proofpoint.

GUIDE D'ACHAT

Guide du RSSI pour bloquer les menaces centrées sur les personnes et l'IA

Principales fonctionnalités

Il s'agit des cinq fonctionnalités dont vous avez besoin pour protéger votre entreprise contre les menaces centrées sur les personnes et sur l'IA :

1. Visibilité complète sur les menaces et analyse des risques
2. Protection automatisée contre les menaces pour l'email et d'autres vecteurs
3. Sécurité pour les communications d'entreprise de confiance
4. Sensibilisation des collaborateurs
5. Protection contre la prise de contrôle de comptes

Présentation

Les cybercriminels ne ménagent pas leurs efforts pour exfiltrer des données et exploiter les communications d'entreprise à des fins lucratives. Mais si le volume de menaces ne cesse d'augmenter, les tactiques employées, en revanche, ne varient guère. Le phishing, les malwares, les ransomwares, le piratage de la messagerie en entreprise (BEC, Business Email Compromise) et l'ingénierie sociale restent des méthodes privilégiées pour cibler les utilisateurs.

Ce qui a changé en revanche, c'est que l'IA optimise ces tactiques familières. Les cybercriminels utilisent des grands modèles de langage pour créer des leurres de phishing hyperpersonnalisés, automatiser 80 à 90 % de la chaîne d'attaque et lancer des campagnes multicanales en plusieurs étapes à une échelle sans précédent. En 2025, Proofpoint a observé une augmentation de 94 % des menaces email ciblant les clients. L'IA introduit également de nouveaux vecteurs d'attaque, tels que les attaques par injection d'invites. Celles-ci exploitent les assistants d'IA d'entreprise en insérant des instructions cachées dans les emails.

Dans ce guide, nous allons examiner les principales fonctionnalités dont votre entreprise a besoin pour établir un dispositif de défense efficace contre toutes les menaces centrées sur les personnes et l'IA, qu'elles soient transmises par email ou par d'autres vecteurs. Nous vous suggérerons également divers critères pour vous guider dans le choix d'une plate-forme de sécurité adaptée à vos besoins.

Figure 1. Menaces et risques dans les environnements de travail numériques

1. Visibilité complète sur les menaces et analyse des risques

Pour bloquer les menaces centrées sur les personnes et l'IA, vous devez déterminer qui sont les utilisateurs ciblés et par quels moyens ils sont visés. Vous pourrez ainsi appliquer des contrôles de sécurité adaptatifs pour protéger les utilisateurs les plus à risque.

Une visibilité complète sur les menaces couvrant l'email et les canaux numériques vous offre une vision globale de vos vulnérabilités.

Voici les informations qu'une solution doit être en mesure de vous communiquer :

- **Personnes prises pour cible**, ainsi que les menaces auxquelles elles sont confrontées et leurs interactions éventuelles avec les cybercriminels
- **Informations d'investigation numérique**, telles que le cybercriminel impliqué, la famille de menaces, les utilisateurs concernés, les techniques d'attaque, les thèmes exploités et les objectifs de la campagne d'attaque
- **Utilisateurs à risque**, afin d'identifier les personnes qui posent un risque pour votre entreprise et les raisons
- **Menaces associées aux communications d'entreprise de confiance**, dont les domaines ou sites Web usurpés et similaires susceptibles de nuire à votre image de marque
- **Changements de comportement et threat intelligence**, susceptibles de révéler que l'un de vos fournisseurs ou un tiers de confiance a peut-être été compromis
- **Activités suspectes**, qui pourraient indiquer de possibles prises de contrôle de comptes

Une plate-forme optimisée par l'IA peut corréler les signaux à travers ces dimensions, en utilisant des graphes de relations pour établir une base de référence des comportements de communication normaux, des modèles de langage pour interpréter l'intention du message et la threat intelligence pour contextualiser le comportement des cybercriminels. Vous obtenez ainsi des informations sur les risques plus précises et exploitables que celles fournies par une simple analyse manuelle.

4,88 Mio $

Coût moyen d'une compromission des données lors d'une attaque de phishing ou BEC[1]

1. IBM, *Rapport sur le coût d'une violation de données*, 2024.

La visibilité n'est pas uniquement importante lors des déploiements initiaux, elle doit être constante. Vous pourrez ainsi ajuster votre niveau de protection en continu, dès que les caractéristiques des attaques changent.

2. Protection automatisée contre les menaces pour l'email et d'autres vecteurs

Le paysage des menaces est en constante évolution. Malheureusement, les entreprises ne disposent pas toujours des compétences en sécurité et des ressources requises pour rester à niveau. Ainsi, il est courant que les équipes n'aient tout simplement pas le temps d'examiner chaque événement de sécurité. De plus, le coût des incidents est en hausse.

C'est pourquoi vous avez besoin d'une solution capable de détecter et de bloquer les menaces avec précision et efficacité, sans affecter la productivité. Compte tenu du rôle croissant joué par l'IA dans la génération et la distribution des menaces, il est impératif que vos fonctionnalités de détection soient également optimisées par l'IA.

Voici toutes les actions qu'une solution devrait pouvoir exécuter de façon automatique :

- **Blocage des menaces avant la remise** avec une efficacité d'au moins 99,999 % pour qu'elles n'atteignent jamais les boîtes de réception de vos utilisateurs
- **Détection et blocage des menaces générées par l'IA**, y compris les messages BEC créés par l'IA, le phishing personnalisé par l'IA et les attaques par injection d'invites cachées qui ciblent les assistants d'IA tels que Microsoft Copilot
- **Analyse des modèles de comportement des emails envoyés en interne**, qui s'appuie sur une threat intelligence optimisée par l'IA et des modèles d'apprentissage automatique pour détecter les activités de phishing latéral
- **Examen et blocage des URL malveillantes en temps réel** pour s'assurer qu'elles n'arrivent pas jusqu'aux utilisateurs via des emails ou des plates-formes de messagerie et de collaboration
- **Détection et neutralisation des comptes de fournisseurs d'identité compromis** hébergés dans le cloud
- **Analyse des codes QR suspects avant la remise** à l'aide d'une vision par ordinateur optimisée par l'IA et d'une analyse sémantique, et sandboxing
- **Insertion d'avertissements** dans les messages suspects

Lorsqu'une attaque parvient à obtenir un accès initial, il est capital de pouvoir détecter et neutraliser cette menace rapidement. Une intervention rapide peut faire toute la différence entre un incident mineur et une compromission à grande échelle.

3. Sécurité pour les communications d'entreprise de confiance

Les communications numériques constituent un élément vital pour les entreprises. Il n'est donc pas surprenant que les cybercriminels mettent tout en œuvre pour infiltrer les communications de confiance. Les attaques telles que le phishing, les ransomwares ou les menaces BEC enregistrent un taux de réussite plus élevé lorsque les destinataires pensent (à tort) qu'ils interagissent avec des sources de confiance.

Pour accroître leurs chances de réussite, les cybercriminels ont recours à un large éventail de tactiques d'usurpation d'identité. Celles-ci sont devenues beaucoup plus efficaces grâce à l'IA. Les cybercriminels peuvent désormais générer en quelques secondes des messages soignés et contextualisés, capables d'imiter le ton et le style d'écriture d'un cadre. Il est donc impératif de mettre en place plusieurs couches de protection pour les arrêter.

Optez pour une solution offrant les avantages suivants :

- **Authentification des emails** générés par les utilisateurs et les applications
- **Environnement dédié sécurisé** pour le relais des emails transactionnels générés par des applications
- **Prise en charge de l'implémentation DMARC** pour optimiser l'efficacité de l'authentification des emails et assurer une conformité complète à DMARC
- **Protection contre les domaines similaires**, notamment par des fonctionnalités de détection et une aide au blocage et à la mise hors service de ces domaines malveillants
- **Surveillance des comptes fournisseurs compromis** au moyen de l'IA comportementale et de la threat intelligence, et exécution d'actions automatisées pour s'en protéger

La sécurisation de vos communications d'entreprise de confiance permet de protéger non seulement vos collaborateurs, mais aussi vos partenaires commerciaux et vos clients.

4. Sensibilisation des collaborateurs

Même si la technologie bloque 99 % des menaces, le pour cent restant peut toujours donner lieu à un incident majeur. C'est ici que le comportement humain devient un facteur primordial. Les cybercriminels ont généralement besoin d'une interaction de vos utilisateurs pour mener à bien leurs campagnes malveillantes.

Et ce ne sont pas seulement les attaques qui sont préoccupantes. Les utilisateurs sacrifient souvent la sécurité de leur entreprise pour des questions de facilité. Selon le rapport State of the Phish 2024 de Proofpoint :

- 71 % des collaborateurs admettent avoir des comportements à risque, tels que réutiliser des mots de passe ou cliquer sur des liens inconnus.
- 96 % de ces collaborateurs savaient que leur comportement était risqué, mais l'ont fait quand même.

Avec l'intégration croissante des outils d'IA dans les workflows quotidiens, les collaborateurs sont également confrontés à de nouveaux risques, tels que le partage de données sensibles avec des applications d'IA non approuvées ou le déclenchement involontaire d'injection d'invites cachées lors des interactions avec des assistants d'IA.

Lorsque vous combinez attaques et comportement négligent des utilisateurs, les chances de réussite d'une compromission se multiplient. Il est donc essentiel de sensibiliser vos utilisateurs à la sécurité informatique.

Optez pour une solution offrant les avantages suivants :

- **Utilisation des données sur les menaces** pour identifier les utilisateurs les plus ciblés et à risque
- **Formation des utilisateurs axée sur les risques** qui s'appuie sur des exemples tirés de la vie réelle, tels que les menaces ciblant directement votre entreprise
- **Changement réel des comportements** au lieu de se contenter de dispenser la formation annuelle requise des utilisateurs
- **Motivation des collaborateurs** en leur offrant une visibilité sur leur score de risque individuel et leur impact sur la posture de sécurité de l'entreprise
- **Évaluation de l'efficacité** et mise à disposition de rapports utiles pour vous aider à affiner votre stratégie
- **Présentation des risques liés à l'IA dans le contenu de formation**, en expliquant notamment comment utiliser les outils d'IA générative en toute sécurité et identifier les attaques d'ingénierie sociale générées par l'IA

Une technologie performante associée à la vigilance humaine est fondamentale pour bloquer les menaces centrées sur les personnes. Chacun a un rôle vital à jouer dans la sécurisation de vos opérations commerciales.

71 %

des collaborateurs admettent avoir adopté des comportements à risque, tels que la réutilisation de mots de passe ou le fait de cliquer sur des liens inconnus[2]

2. Proofpoint, *Rapport State of the Phish 2024*, 2024.

5. Protection contre la prise de contrôle de comptes

Les données de Proofpoint attestent que 99 % des entreprises subissent régulièrement des tentatives de prise de contrôle de comptes. Ces attaques sont une forme d'usurpation d'identité dans le cadre de laquelle un cybercriminel obtient un accès à un compte en ligne et en prend effectivement le contrôle. Sans surprise, les fournisseurs d'identité cloud tels que Microsoft Entra ID, Google et Okta sont les plus ciblés. Ces comptes servent à l'authentification unique (SSO) auprès d'une série d'applications d'entreprise.

Par ailleurs, vos comptes ne sont pas les seuls dont vous devez vous préoccuper. Les cybercriminels compromettent également les comptes de partenaires commerciaux de confiance pour mener des opérations de reconnaissance et lancer de nouvelles attaques. Ces comptes compromis servent de points d'entrée pour lancer des attaques en plusieurs étapes qui se propagent à l'ensemble de l'écosystème d'une entreprise pour voler des données sensibles, réaliser des transactions frauduleuses et semer le chaos.

L'IA et l'apprentissage automatique sont essentiels pour surveiller les communications professionnelles à grande échelle et automatiser la réponse. Les modèles d'IA comportementale peuvent détecter les signaux les plus subtils d'une compromission de compte, par exemple des comportements de connexion et d'envoi d'emails inhabituels, ou des changements dans les relations de communication, susceptibles d'échapper aux systèmes basés sur des règles.

Optez pour une solution offrant les avantages suivants :

- **Surveillance continue de tous les comptes** associés à des services de fournisseur d'identité cloud tels que Microsoft Entra ID, Google et Okta
- **Threat intelligence utilisée** en association avec des données comportementales et l'apprentissage automatique pour détecter les comptes compromis
- **Protection contre les attaques de prise de contrôle de comptes** qui contournent l'authentification multifacteur (MFA) ; 65 % des comptes piratés étaient protégés par MFA[4]
- **Accélération des investigations** grâce à une vue centralisée des activités postérieures à la prise de contrôle de comptes
- **Automatisation de la réponse** par des actions telles que la suspension de comptes, les réinitialisations forcées de mots de passe et l'annulation des modifications malveillantes apportées aux règles de la boîte email et aux paramètres MFA
- **Suppression des applications** tierces suspectes dans le cadre du nettoyage postérieur à la prise de contrôle de comptes

La prise de contrôle de comptes peut coûter cher à votre entreprise et nuire à votre image de marque. Une protection rigoureuse est essentielle pour limiter le risque.

Évitez d'adopter une approche fragmentée

À mesure que vous mettez en place vos défenses pour l'email et d'autres canaux, les solutions individuelles de divers éditeurs de solutions spécialisés peuvent vous sembler le choix logique. En effet, ces éditeurs semblent parfaitement préparés à répondre à des types d'attaques précis. Cependant, cette approche cloisonnée présente plusieurs inconvénients.

Tout d'abord, elle génère des angles morts de sécurité. Lorsque les outils ne sont pas parfaitement intégrés, les équipes de sécurité éprouvent des difficultés à disposer d'une visibilité sur tout l'environnement de sécurité. Cette visibilité lacunaire accroît le risque d'avoir des menaces échappant à la détection, sans compter qu'elle retarde la réponse aux incidents.

Les outils fragmentés ne peuvent pas non plus offrir l'approche globale de l'IA nécessaire pour bloquer les menaces actuelles. Les modèles de langage, la vision par ordinateur, l'analyse comportementale et la threat intelligence doivent impérativement fonctionner de concert et partager des données contextuelles pour détecter les attaques sophistiquées générées par l'IA.

Par ailleurs, la gestion de plusieurs outils de sécurité représente une tâche chronophage et inefficace pour les équipes , qui doivent également corréler les données provenant de points de contrôle cloisonnés . Sans compter que le volume d'alertes considérable généré par ces plates-formes finit par entraîner une baisse de vigilance face à ces alertes et un risque accru de passer à côté de certaines menaces. Tous ces facteurs augmentent les coûts opérationnels.

Privilégiez donc une approche plus efficace. Adoptez une plate-forme de sécurité globale et préintégrée qui vous protège contre toutes les menaces centrées sur les personnes. De plus, la collaboration avec un partenaire de confiance unique vous garantit non seulement une gestion rationalisée, mais aussi une réduction des coûts.

99 %

des entreprises subissent régulièrement des tentatives de prise de contrôle de comptes[3]

3. Étude de Proofpoint.
4. Ibid.

Conclusion

Une stratégie de sécurité complète, centrée sur les personnes, peut protéger votre entreprise contre un large éventail de menaces. Votre démarche pour atteindre cet objectif doit commencer par le choix de la bonne solution. Optez pour une solution qui regroupe la threat intelligence issue de différents vecteurs : emails, outils de collaboration, plates-formes de messagerie et applications cloud. Elle doit aussi procurer des renseignements pertinents sur les comportements à risque des utilisateurs et contribuer à renforcer votre culture de la sécurité informatique.

Votre solution actuelle est-elle limitée à l'email ? Peut-être devez-vous composer avec des solutions cloisonnées ? Si tel est le cas, vous pouvez certainement faire mieux. Le moment est venu d'évaluer l'efficacité de votre dispositif de sécurité contre les menaces centrées sur les personnes, qu'elles soient diffusées par email ou par d'autres vecteurs.

Consolidez vos défenses avec Proofpoint

Proofpoint Prime Threat Protection offre une plate-forme préintégrée de protection contre les menaces, pour une sécurité complète. Proofpoint Prime bloque les menaces au sein des environnements de travail modernes, dont l'email et les canaux numériques. Non seulement la plate-forme vous protège contre un large éventail de menaces, mais elle le fait en outre avec une précision de détection inégalée. Optimisé par la plate-forme Proofpoint Nexus AI — un ensemble de moteurs d'IA incluant des modèles de langage, l'apprentissage automatique, la vision par ordinateur, les graphes de relations et la threat intelligence —, Proofpoint Prime offre une efficacité de détection de 99,999 % contre les menaces traditionnelles et celles générées par l'IA.

Elle fournit également des informations détaillées sur le facteur de risque humain et renforce la résilience des utilisateurs. Enfin, elle vous prémunit contre les comptes utilisateur et fournisseur compromis afin de préserver la sécurité de vos communications d'entreprise.

Proofpoint propose la seule architecture de cybersécurité moderne offrant une approche adaptative pour protéger les ressources les plus importantes et les plus à risque de votre entreprise : vos collaborateurs. C'est pourquoi près de 2,7 millions de clients de toutes tailles, dont plus de 80 entreprises du classement Fortune 100, font confiance à Proofpoint.

proofpoint.

Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir la fuite de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et confiance. Pour en savoir plus, consultez le site www.proofpoint.com/fr.

Suivez-nous : LinkedIn

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →