HORNETSECURITY

FACT SHEET

365 4 TOTAL PROTECTION

PLAN 4 - COMPLIANCE & AWARENESS

NEXT-GEN PROTECTION FOR MICROSOFT 365:
EMAIL SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS

PLAN 1	PLAN 2	PLAN 3	PLAN 4
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES, PLANNER & TEAMS	PERMISSION MANAGEMENT	PHISHING & ATTACK SIMULATION	COMMUNICATION PATTERN ANALYSIS
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS	SECURITY AWARENESS	AI RECIPIENT VALIDATION
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT	ESI® REPORTING	SENSITIVE DATA CHECK

365 Total Protection covers all aspects of an organization's Microsoft 365 security management and data protection: email security, backup and recovery, compliance, permission management and security awareness. The solution integrates seamlessly with Microsoft 365, providing much-needed layers of additional security and data protection against spam, malware, and advanced threats.

- **Spam and malware protection** - AI & Machine Learning combined with other technologies guarantee 99.99% detection rate for spam and 99.9% for viruses.
- **Email encryption** - Outgoing emails are automatically encrypted with one of the common encryption technologies (PGP, S/MIME or TLS), depending on the set policy and availability of the corresponding certificates, without any further user intervention.
- **Email signatures and disclaimers** - Set up automatically integrated ad banners or links in email signatures for external corporate email communication and add uniform and legally compliant company disclaimers.

- **Advanced Threat Protection** - Protects your email traffic from insidious variety of cyber-attacks by freezing, URL scanning, rewriting, and sandboxing to keep the IT infrastructure secure.
- **Email archiving** - Helps organizations comply with retention mandates by creating a searchable repository to support compliance reporting and audits. Emails can be archived for up to 10 years.
- **Email continuity** - As your regular email server waits to restore services, the new emails get queued up for delivery and synchronized back to the email continuity portal.

- **Automated backups for mailboxes, teams, Planner, OneDrive, and SharePoint** - M365 data is automatically backed up several times a day. Manual backups are also possible at any time.
- **Recovery of M365 mailboxes, Teams Chats, Planner, OneDrive, and SharePoint** - Full and granular recovery options.
- **Backup and recovery of endpoints** - Any Windows-based endpoint can be backed up without requiring a VPN.

- **Permission management** – Quick Actions to fix permissions on multiple sites, full overview of all M365 permissions within the company. Advanced filtering for quick permissions check. Breakdown of nested groups to get a transparent view of users' effective access rights.
- **Permission alerts** - Daily summary of critical permission changes happening across your M365 tenant regarding sharing of sites, files, and folders in and out of your organizations.
- **Permission audit** - Audit function for approval or rejection of possible violations via reverting the site settings according to the assigned compliance policy or removing given access.

- **Phishing and attack simulation** - Individually customized phishing scenarios lead to bogus login pages, contain attachments with macros, and emails with response threads.
- **Security Awareness Service** - Fully automated Awareness Benchmarking, Spear-Phishing -Simulation and E-Training to sensitize and protect employees against cyber threats.
- **ESI® reporting** - The ESI® Awareness Benchmark enables standardized, transparent measurement of security behavior on enterprise, group, and user level.

- **Communication pattern analysis** – Automatically learns your email communication patterns and helps secure your outgoing communications within and outside of the tenant.
- **AI Recipient Validation** - AI Recipient Validation analyses emails based on previous communications and triggers warnings in various instances. (Email texts and attachments are not transmitted to Hornetsecurity's servers. Any analysis of these is done in the local Outlook client.)
- **Sensitive data check** - Users are notified immediately when the email they are trying to send contains sensitive information like Personal Identifiable Information.