







PROTECTION AVANCÉE DES COURRIELS ET DES DONNÉES ALIMENTÉE PAR L'IA, MÊME CONTRE LES MENACES LES PLUS SOPHISTIQUÉES.

Les pirates travaillent sans relâche à développer de nouvelles menaces numériques, ce qui complique la tâche des logiciels de sécurité qui doivent suivre le rythme et protéger les utilisateurs contre des méthodes d'attaque en constante évolution. Les rançongiciels, la fraude au PDG (CEO fraud), l'hameçonnage ciblé (spear phishing) et les attaques hybrides ne sont que quelques exemples des dangers qui circulent dans l'espace numérique.


















Avec l'essor d'outils d'IA largement accessibles, les cybercriminels peuvent créer facilement des courriels d'hameçonnage au rendu impeccable et, dans certains cas, contourner des mesures de protection en utilisant des générateurs de texte pour produire du code malveillant.

Avec la solution Advanced Threat Protection (ATP), vous n'avez pas à vous soucier de ce qui précède. En mettant l'IA à profit, ATP vous permet de garder une longueur d'avance sur les pirates, en vous protégeant contre les attaques de type jour-zéro et même les menaces les plus sophistiquées.

ATP SÉCURISE VOS BOÎTES AUX LETTRES ET AIDE À RÉDUIRE LES RISQUES LIÉS AUX COMMUNICATIONS PAR COURRIEL.

-  **Analyses ciblées basées sur l'IA** – Détecte des menaces inédites et même les plus sophistiquées.
-  **Moteur de bac à sable (Sandbox Engine)** – Teste les pièces jointes de courriel dans un environnement contrôlé pour repérer les fichiers malveillants.
-  **Rapports** – Vue d'ensemble des tentatives d'attaque, alertes de sécurité, rapports ATP et informations médico-légales.
-  **La protection avancée contre les menaces assure la sécurité de vos boîtes mail.**

BAC À SABLE ATP VS. RANÇONGIÉELS ET VIRUS POLYMORPHES

TYPES DE FICHIERS	ANALYTIQUE BINAIRE	BAC À SABLE 500+ CAPTEURS D'ANALYSE COMPORTEMENTALE	RAPPORTS ET ANALYTIQUE
 EXE	MACRO OBJETS URL D'OBFUSSION MÉTADONNÉES JAVASCRIPT	 DÉTECTION D'ÉVASION ANTI-VM	 SURVEILLANCE DES MENACES EN DIRECT
 PDF	 HEURISTIQUE	 MOTEUR D'APPRENTISSAGE AUTOMATIQUE	 ALERTES DE SÉCURITÉ
 OFFICE	 ANALYSE STATIQUE	 SURVEILLANCE DU SYSTÈME DE FICHIERS	 RAPPORTS ATP
 ARCHIVES	 DÉTECTION D'ÉCLOSION DE MENACES (« HEURE ZÉRO »)	 ANALYSE DU TRAFIC RÉSEAU	 INFORMATIONS MÉDICO-LÉGALES
		 SURVEILLANCE DES PROCESSUS ET DU REGISTRE	
		 ANALYSE MÉDICO-LÉGALE DE LA MÉMOIRE	



MOTEURS ATP

FONCTIONNALITÉS ET AVANTAGES

Moteur de bac à sable (Sandbox Engine)

Les pièces jointes sont analysées en exécutant les fichiers suspects dans un environnement de test virtuel, afin d'identifier des effets potentiellement dangereux. Si le document est reconnu comme un logiciel malveillant, le courriel est déplacé directement en quarantaine.

Liens sécurisés (Secure Links)

Finis les clics risqués sur des liens dans les courriels. Secure Links remplace le lien d'origine par une version réécrite qui transite par la passerelle Web sécurisée de Proofpoint. Secure Links utilise l'intelligence artificielle (dont l'apprentissage automatique et l'apprentissage profond) pour fournir une protection avancée contre l'hameçonnage, y compris lors d'attaques très ciblées. Des algorithmes supervisés et non supervisés analysent plus de 47 caractéristiques des URL et des pages Web (comportements malveillants, techniques d'obfuscation, redirections d'URL). Des modèles de vision par ordinateur analysent aussi des images afin d'en extraire des éléments utilisés dans les attaques d'hameçonnage (logos de marque, codes QR et contenu textuel suspect intégré aux images).

Analyse d'URL (URL Scanning)

Conserve le document joint au courriel dans sa forme d'origine et vérifie uniquement la cible des liens qu'il contient.

Gel temporaire (Freezing)

Les courriels qui ne peuvent pas être classés clairement sur-le-champ sont retenus pendant une courte période. Ils sont ensuite soumis à une vérification supplémentaire à l'aide de signatures mises à jour.

Déchiffrement de documents malveillants (Malicious Document Decryption)

Les pièces jointes chiffrées sont déchiffrées au moyen de modules appropriés dans le courriel. Le document déchiffré est ensuite soumis à une analyse antivirus approfondie.

Analyses médico-légales de fraude ciblée, alimentées par l'IA (AI-powered Targeted Fraud Forensics)

Analyse des tentatives de fraude :
vérifie l'authenticité et l'intégrité des métadonnées et du contenu.

Détection de l'usurpation d'identité :
repère et bloque les identités d'expéditeur falsifiées.

Système de reconnaissance d'intention :
signale des motifs de contenu qui suggèrent une intention malveillante.

Détection « spy-out » :
défense contre les attaques d'espionnage visant à obtenir de l'information sensible.

Détection de faits feints :
analyse du contenu, indépendante de l'identité, afin d'identifier des nouvelles reposant sur des faits falsifiés.

Détection d'attaques ciblées :
repère des attaques dirigées contre des personnes particulièrement à risque.

Analyseur de codes QR (QR Code Analyzer)

L'analyseur de codes QR de Proofpoint peut détecter des codes QR intégrés directement dans un courriel ou une image. Tous les codes QR sont détectés et analysés très rapidement afin de repérer du contenu malveillant. Il prend en charge les formats d'image courants, notamment GIF, JPEG, PNG et BMP.

"AutoRemediate" – Remédiation automatique

La remédiation automatique permet aux administrateurs de 365 Total Protection de supprimer des courriels des boîtes aux lettres Microsoft 365 des utilisateurs, même après leur livraison. De plus, les courriels déjà livrés puis identifiés ultérieurement comme une menace sont automatiquement supprimés des boîtes aux lettres des utilisateurs.

Alerte d'autoremédiation (AutoRemediate Alert)

Ces alertes avisent les administrateurs si des courriels déjà livrés sont ensuite classés comme malveillants, afin qu'ils puissent déclencher immédiatement des actions.