HORNETSECURITY

365 TOTAL PROTECTION PLAN 4

AMPLÍA TU CARTERA Y LA SEGURIDAD DE TUS CLIENTES

TODO LO QUE NECESITAS SABER SOBRE EL NUEVO 365 TOTAL PROTECTION PLAN 4

¿QUÉ OFRECE EL NUEVO PLAN 4?

365 Total Protection Plan 4 siempre ha sido la suite de seguridad de Microsoft 365 más completa del mercado, pero hemos decidido ampliarlo y mejorarlo aún más con AI.MY, el AI Cyber Assistant, y las nuevas soluciones que ofrece.

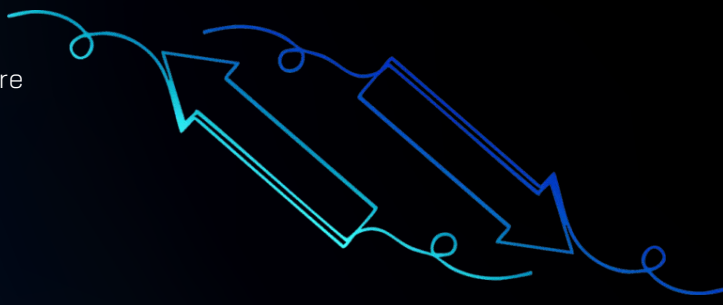
PLAN 4

INCLUDES 1 + 2 + 3

			POWERED BY AI CYBER ASSISTANT		
SECURITY AWARENESS	PERMISSION MANAGEMENT	DMARC REPORTING & MANAGEMENT	AI RECIPIENT VALIDATION	TEAMS PROTECTION	AI EMAIL SECURITY ANALYST
PHISHING & ATTACK SIMULATION	PERMISSION ALERTS	ENHANCED EMAIL REPUTATION & DELIVERY	COMMUNICATION PATTERN ANALYSIS	CHAT-BASED THREATS MONITORING	AI ANALYSIS OF USER REPORTS
ESI® REPORTING	PERMISSION AUDIT	EASY DNS MANAGEMENT & OPTIMISATION	SENSITIVE DATA CHECK	AI PHISHING DETECTION & RESPONSE	AI RESPONSE & AWARENESS

AI Cyber Assistant incorpora AI Email Security Analyst y Teams Protection, dos nuevas soluciones que amplían lo bueno y reducen lo malo.

AUMENTA



- Los recursos del SOC.
- Compromiso de los usuarios finales y concienciación sobre la seguridad.
- La postura general de seguridad.

REDUCE

- El tiempo que los equipos SOC dedican a analizar los correos electrónicos notificados por los usuarios.
- El número de usuarios finales desmotivados.
- Amenazas que llegan a través de los chats de Teams.

AI EMAIL SECURITY ANALYST AUTOMATIZA EL ANÁLISIS Y LA RESPUESTA DE LOS CORREOS ELECTRÓNICOS REPORTADOS

LOS PUNTOS DÉBILES:

- Falta de información y transparencia para los usuarios finales cuando se notifican correos electrónicos.
- Los equipos del SOC dedican una cantidad considerable de recursos a revisar manualmente los correos electrónicos.
- Riesgos de seguridad derivados de la fatiga de los usuarios, desmotivados y poco concienciados por la falta de feedback.

LA SOLUCIÓN:

- Con AI Email Security Analyst, los empleados reciben automáticamente un análisis en tiempo real y basado en inteligencia artificial de sus informes de correo electrónico, lo que les permite formarse de manera indirecta en las mejores prácticas de seguridad del correo electrónico.
- Liberación de recursos del SOC, al tiempo que se mantienen y mejoran los servicios de seguridad del correo electrónico gracias a la automatización y la retroalimentación instantánea.

DEJA QUE AI.MY AUTOMATICE EL ANÁLISIS Y LA RESPUESTA A LOS CORREOS ELECTRÓNICOS REPORTADOS

Los administradores de una empresa con **1000 empleados**

revisan manualmente alrededor de

correos electrónicos reportados **al mes**

dedicando

de media

TEAMS PROTECTION PROTEGE LOS CHATS DE TEAMS CONTRA URL MALICIOSAS Y BRECHAS DE SEGURIDAD

LOS PUNTOS DÉBILES:

- Falta de visibilidad sobre el contenido malicioso compartido a través de Teams.
- Exposición constante: los usuarios finales están constantemente expuestos a posibles mensajes maliciosos.
- Comunicación externa: cada vez más usuarios utilizan Teams para las comunicaciones externas.
- La eficiencia se ve afectada, ya que tanto los usuarios como los equipos de IT deben hacer frente a enlaces maliciosos, malware y mucho más.

LA SOLUCIÓN:

- Advertencia automática a los usuarios cada vez que se comparten enlaces maliciosos a través de los chats de Teams.
- Elimina conversaciones completas que contengan mensajes maliciosos e impide que sus remitentes inicien sesión en Teams.

DEJA QUE AI.MY ANALICE LOS ENLACES EN TEAMS EN BUSCA DE POPTENCIALES RIESGOS

Una empresa con
1000 empleados

envía

35000

mensajes de Teams a la semana,
de los cuales el 12% contiene enlaces

lo que equivale a

4200

enlaces potencialmente maliciosos

¿POR QUÉ DEBERÍAN HACER EL UPGRADE MIS CLIENTES?

El nuevo 365 Total Protection Plan 4 ofrece soluciones que benefician a todos, ya que refuerzan tanto a los usuarios finales como a los administradores, lo que fortalece la postura de seguridad de la empresa de manera sencilla:

- Se anima a los usuarios finales a informar sobre correos electrónicos sospechosos y a recibir automáticamente formación sobre seguridad informática para que aprendan a adoptar comportamientos seguros.
- Los equipos del SOC se liberan, en gran medida, de la carga de revisar manualmente los correos electrónicos, por lo que pueden reasignar sus recursos a tareas más urgentes.
- Los chats de Microsoft Teams, un vector de ataque que a menudo pasa desapercibido, quedan protegidos automáticamente y se notifica a los usuarios de inmediato cuando se comparte un enlace malicioso en una conversación, lo que garantiza que todos los frentes estén cubiertos.

¡Descubre el futuro de la ciberseguridad con de la solución más completa del mercado para Microsoft 365!