HORNETSECURITY
BY proofpoint

FACTSHEET

365 TOTAL PROTECTION

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

La solution 365 Total Protection de Hornetsecurity offre la plus large gamme de fonctions de sécurité M365 qui rationalisent et protègent les opérations de votre entreprise. Développée par des experts en sécurité de confiance, 365 Total Protection s'intègre de manière transparente à Microsoft 365 et permet aux entreprises de bénéficier d'une technologie de pointe alimentée par AI, facile à utiliser et d'une efficacité inébranlable.

365 MULTI-TENANT MANAGER FOR MSPS

STOP MANUALLY MANAGING M365 TENANTS
AND START SAVING YOUR TIME!

PLAN 4

INCLUDES 1 + 2 + 3

- SECURITY AWARENESS
- PERMISSION MANAGEMENT
- DMARC REPORTING & MANAGEMENT

POWERED BY AI CYBER ASSISTANT

- AI RECIPIENT VALIDATION
- TEAMS PROTECTION
- AI EMAIL SECURITY ANALYST

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 2

INCLUDES 1 + 2

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

PLAN 1

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMER

		PLAN 1 LA BASE DE VOTRE SÉCURITÉ MICROSOFT 365	PLAN 2 TOUTES LES FONCTIONNALITÉS DE SÉCURITÉ DONT VOTRE ENVIRONNEMENT M365 A BESOIN	PLAN 3 SAUVEGARDE ET SÉCURITÉ ILLIMITÉES POUR UNE PROTECTION TOTALE CONTRE LA PERTE DE DONNÉES	PLAN 4 VOTRE SOLUTION POUR UN M365 SÉCURISÉ, CONFORME ET MAÎTRISÉ
PROTECTION ESSENTIELLE	FILTRE CONTRE LES POURRIELS, LES LOGICIELS MALVEILLANTS ET L'HAMEÇONNAGE	✓	✓	✓	✓
	CONTRÔLE DU CONTENU	✓	✓	✓	✓
	FILTRE DE CONFORMITÉ	✓	✓	✓	✓
	SUIVI DES COURRIELS	✓	✓	✓	✓
	CATÉGORISATION DES COURRIELS	✓	✓	✓	✓
	EMAIL ENCRYPTION	✓	✓	✓	✓
	SIGNATURES ET MENTIONS LÉGALES	✓	✓	✓	✓
ADVANCED THREAT PROTECTION	DÉTECTION DES MENACES BASÉES SUR L'IA		✓	✓	✓
	BAC À SABLE		✓	✓	✓
	RÉÉCRITURE DES LIENS	✓	✓	✓	✓
	DÉTECTION DE L'HAMEÇONNAGE PAR CODE QR		✓	✓	✓
	ANALYSE DES GRAPHES SOCIAUX		✓	✓	✓
	DÉTECTION DES FRAUDES		✓	✓	✓
	DÉCHIFFREMENT DES PIÈCES JOINTES		✓	✓	✓
	RÉPONSE AUX MENACES PAR COURRIEL		✓	✓	✓
	PROTECTION MICROSOFT TEAMS				✓
RÉPONSE AUX INCIDENTS ET REPRISE DES ACTIVITÉS	CORRECTION AUTOMATIQUE ET MANUELLE DES MENACES		✓	✓	✓
	ARCHIVAGE		✓	✓	✓
	CONTINUITÉ DES ACTIVITÉS		✓	✓	✓
	ANALYSTE DE LA SÉCURITÉ DES COURRIELS AVEC IA				✓
SAUVEGARDE ET RESTAURATION	SAUVEGARDE ET RESTAURATION DES DONNÉES MICROSOFT 365			✓	✓
	ESPACE DE SAUVEGARDE ET RESTAURATION ILLIMITÉES			✓	✓
	APPROBATION À QUATRE YEUX			✓	✓
CONFORMITÉ ET FORMATION	SIMULATION D'ATTAQUES PAR HAMEÇONNAGE				✓
	MOTEUR DE PROFILAGE DES UTILISATEURS ET DE SENSIBILISATION				✓
	FORMATION DE SENSIBILISATION				✓
	PROTECTION CONTRE LES FUITES DE DONNÉES				✓
	GESTION ET PRODUCTION DE RAPPORT DMARC				✓
	REGROUPEMENT DES RAPPORTS DMARC				✓
	AUDIT CONTINU ES PERMISSIONS DANS MICROSOFT 365				✓
	POLITIQUES DE CONFORMITÉ PRÊTES À L'EMPLOI				✓
	CORRECTION AUTOMATISÉE DES POLITIQUES				✓

HORNETSECURITY
BY proofpoint

AI POWERED

HORNETSECURITY

FACT SHEET

ADVANCED THREAT PROTECTION

Protection avancée des e-mails et des données grâce à l'IA, même contre les menaces les plus sophistiquées.

Les cybercriminels travaillent sans relâche pour développer de nouvelles cybermenaces, ce qui rend difficile pour les logiciels de sécurité de suivre le rythme et de protéger les utilisateurs contre les nouvelles méthodes d'attaque émergentes. Les ransomwares, les fraudes au PDG, le spear phishing et les attaques mixtes ne sont que quelques exemples des dangers qui se cachent dans le cyberespace.

Avec l'essor des outils d'IA largement disponibles, les cybercriminels peuvent facilement créer des e-mails de phishing impeccables, voire contourner les mesures de protection et utiliser des outils de génération de texte d'IA pour créer des codes malveillants.

Avec Advanced Threat Protection, vous n'avez à vous soucier de rien de ce qui précède. En utilisant l'IA à son avantage, Advanced Threat Protection vous permet de garder une longueur d'avance sur les cybercriminels, en vous protégeant contre les attaques Zero Day et même contre les menaces les plus sophistiquées.

Qu'est-ce qui est affecté ? | **Comment Advanced Threat Protection vous aide-t-il ?** | **Quelles sont les améliorations ?**

Communication par email

Analyse approfondie ciblée basée sur l'IA

Détecte les menaces les plus récentes et les plus sophistiquées.

Moteur "sandbox"

Teste les pièces jointes aux emails pour détecter les fichiers malveillants dans un environnement contrôlé.

Rapports

Obtenir une vue d'ensemble de toutes les tentatives d'attaques, des alertes de sécurité, des rapports ATP et des informations détaillées.

Boites aux lettre électroniques sécurisées

FILETYPES	BINARY ANALYTICS	SANDBOX 500+ BEHAVIOURAL ANALYSIS SENSORS	REPORTING AND DATA ANALYTICS
EXE	MACRO	ANTI VM EVASION DETECTION	LIVE THREAT MONITOR
PDF	OBFUSCATION	MACHINE LEARNING ENGINE	SECURITY ALERTS
OFFICE	URL	FILESYSTEM MONITOR	ATP-REPORTS
ARCHIVE	OBJECTS	NETWORK TRAFFIC ANALYSIS	FORENSIC INFORMATION
	METADATA	PROCESS- AND REGISTRY MONITOR	
	JAVASCRIPT	FORENSIC MEMORY ANALYSIS	
	HEURISTIC		
	STATIC ANALYSIS		
	ZERO HOUR THREAT OUTBREAK DETECION		

Advanced Threat Protection contre les ransomwares et les virus polymorphes

HORNETSECURITY

FACT SHEET

Moteurs ATP	Fonctionnalités et avantages
Moteur Sandbox	Les pièces jointes aux emails sont analysées pour détecter d'éventuels codes malveillants en exécutant le fichier suspect dans un environnement de test virtuel et en identifiant les effets potentiellement dangereux. Si le document envoyé avec l'email s'avère être un logiciel malveillant, l'email est placé directement en quarantaine.
Secure Links	Fini les clics risqués sur les liens dans les emails Secure Links remplace le lien original par une version réécrite qui passe par la passerelle web sécurisée de Hornetsecurity. Secure Links utilise l'intelligence artificielle, y compris l'apprentissage automatique et l'apprentissage approfondi, pour fournir une protection avancée contre le phishing, même dans les attaques à ondes courtes et très ciblées. Les algorithmes d'apprentissage automatique supervisés et non supervisés analysent plus de 47 caractéristiques des URL et des pages web, recherchant les comportements malveillants, les techniques d'obscurcissement et les redirections d'URL, tandis que les modèles de vision par ordinateur analysent les images pour extraire les caractéristiques pertinentes utilisées dans les attaques de phishing, y compris les logos de marque, les QR codes et le contenu textuel suspect intégré dans les images.
URL Scanning	Laisse le document joint à un email dans sa forme originale et ne vérifie que la cible des liens qu'il contient.
Blocage	Les emails qui ne peuvent pas être clairement classés immédiatement sont retenus pendant un court laps de temps.
Décryptage de documents malveillants	Les pièces jointes cryptées sont décryptées à l'aide de modules de texte appropriés dans un email. Le document décrypté est ensuite soumis à une analyse antivirus approfondie.
Enquêtes ciblées sur la fraude alimentées par l'IA	**Analyse des tentatives de fraude :** vérification de l'authenticité et de l'intégrité des métadonnées et du contenu d'email. **Reconnaissance de l'usurpation d'identité :** détection et blocage des fausses identités d'expéditeurs. **Système de reconnaissance des intentions :** alerte sur les modèles de contenu qui suggèrent une intention malveillante. **Détection d'espionnage :** défense contre les attaques d'espionnage visant à obtenir des informations sensibles. **Identification des faits falsifiés :** analyse de contenu indépendante de l'identité des informations sur la base de faits falsifiés. **Détection des attaques ciblées :** détection des attaques ciblées sur des personnes particulièrement exposées.
QR Code Analyzer	L'analyseur de code QR de Hornetsecurity est capable de détecter les codes QR intégrés directement dans un e-mail ou une image. Tous les codes QR sont détectés et analysés à la vitesse de la lumière à la recherche de contenus malveillants. Il prend en charge tous les types d'images courants tels que GIF, JPEG, PNG et BMP.

AI POWERED

HORNETSECURITY

FACT SHEET

SPAM & MALWARE PROTECTION

Protection efficace contre le spam et les logiciels malveillants grâce à un système de filtrage multi-niveaux entièrement automatisé.

Représentant plus de 50 % de l'ensemble du trafic de courrier électronique, le spam est la méthode la plus intrusive utilisée par les cybercriminels pour introduire des logiciels malveillants et des virus dans les systèmes des entreprises. Outre le risque d'infection par un ransomware, un spyware ou un cryptomineur, les flux de travail importants peuvent également être interrompus par le flot ennuyeux d'emails indésirables. Un système de filtrage à plusieurs niveaux est indispensable pour empêcher le spam et le phishing d'atteindre les boîtes de réception et de perturber le flux de travail.

Vos boîtes aux lettres méritent les filtres les plus puissants

- **Détection dynamique des propagations de virus**
- **Détection du spam à plusieurs niveaux et niveaux de filtrage dynamiques**
- **Filtrage des messages sortants**

Qu'est-ce qui est affecté ?

Environnement de la messagerie éléctronique

Comment Spam & Malware Protection vous aide-t-il ?

Taux de détection de spam (99,9 %) et de virus (99,99 %) les plus élevés du marché.

Maximiser la sécurité pour les besoins spécifiques des environnements via la création de règles avancées dans le filtre de conformité.

Les e-mails sortants sont vérifiés pour détecter spam et virus.

Quelles sont les améliorations ?

Communication sécurisée par courrier électronique entrant et sortant

HORNETSECURITY

FACT SHEET

DES MÉCANISMES D'ANALYSE PRÉCIS ET DES FILTRES FIABLES :

Filtre anti-phishing : Le suivi des liens et d'autres mécanismes protègent efficacement contre les emails de phishing. Les commandes de scripts malveillants rechargeables sont notamment détectées. Cela permet, par exemple, de détecter les téléchargements dangereux de type "drive-by download".

Filtre newsletters : Les newsletters non classées comme spam et autres pubs qui interrompent inutilement le flux de travail sont filtrées et stockées en vue d'une récupération ultérieure. Ils sont répertoriés dans le rapport de quarantaine individuel et peuvent être délivrés et autorisés en un clic si nécessaire.

Suivi des liens : Les emails entrants et sortants sont automatiquement analysés pour détecter les URL malveillantes.

Mise à jour automatique des signatures de virus : les filtres de logiciels malveillants sont constamment mis à jour. L'entreprise utilise notamment ses propres scanners, qui sont spécialisés dans les logiciels malveillants diffusés par email.

Filtrage des messages sortants : Les emails sortants sont contrôlés pour détecter les spams et les virus afin d'empêcher le client d'envoyer ou de transférer involontairement des logiciels malveillants et des emails non sollicités.

Gestion des bounces : Seuls les bounces authentiques parviennent au destinataire dans le trafic d'emails ; les bounces en réponse à du spam avec de fausses adresses d'expéditeur sont filtrés de manière fiable.

Filtre de contenu pour les pièces jointes : Les pièces jointes indésirables peuvent être rejetées ou placées en quarantaine.

Détection dynamique des attaques de virus : Les virus nouveaux et inconnus sont arrêtés par le système d'alerte rapide. Vade analyse en permanence les emails entrants sur des comptes dits "honeypot" (adresses email dont le seul but est de recevoir des spams) pour détecter les pièces jointes, les liens, les expéditeurs ou les contenus inhabituels. La dérivation des signatures à partir de ces éléments est effectuée dans un temps de réaction le plus court possible (en général <5 minutes).

Moins de 0,00015 faux positifs : Le nombre d'email normaux classés par erreur comme spam est inférieur à 0,00015.

GÉRER ET RESPECTER FACILEMENT LES **POLITIQUES DE CONFORMITÉ**

Rapports de quarantaine à intervalles configurables : Les utilisateurs peuvent adapter leurs rapports de quarantaine à leurs méthodes de travail et les programmer à des moments précis, voire plusieurs fois par jour.

Déblocage en un clic : Les messages électroniques en quarantaine peuvent être délivrés du rapport de quarantaine d'un simple clic, qu'il s'agisse de spams présumés ou de messages électroniques non sollicités.

Bonne vue d'ensemble grâce au blocage : La grande majorité des emails non sollicités sont directement bloqués. Cela permet à l'utilisateur d'avoir un aperçu rapide des emails actuellement en quarantaine.

Allège la charge du serveur de messagerie : Spam and Malware Protection ne laisse passer que les messages valides, ce qui augmente considérablement la performance du serveur de messagerie du client.