AI POWERED

HORNETSECURITY

FACT SHEET

SPAM & MALWARE PROTECTION

Protección eficaz contra el spam y el malware con un sistema de filtrado multinivel totalmente automatizado.

El spam, que representa más del 50% de todo el tráfico de correo electrónico, es el método más intrusivo que utilizan los ciberdelincuentes para introducir malware y virus en los sistemas corporativos. Además del peligro de infección con ransomware, spyware o cryptominer, los flujos de trabajo importantes también pueden verse interrumpidos por la molesta avalancha de correos spam no deseados. Un sistema de filtrado multinivel es imprescindible para impedir que el spam y el phishing lleguen a las bandejas de entrada e interrumpan el flujo de trabajo.

Los buzones de correo merecen los filtros más potentes

- **Detección dinámica de virus**
- **Detección de spam multinivel y niveles de filtrado dinámicos**
- **Filtrado de salidas**

¿Qué se ve afectado?	¿Cómo te ayuda Spam & Malware Protection?			¿Qué mejora?
Entorno de correo electrónico	Los mayores índices de detección de spam (99,9%) y virus (99,99%) del mercado.	Maximización de la seguridad para las necesidades específicas de los tenant mediante la creación de reglas avanzadas dentro del filtro de cumplimiento.	Los correos electrónicos salientes se comprueban en busca de spam y virus.	Comunicación segura por correo electrónico entrante y saliente

HORNETSECURITY

FACT SHEET

MECANISMOS DE ANÁLISIS PRECISOS Y FILTROS CONFIABLES:

Phishing-Filter: El rastreo de enlaces y otros mecanismos protegen eficazmente contra los correos electrónicos de phishing. Entre otras cosas, se detectan comandos de scripts maliciosos. Esto permite, por ejemplo, la detección de las peligrosas descargas „drive by".

Infomail-Filter: Los boletines no clasificados como spam y otros correos promocionales que interrumpen el flujo de trabajo innecesariamente se clasifican y almacenan para su posterior recuperación. Se incluyen en el informe individual de cuarentena y pueden entregarse y ponerse en la lista blanca con un clic del ratón si es deseado.

Link-Tracking: Los correos electrónicos entrantes y salientes se escanean automáticamente en busca de direcciones URL maliciosas.

Actualización automática de la firma de virus: Los filtros de malware se actualizan constantemente y están siempre al día. Entre otras cosas, la empresa utiliza sus propios escáneres, que están especializados en el malware propagado por correo electrónico.

Outbound Filtering: Los correos electrónicos salientes se revisan en busca de spam y virus para evitar que el cliente envíe o reenvíe involuntariamente correos electrónicos maliciosos y spam.

Bounce-Management: En el tráfico de correo entrante, sólo los rebotes reales llegan al destinatario; los rebotes en respuesta al correo basura con direcciones de remitentes falsas se filtran de manera confiable.

Content Filter para los archivos adjuntos: Los adjuntos no deseados pueden rechazarse o ponerse en cuarentena.

Dynamic Virus Outbreak Detection: El sistema de alerta temprana detiene virus nuevos y anteriormente desconocidos. Hornetsecurity analiza permanentemente los correos entrantes en las llamadas cuentas „honeypot" (direcciones de correo electrónico que sólo tienen el propósito de recibir spam) en busca de archivos adjuntos, enlaces, remitentes o contenidos inusuales. La subsiguiente derivación de firmas se realiza en el tiempo de reacción más corto posible (normalmente <5 minutos).

Menos de 0,00015 falsos positivos: El número de correos electrónicos clasificados como spam accidentalmente, pero que son comunes, es inferior a 0,00015.

GESTIÓN Y FÁCIL CUMPLIMIENTO DE LAS **POLÍTICAS DE CONFORMIDAD:**

One-Click-Release: Los correos electrónicos en cuarentena pueden entregarse desde el informe de cuarentena con un solo clic del ratón, independientemente de que sean presuntamente spam o correos promocionales.

Buena visibilidad gracias al bloqueo: La gran mayoría de los correos electrónicos de spam se bloquean directamente. Esto le da al usuario una visión rápida de los correos electrónicos que están en cuarentena.

Alivio del servidor de correo: Spam and Malware Protection solo permite el paso de mensajes válidos, lo que aumenta significativamente el rendimiento del servidor de correo del cliente.