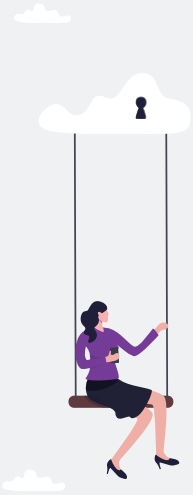
proofpoint.

EBOOK



Sécuriser Microsoft 365

Comment une solution de sécurité dédiée peut protéger les utilisateurs et les données et optimiser la valeur de votre investissement cloud

proofpoint.com/fr

Introduction

Rares sont les outils qui sont aussi essentiels que Microsoft 365 pour les entreprises modernes. Pour bon nombre d'entre elles, la plate-forme favorise le télétravail, la collaboration au niveau mondial et la migration vers le cloud.

Malheureusement, l'omniprésence de la plate-forme et son rôle central dans les entreprises peuvent en faire une cible de choix pour les cybercriminels — et souvent le principal vecteur de compromission de leurs victimes. En parallèle, l'accélération de l'adoption des modèles de travail à distance et hybrides a poussé les menaces et les fuites de données d'origine interne sur le devant de la scène.

Les attaques avancées actuelles reposent sur le phishing et l'ingénierie sociale, et pas seulement sur des vulnérabilités techniques. Les cybercriminels incitent les utilisateurs à installer des ransomwares et autres malwares, à divulguer leurs identifiants de connexion, à partager des informations sensibles et même à transférer des fonds. En outre, ils ne cessent de renforcer ces attaques centrées sur les personnes, ce qui les rend plus courantes, coûteuses et sophistiquées que jamais.

Les menaces, les emails à diffusion massive et le spam affaiblissent également votre investissement Microsoft 365. Ces importants volumes d'emails indésirables n'entravent pas seulement la productivité des collaborateurs, ils peuvent aussi accroître la charge de travail des équipes informatiques et de sécurité déjà fort sollicitées.

Bien que Microsoft 365 soit un outil de collaboration essentiel, les experts tels que Gartner et Forrester recommandent une sécurité plus complète de la messagerie, du cloud et des données que les défenses natives de la plate-forme[1,2].

Cet eBook s'intéresse à ces menaces modernes, aux bonnes pratiques de protection des utilisateurs et des données, ainsi qu'aux fonctionnalités requises pour renforcer les défenses de Microsoft 365.

1 Mark Harris, Peter Firstbrook, et al. (Gartner), « Market Guide for Email Security » (Guide du marché de la protection de la messagerie), octobre 2021.

2 Jess Burn, Joseph Blankenship, et al. (Forrester), « Best Practices: Phishing Prevention » (Bonnes pratiques : prévention du phishing), novembre 2021.

SECTION 1

Comment les cybercriminels ciblent les utilisateurs de Microsoft 365

Sans surprise, la plupart des attaques ciblées débutent par la réception d'un email.

La messagerie électronique permet aux auteurs d'attaques d'exploiter facilement le facteur humain pour dérober des identifiants de connexion, des données et plus encore par divers moyens, du phishing aux malwares. Ces menaces peuvent avoir des répercussions considérables sur les résultats financiers de votre entreprise. Le coût total moyen d'une compromission de données atteint aujourd'hui un niveau record de 4,35 millions de dollars à l'échelle mondiale, soit une hausse de 43 % au cours des trois dernières années[3]. Ce chiffre est encore plus élevé aux États-Unis, avec 9,44 millions de dollars, soit une augmentation de 15 % par rapport à 2019[4].

3 Ponemon Institute, « Cost of a Data Breach 2022 » (Rapport 2022 sur le coût des compromissions de données) et « Cost of a Data Breach 2019 » (Rapport 2019 sur le coût des compromissions de données), juillet 2022 et août 2019.

4 Ibid.

66 %

des entreprises ont été victimes d'au moins une attaque de spear phishing hautement ciblée en 2021

Phishing

Identifié pour la première fois comme une menace il y a plus de 20 ans, le phishing s'est transformé en une sorte de petite industrie artisanale. Les cybercriminels ont recours à un large éventail de techniques pour dérober des identifiants de connexion, détourner des fonds et s'emparer de données de valeur.

Le phishing revêt désormais une structure multicouche et échappe à de nombreux dispositifs de défense traditionnels. Les attaques peuvent frapper une base très large ou, au contraire, être hautement ciblées. Certaines utilisent des malwares, d'autres non. Il arrive même que les cybercriminels envoient des emails de phishing par l'intermédiaire de services marketing légitimes pour contourner les filtres antispam et autres mécanismes de défense.

Environ 66 % des entreprises ont été victimes d'au moins une attaque de spear phishing hautement ciblée en 2021. 65 % ont subi au moins une attaque par piratage de la messagerie en entreprise (BEC, Business Email Compromise)[5]. (Consultez la section « Piratage de la messagerie en entreprise et usurpation de l'identité de fournisseurs » à la page suivante.)

Quelles que soient les tactiques utilisées, les attaques de phishing affichent un taux de réussite élevé. 83 % des entreprises américaines ont subi une attaque de phishing fructueuse l'année dernière, contre 57 % l'année précédente[6].

Malwares

Chaque jour, l'AV-TEST Institute enregistre plus de 450 000 nouvelles souches de malware et applications dangereuses[7]. Mais la créativité des cybercriminels ne s'arrête pas là.

Ils sont toujours plus inspirés pour trouver de nouvelles cibles. Ils utilisent des outils automatisés pour extraire des informations sur vos collaborateurs des profils publics disponibles sur les réseaux sociaux. Ils savent où travaillent vos utilisateurs. De même, le poste que leurs cibles occupent, leurs centres d'intérêt, leurs loisirs, leur situation matrimoniale ou encore leurs précédents emplois n'ont plus de secret pour eux.

Grâce à ces informations, les cybercriminels peuvent identifier les utilisateurs disposant des données ou de l'accès souhaités et élaborer des emails suffisamment convaincants pour piéger les collaborateurs. Une fois que le destinataire a mordu à l'hameçon, une charge virale malveillante est injectée dans le système.

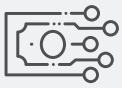
5 Proofpoint, « State of the Phish 2022 », février 2022.
6 Ibid.
7 AV-TEST Institute, « Logiciels malveillants » (https://www.av-test.org/fr/statistics/malware/), consulté en août 2022.

Piratage de la messagerie en entreprise et usurpation de l'identité de fournisseurs

Les attaques BEC et l'usurpation de l'identité de fournisseurs apparaissent comme de nouvelles menaces majeures. Selon le FBI, ces attaques ont coûté aux victimes plus de 43 milliards de dollars depuis 2016, en pertes réelles et potentielles.

Lors de ces attaques, le cybercriminel usurpe l'identité d'une personne incarnant une figure d'autorité, d'un partenaire commercial, d'un client ou d'un fournisseur. Pour ce faire, il peut utiliser une adresse email usurpée ou un domaine de messagerie similaire. Dans certains cas, il peut utiliser un compte de messagerie légitime mais compromis, ce qui est presque impossible à détecter avec les seules fonctions natives de Microsoft 365. Quelles que soient les tactiques employées par les cybercriminels, l'objectif est le même : inciter la cible à envoyer ou à détourner des fonds.

Par exemple, un email semblant provenir d'un fournisseur de confiance peut demander à un collaborateur du service de comptabilité d'effectuer diverses actions :



Transférer des fonds

Détourner un paiement

Modifier les coordonnées d'un compte bancaire

Dans la majorité des cas, l'argent va directement alimenter le compte de l'imposteur. En moyenne, une attaque rapporte près de 180 000 dollars.

Les attaques BEC ne se limitent pas à des transferts frauduleux. Les auteurs d'attaques peuvent également convaincre les destinataires d'envoyer des données personnelles, des détails de fiche de paie, et bien plus encore.

Ces attaques ciblent des collaborateurs à tous les échelons, peu importe la division, l'équipe ou le département auquel ils appartiennent. C'est pourquoi il peut se révéler nécessaire d'étendre votre protection contre les attaques BEC à tous les utilisateurs au sein de votre environnement, et pas seulement à quelques-uns.

Compromission de compte

La prise de contrôle d'un compte Microsoft 365 de confiance offre aux cybercriminels une mine d'informations pouvant servir de rampes de lancement pour toutes sortes d'autres attaques.

Les utilisateurs à privilèges constituent souvent des cibles de choix. S'il a accès au compte de messagerie d'un PDG ou d'un VP des ressources humaines, un cybercriminel peut mettre la main sur presque toutes les données du réseau. Il peut également exploiter les relations de confiance du dirigeant pour lancer des attaques BEC contre des partenaires commerciaux, ce qui perturbe les processus normaux et peut porter atteinte à l'une des ressources les plus précieuses de votre entreprise : sa réputation.

Tactiques sophistiquées

Presque toutes ces attaques ont recours à une ou à plusieurs formes d'ingénierie sociale, l'art subtil de la manipulation. Elles incitent des personnes à faire quelque chose qui n'est pas dans leur intérêt.

Les cybercriminels s'appuient sur l'ingénierie sociale pour convaincre leurs victimes de cliquer sur des liens dangereux, d'ouvrir des pièces jointes malveillantes, de détourner de l'argent et d'envoyer des données sensibles.

L'essor spectaculaire des attaques par téléphone fait partie des développements récents les plus inattendus. Ces attaques exigent un haut niveau d'interaction directe, puisque les leurres envoyés par email ne contiennent ni malwares ni URL malveillantes. Elles passent généralement inaperçues si aucune couche de protection n'est ajoutée aux défenses natives de Microsoft 365. L'objectif est de convaincre la victime d'appeler un faux numéro de service client.

Une fois que la victime appelle, le cybercriminel l'incite à lui octroyer un accès à distance à son ordinateur ou à télécharger manuellement un malware. D'après nos données, plus de 100 000 tentatives de lancement d'attaques par téléphone ont lieu chaque jour.

SECTION 2

Une protection acceptable ne suffit plus

Les fonctions de sécurité et de conformité intégrées de Microsoft 365 peuvent vous aider dans une certaine mesure, mais face à la multiplication et à l'évolution des menaces, d'autres couches de protection pourraient s'avérer nécessaires.

Dans certains cas, la cybersécurité peut avoir été reléguée au second plan alors que les entreprises peinaient à prendre en charge les modèles de travail à distance et hybrides pour rester viables. Maintenant que le pire de la pandémie de COVID-19 est derrière elles, de nombreuses entreprises cherchent à optimiser leur investissement cloud.

Une protection insuffisante contre les cybermenaces et les fuites de données peut entraîner des compromissions de données coûteuses et dommageables pour votre marque, votre réputation et vos résultats financiers. C'est pourquoi il est essentiel de renforcer la protection de Microsoft 365 pour préserver votre sécurité et votre conformité.

Les attaques d'aujourd'hui ciblent les personnes

Les cybercriminels savent que la plupart de vos collaborateurs utilisent Microsoft 365 plus que n'importe quel autre outil professionnel. Bon nombre de ces collaborateurs ont accès à des fonds ou à des données de valeur. Mais d'autres présentent des vulnérabilités, des profils d'attaque et des privilèges d'accès qui ne sont pas toujours aussi évidents.

Les cybercriminels ont recours à des techniques d'ingénierie sociale pour inciter les utilisateurs à :

Ouvrir des pièces jointes infectées

Visiter des sites malveillants

Divulguer des informations (notamment des identifiants de connexion ou des données financières)

Octroyer un accès persistant à leurs comptes via OAuth

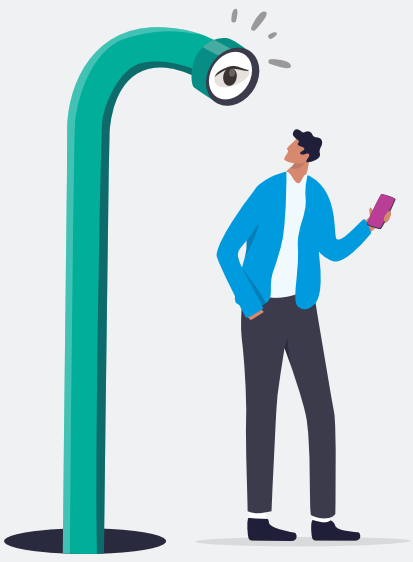
Une fois qu'ils ont infiltré le système d'un utilisateur à l'aide d'un malware, d'identifiants de connexion dérobés ou de l'accès à une application OAuth, les cybercriminels peuvent mettre en péril vos collaborateurs, vos données et vos systèmes.

Rien d'étonnant dès lors à ce que la sécurité s'invite désormais dans les conseils d'administration. C'est pourquoi la protection de votre environnement Microsoft 365 est une décision stratégique. Tout programme de cybersécurité efficace doit se focaliser sur les personnes.

Sans visibilité, aucune protection n'est possible

La visibilité est à la base de la protection de votre déploiement Microsoft 365 contre les menaces externes et les fuites de données d'origine interne.

Il est essentiel de disposer des renseignements adéquats pour mettre au jour les attaques et prendre les mesures qui s'imposent. Sans protection capable de fournir des rapports détaillés, autant chercher une aiguille dans une botte de foin.



Le blocage des menaces avant qu'elles n'atteignent la boîte de réception des utilisateurs présente deux avantages majeurs. D'une part, vous bénéficiez de renseignements sur l'ensemble de l'attaque et pas uniquement sur les dernières phases de celle-ci, lorsque le mal est fait. D'autre part, l'interception des menaces à un stade précoce, idéalement avant qu'elles n'atteignent vos utilisateurs, vous permet de les bloquer avant que votre environnement ne soit compromis.

De même, vous ne pouvez pas protéger les données ni résoudre les fuites de données sans une visibilité qui repose sur les fonctions de Microsoft Information Protection (MIP). Vous avez besoin d'informations sur l'endroit où résident vos données sensibles et ce que vos utilisateurs font avec celles-ci. Vous avez également besoin de contexte pour déterminer si des risques internes sont imputables à un utilisateur négligent, compromis ou malveillant.

L'enjeu est d'autant plus grand dans l'environnement professionnel actuel en constante mutation. Les données évoluent au rythme des innovations et des acquisitions. Pour les protéger, vous avez besoin de fonctionnalités prédictives pour identifier les données sensibles afin de mettre en place des protections qui tirent un meilleur parti de vos investissements MIP.

Le morcellement de la sécurité, de la prévention des fuites de données (DLP) et de la conformité n'est pas viable

Les cybercriminels coordonnent désormais leurs attaques sur plusieurs vecteurs, attestant de l'évolution constante du paysage des menaces. Ils compromettent souvent des comptes utilisateur pour exploiter un accès normalement réservé aux collaborateurs internes aux données, systèmes et autres ressources stratégiques.

C'est la raison pour laquelle une stratégie de défense multicouche intégrée est primordiale. Pour être efficace, la solution mise en œuvre doit s'intégrer avec l'ensemble de votre écosystème de sécurité, de protection des informations et de conformité : de vos défenses de la messagerie à votre système de prévention des fuites de données (DLP), en passant par votre solution CASB (Cloud Access Security Broker) et votre plate-forme de gestion des identités.

Une coordination intelligente et automatisée peut vous aider à prévenir, détecter et neutraliser les menaces qui ciblent les personnes par le biais de Microsoft 365.

Menaces

Avec la migration des utilisateurs vers OneDrive, Teams et d'autres outils de productivité Microsoft 365, la sécurité des données devient un véritable casse-tête. Vous devez être en mesure d'identifier et de protéger les données que vos collaborateurs créent, consultent et partagent.

Ce n'est pas toujours facile avec les seules fonctions natives de Microsoft 365. La fonction de détection des menaces intégrée à la plate-forme peut ne pas offrir la visibilité dont vous avez besoin sur les cybermenaces, les activités des utilisateurs et les mouvements de données via les emails, le cloud et les endpoints.

Fuite de données

Tous les utilisateurs représentent un risque pour les entreprises. Mais ce risque est unique et évolue en permanence. Certains utilisateurs sont malintentionnés, beaucoup sont négligents et d'autres enfin peuvent être compromis. C'est pourquoi les règles universelles de sécurité et d'accès aux données n'offrent pas de protection contre les risques internes et les menaces qui ciblent les personnes par le biais de Microsoft 365.

Vous avez besoin d'une visibilité et de contrôles reposant sur les personnes, les données et les menaces pour obtenir un contexte en temps réel. Ce n'est qu'ainsi que vous pourrez prévenir toute utilisation abusive et fuite de données au sein de l'entreprise.

L'impact des pannes inattendues des services de messagerie

Les entreprises actuelles ont besoin d'un accès fiable à leur messagerie. Une panne inopinée peut engendrer des coûts exorbitants. C'est pourquoi il est primordial de garantir un accès continu à la messagerie électronique.

Les pannes de Microsoft 365 font partie du quotidien, mais elles ne devraient pas entraîner l'arrêt de vos activités. Optez pour des fonctionnalités de continuité des opérations permettant à vos utilisateurs de rester productifs même lorsque Microsoft 365 est indisponible.

SECTION 3

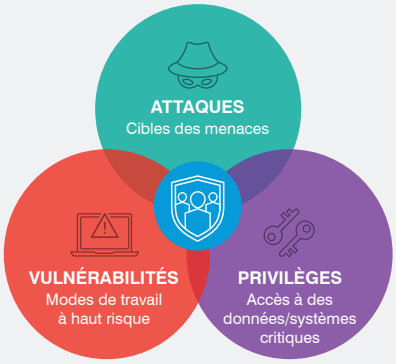
Calcul de la valeur d'une sécurité renforcée

En n'adoptant pas de solution de sécurité dédiée pour votre déploiement Microsoft 365, vous avez peut-être l'impression de faire des économies.

Mais une protection insuffisante de votre investissement risque de vous faire perdre du temps, des données et de l'argent, et même d'entacher votre réputation. Voici comment le renforcement des fonctions natives de Microsoft 365 peut préserver votre sécurité et votre conformité.

Pour les équipes de sécurité

La sécurité n'a jamais été une partie de plaisir. De nos jours, les menaces avancées rendent la situation encore plus compliquée. Avec l'instauration de réglementations sur la conformité et la multiplication des attaques de grande envergure, les questions de sécurité focalisent l'attention du conseil d'administration. Une protection performante ne suffit plus. Il est désormais impératif de bénéficier d'une visibilité suffisante pour identifier les menaces qui ciblent vos collaborateurs et les risques qu'elles font peser sur votre entreprise.



Menaces

Sans la visibilité et les renseignements nécessaires pour résoudre les problèmes de sécurité, vous risquez de perdre du temps. Selon le Ponemon Institute, la détection et la neutralisation des compromissions constituent le coût le plus important, avec 1,44 million de dollars par compromission[8], soit une hausse de 16 % par rapport à l'année précédente. C'est la première fois en six ans que ces coûts dépassent la perte de revenus résultant d'une compromission.

Les cybercriminels exploitent les outils sur lesquels vos utilisateurs s'appuient pour faire leur travail. Que les pirates réclament une rançon en échange de la restitution de fichiers SharePoint critiques, hébergent des fichiers malveillants sur OneDrive ou exploitent des vulnérabilités de Teams, les utilisateurs de Microsoft 365 font face à une avalanche de menaces. Des couches de protection supplémentaires s'avèrent donc indispensables.

Posez-vous les questions suivantes :

- Quelle est l'ampleur de la perte de productivité engendrée par la résolution des incidents liés à la messagerie qui auraient pu être neutralisés ?
- Combien de temps consacrez-vous à l'identification et à la correction des comptes compromis ? À l'investigation, à la hiérarchisation et à la confirmation des menaces ? À la suppression des emails contenant des URL ou des pièces jointes malveillantes dans les boîtes email des utilisateurs ?
- De quelle manière quantifiez-vous le risque posé par l'exposition prolongée des utilisateurs à de tels emails ?
- Combien de temps perdez-vous du fait de la mise en œuvre désordonnée de mesures de sécurité censées contenir rapidement les menaces et protéger la réputation de votre entreprise ? (Ce temps peut varier de quelques heures à plusieurs jours par alerte.)
- De combien de temps supplémentaire avez-vous besoin pour identifier les menaces qui ciblent votre environnement lorsque vous ne disposez que d'une visibilité limitée ?
- En cas de panne de la messagerie de Microsoft 365, quel est l'impact sur la sécurité de l'utilisation par les utilisateurs de leur messagerie personnelle ? (Une étude de Gartner a estimé le coût à plus de 300 000 dollars par heure[9]. Certaines pannes Microsoft ont duré plusieurs jours[10].)
- Quelle somme êtes-vous prêt à payer pour récupérer des fichiers faisant l'objet d'une demande de rançon — et quelle somme pouvez-vous consacrer à la reprise des opérations si vous refusez de payer — lors d'attaques non détectées par les seules fonctions natives de Microsoft 365 ?

8 Ponemon Institute, « Cost of a Data Breach Report 2022 » (Rapport 2022 sur le coût des compromissions de données), juillet 2022.

9 Andrew Lerner (Gartner), « The Cost of Downtime » (Le coût de l'indisponibilité des services), juillet 2014.

10 Ed Targett (Computer Business Review), « Microsoft Office 365 Outage: Day Two as Enterprise User Grumbles Grow » (Panne de Microsoft Office 365 : deuxième jour de protestation des utilisateurs d'entreprise), janvier 2019.

Prévention des fuites de données et protection des informations

Les entreprises sont constamment exposées à un risque de fuite de données, qu'il soit personnifié par un utilisateur interne malintentionné, un pirate externe à l'entreprise, voire un collaborateur bien intentionné qui expose involontairement des informations essentielles.

Rien qu'en 2021, les entreprises ont signalé 1 882 violations de données, soit une hausse spectaculaire de 68 % par rapport à 2020[11]. (Ce chiffre inclut les compromissions de données, les expositions et les fuites.)

Les craintes concernant les responsabilités en cas de compromission de données ont amené les conseils d'administration à s'intéresser aux problèmes de sécurité. C'est pourquoi vous devez poser un regard critique sur la sécurité de Microsoft 365.

Déterminez si la solution vous permet de rechercher des données sensibles (y compris différents types de fichiers), de résoudre des problèmes sur l'ensemble des canaux, ou encore d'appliquer des règles et de générer des rapports si celles-ci ne sont pas respectées. Envisagez de renforcer les fonctions natives de Microsoft 365 avec une solution capable d'appliquer des règles aux emails sortants, à OneDrive, à SharePoint et à Teams, ainsi que d'offrir une visibilité sur la messagerie, les endpoints et le cloud.

Les violations de données peuvent être le fait d'utilisateurs malveillants, négligents ou compromis. Aucune approche unique ne permet de les neutraliser. Il est essentiel de disposer de contexte et d'informations sur le type d'utilisateurs auquel vous avez affaire.

Voici quelques questions à vous poser :

- Quelle est la valeur des données Microsoft 365 que les collaborateurs qui quittent l'entreprise emportent avec eux ?
- Combien coûterait le vol ou l'exposition de données si votre solution DLP n'était pas capable de protéger vos ressources les plus précieuses sur les principaux canaux qu'utilisent vos collaborateurs pour faire leur travail ? Êtes-vous en mesure de détecter les données sensibles parmi tous les types de fichiers susceptibles d'en contenir, que ce soit dans les emails, dans le cloud ou sur les endpoints ?
- Êtes-vous en mesure de définir des règles de manière centralisée ?
- Pouvez-vous identifier rapidement le contenu et les actions qui ont déclenché une alerte ? Possédez-vous le contexte nécessaire pour déterminer si un incident d'origine interne est imputable à un utilisateur malveillant, négligent ou compromis, ainsi que pour prendre les mesures appropriées ?
- Avez-vous la certitude que votre propriété intellectuelle est protégée ?
- Disposez-vous d'un workflow de réponse aux incidents pour résoudre les problèmes ? Votre processus de réponse automatisée permet-il de bloquer et de neutraliser les menaces en ligne au niveau de la messagerie, des partages de fichiers et des sites Teams et Microsoft SharePoint ? Avez-vous besoin d'une solution DLP distincte pour réduire la surface d'attaque sur chacun de ces canaux ? Comment assurez-vous la synchronisation de ces règles et la cohérence des rapports ?
- Lorsque vous enquêtez sur une alerte DLP, obtenez-vous un aperçu clair et pertinent du déroulement des événements ? Est-il facile de partager des informations avec des équipes non techniques, comme le département juridique et les RH ?
- Savez-vous qui dispose d'un accès privilégié aux données et aux systèmes, et pouvez-vous créer des règles basées sur des personnes et des groupes d'utilisateurs ?

11 Identity Theft Resource Center, « First Half 2022 Data Breach Analysis » (Analyse des compromissions de données du premier semestre 2022), juillet 2022.

- Pouvez-vous identifier rapidement les applications tierces à risque auxquelles vos utilisateurs accèdent et êtes-vous capable de protéger votre entreprise contre ces applications ?
- En plus d'utiliser des détecteurs intégrés ou personnalisés pour identifier les données sensibles, pouvez-vous interpréter dynamiquement vos données grâce à l'intelligence artificielle et à l'apprentissage automatique afin de mettre en lumière les risques ?
- Vos règles DLP peuvent-elles être optimisées pour une plus grande fidélité ?

Pour les départements informatiques

Si vous êtes administrateur informatique, concentrez-vous sur les coûts des pannes et du support.

Disponibilité et continuité des services

Bien que Microsoft 365 promette une disponibilité de 99,99 %, il n'est pas pour autant à l'abri des pannes. (Il suffit de jeter un rapide coup d'œil aux tweets de Microsoft pour comprendre à quel point les problèmes liés au service sont fréquents.)

Si vous envisagez de renforcer la sécurité de Microsoft 365 et de minimiser ces coûts, posez-vous les questions suivantes :

- Dans quelle mesure vos activités reposent-elles sur la messagerie électronique ? Quelles seraient les conséquences de la perte d'emails de clients ou de prospects en cas de panne de la messagerie ?
- À quelle fréquence le flux d'emails dans Microsoft 365 est-il interrompu ?
- En combien de temps votre équipe informatique est-elle avertie d'une panne ?
- Disposez-vous de données pertinentes et d'une visibilité suffisante pour faire une prévision quant au délai de rétablissement du service ?
- Lorsque des utilisateurs bien intentionnés utilisent leur messagerie personnelle dans le cadre de leurs activités professionnelles, quels risques induisent-ils en matière de sécurité et de conformité ?

Traçage des messages et rapport de non-remise (NDR)

« Qu'est-il advenu de mon message ? » est une question courante à laquelle les professionnels de l'informatique et de la sécurité doivent répondre chaque jour.

Observez attentivement vos processus et posez-vous les questions suivantes :

- Combien de temps pouvez-vous consacrer à la résolution de ces problèmes ?
- À quelle fréquence les journaux de messages sont-ils indexés ? Combien de temps les journaux sont-ils conservés ?
- Le délai pour l'obtention des résultats des requêtes se compte-t-il en minutes ou en heures ?
- La recherche s'effectue-t-elle différemment dans les anciens journaux et les plus récents ?
- Disposez-vous des critères de recherche requis pour retrouver rapidement des journaux ? Les détails fournis par la recherche sont-ils satisfaisants ?
- Quelle est la procédure en place pour contacter le support afin d'obtenir des informations plus détaillées ?
- Quel est l'impact des faux positifs sur le nombre de traces de messages et le temps nécessaire ?

Temps consacré à la suppression des emails et au nettoyage des machines

Lorsque des systèmes sont compromis, l'équipe informatique peut passer des heures, voire des jours, à restaurer l'image des machines infectées.

Elle doit, de plus, supprimer ces emails pour éviter qu'un utilisateur provoque une nouvelle infection en rouvrant involontairement le contenu malveillant ou en le transférant à un autre utilisateur.

Ce processus a des répercussions sur la productivité du personnel informatique et des utilisateurs, généralement d'un jour par incident. Posez-vous les questions suivantes :

- Combien de machines subissent une restauration d'image inutile ou évitable ?
- L'équipe informatique dispose-t-elle d'outils permettant de confirmer les infections et de donner la priorité aux machines exposées mais non compromises ?
- Combien de temps l'équipe informatique consacre-t-elle au nettoyage des messages ?

Pour les équipes responsables de la conformité

La conformité n'est pas une question à prendre à la légère. Le non-respect de vos obligations peut être lourd de conséquences et coûter cher à votre entreprise. Microsoft 365 respecte les principales réglementations concernant les centres de données. Parmi ces impératifs, citons le règlement général sur la protection des données (RGPD) de l'Union européenne, la loi HIPAA (Health Insurance Portability and Accountability Act) ou encore la norme ISO 27001.

Par contre, la plate-forme est limitée au niveau de l'archivage et de la supervision des données de messagerie et de leur mise à disposition rapide en cas de litige ou lors d'audits. À défaut de conserver des archives défendables sur le plan juridique et de disposer de workflows adéquats, l'entreprise risque de gaspiller du temps et des ressources et s'expose, en outre, à des frais de contentieux.

Vous aurez sans doute besoin d'une formule d'abonnement à Microsoft 365 intégrant des fonctions de conformité, ou vous devrez souscrire un abonnement complémentaire afin de vous conformer aux obligations des lois et organismes suivants :

- FINRA (Financial Industry Regulatory Authority) – États-Unis
- SEC (Securities and Exchange Commission) – États-Unis
- OCRCVM (Organisme canadien de réglementation du commerce des valeurs mobilières)
- Financial Services Act – Royaume-Uni

Ces règles visent à protéger les investisseurs en garantissant que les secteurs américain, britannique et canadien des valeurs mobilières agissent de manière honnête et équitable. Les amendes en cas de non-respect des exigences de ces organismes de réglementation peuvent se chiffrer en millions de dollars. À ces sommes viennent encore s'ajouter les coûts liés au déploiement d'autres mesures de sécurité, aux audits et à l'éventuel préjudice porté à la réputation.

Lorsque vous évaluez les capacités natives de Microsoft 365, posez-vous ces questions importantes :

- Si votre entreprise est engagée dans un litige, Microsoft 365 vous permet-il de fournir le relevé de toutes les communications et transactions effectuées par des utilisateurs précis, y compris sur les réseaux sociaux et les plates-formes de collaboration d'entreprise ? Que se passe-t-il en cas d'infractions multiples en cours ?
- En cas de litige, êtes-vous à même de garder du contenu à des fins de conservation légale ?
- De combien de temps l'équipe informatique a-t-elle besoin pour effectuer les activités d'investigation électronique et d'exportation de données ? Quelle est la vitesse d'exécution des recherches ? Microsoft propose-t-il un accord de niveau de service définissant les paramètres de cette fonction essentielle ? Où le traitement de la recherche a-t-il lieu ?
- Après avoir déterminé les données à exporter, êtes-vous en mesure de charger les fichiers de façon automatisée sur un site FTP spécifié ? Ou devez-vous prévoir du temps pour terminer manuellement cette étape du workflow ? Quelles seront les conséquences d'un retard dans la remise des données aux équipes d'analyse ?
- Êtes-vous en mesure de capturer et de conserver tout le contenu de conformité généré par votre entreprise ? Qu'en est-il des données issues des plates-formes de réseaux sociaux ?
- Quelles sont vos capacités de supervision et de surveillance du contenu ? (Diverses réglementations exigent que le contenu soit surveillé et échantillonné.) Tirez-vous parti des dernières technologies ou utilisez-vous une mise en correspondance élémentaire de mots-clés ?

12 Andrew Peck, Jennifer Feldman, et al. (New York Law Journal), « Defensible deletion: The proof is in the planning » (Suppression justifiable : la clé réside dans la planification), janvier 2021.

13 Chris Matthews (MarketWatch), « SEC fines JPMorgan $125 million for failing to keep records » (La SEC inflige une amende de 125 millions de dollars à JPMorgan pour avoir omis de tenir des registres), décembre 2021.

SECTION 4

Avantages de Proofpoint : réduction des risques, rationalisation des opérations et diminution des coûts

Face à la complexité et à l'évolution constante des menaces et des exigences de conformité, il est indispensable d'adopter une nouvelle approche en matière de protection contre les menaces, de prévention des fuites de données et de conformité.

C'est la raison pour laquelle nous proposons une approche unique centrée sur les personnes, qui vous offre les avantages suivants :

- Protection contre les menaces et prévention des fuites de données les plus efficaces du secteur
- Visibilité et contexte exploitables pour les menaces internes et externes
- Approche moderne et intégrée des menaces, des fuites de données et des risques de conformité
- Expérience utilisateur de qualité

Voici comment nous pouvons vous aider à renforcer la sécurité de Microsoft 365.

Protection renforcée contre le phishing, les attaques BEC et autres menaces

Notre moteur de détection piloté par l'intelligence artificielle s'appuie sur une analyse comportementale avancée pour bloquer un large éventail de menaces, y compris celles difficiles à détecter qui n'utilisent ni pièces jointes ni URL malveillantes, comme les attaques BEC.

Grâce à des modèles d'apprentissage automatique et d'analyse comportementale entraînés avec plusieurs billions de points de données, nous détectons et bloquons 2,2 millions de menaces BEC chaque mois. Nous fournissons des informations d'investigation numérique détaillées permettant de comprendre pourquoi un message a été identifié comme BEC et bloqué.

Vous bénéficiez également d'une visibilité sur :

- Les collaborateurs de votre entreprise ciblés par des attaques BEC
- Les principaux thèmes BEC visant votre entreprise
- L'évolution des menaces BEC ciblant votre entreprise au fil du temps

Notre solution globale et intégrée offre une visibilité étendue sur les activités et les comportements utilisateur malveillants afin de bloquer d'autres menaces modernes. Par ailleurs, elle automatise les étapes clés de la réponse aux incidents pour vous aider à protéger les utilisateurs à l'échelle de l'entreprise.

L'analyse prédictive des URL permet d'évaluer et de neutraliser les URL dangereuses avant que les messages ne soient remis en boîte de réception et au moment où les utilisateurs cliquent dessus. Vous pouvez bloquer les pièces jointes contenant des liens dangereux et réécrire les URL suspectes dans quelque fichier que ce soit : texte (.txt), texte enrichi (.rtf) ou HTML.

Grâce à un temps d'analyse moyen inférieur à trois minutes, nous bloquons les pièces jointes dangereuses avant que vos utilisateurs n'aient la possibilité d'interagir avec celles-ci, et ce sans nuire à leur productivité. Nous prenons en charge un large éventail de types de fichiers, dont les formats PDF et HTML, et pas seulement les documents Office.

Pour les sites Web et les utilisateurs à risque, notre technologie d'isolation des URL ouvre les liens inconnus figurant dans les emails dans un environnement autonome et sécurisé afin de tenir les menaces à l'écart du vôtre.

L'affichage d'avertissements configurables en cas d'emails suspects, associé à une fonctionnalité de signalement en un clic, recommande aux utilisateurs de redoubler de prudence et leur permet de signaler facilement des messages potentiellement malveillants.

Protection des données la plus efficace du secteur

Protégez les données contre les menaces externes et internes grâce à des informations contextuelles centrées sur les personnes qui permettent de mettre en corrélation les contenus, les comportements et les menaces. La vue chronologique permet de retracer les événements derrière chaque alerte DLP. Vous pouvez évaluer rapidement les intentions des utilisateurs, collaborer facilement avec d'autres équipes telles que le département juridique et les RH, ainsi que prendre des mesures appropriées.

Nous simplifions la création, l'application et la mise en œuvre de règles unifiées au niveau de la messagerie, du cloud et des endpoints afin de préserver la sécurité et la conformité de vos données.

Notre moteur de classification des données piloté par l'intelligence artificielle permet de lancer rapidement votre programme DLP et optimise votre workflow. Vous avez le choix entre des centaines de classificateurs pré-entraînés. Vous pouvez également laisser notre moteur DLP créer des classificateurs personnalisés à partir de documents de référence. Le moteur interprète dynamiquement vos données dans les référentiels cloud et sur site pour suggérer des dictionnaires, que vous pouvez appliquer en un clic sur tous les canaux.

L'analyse algorithmique intégrée, le moteur d'identifiants intelligents et les dictionnaires vous permettent de vous concentrer sur la définition et la gestion des règles de données propres à votre entreprise. Nos workflows DLP prêts à l'emploi vous facilitent également la tâche lorsqu'il s'agit d'identifier, de gérer et de signaler des compromissions.

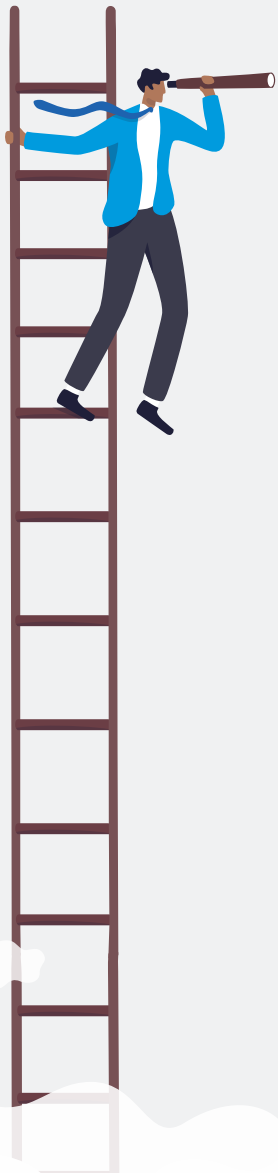
Protection contre la prise de contrôle de comptes

Grâce à notre approche multicouche, nous vous aidons à protéger vos comptes Microsoft 365 au moyen d'alertes en temps réel en cas d'activités suspectes, de mesures de correction automatisées et de contrôles d'accès basés sur le niveau de risque.

Lorsqu'un incident se produit, vous pouvez enquêter sur les activités et alertes antérieures à l'aide de notre tableau de bord intuitif. Des règles efficaces vous alertent en temps réel en cas d'incident, appliquent les mesures nécessaires aux comptes compromis, mettent en quarantaine les fichiers malveillants et appliquent une authentification tenant compte des risques, le cas échéant.

L'intégration avec Okta permet d'identifier un large éventail d'activités suspectes ou dangereuses, comme :

- Les connexions Microsoft 365 réussies mais suspectes
- Les tentatives de connexion infructueuses
- Les accès inattendus aux applications métier
- Les élévations de privilèges permettant d'accéder à des ressources cloud stratégiques
- Les élévations exemptant les utilisateurs des facteurs d'authentification habituels



Visibilité et sécurité renforcées pour le cloud

Nous adoptons une approche centrée sur les personnes de la protection contre les menaces cloud, de la découverte des applications non approuvées (Shadow IT) et de la gouvernance des applications cloud et tierces utilisant OAuth.

Nous allons bien au-delà de la sécurité native de Microsoft 365 pour protéger les utilisateurs, les données sensibles et les applications cloud contre les menaces externes et les risques de conformité. Identifiez vos VAP (Very Attacked People™, ou personnes très attaquées) et appliquez des contrôles basés sur le niveau de risque pour sécuriser leurs comptes.

Réponse ultrarapide aux incidents dans toute l'entreprise

Supprimez automatiquement les emails malveillants des boîtes de réception, y compris ceux signalés par les utilisateurs ou détectés comme dangereux après leur remise. Lorsque des messages malveillants sont détectés, nous les supprimons automatiquement des boîtes de réception des utilisateurs, même s'ils ont été transférés à d'autres personnes. Cette fonctionnalité réduit considérablement le temps que les équipes chargées de la sécurité et de la messagerie consacrent à l'investigation et à la neutralisation des menaces email.

Nous pouvons également neutraliser les prises de contrôle de comptes avant qu'elles n'aient des conséquences négatives à long terme pour vos données, vos opérations, vos relations commerciales et votre réputation.

Archivage intelligent et ultrarapide

Quel que soit le volume de vos archives, nous vous garantissons un délai de recherche de 20 secondes ou moins.

Notre solution d'archivage dans le cloud prend en charge plus de 500 types de fichiers sur site et dans le cloud, pas seulement les emails. Qui plus est, nous ne limitons pas le nombre de dossiers d'investigation électronique (e-discovery) ou d'archives que vous êtes tenu de conserver légalement, ni même le nombre d'exportations de données que vous pouvez inclure, qu'il s'agisse de 10 000 ou 100 000 boîtes email (voire plus).

Programmes de sensibilisation à la sécurité informatique visant à modifier le comportement des utilisateurs

Nous proposons une bibliothèque très complète de contenus attrayants, basés sur des techniques d'attaque réelles. Ceux-ci s'inspirent de nos propres informations de threat intelligence et tiennent compte des lacunes au niveau des connaissances de vos utilisateurs. Par ailleurs, ces ressources sont suffisamment souples pour être adaptées aux défis de sécurité uniques de votre entreprise et aux emplois du temps des utilisateurs.

Outre les formations de sensibilisation de base, nous proposons des simulations d'attaques de phishing et des formations de suivi ponctuelles à l'intention des utilisateurs qui se sont laissés piéger. Nos rapports simples et intuitifs vous permettent de suivre les progrès accomplis afin de vous aider à identifier les domaines à améliorer et de contribuer à l'épanouissement de vos utilisateurs.

Support de premier ordre

Nous installons et personnalisons entièrement votre déploiement, en nous appuyant sur les dernières tendances et bonnes pratiques du secteur. Après le déploiement, nous proposons un support 24 heures sur 24, 7 jours sur 7 et 365 jours par an, sans module complémentaire complexe.

Nous pouvons nous vanter d'un taux de satisfaction des clients de plus de 95 % et d'un taux de renouvellement annuel dépassant les 90 %. Il n'est dès lors pas étonnant que nous comptions parmi nos clients plus de la moitié des entreprises de l'index Fortune 100.

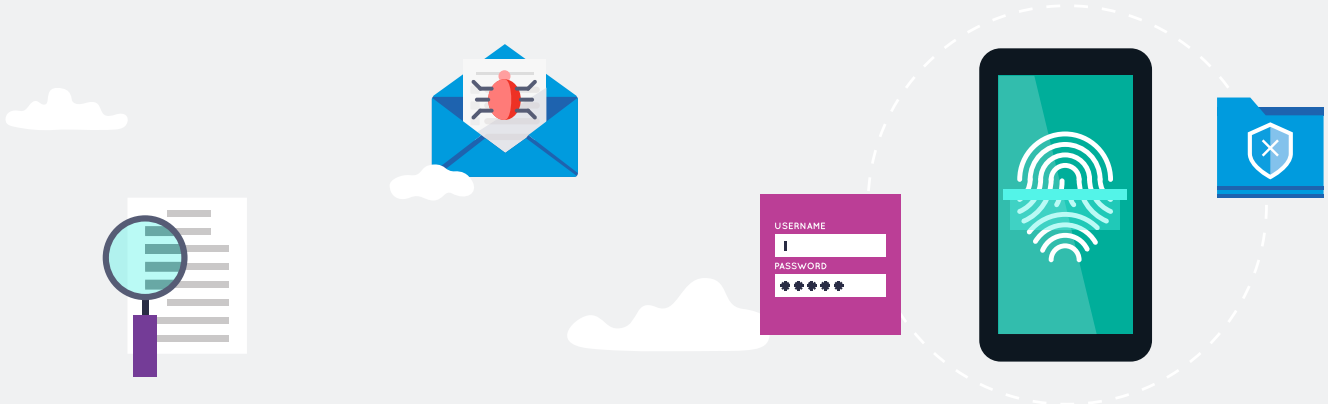
Sécurité complète et intégrée capable de rationaliser les opérations

Notre plate-forme de sécurité complète et intégrée allie de puissantes fonctions de protection de la messagerie, du cloud et des informations afin de relever les principaux défis actuels en matière de sécurité et de conformité. Elle s'intègre également avec les solutions des éditeurs de sécurité les plus réputés, comme Palo Alto Networks, Okta et CrowdStrike, afin de rationaliser votre workflow et d'aider votre équipe de sécurité à travailler de manière plus efficace et plus rapide.

Ensemble, ces solutions offrent une sécurité unifiée, centrée sur les personnes et capable de protéger votre environnement Microsoft 365.

Grâce à notre approche éprouvée de la sécurité et de la conformité pour Microsoft 365 :

- Limitez les risques.
- Libérez des ressources informatiques et de sécurité stratégiques.
- Réduisez les coûts.
- Renforcez l'efficacité de vos opérations de sécurité.



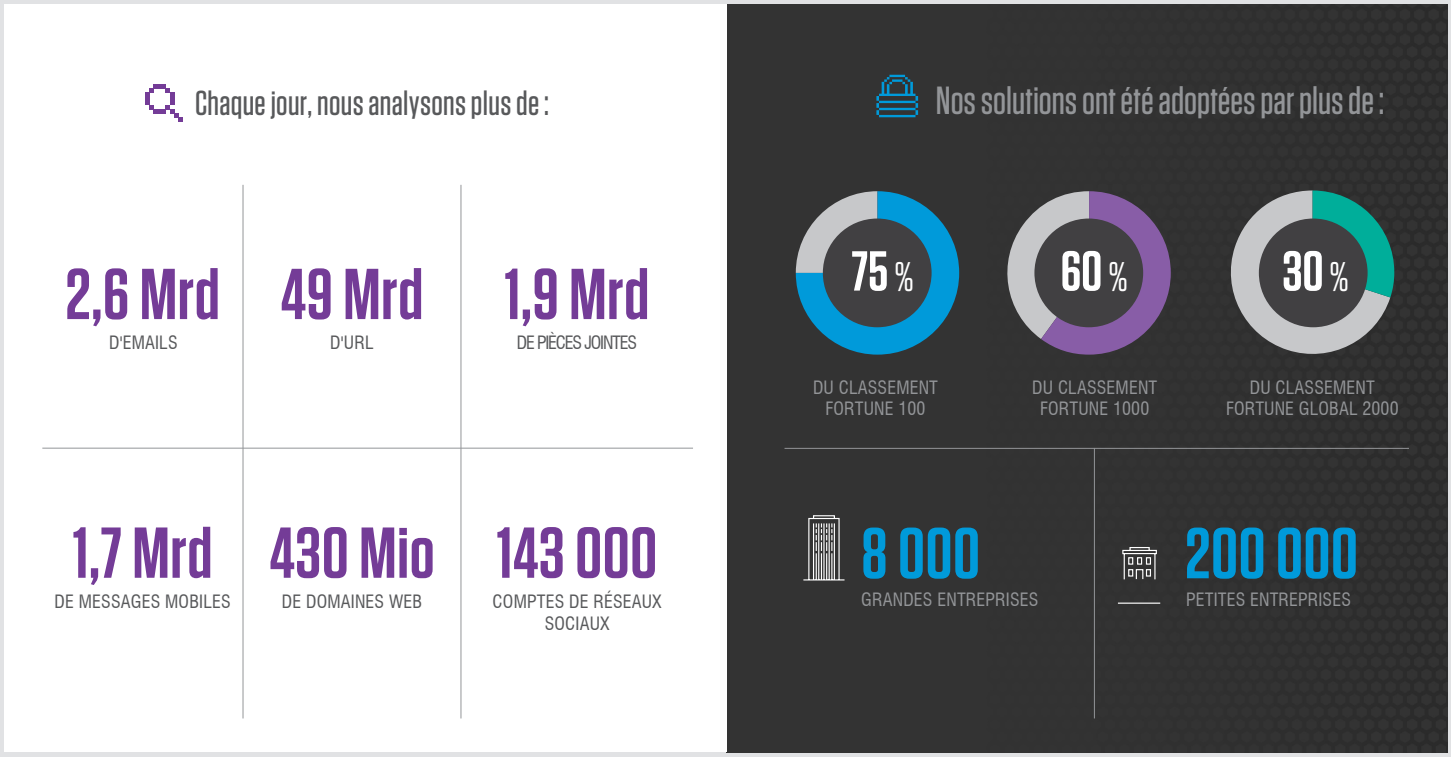
SECTION 5

Étapes suivantes

Pour en savoir plus sur Proofpoint et découvrir comment nous pouvons vous aider à renforcer la sécurité de votre déploiement Microsoft 365 à l'aide d'une approche centrée sur les personnes de la protection, de la prévention des fuites de données et de la conformité au niveau de la messagerie, du cloud et des endpoints, consultez le site proofpoint.com/fr.

À propos de Proofpoint

Le graphique des menaces Nexus de Proofpoint compile les meilleures recherches sur la sécurité, technologies et données sur les menaces du secteur pour vous protéger tout au long du cycle des attaques. Aucun autre éditeur ne bénéficie d'une telle visibilité sur la façon dont les cyberattaques actuelles ciblent les personnes.



EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0501-004-03-02 10/22