FACT SHEET

Advanced Threat Protection

HORNETSECURITY vade

Contrer les menaces modernes avec les mécanismes de défense les plus avancés

Le risque d'une cyberattaque ciblée avec des ransomwares, des fraudes au PDG et des chevaux de Troie augmente considérablement. Protégez votre entreprise contre les attaques dévastatrices de logiciels malveillants grâce à la protection avancée contre les menaces.

Protection contre :

- Ransomware
- Attaques combinées
- Attaques ciblées
- compromission d'email des entreprises

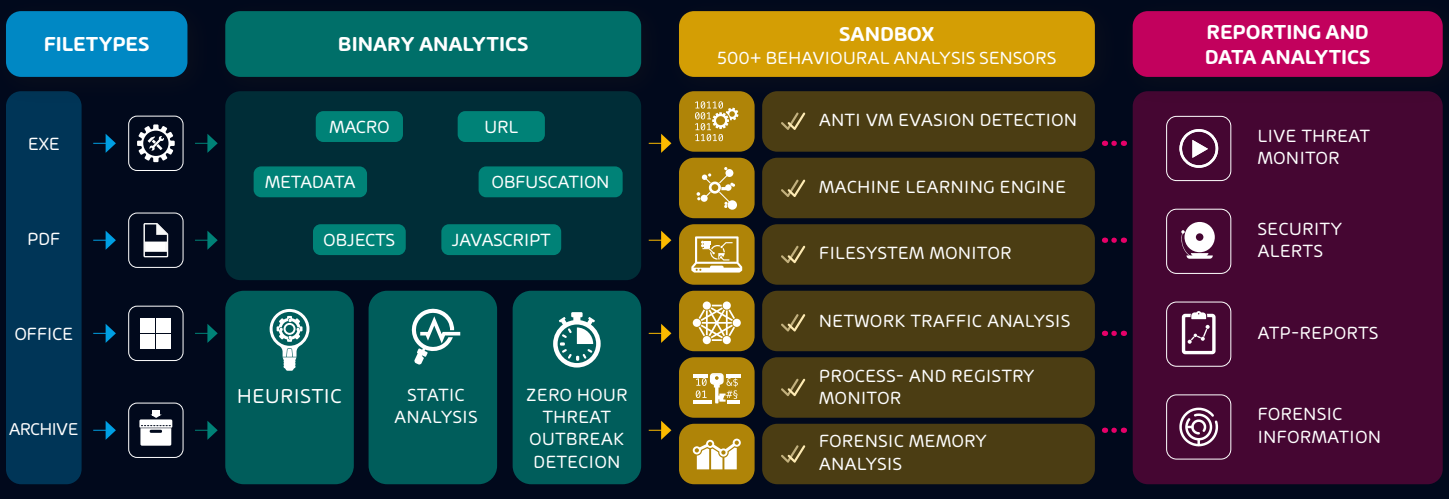
Mécanismes de protection contre la fraude

- Analyse des emails frauduleux au niveau du contenu et des méta données.
- Analyse des données de transport SMTP dans le contexte de la structure de gestion d'une entreprise.
- Les demandes d'informations critiques ne peuvent provenir que de sources internes à l'entreprise.
- Les emails externes - dont les expéditeurs prétendent être des gestionnaires - sont bloqués.

Mécanismes de protection contre les rançongiciels

- L'ATP Sandbox accède aux bases de données de renseignements sur les menaces lors de l'analyse des pièces jointes aux emails.
- Les indicateurs de compromission (IoC) stockés sont classés à l'aide de plus de 50 moteurs antivirus disponibles sur le marché.
- Enrichissement des analyses avec des informations sur les sommes de hachage déjà connues (par exemple, des pièces jointes défectueuses ou des adresses IP en rapport avec des instances malveillantes).
- Alarme en temps réel : Notification en temps réel des équipes de sécurité informatique en cas d'attaques graves contre l'entreprise. Contient des informations détaillées sur le type et la portée de l'attaque.

Fig. : Advanced Threat Protection contre les ransomwares et les virus polymorphes



FACT SHEET

Advanced Threat Protection

Mécanismes d'analyse précis et filtres fiables :

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	Secure Links protège les utilisateurs contre les liens malveillants dans les emails. Il remplace le lien original par une version réécrite qui passe par la passerelle web sécurisée de Vade. Si un utilisateur clique sur un lien, une analyse approfondie du Web est lancée : Le service analyse de manière récurente le site cible et suit les liens à la recherche de ressources web malveillantes. Le système bloque l'accès aux sites malveillants et empêche les pirates et les cybercriminels d'accéder aux données confidentielles de l'utilisateur ou d'infecter son ordinateur avec des logiciels malveillants.
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	**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	Afin d'avoir une longueur d'avance sur les acteurs menaçants, Vade a développé une fonction capable de faire plus que simplement analyser les codes qr. L'analyseur de codes qr détecte également les codes QR intégrés dans d'autres images - les attaquants pourraient commencer à utiliser cette astuce pour contourner les simples applications d'analyse de codes QR. Le QR code analyzer peut détecter les qr codes à la vitesse de la lumière et peut analyser différents types, y compris les urls et les textes. Il prend en charge tous les types d'images courants tels que gif, jpeg, png et bmp.