Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **January 2019**
Sponsored by **NetGovern**

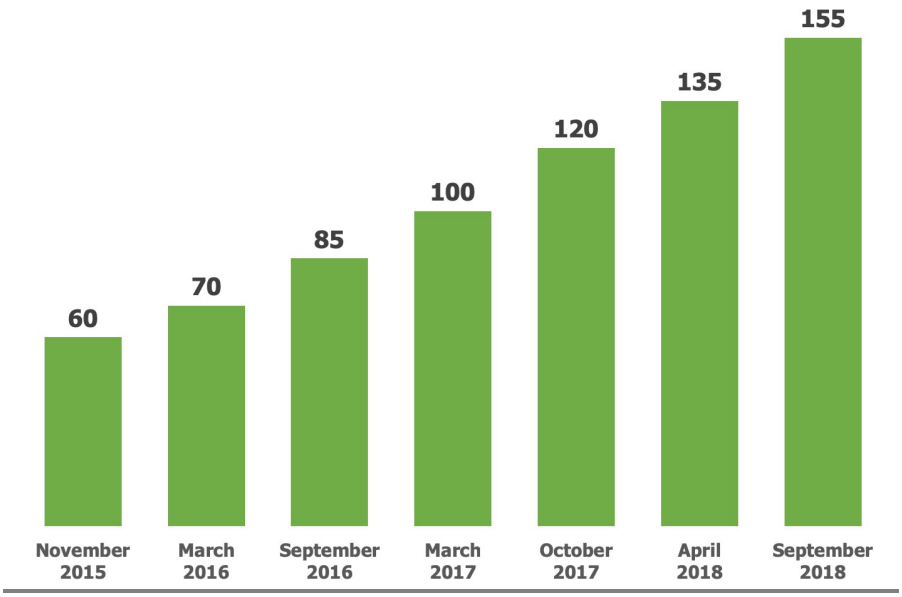
Why Your Company Needs Third-Party Solutions for Office 365

Version traduite en Français

Résumé

Office 365 est une plate-forme de communication et de collaboration performante et robuste. Microsoft a rassemblé plusieurs fonctionnalités répondant à de nombreuses exigences de l'entreprise en matière de messagerie, de messagerie vocale, de productivité de bureau et de collaboration qui se sont avérées très performantes, comme en témoigne la croissance importante du nombre d'utilisateurs de la plate-forme, comme indiqué dans Figure 1.

Figure 1
Nombre d'abonnés Microsoft Office 365 dans les organisations commerciales
millions d'abonnés



Source: Microsoft

Microsoft tente de fournir un service de cloud qui remplit de nombreuses fonctions pour une large gamme de productivité, de sécurité, de conformité et de protection des données. C'est une tâche importante qui comporte de nombreuses complexités et interdépendances. Comme toute grande plate-forme avec une base d'utilisateurs importante et diversifiée, elle fournit souvent une capacité acceptable dans de nombreux domaines, mais ne fournit pas nécessairement l'ampleur des capacités ou des solutions spécialisées pour les clients dont les besoins et les exigences vont au-delà de l'essentiel. Il peut s'agir de sociétés recherchant des fonctionnalités plus approfondies ou de meilleures performances dans des domaines spécifiques, ou de sociétés ayant des besoins spécifiques, telles que des sociétés des secteurs réglementés ou soumises à une nouvelle législation multisectorielle sur la protection des données devant satisfaire à leurs exigences légales, réglementaires ou de meilleures pratiques.

Les interconnexions étroites entre plusieurs services créent également des points de défaillance uniques, tels que la panne de service MFA (Multi Factor Authentication) survenus en novembre 2018. En outre, Osterman Research a constaté que de nombreuses solutions tierces constituent souvent une meilleure alternative à certaines des fonctionnalités natives de la plate-forme Office 365.

En résumé, Osterman Research estime qu'Office 365 et Exchange Online sont des plates-formes importantes et performantes dont l'utilisation par toute entreprise peut

Microsoft a rassemblé de nombreuses fonctionnalités qui peuvent répondre à toute une gamme d'exigences d'entreprise en matière de messagerie, de messagerie vocale, de productivité de bureau et de collaboration.

être sérieusement envisagée. Cependant, les décideurs doivent comprendre leurs véritables besoins et identifier toute caractéristique ou tout écart de performance vis-à-vis de la plate-forme. Office 365 fournit une base solide sur laquelle de nombreuses organisations devraient ensuite ajouter des solutions tierces afin de fournir des niveaux plus élevés de sécurité, de gestion de contenu, de chiffrement et d'autres fonctionnalités. **Nous notons que l'utilisation de solutions tierces permet souvent aux entreprises de souscrire à des plans Office 365 moins coûteux.**

POINTS CLES

- **De nombreuses organisations vont implémenter des solutions tierces**
  Notre étude a révélé que près du tiers des entreprises qui implémentaient Office 365 prévoyaient d'utiliser une combinaison de plans moins coûteux en association avec des solutions tierces qui fourniraient des fonctionnalités améliorées de sécurité, d'archivage ou autres que celles disponibles nativement dans la plate-forme Office 365. En fait, 37% du budget typique d'Office 365 en 2019 seront consacrés à la sécurité de tiers, à l'archivage et à d'autres solutions.

- **La messagerie électronique est l'application centrale d'Office 365**
  Il n'est donc pas surprenant que la grande majorité (93%) des entreprises considèrent la messagerie électronique comme une fonctionnalité importante ou extrêmement importante d'Office 365. En revanche, les autres fonctionnalités Office 365 ne sont pas considérées comme étant aussi importantes, notamment Skype for Business (54%), SharePoint Online (47%) et OneDrive for Business (45%).

- **Limitations pour les menaces ciblées et plus avancées**
  La plupart des organisations actuellement abonnées à Office 365 s'appuient sur la sécurité de base offerte de manière native sur la plate-forme. Pour ceux qui utilisent une version avec protection avancée contre les menaces (ATP) de Microsoft, il s'agit d'une offre de sécurité plus performante, mais elle présente certaines limitations, notamment le fait que tout le contenu n'est pas activement analysé sur place pour les menaces intégrées dans SharePoint Online, OneDrive for Business et Microsoft Teams; Analyser les pièces jointes aux courriels à la recherche de menaces inconnues à l'aide d'ATP peut retarder la livraison et avoir un impact sur la productivité des utilisateurs. Les abonnés Office 365 intéressés par ATP doivent envisager les options de sécurité proposées par des fournisseurs de sécurité spécialisés.

- **Absence de vue consolidée des menaces**
  Les divers rapports de menace du Centre de sécurité et de conformité ne fournissent pas une vue consolidée, contrairement à certaines solutions de sécurité tierces.

- **La gestion hybride doit être considérée**
  De nombreuses entreprises sont en train de passer à des environnements hybrides lors de leur migration éventuelle vers Office 365. Notre étude a révélé que 13% des entreprises prévoient de conserver une configuration hybride à long terme, bien que les grandes entreprises soient beaucoup plus susceptibles de maintenir des déploiements hybrides que les plus petites. Les environnements hybrides introduisent des complexités de gestion et d'administration supplémentaires, parfois imprévues, qui, si elles ne sont pas correctement traitées avec de nouveaux processus et outils tiers, risquent de nier de nombreux avantages de la mise en œuvre d'Office 365.

- **Certaines applications n'existeront que dans le cloud**
  Alors que les utilisateurs travaillant toujours sur site jouissent d'une plus grande parité avec ce qui est disponible dans le cloud, en particulier avec la version Office 2019[i], certaines applications, telles que Workplace Analytics[ii], ne seront disponibles que sous forme de service cloud. Les organisations qui souhaitent tirer parti de telles solutions devront faire un effort d'intégration.

En fait, 37% du budget typique d'Office 365 en 2019 seront consacrés à la sécurité de tiers, à l'archivage et à d'autres solutions.

- **Limitations pour empêcher l'usurpation d'identité**
  L'usurpation d'identité par le biais de domaines usurpés, similaires et ressemblants est un problème très grave dans le contexte des tentatives d'hameçonnage et d'harponnage. Office 365 avertira le destinataire d'un message suspect qui usurpe le nom de domaine de l'organisation, mais la correspondance du domaine doit être exacte. Office 365 ne traite pas les correspondances de domaines similaires qui ressemblent ou au domaine de l'organisation.

- **Limitations de la prévention contre les pertes de données (DLP)**
  Les stratégies DLP dans Office 365 sont évaluées par ordre de priorité ou d'exécution, et la première règle correspondant au contenu identifié dans un message électronique ou un document est appliquée. Il n'existe aucune possibilité de définir la priorité ou l'ordre d'exécution des stratégies DLP, en dehors de la séquence de leur création.

- **Problèmes liés aux capacités de cryptage**
  Microsoft se fiant aux messages basés sur les liens pour les destinataires sans Outlook signifie que les messages chiffrés peuvent être considérés comme du phishing, d'autant plus qu'ils demandent ensuite un nom d'utilisateur et un mot de passe pour se connecter. Dans la mesure le process d'hameçonnage courant consiste à utiliser un faux écran de connexion Office 365, les utilisateurs avertis peuvent refuser de traiter des messages chiffrés, ou bien se désensibiliser à la menace d'hameçonnage et ouvrir par inadvertance un message d'hameçonnage et donner accès à leurs informations d'identification.

- **Limitations dans eDiscovery**
  Il n'y a pas de workflow d'un cas d'eDiscovery dans Office 365 et les recherches de mots-clés démarrées dans l'outil de recherche de contenu ne peuvent pas être importées dans un cas d'eDiscovery.

- **Un nombre limité de types de fichiers sont indexés**
  Lors de la recherche d'eDiscovery et de l'évaluation d'une recherche, tout fichier non inclus dans les 58 types de fichiers pris en charge par Microsoft sera signalé comme non traité.

- **Pas de stockage à long terme des journaux d'audit à des fins de conformité**
  Le journal d'audit Office 365 conserve les événements d'audit pendant seulement 90 jours et il n'y a aucun moyen d'augmenter ce laps de temps (bien que Office 365 Enterprise Plan E5 fournisse une année de stockage). Cela a des implications importantes pour les organisations qui doivent se conformer à des exigences légales ou réglementaires en matière de rétention qui dictent la conservation de ces données pendant des périodes beaucoup plus longues.

À PROPOS DE CE LIVRE BLANC

Ce document blanc a été sponsorisé par NetGovern; des informations sur la société sont fournies à la fin du document. Le document comprend des données provenant d'une enquête approfondie réalisée par Osterman Research en octobre 2018. Nous avons interrogé 124 organisations comptant 1 400 employés en moyenne pour comprendre leurs problèmes de gestion d'Office 365, les fonctionnalités supplémentaires qu'elles souhaiteraient disposer et d'autres informations pertinentes sur leurs environnements Office 365. Les données de l'enquête seront publiées dans un rapport d'enquête distinct après la publication de ce livre blanc.

Le document comprend des données provenant d'une enquête approfondie réalisée par Osterman Research en octobre 2018.

Considérations relatives à la sécurité Office 365

ACCÈS À LA QUARANTAINE DE SPAM

Les décideurs doivent prendre en compte un certain nombre de problèmes liés à la mise en quarantaine des spams Office 365 lorsqu'ils évaluent des solutions tierces susceptibles de fournir de meilleures capacités de sécurité.

- Seuls 500 messages peuvent être affichés dans la quarantaine du courrier indésirable. Il n'est pas possible d'en voir plus. Un utilisateur final peut essayer de filtrer sa liste de courrier indésirable pour rechercher les courriels professionnels valides capturés par inadvertance en tant que courrier indésirable, mais la limite d'interface et de messages ne facilite pas la tâche. Il est plus probable que les messages valides étiquetés comme courrier indésirable resteront non détectés.

- Un administrateur ne peut pas afficher tous les messages en quarantaine dans une seule liste. Ils doivent être divisés en différents types de messages en quarantaine, tels que spam, logiciels malveillants, hameçonnage et message groupé.
- Les spams en quarantaine sont conservés pendant une durée maximale de 30 jours (depuis septembre 2018), après quoi ils sont supprimés et ne peuvent plus être récupérés. Microsoft indique que la durée par défaut est également de 30 jours, mais plusieurs « tenant » ont été déployés avec une valeur par défaut à 15 jours. Un administrateur peut diminuer le délai mais pas l'augmenter. Si un e-mail professionnel valide est en faux positif (Eg : Mail chiffré) et que l'utilisateur final ne vérifie pas sa quarantaine dans un délai de 30 jours, ce message sera perdu.

- Il n'est pas possible de créer différentes stratégies pour traiter différents types de courrier indésirable et de messages groupés, tels que le courrier indésirable, les logiciels malveillants, l'hameçonnage et les correspondances groupées. Une politique anti-spam peut être différenciée en fonction du destinataire, mais pas en fonction du type de message.

- Lors de l'ajout d'un en-tête X dans une politique, celui-ci doit être identique pour chaque type de courrier indésirable ou de message groupé. Il n'y a pas d'option permettant de différencier l'en-tête X en fonction du type (par exemple, spam, logiciel malveillant, hameçonnage ou message groupé).

- Bien que le courrier indésirable ne soit qu'une catégorie de messages pouvant être mis en quarantaine, un seul paramètre anti-courrier indésirable définit la période de quarantaine pour toutes les catégories de messages mis en quarantaine. Il n'y a pas d'option pour définir une période de rétention différente en fonction des différents types de messages en quarantaine.

- Pour les utilisateurs finaux, il n'y a pas de flux d'informations pour libérer le spam de la quarantaine. Si un utilisateur souhaite libérer un message dans sa boîte de réception, l'action est exécutée directement. Il n'est pas possible de demander à un administrateur de vérifier le message avant le déclenchement de l'action de libération.

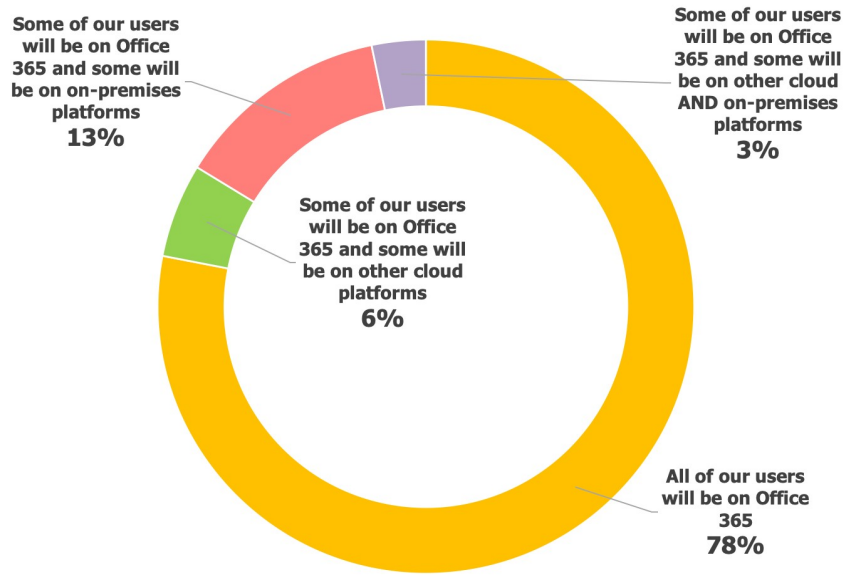
- Les messages des expéditeurs bloqués sont toujours envoyés à la quarantaine du courrier indésirable, au lieu d'être simplement supprimés immédiatement. Cela peut surcharger la quarantaine avec du spam, ainsi que des courriers électroniques d'expéditeurs bloqués.

Il n'est pas possible de créer différentes stratégies pour traiter différents types de spam et de messages groupés.

- La quarantaine ne partage pas les informations avec les utilisateurs sur le nombre de messages similaires reçus avec une ligne de sujet et un expéditeur similaires par d'autres personnes de l'organisation. Un nombre plus élevé indiquerait la probabilité que le message soit du spam ou une tentative d'hameçonnage, mais cette information n'est pas proposée pour aider les utilisateurs à prendre des décisions plus facilement sur la probabilité qu'un message soit malveillant.

- La nouvelle fonctionnalité zéro heure automatique purge (ZAP) de Microsoft ne prend pas en charge la mise en quarantaine du courrier indésirable. Même s'il peut reclasser automatiquement les messages classés incorrectement comme courrier indésirable ou mal classés et déplacer des messages entre la boîte de réception de l'utilisateur et les dossiers Courrier indésirable, il ne peut pas déplacer automatiquement les messages entre la quarantaine du courrier indésirable et la boîte de réception. De plus, ZAP fonctionne uniquement avec les boîtes de réception Exchange Online, ce qui pose un problème pour les organisations qui gèrent un environnement hybride. Comme le montre la figure 2, il s'agit d'un problème important pour les organisations qui déploient Office 365, étant donné le grand nombre d'autres solutions qui coexisteront avec Office 365.

Figure 2
Environnements de déploiement une fois qu'Office 365 est entièrement déployé



Source: Osterman Research, Inc.

- Un administrateur peut activer les notifications de courrier indésirable pour les utilisateurs finaux. Il s'agit d'un message électronique quotidien contenant la liste des messages de la quarantaine adressés à l'utilisateur et classés comme courrier indésirable. Il faut cependant signaler les points suivants :
    - La notification est pour le spam seulement. Les autres types de messages retenus en quarantaine en sont exclus.
    - Les notifications concernant les spams en quarantaine ne peuvent être envoyées qu'à tout le monde ou à personne. Office 365 ne permet pas de spécifier avec précision quels utilisateurs doivent recevoir des notifications ou non.
    - Il n'est pas possible de spécifier l'heure à laquelle le message de notification de courrier indésirable doit être envoyé depuis la quarantaine ni la fréquence à laquelle il devrait se produire en dessous de l'unité de jours (par exemple, il n'est pas possible de demander un message de notification toutes les quelques heures). Lorsque la notification de courrier indésirable est reçue au milieu de la nuit, la notification peut être manquée.
    - Bien que les messages puissent être supprimés de la quarantaine à partir du message de notification, chacun d'entre eux doit être traité individuellement, ce qui nécessite une nouvelle fenêtre de navigateur supplémentaire pour chaque message que l'utilisateur souhaite libérer dans sa boîte de réception.
    - Le message de notification répertorie les messages en quarantaine à l'aide du Temps universel coordonné (UTC) pour tous les utilisateurs. Il ne prête aucune attention aux paramètres de date / fuseau horaire de l'utilisateur, affichant ainsi les messages dans un format techniquement correct mais non pertinent pour l'utilisateur.

Alors que les messages peuvent être libérés de la quarantaine à partir du message de notification, chacun d'entre eux doit être traité à son tour.

- Il n'est pas possible de générer un message de notification de courrier indésirable dès qu'un nouveau message de courrier indésirable est reçu. Les notifications sont envoyées quotidiennement et pas plus fréquemment.

MENACES CIBLÉES ET PLUS AVANCÉES

Protection avancée contre les menaces (ATP), le service de sécurité proposé dans Office 365 Plan E5 (ou disponible en tant que service autonome), offre une protection contre les menaces avancées masquées dans les URL, les messages d'hameçonnage et les documents. En dépit du coût supplémentaire qu'il représente, l'ATP présente plusieurs limitations. Bien que les organisations puissent bénéficier d'une meilleure protection grâce à ATP plutôt qu'avec le service de protection standard d'Office 365, la diversité des risques justifie le plus souvent d'envisager l'utilisation d'offres tierces offrant une protection plus avancée. En fait, nous avons rencontré des organisations avec Office 365 ATP qui ont également ajouté une couche de sécurité supplémentaire. Les questions à considérer comprennent:

- ATP offre la possibilité de vérifier les pièces jointes et les liens à la recherche de menaces inconnues et émergentes, mais avant de pouvoir le faire, un administrateur doit configurer des stratégies pour appliquer des pièces jointes et des liens sûrs aux individus, aux groupes et à l'organisation. Aucune protection contre les menaces n'est activée par défaut. Même lorsqu'ils sont activés, les utilisateurs doivent être connectés à Office 365 pour que les liens sécurisés et les pièces jointes sécurisées fonctionnent.

- Bien qu'ATP prenne en charge le contenu au repos dans SharePoint Online, OneDrive for Business et Microsoft Teams, tout le contenu n'est pas analysé de manière active sur place pour détecter les menaces intégrées. Les fichiers sont analysés uniquement en fonction de divers critères de sélection, tels que les activités de partage, l'accès invité et d'autres signaux de menace. ATP ne peut pas fournir un tableau de bord en temps réel des fichiers malveillants dans Office 365. En outre, de nombreuses entreprises stockent des contenus dans d'autres applications SaaS, telles que Box ou G-Suite, qui ne sont pas couvertes par ATP.

- L'analyse des pièces jointes des courriers électroniques à la recherche de menaces inconnues à l'aide d'ATP peut retarder la livraison et avoir un impact sur la productivité des utilisateurs. Lorsque l'ATP a été lancé pour la première fois, certains clients se sont plaints de la longueur moyenne de livraison des courriers électroniques retardée de 10 à 15 minutes voire de trois à cinq heures aux heures de pointe. Fin 2017, Microsoft a affirmé que sa latence moyenne était d'environ 60 secondes, mais certains clients continuent de se plaindre en 2018 que le temps de traitement moyen qu'ils subissent est inacceptable. Microsoft a mis en place diverses mesures pour réduire l'impression de retard, notamment la livraison dynamique et la prévisualisation de document, cette dernière permettant à l'utilisateur de visualiser et d'éditer une version sécurisée du document alors que le document complet est en cours d'analyse. Il reste à voir combien de temps ces versions sécurisées livrées via Document Preview resteront sûres, les acteurs de la menace travaillant activement à contourner les nouveaux contrôles.

- Les liens sécurisés vérifieront une URL au moment du clic par rapport aux listes noires connues de sites malveillants. Il n'évalue pas réellement la présence de menaces sur l'URL de destination au moment du clic. Les liens sécurisés enverront un utilisateur sur un site Web malveillant si ce site ne figure pas sur une liste noire de sites malveillants. Certaines solutions tierces proposent une analyse dynamique des URL pour vérifier les URL suspectes avant le clic.

- Les liens sécurisés évaluent les URL au moment du clic, mais une fois qu'un lien est considéré comme malveillant quand un utilisateur clique dessus, la protection avancée contre les menaces ne permet plus de supprimer les instances du même courrier électronique des boîtes aux lettres des autres utilisateurs.

Nous avons rencontré des organisations avec Office 365 ATP qui ont également ajouté une couche de sécurité supplémentaire

- Microsoft ajoute partiellement le test d'url à son répertoire de vérification grâce à une intégration à pièces jointes sécurisées. Les documents liés via une adresse URL dans un courrier électronique ou un document seront désormais déclenchés au moment du clic dans les pièces jointes sécurisées (pour les types de fichiers pris en charge, tels que les documents Word, Excel et PowerPoint, ainsi que les documents PDF). À l'avenir, Microsoft s'attend à utiliser le test réel pour toutes les URL, bien que celle-ci ne soit pas encore disponible. D'autres solutions, les meilleures de leur catégorie, offrent une un test d'URL complète, capable de détecter des attaques sans logiciels malveillants, telles que l'hameçonnage par les justificatifs d'identité.

- Les liens sécurisés sont conçus principalement pour les utilisateurs de Word, Excel et PowerPoint, dans la mesure où ils utilisent les versions Office 365 ProPlus sur des périphériques Windows ou iOS et Android et sont connectés au service Office 365. Il ne vérifie pas les liens dans d'autres formats de fichier ou lorsque l'utilisateur est sur un Mac. Et, comme indiqué ci-dessus, le lien est uniquement comparé à des listes noires contrôlées, au lieu de vérifier si le lien est actuellement sans danger pour l'utilisateur final.

- Les pièces jointes sécurisées utilisent une sandbox virtuelle pour évaluer la présence de logiciels malveillants et d'autres menaces dans un document. Cette approche n'est pas efficace contre certains types de menaces, comme les ransomware protégés par mot de passe, envoyés avec le mot de passe dans le corps du courrier électronique. Les offres concurrentielles vont au-delà du sandboxing sur les machines virtuelles et incluent la prochaine génération de mécanismes de détection avancée, tels que l'inspection approfondie du contenu, l'analyse récursive des documents incorporés, l'évaluation des menaces au-dessous des niveaux de l'application et du système d'exploitation, l'identification du code en veille, le sandboxing machines physiques contrôlées pour analyser les logiciels malveillants qui échappent au déclenchement du sandboxing virtuel, etc. À notre avis, l'ATP de Microsoft n'est pas aussi performant que les meilleures offres tierces avancées sur le marché.

- Les liens sécurisés ont déjà été amenés à approuver des liens malveillants pour les utilisateurs finaux. Par exemple, la limitation Punycode a été exploitée pour tromper le vérificateur de liens malveillants avec la version sécurisée ASCII, en utilisant ensuite la version Unicode du lien pour diriger le navigateur vers un site malveillant. Des acteurs malveillants évaluent constamment comment échapper aux contrôles de Microsoft.

- Ni les pièces jointes sécurisées ni les liens sécurisés ne sont efficaces contre les messages de fraude au Président (CEO fraud) et de compromission des courriels professionnels qui ne contiennent généralement pas de lien dangereux ni de pièce jointe. Certaines solutions tierces offrent une protection dédiée à ces menaces, y compris une protection contre les attaques de domaine homographes.

- Les clients ne peuvent pas surveiller le statut d'ATP dans Office 365; sa santé de service est groupée avec d'autres services. Cela signifie que les clients payant le coût supplémentaire pour le service ne peuvent pas savoir si le service est actuellement affecté par une panne ou une autre dégradation, ou s'il est simplement non performant.

- ATP manque de fonctionnalités hybrides, ce qui signifie que les clients disposant d'Exchange ou de SharePoint sur place, par exemple, doivent disposer d'une deuxième offre distincte de protection contre les menaces. ATP ne traite que certaines charges de travail Office 365 dans des conditions spécifiques et ne traite pas des données et des systèmes au-delà de Office 365. Cela peut causer des problèmes à de nombreux clients exploitant un environnement hybride.

Office 365 propose deux moteurs de prévention des pertes de données (DLP).

- Selon Microsoft, ATP et Exchange Online Protection (EOP) n'identifient ensemble que 600 millions de courriers électroniques sur 400 milliards chaque mois comme malveillants ; Il s'agit d'un **taux de capture malveillant de 0,15%. Ceci est nettement inférieur au taux d'emails malveillants de 0,99% identifié par FireEye**, par exemple.

CAPACITÉS DE PRÉVENTION DES PERTES DE DONNÉES

Office 365 propose deux moteurs de prévention des pertes de données (DLP): une approche plus ancienne et établie, transmise depuis Exchange Server sur site, et une nouvelle approche unifiée via le Centre de sécurité et de conformité. Les deux offrent des fonctionnalités DLP, mais souffrent d'un certain nombre de faiblesses.

DLP dans Exchange Online:

- Les règles DLP ne prennent en charge que les actions de base lorsque des informations sensibles sont identifiées, sans certaines des capacités des offres concurrentes. Par exemple, bien que les règles DLP puissent empêcher un message et certains types de documents de circuler dans Exchange Online lorsque des informations sensibles sont identifiées, il est impossible de supprimer ou de nettoyer les informations sensibles contenues dans le message ou le document, ou de les chiffrer automatiquement le cas échéant, et continue de transmettre le message au destinataire. Une intervention humaine de l'expéditeur d'origine ou d'un administrateur est nécessaire pour résoudre le problème identifié, ce qui peut créer un arriéré de messages nécessitant une évaluation et une intervention manuelles pour être résolus.

- Les empreintes de base de documents sont disponibles, où un modèle de document sensible peut être enregistré et utilisé pour identifier des documents futurs ayant la même structure. Cependant, seules les correspondances complètes avec l'empreinte de document spécifique seront identifiées, tandis que les correspondances partielles éviteront la détection.

- Un message qui enfreint une règle DLP ne peut être acheminé que pour révision ou approbation vers une personne explicitement nommée ou le responsable de l'expéditeur. Il n'y a plus d'options nuancées, telles que la recherche d'annuaire basée sur le nom de l'expéditeur ou le nom du service pour trouver le responsable de la conformité local, ou l'acheminement des messages vers une quarantaine pour analyse par un groupe d'administrateurs.

- Les règles DLP détecteront les informations sensibles uniquement dans un ensemble spécifique de 58 types de fichiers, qui sont pondérés en faveur des différentes variantes de formats de fichiers Word, Excel, PowerPoint et autres formats de fichiers Office. Les types de fichiers non pris en charge contenant des informations sensibles ne seront pas capturés s'ils sont envoyés via Exchange Online. De même, les informations sensibles cachées dans les images ne seront pas identifiées, car Office 365 ne peut pas effectuer de ROC sur les documents numérisés et les captures d'écran.

DLP dans Office 365 Centre de sécurité et de conformité est la nouvelle approche en cours de développement qui fonctionne sur plusieurs charges de travail Office 365 (mais pas toutes), et surpasse les capacités de l'approche Exchange Online. Les problèmes à prendre en compte par les clients incluent:

- Les stratégies DLP ne peuvent pas signaler de manière proactive les erreurs d'envoi d'e-mails, telles que l'adressage d'un e-mail au mauvais destinataire. Office 365 n'analyse pas les schémas d'envoi normaux d'un utilisateur pour avertir des messages mal adressés et ne dispose pas de fonctionnalités avancées de détection des anomalies permettant de détecter une intention malveillante dans le comportement d'envoi d'un courrier électronique.

Les stratégies DLP ne peuvent pas signaler de manière proactive les erreurs d'envoi d'e-mails, telles que l'adressage d'un e-mail au mauvais destinataire.

- Les stratégies DLP sont évaluées par ordre de priorité ou d'exécution et la première règle qui correspond au contenu identifié dans un message électronique ou un document est appliquée. Il n'existe aucune possibilité de définir la priorité ou l'ordre d'exécution des stratégies DLP, en dehors de la séquence de leur création. Lorsqu'une nouvelle stratégie est créée, elle est ajoutée à la fin de la priorité ou de l'ordre d'exécution. De manière implicite, pour élever l'ordre d'exécution d'une nouvelle stratégie DLP, les stratégies actuelles doivent être supprimées et recréées après la création de la nouvelle stratégie DLP. Cela introduira sans aucun doute des erreurs.

- Il n'existe pas d'analyse équilibrée de la stratégie DLP qu'il serait préférable d'appliquer à un message ou à un document spécifique, ni d'essai d'identification de la "meilleure correspondance" message par message ou document par document. En d'autres termes, une stratégie générale ayant une priorité ou un ordre d'exécution supérieur sera appliquée avant une stratégie spécifique ayant une priorité ou un ordre d'exécution inférieur.

- Il n'y a pas d'options de flux de travail pour les messages et les fichiers qui violent une stratégie DLP. Par exemple, si un message électronique déclenche une stratégie, il est bloqué ou chiffré. Aucune option d'action de stratégie ne permet d'acheminer le message en violation à un administrateur ou à une file d'attente d'administration pour vérification. Comme dans le cas de DLP dans Exchange Online, DLP dans le Centre de sécurité et de conformité n'offre aucune option nuancée permettant de demander une révision par une personne autre que l'utilisateur final d'origine.

- Bien qu'Office 365 offre des fonctionnalités DLP, celles-ci sont limitées à Exchange Online, SharePoint Online et OneDrive for Business. Les nouveaux outils de conversation dans Office 365, tels que Yammer et Microsoft Teams, sont exclus, de même que les autres systèmes de stockage de documents et de conversation en dehors d'Office 365. Cette couverture partielle des charges de travail Office 365 signifie qu'Office 365 ne propose pas de moteur de correction et de règles DLP unifié pouvant être utilisé pour tous les systèmes de stockage de documents et de conversation utilisés dans l'entreprise, ni pour tout gérer dans Office 365. Microsoft a promis la possibilité de bloquer les messages de discussion dans les équipes Microsoft avant la fin du mois de mars 2019.

- L'analyse du contenu pour des données sensibles repose sur les modèles de filtres fournis par Microsoft ou sur une définition personnalisée créée par le client. Le contournement de ces filtres est simple à contourner pour exfiltrer les données d'une organisation ; les algorithmes de correspondance recherchent des correspondances exactes et sont faciles à tromper.

- Bien qu'une stratégie DLP puisse être déclenchée en fonction du contenu de la ligne d'objet d'un e-mail, si l'action de stratégie consiste à chiffrer le message, elle sera sans effet car le chiffrement proposé par Office 365 transmet l'objet en texte clair, il n'est pas chiffré.

- Aucune stratégie DLP adaptée à l'organisation n'est activée automatiquement dans Office 365, chacune doit être configurée et ajustée manuellement. Trop peu d'organisations disposent des compétences en cybersécurité disponibles pour configurer efficacement les stratégies DLP. Microsoft a récemment introduit de nouvelles fonctionnalités de renseignement permettant de détecter les informations sensibles qui doivent être protégées par une stratégie DLP et qui avertissent un administrateur qu'un type de mesure corrective est prise. Reste à savoir si cette approche de recommandation souple est suffisante. Il existe également une stratégie DLP par défaut qui recherche la présence d'un ou de plusieurs numéros de carte de crédit envoyés à une personne extérieure à l'organisation. Ceci est en mode Conseils de stratégie avec une alerte pour l'utilisateur final.

Les divers rapports de menaces du Centre de sécurité et de conformité fournissent une vue fragmentée des menaces auxquelles une organisation est confrontée.

- Les stratégies DLP ne peuvent pas cibler des groupes ou des régions spécifiques pour aider les entreprises mondiales confrontées à différentes exigences réglementaires dans le monde. L'exception à cette règle semble être pour les organisations utilisant le nouveau service Multi-Géo, ce qui permet une personnalisation basée sur la géo (mais pas nécessairement le pays).

- Les documents dans SharePoint Online et OneDrive for Business identifiés par une stratégie DLP comme contenant des informations sensibles sont bloqués sur place, afin d'empêcher tout accès au-delà du propriétaire du document, de la personne effectuant la dernière modification et du propriétaire du site. Il n'est pas possible de nettoyer automatiquement le document d'informations sensibles ou de chiffrer les informations sensibles dans le document tout en gardant le reste du document à disposition. Plus important encore, rien ne prévoit que les personnes autres puissent avoir une justification valable pour accéder au document avec les informations sensibles intactes. La position de blocage et de prévention d'Office 365 peut entraîner des problèmes pour des processus commerciaux valides.

- Les actions d'un administrateur lors de la création ou de la modification d'une stratégie DLP ne sont pas consignées dans le journal d'audit Office 365. Cela rend impossible de savoir qui a créé une stratégie DLP et comment elle a été modifiée (et par qui) au fil du temps.

- Les stratégies DLP et les types d'informations sensibles ne peuvent pas identifier le texte scanné dans les images ou le texte scanné. OCR n'est pas pris en charge

Absence de visibilité d'un volet sur les attaques de logiciels malveillants et autres

Les divers rapports de menaces du Centre de sécurité et de conformité fournissent une vue fragmentée des menaces pesant sur une entreprise via des vecteurs d'attaque de logiciels malveillants et non malveillants, mais pas une vue consolidée. Les différents rapports distincts sont axés sur des types d'attaques spécifiques, ce qui signifie qu'un administrateur de sécurité doit manuellement mettre en corrélation ce qui se passe dans l'ensemble de l'entreprise afin d'obtenir une vue d'ensemble.

Office 365 offre les rapports de menace suivants via Threat Explorer (Gestion des menaces> Explorer):

- **Logiciel malveillant (dans les courriels)**
  Affiche les menaces de logiciels malveillants détectés dans les e-mails via l'analyse antivirus, la détonation ATP ou la détection de réputation. Affiche les principales familles de logiciels malveillants et les principaux utilisateurs qui sont ciblés par des logiciels malveillants.
- **Hameçonnage**
  Affiche les courriers électroniques contenant des URL malveillantes et indique comment ils ont été détectés (par URL, par réputation, par heuristique ou par apprentissage automatique). Affiche également les URL sur lesquelles l'utilisateur a cliqué et si les URL en question ont été bloquées ou non.

- **Rapporté par l'utilisateur**
  Affiche les messages que les utilisateurs ont signalés pour la reclassification, par exemple, un courrier électronique qui a été envoyé mais que l'utilisateur estime être un courrier électronique d'hameçonnage ou contenir un programme malveillant. Affiche également les soumissions pour les faux positifs, dans lesquelles un utilisateur affirme qu'un message classé comme courrier indésirable ne l'est pas.

- **Tous les emails**
  Affiche une liste de toutes les activités de courrier électronique entre utilisateurs

et de tous les messages électroniques envoyés depuis des sources externes dans le client Office 365.

- **Logiciel malveillant (dans les fichiers)**
  Répertorie les fichiers stockés dans Office 365 qui ont été détectés comme logiciels malveillants via le processus de détonation de fichier Protection avancée contre les menaces. Cela inclut uniquement les fichiers analysés via la détonation de fichiers ATP; il ne s'agit pas d'affirmations sur tous les fichiers existants (par exemple, ceux qui n'ont pas été détonés ou vérifiés).

Il n'est pas possible d'afficher une seule liste consolidée de tous les types de menaces, puis de sous-filtrer à l'aide de facettes.

Hameçonnage d'identification et fraude par courrier électronique

Nous avons identifié plusieurs limites d'Office 365 dans la lutte contre l'hameçonnage :

- Microsoft ne semble pas être en mesure d'identifier de manière fiable les tentatives d'hameçonnage d'identifiants menant à un écran de connexion Office 365 imité. En 2018, de nombreux courriels de ce type ont été envoyés aux utilisateurs finaux. Puisque ni la charge utile ni le lien lui-même ne sont malveillants, ATP n'offre aucun avantage. Microsoft n'identifie pas systématiquement le contenu du message avec imitation pour son propre service.

- Office 365 avertira le destinataire d'un message suspect qui usurpe le nom de domaine de l'organisation, mais la correspondance doit être exacte. Il s'agit du Service de protection anti-hameçonnage de domaine exact dans Exchange Online Protection. Office 365 ne traite pas les quasi-correspondances en raison de domaines similaires, ressemblant ou semblant similaires au domaine de l'entreprise (par exemple, rnicrosoft.com vs. microsoft.com), et sans services cloud Microsoft supplémentaires, il sera difficile d'identifier les messages frauduleux de messagerie qui ont été envoyé par des comptes internes compromis. Avec les attaques d'usurpation d'identité par le biais de la prise de contrôle de boîtes aux lettres légitimes, le manque de fonctionnalités de détection avancées d'Office 365 est inquiétant.

- Protéger les utilisateurs de l'identité d'autres utilisateurs nécessite l'intervention manuelle d'un administrateur pour créer une stratégie anti-hameçonnage et répertorier chaque expéditeur spécifique à protéger. Cette liste doit être mise à jour manuellement par l'administrateur, car l'intégration avec Azure AD en fonction des rôles n'est pas prise en charge, par exemple pour protéger un nouveau vice-président ou PDG.

- Les méthodes traditionnelles de classification du courrier indésirable en fonction du volume de messages ne fonctionnent pas pour la classification des messages d'hameçonnage d'identification et de fraude par courrier électronique. La fraude peut être perpétuée par un seul message.

- Office 365 ne fournit pas une méthode simple pour supprimer les e-mails d'hameçonnage et d'emprunt d'identité des boîtes aux lettres ayant traversé des filtres. Sans revenir à PowerShell, il n'existe aucun moyen de supprimer un courrier électronique dans plusieurs boîtes aux lettres ni un moyen simple d'annuler une rétractation (certaines solutions tierces permettent de réaliser cela assez facilement). Le même problème s'applique à DLP dans Office 365: en cas de fuite interne d'informations, il est nécessaire de prendre des mesures pour supprimer ces informations. Par exemple, depuis le *New-ComplianceSearchAction* La commande PowerShell destinée à la purge des e-mails d'hameçonnage ne peut que supprimer des messages, ce qui laisse les e-mails d'hameçonnage

Nous avons identifié plusieurs problèmes dans Office 365 dans le contexte de l'hameçonnage par les informations d'identification et de la fraude par courrier électronique.

accessibles aux utilisateurs finaux s'ils récupèrent des éléments supprimés via Outlook ou Outlook Web Access. ZAP (Purge automatique à zéro heure) ne fonctionne qu'avec le spam et les messages malveillants, et non les messages d'hameçonnage et d'usurpation d'identité.

- L'Anti Spoofing cible les utilisateurs, et les adresses autorisés à usurper le domaine de l'organisation. Cela offre une protection à leurs propres utilisateurs internes et à tout partenaire commercial ou client qui reçoit un courrier électronique valide ou non valide de leur domaine. IL fait partie du centre de sécurité et de conformité. Il convient de noter que le contrôle de stratégie granulaire n'est pas disponible pour l'anti spoofing; par contre, la fonctionnalité ne peut être définie que sur «activé» ou «désactivé». En outre, la fonctionnalité de création de rapports pour cet outil est limitée. L'Anti Spoofing a été initialement publié pour les clients du plan Enterprise E5 (ou ceux avec le complément ATP), mais a été rendu disponible dans le cadre d'EOP en août 2018.

- Les mécanismes d'authentification de messagerie courants, tels que SPF, DKIM et DMARC, sont en mesure d'identifier l'usurpation d'identité de marque lorsqu'ils sont correctement implémentés. Cependant, ils ne sont pas aussi efficaces pour identifier les usurpations de marque lorsque des noms de domaine identiques ou proches avec leur propre authentification de messagerie électronique sont utilisés. La capture et la classification appropriée de tels messages nécessitent d'aller au-delà des approches courantes d'authentification de messagerie.

SUPPORT POUR ARCHITECTURES HYBRIDES

Les fonctionnalités de sécurité d'Office 365 offrent une prise en charge incomplète pour les organisations dotées d'architectures hybrides:

- ATP manque de fonctionnalités hybrides, ce qui signifie que les clients disposant d'Exchange ou de SharePoint sur place, par exemple, doivent disposer d'une deuxième offre distincte de protection contre les menaces. ATP ne traite que certaines charges de travail Office 365 dans des conditions spécifiques et ne traite pas des données et des systèmes au-delà de Office 365. Cela peut causer des problèmes à de nombreux clients exploitant un environnement hybride.

- Les stratégies DLP définies dans le Centre de sécurité et de conformité ne s'appliquent qu'à des charges de travail Office 365 spécifiques. Ces stratégies ne sont pas également appliquées aux serveurs locaux de Microsoft ou d'autres fournisseurs.

- La recherche dans le Centre de sécurité et de conformité concerne uniquement certaines charges de travail d'Office 365 et ne fonctionne pas avec les environnements Exchange, SharePoint et OneDrive for Business sur place.

Toute entreprise qui investit dans les fonctionnalités de sécurité d'Office 365 - avec tous leurs problèmes associés - devra toujours acquérir et gérer un ensemble de services de sécurité complètement séparé pour les charges de travail et les données autres qu'Office.

SOLUTIONS DE SÉCURITÉ PAR TIERCES PARTIES PARALLÈLES

Même les meilleures offres d'Office 365 ne traitent pas, ne résolvent pas et n'atténuent pas toutes les menaces à la sécurité rencontrées par les organisations qui utilisent les plans Office 365 les plus coûteux (par exemple, E3 et E5). Par exemple, les e-mails d'hameçonnage parviennent toujours aux boîtes de réception des utilisateurs finaux, ce qui augmente les risques de vol d'informations d'identification et de compromission de compte. Microsoft préfère proposer sa propre monoculture de services de sécurité, plutôt que de fournir des points d'intégration à haute fonctionnalité pour des offres tierces susceptibles de renforcer le support client

Les fonctionnalités de sécurité d'Office 365 offrent une prise en charge incomplète pour les organisations dotées d'architectures hybrides.

global. À Ignite 2017, par exemple, Microsoft s'est vanté de sa part de marché sur le marché des logiciels malveillants, affirmant avoir trois fois plus de clients que son plus proche concurrent. Dans le paysage de menaces en rapide évolution dans lequel les entreprises se retrouvent au travail, Microsoft et ses clients seraient mieux servis si Microsoft offrait de meilleures possibilités aux fournisseurs de solutions de sécurité tierces de fournir des services de sécurité complémentaires renforçant les capacités de sécurité d'Office 365.

CAPACITÉS DE RÉTRACTION

Le client Outlook offre une fonctionnalité de rappel de message qui permet de supprimer ou de remplacer un message dans la boîte aux lettres du destinataire sous certaines conditions. Rappel de message est une option "meilleurs efforts" de l'utilisateur final dans le client Outlook et n'est pas disponible dans Outlook Web Access, ni en tant qu'option de niveau de service Office 365. Le rappel fonctionne si le message d'origine n'a pas été lu, il reste dans la boîte de réception du destinataire, le client Outlook du destinataire est ouvert et le destinataire se trouve dans le même client Office 365. Rappel de message a les limitations suivantes:

- Il échoue si le message a déjà été lu. Le message original et le message de rappel resteront dans la boîte de réception du destinataire.
- Il échoue si le destinataire se trouve dans un autre client Office 365, n'utilise pas Outlook ou a déplacé le message (par une règle automatisée ou une action manuelle) dans un dossier autre que la Boîte de réception.
- Les messages rappelés peuvent être récupérés par le destinataire, grâce à la récupération des éléments supprimés. Étant donné que le message rappelé est supprimé, ce qui le déplace dans le dossier Éléments récupérables et non dans les éléments supprimés, le destinataire peut récupérer ces éléments dans les délais impartis.

Les documents joints au message rappelé seront soumis aux mêmes conditions et limitations. Le rappel peut fonctionner, mais il existe de nombreuses conditions communes dans lesquelles ils ne fonctionneront pas.

Archivage et gestion de contenu

Lorsqu'on envisage Office 365, l'une des questions cruciales à laquelle les entreprises sont confrontées est de savoir s'il s'agit d'un remplacement complet de tous les serveurs et de toutes les fonctionnalités Microsoft sur site ou d'un ajout aux fonctionnalités actuelles sur site.

Dans les limites d'Office 365, l'objectif de conception signifie l'ajout de nouvelles sources de contenu (par exemple, Microsoft Teams) et de nouveaux types de contenu (par exemple, conversations Microsoft Teams, chiffrement de messages Office 365, planificateur, flux, etc.). Ce contenu supplémentaire doit être sécurisé, contrôlé et régi.

Dans une perspective plus large, se pose également la question de savoir si les fonctionnalités natives d'Office 365 fournissent un support adéquat pour les sources de contenu non-Microsoft, et même pour les sources de contenu Microsoft autres qu'Office 365.

IL N'Y A AUCUN EQUIVALENT A UN JOURNAL DE COURRIEL

Au lieu d'avoir un journal de courrier électronique classique, Microsoft a amélioré son modèle Office 365 afin d'obtenir le même «résultat de conformité» d'un service de journal. En bref, en plaçant toutes les boîtes aux lettres pertinentes en litige ou en conservation, tous les courriels envoyés et reçus sont conservés indéfiniment et ne peuvent pas être supprimés par les utilisateurs. Les boîtes aux lettres inactives (c.-à-

Lorsqu'on envisage Office 365, l'une des questions cruciales à laquelle les entreprises sont confrontées est de savoir s'il s'agit d'un remplacement complet de tous les serveurs et de toutes les fonctionnalités Microsoft sur site ou d'un ajout aux fonctionnalités actuelles sur site.

d. celles appartenant à d'anciens employés) peuvent également être mises en attente indéfinie (actuellement sans pénalité de licence, mais cela peut changer).

Si une organisation a un journal existant lors de sa migration vers Office 365, elle aura donc besoin d'un plan pour:

- Migration du contenu du journal existant vers Office 365 ou
- Transférer le journal existant dans un service de journal tiers et continuer à écrire dans ce journal à partir d'Office 365

La première option peut être obtenue avec un logiciel de migration spécialisé. Toutefois, les instructions de Microsoft sur la migration du contenu du journal restent floues. Il existe diverses limitations à l'utilisation des boîtes aux lettres dans Office 365 pour conserver les messages appartenant à plusieurs utilisateurs.[iii]. Bien que l'utilisation suggérée de boîtes aux lettres partagées sous licence appropriée puisse être utilisée, une organisation peut être amenée à utiliser plusieurs centaines (voire des milliers) de boîtes aux lettres partagées pour traiter le retard de journal. Cela complique quelque peu la découverte électronique et risque de nuire aux journaux traditionnels.

La deuxième option implique la nécessité de maintenir et de rechercher sur deux sites pour répondre aux besoins en matière de gouvernance de l'information et de découverte électronique, mais cela peut permettre de réduire les coûts et de proposer une solution plus pratique, en particulier si une organisation a des années de revues à conserver.

CHIFFREMENT

La première version de Microsoft Office 365 Message Cryptage de Microsoft souffrait de nombreuses faiblesses, notamment un manque de capacité, des rapports médiocres et une interface utilisateur inadéquate pour les destinataires. Lors de sa conférence Ignite en 2017, Microsoft a annoncé la publication d'une nouvelle version qui résoudrait certaines des faiblesses de la première (notamment les exigences relatives aux comptes d'utilisateur et aux clients). Cependant, plus d'un an après la publication d'Office 365 Message Cryptage Version 2 (ou OMEv2 en abrégé), l'offre continue de poser des problèmes de performance et de fonctionnalités. Par exemple :

- Le paramètre de chiffrement à ne pas transférer initialement publié avec OMEv2 a imposé des paramètres de chiffrement et de gestion des droits au message et à ses pièces jointes. Les clients ont trouvé ce paramètre trop restrictif pour une utilisation générale. On ignore pourquoi Microsoft pensait que la combinaison des deux était une bonne idée.
- Le paramètre de chiffrement Encrypt Only, publié au 1er trimestre 2018, répond en principe à plusieurs critiques formulées contre Do Not Forward, telles que la suppression de la gestion des droits après livraison. En pratique, Microsoft n'a toujours pas fourni d'option de chiffrement qui fonctionne avec Outlook pour Windows et Mac avec fiabilité. Microsoft a dû introduire de nouveaux paramètres au niveau du client pour résoudre les problèmes de post-livraison empêchant les destinataires de lire les pièces jointes chiffrées. Le nouveau paramètre supprime le chiffrement appliqué aux pièces jointes pour certains destinataires dans des conditions particulières, ce qui semble compromettre le point clé du chiffrement.
- Certains clients d'Office 365 se sont plaints des exigences de version spécifiques et en constante évolution pour Outlook (et des bugs dans les différentes versions qui signifient que le service n'a pas fonctionné), de l'impossibilité d'envoyer des messages chiffrés à d'autres clients hébergés d'Office 365 dans diverses conditions, et du non-respect des règles- divulgation par Microsoft des paramètres de niveau client dans Office 365 empêchant le cryptage de fonctionner.

Microsoft a tenté de fournir un service de chiffrement de bout en bout transparent qui fonctionne en ligne sur le client Outlook.

- Microsoft a tenté de fournir un service de chiffrement de bout en bout transparent qui fonctionne en ligne sur le client Outlook. Il n'a pas été en mesure de le faire depuis l'annonce d'OMEv2 à la fin de 2017 et certaines indications - telles que l'intégration de nouvelles fonctionnalités dans OMEv2 avec des messages basés sur des liens qui s'ouvrent dans un portail de visualisation plutôt qu'en ligne dans Outlook.

- Les messages chiffrés envoyés aux destinataires à l'aide de Google Gmail et Yahoo Mail peuvent utiliser leur identité Google ou Yahoo pour déchiffrer le
- message dans le portail de visualisation. Il s'agit d'un processus transparent pour le destinataire. Toutefois, si l'expéditeur envoie le courrier électronique chiffré au mauvais destinataire, ce dernier pourra accéder au message chiffré en utilisant uniquement leurs informations d'identité Google ou Yahoo. L'expéditeur et l'organisation émettrice ne peuvent pas exiger de vérification d'identité supplémentaire pour s'assurer que le message a bien été reçu par le destinataire approprié, tel qu'une authentification à plusieurs facteurs. Il en résulte une situation de violation de données difficile à identifier par l'entreprise qui envoie.

- De même, si le compte Google ou Yahoo d'un utilisateur est compromis, le pirate informatique pourra utiliser le processus de déchiffrement transparent pour accéder aux messages chiffrés. Cela aboutit également à une situation de violation de données difficile à identifier par l'entreprise d'envoi.

- Si le compte Google ou Yahoo d'un destinataire est compromis, le pirate informatique pourra envoyer des réponses chiffrées à l'expéditeur d'origine et à d'autres destinataires. Cela pourrait être utilisé pour distribuer des messages d'hameçonnage chiffrés qui sont plus difficiles à détecter.

- La dépendance de Microsoft vis-à-vis des messages basés sur des liens pour les destinataires sans Outlook signifie que les messages chiffrés peuvent ressembler à des messages d'hameçonnage, d'autant plus qu'ils demandent un nom d'utilisateur et un mot de passe pour se connecter. Cette conception déclenche tous les drapeaux rouges pour les tentatives d'hameçonnage. D'autres services de messagerie, tels que Gmail, peuvent classer les messages OMEv2 en tant qu'hameçonnage, avertissant le destinataire de ne pas cliquer sur le lien. En d'autres termes, les messages OMEv2 présentent toutes les caractéristiques d'un message d'hameçonnage, ce qui compromet la capacité de l'expéditeur à obtenir des informations essentielles entre les mains du destinataire.

- OMEv2 ne chiffre pas la ligne d'objet du message. Ceci est toujours passé en clair. Cela n'était pas non plus proposé dans OMEv1, mais si la ligne d'objet contient des informations sensibles, elle ne sera pas protégée par un chiffrement, même si le message et les pièces jointes sont chiffrés.

- Un utilisateur final n'a pas la possibilité de chiffrer automatiquement tous les messages qu'il envoie via Outlook. Ceci doit être effectué message par message par un utilisateur final.

- A l'instar de la version d'origine, OMEv2 n'offre aucun aperçu post-livraison ni capacité de création de rapports pour l'expéditeur du message. Le Centre de sécurité et de conformité Office 365 offre un nouveau rapport sur les messages chiffrés aux administrateurs Office 365, mais ce dernier n'est pas disponible pour les utilisateurs finaux et ne rend pas compte des actions de post-livraison du destinataire. Cela a plusieurs implications pour le flux de travail, telles que l'incapacité de l'expéditeur à voir si le message a été ouvert par le destinataire. Des messages ou des appels séparés sont nécessaires pour confirmer la réception. Cela signifie que l'expéditeur ne peut pas modifier le statut du chiffrement ni les droits après l'envoi du message. Si un expéditeur se rend compte qu'il a envoyé un message au mauvais destinataire, il ne peut pas savoir si une violation de données s'est produite ou non. Enfin, si un message chiffré est marqué comme courrier indésirable ou filtré comme courrier indésirable,

Un utilisateur final n'a pas la possibilité de chiffrer automatiquement tous les messages qu'il envoie via Outlook.

l'expéditeur n'a aucun moyen de que son message n'a pas été remis comme prévu. Des messages ou des appels séparés seront nécessaires.

- OMEv2 n'offre pas la possibilité à l'expéditeur de révoquer l'accès au message après son envoi depuis Outlook ou Outlook sur le Web.

- Au quatrième trimestre de 2018, Microsoft a mis en place un processus de révocation (uniquement en prévisualisation) permettant à un administrateur informatique de révoquer des messages au nom d'un expéditeur. Pour cela, l'administrateur doit localiser l'ID du message incriminé (par exemple, via une trace de message dans Exchange Online) et utiliser les applets de commande PowerShell pour mener à bien le processus de révocation.

- La révocation par un administrateur informatique est un processus global : le message est révoqué pour tous les destinataires. Il n'est pas possible de supprimer l'accès pour un destinataire spécifique uniquement, ni d'ajouter un nouveau destinataire au message envoyé précédemment. Ce manque de nuance complique les discussions par courrier électronique cryptées existantes, ce qui entraîne une rupture du flux de travail pour tous les destinataires.

- En règle générale, OMEv2 n'offre le chiffrement que pour les types de fichiers Microsoft Office, pas pour les autres types de fichiers tels que PDF. Il est destiné aux organisations utilisant des documents Word, Excel, PowerPoint, InfoPath et XPS. Les organisations dont les types de fichiers non-Microsoft sont couramment utilisés ne trouveront pas grand intérêt pour OMEv2. En septembre 2018, Microsoft a annoncé que les documents PDF seraient pris en charge d'ici la fin de 2018. Cependant, Microsoft mentionne discrètement que même si les documents PDF seront chiffrés en transit, ils ne le seront pas une fois le message reçu. Cela signifie que les documents PDF sont gérés différemment des documents Office, une incohérence qui entraînera certainement des violations de données par les utilisateurs finaux qui assument un chiffrement durable de toute pièce jointe à un courrier électronique.

ARCHIVAGE

L'archivage- (transfert de données d'entreprise d'un système d'entreprise vers un emplacement séparé et sécurisé pour un stockage optimisé, l'immuabilité et une meilleure gouvernance des données) n'est pas proposé pour certains types de contenu importants dans Office 365. Ceux-ci incluent SharePoint, Skype for Business, des types de message supplémentaires et du contenu tiers.

- Le contenu SharePoint, tel que les documents et les éléments de liste, peut être conservé sur place par le biais de stratégies de rétention, ou déplacé vers un autre emplacement de SharePoint après son expiration ou sa perte de pertinence. Ces actions de rétention ou de déplacement peuvent être déclenchées en fonction de déclencheurs d'événements spécifiques basés sur la date et uniquement. Pour les organisations respectant les limites de stockage assignées pour SharePoint, la gestion des enregistrements sur place dans SharePoint peut suffire. Cependant, ce qui n’est pas possible, c’est d’archiver un contenu SharePoint qui n’est plus à jour sur des systèmes de stockage alternatifs et moins chers. Bien qu'il soit possible d'acheter une capacité de stockage SharePoint illimitée, cela entraîne une tarification avantageuse. Les entreprises qui disposent de grandes quantités de données SharePoint ne sont pas bien servies si elles souhaitent conserver leur contenu SharePoint bien ajusté et à jour sans générer de frais de stockage supplémentaires à long terme pour SharePoint, ou si elles souhaitent archiver le contenu hors de SharePoint Online en fonction de déclencheurs d'événements dépassant la date métadonnées. En outre, SharePoint n’est pas compatible une seule fois avec la fonction WORM (écriture unique, lecture multiple) - un problème sérieux pour les organisations des industries réglementées.

L'archivage n'est pas proposé pour certains types de contenu importants dans Office 365.

- Skype Entreprise Online s'appuie sur Exchange Online pour l'archivage si certaines conditions sont remplies. Aucun service d'archivage natif pour Skype Entreprise Online n'est disponible. Par défaut, les transcriptions de messagerie instantanée Skype sont conservées dans le dossier Historique des conversations de la boîte aux lettres Exchange Online de chaque utilisateur. Toutefois, à moins que la boîte aux lettres ne soit en attente légale ou contentieuse, un utilisateur peut supprimer ses transcriptions de messagerie instantanée à volonté, ce qui ne constitue pas une archive immuable ou fiable des messages passés. La nécessité d'une suspension légale pour forcer la conservation des messages Skype signifie que toutes les boîtes aux lettres Exchange Online doivent être en attente à tout moment pour que cela fonctionne, ce que nous considérons comme une conception étrange. Si une boîte aux lettres est en attente, les messages instantanés entre homologues et à plusieurs parties sont conservés, ainsi que les activités de téléchargement de contenu pendant les réunions. D'autres actions dans Skype for Business ne sont pas conservées, telles que les transferts de fichiers d'égal à égal, l'audio / vidéo pour les messages instantanés et les conférences entre homologues, le partage d'applications et les annotations de conférence.

- Les messages texte sur les terminaux BlackBerry seront archivés dans Office 365 si un accord avec une tierce partie est en place pour capturer ces messages. Les messages texte sur d'autres appareils, y compris iOS et Android, ne sont pas capturés. BlackBerry ayant maintenant une faible part de marché par rapport à iOS et Android, la capture de messages BlackBerry n'est pas aussi utile qu'elle pouvait l'être autrefois.

- Le contenu de messagerie, collaboration, médias sociaux et autres sources de contenu tiers spécifiques peut être archivé dans Exchange Online dans Office 365 en tant que messages électroniques convertis si des accords ont été conclus avec un partenaire de données tiers. Les messages sont stockés dans la boîte aux lettres Exchange Online appartenant à l'utilisateur spécifique. Pour le contenu dont le contenu ne peut pas être suivi par une personne nommée, une boîte aux lettres fourre-tout est utilisée. La plupart du contexte du contenu de Twitter, Facebook, Yahoo! Messenger, DropBox et Salesforce Chatter sont perdus lorsque ces sources multimédia enrichies sont converties en messages électroniques, ce qui rend difficile la recréation d'une chaîne d'événements historiquement valide.

E-discovery et gouvernance des données

L'e-discovery est un élément essentiel de toute messagerie électronique et de toute collaboration en raison de la nécessité de produire des informations à l'appui des litiges et du fait qu'une très grande partie des données d'entreprise est généralement stockée dans les plates-formes de messagerie et de collaboration des entreprises. Office 365 offre des fonctionnalités utiles dans le contexte de découverte électronique, mais il comporte certaines limitations. Par exemple :

- Microsoft n'offre pas de contrat de niveau de service (SLA) pour une recherche de contenu ou une recherche électronique, mais affirme que 100 boîtes aux lettres peuvent être recherchées en 30 secondes et 10 000 boîtes aux lettres en quatre minutes. En pratique, les recherches prennent beaucoup plus de temps pour renvoyer les résultats.

- Des stratégies de conservation, de préservation et de suppression distinctes ne peuvent pas être créées pour la boîte aux lettres d'un utilisateur et ses archives en ligne. Ce qui est défini pour l'un est défini pour les deux, une limitation pour les organisations qui souhaitent définir des stratégies distinctes.

- La fonctionnalité avancée d'e-discovery dans Office 365 n'est pas «en place». Les outils avancés fournissent des fonctionnalités de découverte électronique au sein de la suite d'applications Office 365 et ne sont pas intégrés directement aux sources de données. Par conséquent, l'effort est un processus en deux étapes,

Microsoft propose toute une gamme de fonctionnalités de découverte électronique pour la recherche de contenu réactif dans Office 365.

nécessitant une recherche et une exportation de données à l'aide des capacités limitées du Centre de sécurité et de conformité, en sélectionnant le centre de découverte électronique avancé comme destination avant de pouvoir exécuter les outils avancés. Par conséquent, il n'existe aucun moyen d'itérer et de rechercher sur les données source sans plusieurs opérations en aveugle manuelles et répétitives.

- Il n'y a plus de limite au nombre de boîtes aux lettres pouvant être recherchées. C'était le cas avec la découverte électronique dans Exchange Online, mais ce problème a été résolu / supprimé dans la découverte électronique dans le nouveau centre de sécurité et de conformité.

- Les suspensions légales peuvent être appliquées aux données des emplacements Office 365 (beaucoup, pas à toutes) ou aux données tierces importées dans Office 365 (puis stockées dans la boîte aux lettres Exchange de l'utilisateur).

- En 2018, les réglementations relatives à la protection de la vie privée ont radicalement changé au-delà des obligations traditionnelles en matière de sécurité des données. Avec cela, on pouvait espérer pouvoir gérer la recherche (demandes d'accès par sujet) et le droit d'être oublié (découverte et suppression). Alors qu'Office 365 dispose de fonctionnalités de base pour prendre en charge ces exigences, il incombe toujours au service informatique de les remplir via des processus et des interfaces d'administration centrés sur l'informatique. Avec le RGPD et la nouvelle loi californienne sur la protection des consommateurs, ces demandes vont probablement augmenter en 2019. Par conséquent, les services informatiques des entreprises doivent anticiper un volume de demandes croissant, qui devraient être réellement déléguées aux détenteurs de succès juridiques ou clients. Des outils tiers sont disponibles pour prendre en charge cette exigence de conformité et l'empêcher de devenir un goulot d'étranglement informatique.

Microsoft propose une gamme de fonctionnalités de découverte électronique pour la recherche de contenu réactif dans Office 365, ainsi qu'un service plus avancé de découverte électronique appelé Découverte Electronique Avancée qui ajoute à l'analyse de texte, à l'apprentissage automatique, à la pertinence et au codage prédictif pour une évaluation précoce des cas. La découverte électronique avancée est disponible dans le plan premium Enterprise E5 et constitue un coût supplémentaire au plan Enterprise E3. Toutefois:

- Il n'y a pas de flux de travail ou de suivi de projet d'un dossier de découverte électronique, tel que le statut du dossier (hormis Actif et Fermé), qui est impliqué et quelles tâches sont effectuées et par qui.

- Un administrateur n'a pas la possibilité, dans le Centre de sécurité et de conformité, d'envoyer des alertes de mise en attente légale, des rappels ou des remontées. Ceux-ci doivent être traités hors bande. Comme ci-dessus, le manque de capacité de flux de travail et de suivi de projet n'est pas idéal.

- Les recherches de mots-clés lancés dans l'outil de recherche de contenu ne peuvent pas être importées dans un cas de découverte électronique. Les deux services sont différents et n'offrent aucune intégration. Le seul moyen pour une recherche de fonctionner dans un dossier de découverte électronique est de le créer dans le dossier.

- Les cas de découverte électronique sont constitués de mises en attente et de recherches. Aucune recherche dans un dossier de découverte électronique dans l'organisation ne peut avoir exactement le même nom. Office 365 n'autorise l'utilisation d'un seul nom qu'une seule fois dans les cas de découverte électronique sur l'ensemble du tenant.

- Tous les cas sont créés et gérés de manière ad hoc, un responsable de la conformité saisissant des termes de recherche ad hoc. Il n'est pas possible de créer un modèle de cas pour la répétabilité et l'audit, avec des requêtes et des emplacements de recherche standard, des actions clés et des exigences à compléter, ainsi qu'un journal d'audit de ce qui a été réalisé et de ce qui n'a pas été fait. Cela préoccupe particulièrement les entreprises qui ne font pas toujours de la découverte électronique ; l'approche ad-hoc signifie que les acquis et les approches antérieurs risquent d'être oubliés et négligés dans une affaire de découverte électronique en cours, exposant éventuellement une organisation à une sanction en cas de production insuffisante d'éléments de preuve.

- Il n'est pas possible de configurer une zone de recherche plus limitée pour les gestionnaires de découverte électronique recherchant des référentiels OneDrive et SharePoint Online, ainsi que des boîtes aux lettres Exchange. Tout gestionnaire de découverte électronique peut effectuer une recherche dans tout dossier OneDrive, site SharePoint Online ou boîte aux lettres Exchange partout dans le monde. Celles-ci devraient pouvoir être restreintes par région géographique ou par pays pour sauvegarder et protéger les données.

- Il n'est pas possible de définir l'étendue de la recherche sur les courriers électroniques pour exclure le bloc de signature. Par conséquent, si un mot clé apparaît dans les signatures de courrier électronique, il générera un taux élevé de faux positifs.

- Les fonctionnalités de découverte électronique du Centre de sécurité et de conformité adoptent une approche unifiée du contenu réactif dans trois conteneurs de stockage dans Office 365 - des boîtes aux lettres d'utilisateurs et de groupes dans Exchange Online, des sites dans les dossiers SharePoint et OneDrive et Exchange. Les charges de travail qui stockent le contenu dans ces conteneurs peuvent être recherchées ; mais d'autres charges de travail qui ne sont pas exclues (telles que Yammer, Microsoft Stream et Microsoft Planner). En outre, un dossier de découverte électronique créé dans le Centre de sécurité et de conformité ne peut pas rechercher de contenu réactif dans des référentiels de contenu autres qu'Office 365, tels que ceux gérés sur site ou dans d'autres services de cloud. Cette approche limitée signifie que toute organisation dont le contenu se situe en dehors d'Office 365, y compris SharePoint 2013 et 2016 sur place, aura besoin de plusieurs outils de découverte électronique, en plus d'avoir à instancier, exécuter et coordonner plusieurs cas de découverte électronique dans chaque outil.

- La recherche dans les dossiers publics Exchange est une proposition tout ou rien. Il est impossible de cibler la recherche sur une liste ciblée.

- Les résultats de la recherche pour Exchange Online, SharePoint Online et OneDrive doivent être exportés à partir d'Office 365 pour faciliter le processus de révision ; le contenu Exchange en un ou plusieurs fichiers PST et le contenu SharePoint et OneDrive en tant que fichiers individuels (avec une option pour toutes les versions). L'approche Office 365 pose de nombreux problèmes : elle crée un ensemble de contenu dupliqué en dehors d'Office 365 qui doit être protégé, il n'y a pas de rapport sur les actions effectuées sur le contenu exporté dans le cas de la découverte électronique dans Office 365, car Office 365 est aveugle aux actions post-exportation, si la recherche est exécutée à nouveau dans Office 365, une exportation ultérieure est requise, ainsi que l'intégration de plusieurs ensembles de données. Il n'existe aucun lien entre ce qui a été collecté et les décisions de codage prises pour ce contenu afin d'informer cas futurs et réduire le volume de contenu potentiellement réactif dans Office 365. La nécessité d'exporter du contenu vers Azure - avec les retards introduits depuis Office 365 vers Azure, puis Azure vers un ordinateur local - crée des retards inutiles dans un processus urgent pour les responsables de la conformité. Avec la mise en service du RGPD à la fin du mois de mai 2018, l'existence potentielle de

Il n'est pas possible de configurer une zone de recherche plus limitée pour les gestionnaires de découverte électronique qui effectuent des recherches dans les référentiels OneDrive et SharePoint Online.

données à caractère personnel dans des emplacements supplémentaires soulèvera d'importants problèmes de gouvernance des données.

- Les exportations à partir d'Office 365 ne sont pas protégées et risquent donc d'être altérées et spoliées. La sortie est une exportation native brute et non dans un format de conservation, tel que le format d'image légal, proposé par de nombreux outils de collecte de découverte électronique. De plus, Microsoft ne fournit aucune option de chiffrement supplémentaire pour chiffrer l'exportation.

OFFICE 365 N'INDEXE PAS TOUS LES TYPES DE FICHIERS DE CLÉS

Lors de la recherche de la découverte électronique et de l'évaluation précoce du cas, tout fichier non inclus **dans les 58** sera marqué comme non traité. Lors de l'application de règles DLP, les types de fichiers non inclus **dans les 58** ne déclencheront pas les règles de capture. L'implication est la nécessité d'un examen manuel de ces types de fichiers non pris en charge par un responsable de la conformité ou de la sécurité, ce qui augmente les coûts et diminue la rapidité des échanges d'informations.

Les recherches par mot-clé peuvent également manquer de contenu pertinent en raison de l'utilisation d'un index "au mieux". Si une organisation utilise régulièrement des types de fichiers non pris en charge, elle doit rechercher des outils tiers permettant d'indexer des types de fichiers supplémentaires.

DONNÉES SENSIBLES

Office 365 présente plusieurs limitations lors de la recherche de données sensibles dans des messages électroniques :

- L'analyse du contenu pour des données sensibles repose sur les types d'informations sensibles fournis par Microsoft ou sur une définition personnalisée créée par le client. Le matching des données est simple à contourner pour exfiltrer les données ; les algorithmes de correspondance recherchent des correspondances exactes et sont faciles à tromper. Par exemple :
    - La correspondance d'un numéro de carte de crédit peut être contournée en changeant l'un des 16 chiffres du mot équivalent. Par exemple, l'écriture des quatre derniers chiffres sous la forme "997quatre" ne correspond pas à l'expression régulière de la carte de crédit (expressions régulières).
    - La correspondance d'un code SWIFT peut également être contournée en modifiant un chiffre en un mot ou une lettre en équivalent de l'alphabet de l'armée de l'air. Par exemple, au lieu d'écrire le code SWIFT de WPACNZ2W (qui sera comparé au type d'informations sensibles), écrivez-le en tant que WPACNovembreZ2W ne déclenchera pas de correspondance et ne sera donc pas intercepté par la règle DLP. Cela se produit même lorsque l'objet et le corps de l'e-mail spécifient qu'un code SWIFT est inclus dans le message.
- Même sans tenter de dissimuler délibérément la présence d'informations sensibles, les stratégies contenant des informations sensibles ne sont pas notées dans les messages si des métadonnées explicatives sont manquantes dans le courrier électronique. Par exemple, un courrier électronique contenant un numéro de sécurité sociale mais pas la phrase explicative "Numéro de sécurité sociale" ne déclenche pas de stratégie DLP à la recherche de numéros de sécurité sociale.

En résumé, la mise en correspondance de données sensibles nécessite une trop grande perfection dans la manière dont les données sensibles sont formées dans un message et n'utilise pas une évaluation équilibrée de la présence de données sensibles.

Office 365 présente plusieurs limitations lors de la recherche de données sensibles dans des messages électroniques.

AUCUN STOCKAGE À LONG TERME DES JOURNAUX D'AUDIT POUR CONFORMITÉ

Le journal d'audit Office 365 ne conserve les événements d'audit que pendant 90 jours - pour les abonnés Office 365 avec Enterprise E3 ou une version antérieure. Il n'y a aucun moyen d'augmenter ce délai. Cela signifie que le journal d'audit ne peut rien faire pour une organisation qui tente de détecter un problème ou un problème survenu au-delà des trois derniers mois. L'exception concerne les entrées du journal d'audit pour Exchange Online, où un administrateur peut modifier la valeur par défaut de 90 jours pour les entrées du journal d'audit Exchange uniquement. Pour les clients dotés d'Office 365 E5 et Microsoft 365, les entrées du journal d'audit peuvent être conservées pendant un an maximum. Cette modification a été introduite dans l'aperçu public en octobre 2018, mais ne s'applique qu'aux enregistrements du journal d'audit générés après l'entrée en vigueur de la durée la plus longue. Les entrées de journal existantes ne sont pas affectées par la durée de conservation plus longue.

La fonctionnalité de journalisation d'audit dans Office 365 est sujette à plusieurs problèmes, notamment:

- Les événements de flux de messagerie dans Exchange Online ne créent pas d'entrées de journal d'audit. C'est-à-dire que lorsqu'une règle de flux de messagerie se déclenche sur un message électronique, aucun enregistrement de ce déclenchement n'est consigné.

- Les entrées du journal d'audit ne peuvent pas être mises en attente légale ou contentieuse, afin de montrer les actions spécifiques entreprises par les utilisateurs au fil du temps et faisant l'objet d'une demande de découverte ou faisant partie d'une évaluation précoce du dossier.

- L'exportation d'éléments de journal d'audit à partir d'Office 365 est limitée à 5 000 entrées sauf si tous les résultats sont exportés, pour lesquels la limite est fixée à 50 000 éléments. Une organisation avec l'audit activé générera au moins 10 à 20 éléments d'audit par personne et par jour pour un utilisateur léger, et éventuellement quelques centaines d'éléments par jour pour un informaticien actif. Certaines organisations de taille moyenne, sans parler de leurs homologues plus importantes, atteindront la limite de 50 000 articles chaque jour. Dans un tel scénario, un administrateur devra spécifier et générer au moins une exportation par jour, en espérant que le délai de capture des entrées du rapport d'audit ne signifie pas que les éléments devant être collectés ne figurent pas dans le rapport.

- Les événements ne sont pas connectés en temps réel ni disponibles pour une analyse en temps réel. Microsoft indique que cela peut prendre de 30 minutes à 24 heures en fonction de l'événement spécifique enregistré. Les clients ont noté que cela peut prendre encore plus longtemps et que des événements d'audit peuvent ne jamais apparaître du tout.

- Les exportations sont livrées sous forme de fichiers CSV à enregistrer localement (en dehors d'Office 365), dont la collection doit être gérée. Paradoxalement, en tant que fichier exporté d'éléments d'audit, rien n'empêche un administrateur errant de supprimer les preuves de ses actes répréhensibles; le fichier exporté ne garantit pas l'authenticité des informations historiques contenues à l'intérieur.

- La raison pour laquelle des actions spécifiques ont été entreprises par un utilisateur administrateur sur un service Office 365 n'est pas capturée et affichée dans le journal d'audit. Il est impossible de reconstituer le raisonnement derrière un changement sur la base des informations générales présentées dans le journal d'audit.

Dans Azure AD, les éditions gratuites et de base ne conservent les éléments d'audit de l'activité et de la sécurité que pendant sept jours maximum.

- Le service Journal d'audit Office 365 ne capture pas les événements des serveurs Microsoft locaux pour les organisations à configuration hybride, telles que Exchange Server et SharePoint Server, en plus d'Office 365. Il ne peut donc pas fournir une vue consolidée des activités pouvant être auditées aux organisations dotées d'une infrastructure hybride.

Dans Azure AD, les éditions gratuites et de base ne conservent les éléments d'audit de l'activité et de la sécurité que pendant sept jours maximum. Par exemple, il est impossible d'obtenir un aperçu des compromis sur les comptes sans l'identifier presque immédiatement. Avec un abonnement à Azure AD Premium P2, vous pouvez l'augmenter à 30 jours maximum pour les éléments d'activité et à 90 jours pour les éléments de sécurité.

Les organisations qui ont besoin d'un accès à long terme aux éléments de rapport d'audit (tels que des données d'une durée de sept ans en vertu de certaines réglementations en matière de conformité) doivent être conscientes des limitations du service Journal d'audit Office 365.

DÉCOUVERTE ELECTRONIQUE SUR LES DONNÉES DES EX-EMPLOYÉS

L'exécution de la découverte électronique complète implique notamment l'inclusion de données appartenant à d'anciens employés. À ce jour, la fonctionnalité de boîte aux lettres inactive de Microsoft a permis de conserver gratuitement les boîtes aux lettres de'un ex-employé, mais en octobre 2017, l'intention de facturer 3,00 USD par boîte aux lettres par mois, ou 36,00 USD par boîte aux lettres et par an, a été signalée. Toutefois, après avoir reçu une réponse de la part des clients et des MVP, Microsoft a annulé l'introduction de ce coût jusqu'à nouvel ordre.

Nous prévoyons que la croissance exponentielle des données sur les anciens employés rendra inévitable que les boîtes aux lettres inactives attirent de nouvelles conditions de licence en 2019 ou 2020. Cela poussera probablement les entreprises à rechercher des stratégies moins coûteuses pour l'hébergement de données relatives aux anciens employés.

Les autres enjeux à prendre en compte comprennent :

GESTION D'ENVIRONNEMENTS HYBRIDES

L'utilisation d'environnements hybrides dans Office 365 - que ce soit sur site Exchange, d'autres systèmes sur place ou d'autres solutions de cloud - introduit un nouvel ensemble de défis. Par exemple, les déploiements hybrides Office 365 introduisent un certain nombre d'interfaces déconnectées sur site et dans le cloud, qui rendent la gestion et l'automatisation quotidiennes plus difficiles. De plus, la synchronisation des identités des règles sur site aux règles basées sur le cloud rend difficile toute modification sans scripts complexes et comptes hautement privilégiés. Par conséquent, les tâches que le service d'assistance pourrait effectuer avant de ne plus pouvoir effectuer dans des environnements hybrides, ont pour conséquence que la charge administrative hybride accrue annule une grande partie des avantages perçus fournis par Office 365.

Les organisations qui exploitent des environnements hybrides doivent utiliser des solutions tierces pour faire face aux défis posés par les environnements hybrides. Cela est particulièrement vrai pour les grandes entreprises qui auront une plus grande proportion d'utilisateurs et d'applications sur site, même après la migration vers Office 365.

L'AUTHENTIFICATION AVEC AZURE AD FOURNIT UN SEUL POINT D'ECHEC

Les organisations qui exploitent des environnements hybrides doivent utiliser des solutions tierces pour faire face aux défis posés par les environnements hybrides.

En tant que service non régional, les perturbations dans une région d'Azure AD peuvent avoir des effets en cascade sur d'autres centres de données et régions. Bien que l'intention soit qu'Azure AD soit globalement résilient, l'architecture de Microsoft pour Azure n'a pas encore fourni de service d'authentification basé sur le cloud de sécurité. Par exemple, une attaque de foudre au Texas le 4 septembre 2018 a perturbé les systèmes de refroidissement du centre de données du centre-sud des États-Unis à San Antonio. Cela a eu un impact majeur sur les services Office 365 et Azure, des clients hors de la région centre-sud des États-Unis rencontrant des problèmes d'authentification Azure AD.

L'introduction par Microsoft de nouvelles fonctionnalités pour MFA rompt souvent les droits d'authentification actuels, notamment en empêchant les utilisateurs affectés d'utiliser divers services Office 365. Les clients trouvent cela agaçant et perturbant.

L'implémentation Microsoft de MFA dans Azure et Office 365 constitue un point de défaillance unique. Si MFA est hors service, les utilisateurs concernés ne peuvent pas se connecter, comme cela s'est passé deux fois en novembre 2018. Certains clients utilisant des services MFA tiers avec Office 365 ont affirmé ne pas être affectés par les pannes, tels que ceux utilisant Duo et Okta.

EXAMEN DE SURVEILLANCE (CONFORMITÉ FINRA)

Certaines règlementations, tels que ceux appliqués par l'Autorité de réglementation du secteur financier (FINRA), exigent la capture et l'examen des communications entre des personnes particulières, ou des personnes d'un groupe spécifique, afin de garantir qu'aucun sujet néfaste ou non autorisé ne soit divulgué ou discuté. Office 365 offrait auparavant une fonctionnalité de supervision pouvant fonctionner avec les messages Exchange Online, qui posaient de nombreux problèmes.

En mai 2017, Microsoft a remplacé l'ancienne fonctionnalité de supervision par un nouvel outil de supervision nécessitant le plan Enterprise E5 ou le module complémentaire de conformité avancée. Les administrateurs disposant des autorisations d'accès appropriées peuvent configurer une ou plusieurs stratégies de supervision.

- Toute personne devant être couverte par une stratégie de supervision nécessite une licence Enterprise E5 ou le module complémentaire de conformité avancée. Il s'agit d'une exigence de licence par utilisateur et non d'une option au niveau de l'organisation.

- Supervision fonctionne uniquement avec Exchange Online dans Office 365, mais ne concerne pas les autres outils de communication de Microsoft, tels que Microsoft Teams, Yammer et Skype for Business. Cette étendue de la couverture est trop étroite à notre avis.

- Une fois qu'une stratégie de supervision a été configurée, une boîte aux lettres partagée privée est configurée pour recevoir les messages capturés. Les réviseurs doivent se connecter à la boîte aux lettres partagée pour examiner et évaluer chaque message.

- Il n'y a pas de flux de travail intégré pour alerter les relecteurs d'une nouvelle stratégie de supervision qui leur donne la possibilité de relire les messages. Les réviseurs qui conseillent doivent être traités par la personne qui a mis en place la politique de supervision.

- Une personne peut être définie à la fois comme personne à mettre sous surveillance prudentielle et comme réviseur d'une politique donnée. Il n'y a pas de vérification pour imposer la séparation des rôles.

- Il n'est pas possible d'utiliser les types d'informations sensibles de Microsoft dans les stratégies de supervision.

Il n'y a pas de flux de travail intégré pour alerter les relecteurs d'une nouvelle stratégie de supervision qui leur donne la possibilité de relire les messages.

- Lorsque vous ajoutez des conditions à la stratégie de supervision, les mots ou les phrases doivent correspondre exactement. Une variante mal orthographiée ne déclenchera pas la règle de supervision. Il serait utile qu'Office 365 offre la possibilité d'utiliser la correspondance floue pour donner une impression plus large de ce qui se passe dans Exchange Online.

- L'utilisation d'Outlook en tant qu'interface de supervision signifie que les fonctionnalités Outlook standard, telles que la création d'un nouveau courrier électronique, la réponse à un message et la suppression d'un message, sont visibles dans l'interface. Notez que l'option de suppression pour un message individuel est grisée dans la barre d'outils. En cliquant sur le bouton Supprimer d'un message, une invite vous indique que vous ne pouvez pas supprimer le message. En cliquant sur l'option Tout supprimer dans la barre d'outils, tous les messages de la boîte aux lettres sont supprimés, mais un processus en arrière-plan remet ensuite tous les messages dans la boîte aux lettres. Ces éléments d'interface sont déroutants et inutiles.

- Les options de filtre fournies dans Outlook n'ont pas de sens pour la supervision. Il n'est pas possible de trier et filtrer les messages en fonction du contenu ou des métadonnées pertinentes pour la politique de supervision.

- Tenter de supprimer tous les messages d'une boîte aux lettres de supervision ne fait pas l'objet d'un enregistrement d'audit pour les messages.

- Un superviseur peut répondre ou transférer un message depuis la boîte aux lettres de supervision. Cependant, il n'est pas possible d'auditer ou de vérifier quels messages ont été envoyés depuis la boîte aux lettres de supervision.

- Microsoft n'offre aucune fonctionnalité de gestion des travaux ou des dossiers pour les messages dans la boîte aux lettres de supervision. Un processus hors ligne doit être utilisé.

- Un auditeur ayant accès à plusieurs boîtes aux lettres de supervision doit consulter chaque boîte aux lettres de supervision, un à la fois. Il est impossible d'obtenir une vue unifiée pour plusieurs stratégies de supervision.

- Hormis le nom de la boîte aux lettres de supervision, rien n’indique quels sont les paramètres de la stratégie de supervision ni pourquoi les messages sont collectés dans la boîte aux lettres.

- La surveillance prudentielle ne fonctionne que dans Outlook sur le Web. Bien qu'un complément du client Outlook ait été promis (et qu'un autre soit disponible et qu'il puisse être installé, bien qu'avec des commandes PowerShell), il n’est pas fonctionnel pour le moment.

- Il n'y a pas de support de migration entre l'ancienne fonctionnalité Revue de supervision et la nouvelle fonctionnalité de Supervision. Les politiques de l'approche précédente doivent être supprimées ; ils ne peuvent pas être migrés et mis à jour et ils ne sont pas automatiquement mis à jour par Microsoft.

- Bien que les messages soient capturés pour une remise après livraison ou une vérification a posteriori, il n'est pas possible de mettre en quarantaine un message incriminé et de le faire acheminer pour approbation avant sa diffusion. Le dommage pourrait déjà être fait, puisque le message a été envoyé et livré.

- Le journal d'audit d'Office 365 est aveugle aux stratégies de supervision. La création, la modification et la suppression de stratégies de supervision ne font pas l'objet d'un journal d'audit.

Microsoft n'a apporté aucune modification à Supervision depuis mai 2017. Les clients ayant réellement besoin d'une capacité de supervision robuste doivent prendre en compte les offres de tiers.

Les autres enjeux à prendre en compte comprennent :

- Les journaux d'authentification Azure AD ne sont conservés que pendant sept jours pour de nombreux clients Office 365. Cela signifie qu'il peut être impossible de localiser les enregistrements d'une tentative d'hameçonnage ayant abouti à une compromission des informations d'identification du compte, car Azure AD a effacé les enregistrements historiques.

- Office 365 ne prend pas en charge l'utilisation de phrases secrètes, qui sont généralement des phrases plus longues contenant plusieurs mots en langage naturel, plus faciles à retenir qu'un mot de passe avec un modèle difficile. Par exemple, une phrase secrète pourrait être "Je suis Clarke Kent et je suis Superman". Il s'agit d'un "mot de passe" de 34 caractères à la fois facile à mémoriser pour l'utilisateur final mais, en raison de sa longueur, plus difficile à deviner ou à craquer pour un attaquant. Office 365 ne prend pas en charge les phrases secrètes car les comptes Azure AD ne prennent pas en charge l'utilisation des espaces et sont limités à un maximum de 16 caractères.

- Les nouveaux rapports sur l'accès et l'authentification ne peuvent pas être créés par les administrateurs.

Récapitulatif

Office 365 est une plate-forme robuste et performante - Osterman Research recommande aux entreprises d'envisager sérieusement de l'utiliser. Cependant, une plate-forme de la portée et de la taille d'Office 365 ne parviendra jamais à satisfaire toutes les organisations dans tous les cas de figure, mais les avantages de la migration vers cette plate-forme doivent l'emporter sur les limitations qu'elle inclut. Par conséquent, les solutions tierces doivent être sérieusement envisagées pour le déploiement, soit en remplacement des fonctionnalités natives disponibles chez Microsoft, soit en tant que suppléments fournissant des fonctionnalités améliorées pour répondre aux exigences organisationnelles spécifiques.

Promoteur de ce Livre Blanc

Les fichiers sont maintenant partagés de manière automatique sur des dizaines d'applications, puis stockés dans plusieurs emplacements ou sur de nombreux périphériques à travers le monde, ce qui rend difficile la garantie de la sécurité et de la conformité du contenu de votre entreprise. NetGovern fournit une solution de gouvernance de l'information à la fois prescriptive et proactive. Il réduit les risques, tout en vous permettant d'extraire les informations importantes à partir de données non structurées.

NetGovern permet aux organisations réglementées de rechercher instantanément des informations, quel que soit leur emplacement ou leur mode de partage. Nous nous connectons à plusieurs systèmes sur le cloud et sur site, y compris la messagerie, la messagerie instantanée, les serveurs de fichiers et les plateformes de collaboration. Les résultats de recherche consolidés sont améliorés via notre audit intelligent, notre recherche électronique avancée et nos capacités de correction automatisées. Des centaines de clients du monde entier font confiance à nos partenaires certifiés pour les aider à préserver, protéger et enrichir la valeur de leur actif le plus précieux - Information.

netgovern™

www.netgovern.com

@net_govern

+1 866 497 0101

+1 514 392 9220

RÉFÉRENCES

[i] https://www.microsoft.com/en-us/microsoft-365/blog/2018/09/24/office-2019-is-now-available-for-windows-and-mac/

[ii] https://www.microsoft.com/microsoft-365/partners/workplaceanalytics

[iii] https://technet.microsoft.com/en-GB/library/exchange-online-limits.aspx