HORNETSECURITY

365 TOTAL PROTECTION PLAN 4

SCALE YOUR PORTFOLIO AND YOUR CUSTOMERS' SECURITY

EVERYTHING YOU NEED TO KNOW ABOUT THE NEW 365 TOTAL PROTECTION PLAN 4

WHAT DOES THE NEW PLAN 4 DO?

365 Total Protection Plan 4 always has been the most comprehensive Microsoft 365 security suite on the market, but we've decided to make it even bigger and better with AI.MY the AI Cyber Assistant, and the new solutions it powers.

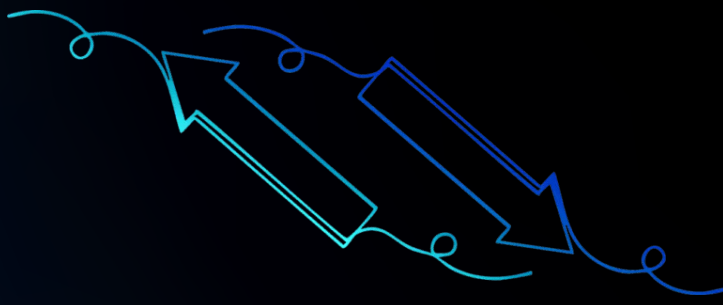
PLAN 4

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 brings AI Email Security Analyst and Teams Protection – Two new solutions that scale up the good and scale down the bad.

SCALE UP



» SOC resources.

» End user engagement and security awareness.

» Overall security posture.

SCALE DOWN

» The time SOC teams spend on analyzing user-reported emails.

» Disengaged end users.

» Threats that come through Teams chats.

AI EMAIL SECURITY ANALYST AUTOMATES THE ANALYSIS AND RESPONSE OF REPORTED EMAILS

THE PAIN POINTS:

» Lack of information and transparency for end users when emails get reported.

» Substantial amount of resources spent by SOC teams on manual email reviews.

» Security risks from fatigued users discouraged and desensitized from the lack of feedback.

THE SOLUTION:

» Empowering employees with AI Email Security Analyst to automatically receive a live and AI-powered analysis of their email reports, indirectly training them on best email security practices.

» Freeing up SOC resources while not only maintaining but also improving email security services thanks to automation and instant feedback.

LET AI.MY AUTOMATE THE ANALYSIS AND RESPONSE TO REPORTED EMAILS

Admins of a company with **1000 emloyees**

manually review about

reported emails **per month**

spending

on average

TEAMS PROTECTION PROTECTS TEAMS CHATS FROM MALICIOUS URLS AND SECURITY BREACHES

THE PAIN POINTS:

- Lack of visibility over malicious content shared via Teams.
- Constant exposure: End users are constantly exposed to potential malicious messages.
- External communication: more users are using Teams for external communications.
- Efficiency suffers as users and IT Teams need to face malicious links, malware and more.

THE SOLUTION:

- Automatically warning users whenever malicious links are shared through Teams chats.
- Deleting entire conversations containing malicious messages and preventing their senders from logging into Teams.

LET AI.MY ANALYZE LINKS IN TEAMS FOR POTENTIAL RISKS

A company with **1000 emloyees**

sends

35000

Teams messages per week with **12% containing links**

equaling

4200

potentially **malicious links**

WHY SHOULD MY CUSTOMERS UPGRADE?

The new 365 Total Protection Plan 4 offers solutions that create win-win situations where both end users and admins get empowered, effortlessly strengthening a company's security posture:

- End users get encouraged to report suspicious emails and automatically receive IT security knowledge and learn secure behaviors.
- SOC teams are greatly relieved of the burden of manually reviewing emails, able to relocate their resources to more pressing areas.
- Microsoft Teams chats, an attack vector that too often flies under the radar, is automatically protected with users being instantly warned when a malicious link is shared in a conversation, ensuring all your flanks are covered.

Unlock the future of cybersecurity today with the most comprehensive solution for Microsoft 365 on the market!