



HORNETSECURITY

FACT SHEET

# 365 TOTAL PROTECTION

## PLAN 4 - COMPLIANCE & AWARENESS

NEXT-GEN PROTECTION FÜR MICROSOFT 365:  
E-MAIL-SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS



BUSINESS

ENTERPRISE

BACKUP

COMPLIANCE & AWARENESS



SPAM & MALWARE PROTECTION



ADVANCED THREAT PROTECTION



BACKUP & RECOVERY OF MAILBOXES & 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

3365 Total Protection bringt alle Aspekte des Security- und Datenschutz-Managements von Microsoft 365 auf das nächste Level: E-Mail-Security, Backup und Recovery, Compliance, Berechtigungsmanagement und Security Awareness. Die Lösung lässt sich nahtlos in Microsoft 365 integrieren und bietet dringend erforderliche zusätzliche Sicherheits- und Datenschutzebenen gegen Spam, Malware und fortschrittlichen Bedrohungen.

✓ **Spam und Malware Protection** – KI und Machine Learning in Kombination mit anderen Technologien garantieren eine Erkennungsrate von 99,99 % für Spam und 99,9 % für Viren.

✓ **Email encryption** – Ausgehende E-Mails werden automatisch mit einer der gängigen Verschlüsselungstechnologien (PGP, S/MIME oder TLS) verschlüsselt, je nach eingestellter Richtlinie und Verfügbarkeit der entsprechenden Zertifikate, ohne dass ein weiterer Benutzereingriff erforderlich ist.

✓ **E-Mail Signaturen und Disclaimer** – Richten Sie automatisch integrierte Werbeflächen oder Links in E-Mail-Signaturen für die unternehmensexterne E-Mail-Kommunikation ein und fügen Sie einheitliche und rechtssichere Disclaimer des Unternehmens hinzu.

✓ **Advanced Threat Protection** – Schützt Ihren E-Mail-Verkehr und die IT-Infrastruktur vor heimtückischen Cyber-Angriffen durch Freezing, URL-Scanning, Rewriting und Sandboxing.

✓ **E-Mail Archivierung** – Hilft Unternehmen bei der Einhaltung von Aufbewahrungsvorschriften, indem ein durchsuchbares Repository zur Unterstützung von Compliance-Reporting und Audits erstellt wird. E-Mails können bis zu 10 Jahre lang archiviert werden.

✓ **Email continuity** – Sollte es zu einem Ausfall der Microsoft-Services kommen und damit der Zugriff auf Ihre E-Mail-Postfächer beeinträchtigt sein, aktiviert sich unmittelbar das E-Mail-Continuity-Feature, das Ihren E-Mail-Verkehr am Laufen hält.

✓ **Automatisierte Backups für Mailboxen, Teams, OneDrive und SharePoint** – M365-Daten werden mehrmals täglich automatisch gesichert. Manuelle Backups sind ebenfalls jederzeit möglich.

✓ **Wiederherstellung von M365-Postfächern, Teams Chats, OneDrive und SharePoint** – Vollständige und granulare Wiederherstellungsoptionen sind verfügbar.

✓ **Backup und Wiederherstellung von Endpunkten** – Jeder Windows-basierte Endpunkt kann gesichert werden, ohne dass ein VPN erforderlich ist.

✓ **Effektives Management von Berechtigungen** – Quick Actions zur Korrektur von Berechtigungen für mehrere Sites auf einmal. Erweiterte Filterung zur schnellen Überprüfung und Aufschlüsselung verschachtelter Gruppen, um einen transparenten Überblick über die effektiven Zugriffsrechte zu erhalten.

✓ **Alerts** – Tägliche Zusammenfassung kritischer Berechtigungsänderungen in Ihrem M365-Tenant in Bezug auf die Freigabe von Websites, Dateien und Ordnern innerhalb und außerhalb Ihrer Organisation.

✓ **Audit-Funktion** – zur Freigabe oder Zurückweisung möglicher Verstöße durch Rückgängigmachung der Site-Einstellungen gemäß der zugewiesenen Compliance-Richtlinie oder Entzug des Zugriffs.

✓ **Phishing-Simulation** – Individuell angepasste Phishing-Szenarien führen zu gefälschten Anmeldeseiten, enthalten Anhänge mit Makros und E-Mails mit Antwort-Threads.

✓ **Security Awareness Service** – Vollautomatisiertes Awareness-Benchmarking, Spear-Phishing-Simulation und E-Training zur Sensibilisierung und zum Schutz der Mitarbeiter vor Cyber-Bedrohungen.

✓ **ESI® reporting** – Der ESI® Awareness Benchmark ermöglicht eine standardisierte, transparente Messung des Sicherheitsverhaltens auf Unternehmens-, Gruppen- und Benutzerebene.

✓ **Analyse von Kommunikationsmustern** – Lernt automatisch Ihre E-Mail-Kommunikationsmuster und hilft, Ihre ausgehende Kommunikation innerhalb und außerhalb des Tenants zu sichern.

✓ **AI Recipient Validation** – analysiert E-Mails auf der Grundlage früherer Kommunikation und löst in verschiedenen Fällen Warnungen aus. (E-Mail-Texte und Anhänge werden nicht an die Server von Hornetsecurity übertragen. Die Analyse dieser wird im lokalen Outlook-Client durchgeführt).

✓ **Sensitive data check** – Benutzer werden sofort benachrichtigt, wenn die E-Mail, die sie zu senden versuchen, sensible Informationen wie personenbezogene Daten enthält.