HORNETSECURITY 365 TOTAL PROTECTION

Microsoft 365 is by far the most prevalent cloud email service for businesses, but this popularity brings inherent risks, as it also makes it the top target for cybercriminals. Email security features are provided by Microsoft, but these are widely used, comparatively basic and, consequently, easier to circumvent.

To provide greater protection, businesses must implement a multi-layered defence - and Hornetsecurity offers a cost-effective and highly efficient solution. Its 365 Total Protection cloud service provides a wealth of email security measures, which includes AI intelligence-based protection, allowing it to evolve as new threats emerge.

Two options are available, with the Business version providing all key threat defence measures, along with live email tracking, content control and compliance filtering. The Enterprise version augments these with ATP (advanced threat protection) cloud sandboxing, URL malware controls, email archiving, e-discovery and forensics analysis tools.

Onboarding from the cloud panel is swift, as you change your domain's MX records, go to the registration link provided and authenticate with your account from the standard Microsoft 365 login screen. Using its Azure connector, 365 Total Protection synchronises all your users, with the entire process taking as little as 30 seconds.

Protection starts immediately, as the default settings activate full spam and malware protection, which blocks suspicious emails before they reach your mailbox. The Spam and Malware filter uses over 15,000 heuristics to reject nuisance messages, such as newsletters and those sent from mass marketing campaigns.

The cloud panel opens with an email live tracking view that shows logs of all inbound and outbound email activity. This is vastly superior to Microsoft's logging, as you can view every detail about individual emails, including header information, and each one is colour coded to clearly show its classification.

Multiple filters can be applied to refine the list and clicking on the coloured icon for an email loads a drop-down menu where you can add the sender to deny or allow lists, report it as spam or release it. Enterprise users can also pass suspect emails to the ATP service for further examination.

Self-service features lighten the support burden, as users can review their emails in the portal and release them, where permitted. Regular reports for each user can be generated and show spam activity, quarantined attachments, plus the reasons for rejection.

The ATP sandbox recognises emails with encrypted attachments and, if the password is in the email message body, it will use it to scan these files. The URL rewrite feature deals efficiently with email web links, as Hornetsecurity opens a web session to its secure proxy to check where the link connects to and see if it includes harmful downloads or other threats.

Fraudulent emails that appear to be legitimate are handled by a targeted forensics filter, which uses first and last name combinations in order to check for authenticity. The compliance filter provides more granular control of emails by applying DLP-like rules to outbound messages that check for specific keywords in the body, subject and attachment.

The continuity service will prove invaluable when the Microsoft 365 services go down, as it keeps copies for three months back for you to use during the outage and transfers them back to your account when the service comes up again. Rule-based encryption for outbound messages is just as easy to implement, as all certificates are centrally managed for you.

Hornetsecurity's 365 Total Protection lives up to its name, as it delivers a smart email security solution that integrates seamlessly with Microsoft 365. It fills the security holes Microsoft leaves behind and, with prices for the Business version starting at only $2 per user per month, is affordable for organisations of all sizes.

Product: 365 Total Protection
Supplier: Hornetsecurity
Web site: www.hornetsecurity.com
Contact: info@hornetsecurity.com
Price: From $2 per user per month