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.