HORNETSECURITY

365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

COMPREHENSIVE SECURITY FOR MICROSOFT 365 TODAY AND FOR THE FUTURE

When choosing a **365 Total Protection Plan**, there are three different onboarding modes from which to select: **MX**, **API**, and a combined **Hybrid** mode that incorporates all the features available.

MX MODE

The **MX record-based mode** is the traditional approach, where an intermediary Secure Email Gateway filters emails for spam, malware, and advanced threats before they reach the mailbox. However, MX mode does not provide the possibility to remediate emails once they are delivered.

API MODE

The main advantage of the **API mode** is its fast, simple deployment—no MX record updates required, making it easy to onboard. Emails can even be retroactively deleted from user mailboxes if they are subsequently found to be malicious. However, in this mode, essential features such as Email Continuity, Email Encryption, or Email Archiving cannot be provided.

HYBRID CLOUD EMAIL PROTECTION – FLEXIBILITY, CONTROL, AND PERFORMANCE COMBINED

Hybrid mode combines all the extensive protection of API and MX mode in one.

In Hybrid mode, emails get checked pre- and post delivery. This offers the highest layer of protection possible for your business. Across a variety of use cases, blending these solutions delivers the most robust defense against email-based attacks. The Secure Email Gateway filters out the bulk of routine threats, while the API layer applies advanced AI and machine learning to examine message bodies and attachments for more subtle risks.

08-25

		HYBRID MODE	API MODE	MX MODE
PLAN 1	SPAM & MALWARE PROTECTION	✓	✓	✓
	EMAIL ENCRYPTION	✓	✗	✓
	EMAIL SIGNATURES & DISCLAIMERS	✓	✗	✓
PLAN 2 (INCLUDES 1)	ADVANCED THREAT PROTECTION	✓	✓	✓
	AUTOREMEDIATE	✓	✓	✗
	EMAIL ARCHIVING	✓	✗	✓
	EMAIL CONTINUITY	✓	✗	✓
PLAN 3 (INCLUDES 1 + 2)	AUTOMATIC BACKUP OF M365 DATA	✓	✓	✓
	GRANULAR RECOVERY WITH END USER SELF SERVICE	✓	✓	✓
	UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE	✓	✓	✓
PLAN 4 (INCLUDES 1 + 2 + 3)	SECURITY AWARENESS SERVICE	✓	✓	✓
	PHISHING & ATTACK SIMULATION	✓	✓	✓
	ESI* REPORTING	✓	✓	✓
	PERMISSION MANAGEMENT	✓	✓	✓
	PERMISSION ALERTS	✓	✓	✓
	PERMISSION AUDIT	✓	✓	✓
	DMARC MANAGER	✓	✓	✓
	ENHANCED EMAIL REPUTATION & DELIVERY	✓	✓	✓
	EASY DNS MANAGEMENT & ORGANISATION	✓	✓	✓
	AI RECIPIENT VALIDATION	✓	✓	✓
	COMMUNICATION PATTERN ANALYSIS	✓	✓	✓
	SENSITIVE DATA CHECK	✓	✓	✓
	TEAMS PROTECTION	✓	✓	✓
	CHAT-BASED THREATS MONITORING	✓	✓	✓
	AI PHISHING DETECTION & RESPONSE	✓	✓	✓
	AI EMAIL SECURITY ANALYST	✓	✓	✓
	AI ANALYSIS OF USER REPORTS	✓	✓	✓
	AI RESPONSE & AWARENESS	✓	✓	✓