a que un virus sea reconocido por los motores de escaneo, protegemos a las empresas de todos los virus que existen, incluso si aún no han sido creados.

CREENCIA

Mis datos están seguros con Microsoft

Microsoft no se hace responsable de la pérdida de datos y correos en M365 y no ofrece opciones nativas de copia de seguridad y recuperación. Ellos mismos recomiendan el uso de un proveedor externo en sus Términos de Servicio para proteger los datos contra las interrupciones y cortes del servidor.



Service Availability

6. **Service Availability.**

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

HECHO

Hornetsecurity ofrece una solución integral de copia de seguridad y recuperación para los buzones de correo de Microsoft 365, los chats de Teams, las cuentas de OneDrive for Business, las bibliotecas de documentos de SharePoint y los dispositivos finales. Su fácil configuración y su gestión multi-tenant facilitan la copia de seguridad, la gestión y la restauración de todos los datos de Microsoft 365 de su empresa, de forma automática y sin complicaciones.

Hornetsecurity ofrece una solución integral que refuerza todos los puntos débiles de seguridad de Microsoft 365

- Análisis dinámicos, sistemas de filtrado multinivel con las tasas de detección más altas del mercado y mecanismos de análisis inteligentes basados en Inteligencia Artificial
- Seguridad avanzada del correo electrónico: sandboxing, reescritura de URL, protección contra el fraude de los CEO
- Protección de primera clase: más segura que EOP y ATP de Microsoft
- Primera elección de las empresas que quieren evitar el tiempo de inactividad de las comunicaciones
- Soporta todas las necesidades de cumplimiento normativo.
- Diseñado específicamente para Microsoft 365 e integrado a la perfección con el mismo: la implementación sólo lleva 30 segundos
- Gestión fácil y sencilla a través del panel de control
- Menor coste total en comparación con la compra de funciones por separado
- Copia de seguridad y recuperación de:
    - Buzones de Microsoft 365 y Teams
    - OneDrive y SharePoint
    - Dispositivos finales basados en Windows

Más información

No ponga en riesgo la seguridad de su empresa. Deje que Hornetsecurity se ocupe mientras usted se centra con seguridad en lo fundamental de su negocio.