HORNETSECURITY

FACT SHEET

365 TOTAL PROTECTION ENTERPRISE BACKUP

Die marktweit einzige All-In-One Security- und Backup-Lösung für Microsoft 365

Schützen Sie Ihr Microsoft 365 vor Phishing, Ransomware und Advanced Persistent Threats sowie Datenverlust mit 365 Total Protection Enterprise Backup, einer einzigartigen cloudbasierten All-in-One-Sicherheits- und Backup-Suite. Profitieren Sie von der Expertise von Hornetsecurity, dem führenden Spezialisten für E-Mail-Sicherheit und Backup, bekannt für seine bewährten und preisgekrönten Services 365 Total Protection (E-Mail-Sicherheit für M365) und 365 Total Backup (Backup und Recovery für M365).

SPEZIELL FÜR MICROSOFT 365 ENTWICKELT **UND NAHTLOS INTEGRIERT**

365 Total Protection Enterprise Backup ist eine leistungsstarke Kombination aus zwei etablierten und hochleistungsfähigen Lösungen, die für Microsoft 365 entwickelt wurden. Das Onboarding dauert nur 30 Sekunden und die ersten Backups lassen sich in weniger als 5 Minuten konfigurieren. Die Lösung zeichnet sich durch ihre Benutzerfreundlichkeit und herausragende Performance aus:

- Höchste Spam- und Malware-Erkennungsraten am Markt
- KI-basierte Filtermechanismen zur Erkennung komplexer Angriffe
- Automatisierte Backups mehrmals täglich – einmal einrichten und fertig
- Richtlinienbasierter Schutz von Dateien auf Ihren Endpoints

1 REGISTER **YOUR ACCOUNT**

2 CONNECT **WITH MICROSOFT**

3 SETUP **COMPLETED!**

Abb.: Einfacher Onboarding-Prozess in drei Schritten

HORNETSECURITY

FACT SHEET

365 TOTAL PROTECTION ENTERPRISE BACKUP – WICHTIGSTE FEATURES:

SPAM FILTERING & ADVANCED EMAIL SECURITY:

- Email Live Tracking: Überwacht den gesamten E-Mail-Verkehr in Echtzeit und ermöglicht die Definition von Filter- und Zustelloptionen.
- Content Control & Compliance Filter: Erweiterter Filter zur automatischen Überprüfung des E-Mail-Verkehrs (einschließlich Dateianhängen) nach selbst definierten Filterregeln.
- Spam and Malware Protection: Mehrstufige Filtersysteme und tiefgreifende Analysen zur sofortigen Erkennung und Abwehr.
- Forensic Analyses & ATP sandbox: KI-basierte Erkennungsmechanismen für eine wirksame Abwehr; Schutz vor gezielten und kombinierten Angriffen durch dynamische Analysen.
- Malware Ex Post Alert: Sofortige Benachrichtigung über E-Mails, die erst im Nachhinein als schädlich eingestuft wurden.

EMAIL ENCRYPTION, CONTINUITY & ARCHIVING:

- Global S/MIME & PGP Encryption: Zuverlässige Verschlüsselung zum Schutz der E-Mail-Kommunikation vor unbefugten Eingriffen und Änderungen.
- Secure Cipher Policy Control: Zentrales TrustChain-Management; individuelle Definition von Sicherheitskriterien für die E-Mail-Kommunikation.
- Email Archiving: Automatisierte, rechtskonforme und revisionssichere E-Mail-Archivierung.
- eDiscovery: Erweiterte E-Mail-Suchfunktionen mit zahlreichen Filtern zum präzisen Auffinden von Nachrichten in Sekundenschnelle.
- Email Continuity Service: Wirksamer Schutz vor Systemausfällen durch automatische und sofortige Aktivierung.

SIGNATURES & DISCLAIMERS:

- Individual User Signatures: Zentrale Kontrolle über unternehmensweite E-Mail-Signaturen.
- 1-Click Intelligent Ads: Richten Sie automatisch integrierte Werbebanner oder Links in E-Mail-Signaturen für die externe E-Mail-Kommunikation Ihres Unternehmens ein
- Company Disclaimer: Automatische Integration von einheitlichen und rechtssicheren Unternehmens-Disclaimern.

BACKUP & RECOVERY:

- Automatisierte Backups für E-Mail-Postfächer, Teams, OneDrive und SharePoint: Die M365-Daten werden mehrmals täglich automatisch gesichert. Manuelle Backups sind ebenfalls jederzeit möglich.
- Wiederherstellung von M365-Postfächern, Teams-Chats, OneDrive und SharePoint: Es steht eine breite Auswahl an vollständigen und granularen Wiederherstellungsoptionen zur Verfügung.
- Windows-basierte EndPoint-Backups und Wiederherstellung: Jeder beliebige EndPoint, ob im Büro oder irgendwo auf der Welt, kann ohne VPN gesichert werden.
- Account Activity Audit: Überprüfen Sie eine Reihe von Vorgängen, wie z. B. die Aktivierung oder Deaktivierung von Postfächern, Teams, OneDrive- und SharePoint-Backups durch die Benutzer sowie ihre Aktivitäten beim Durchsuchen von Daten und ihre Wiederherstellungsanfragen.