Microsoft

Protection et optimisation de votre organisation connectée

avec Microsoft Enterprise Mobility + Security

Sommaire

1

Synthèse

2

Prochaine étape : le contrôle dans le cloud

3

Relever les défis relatifs à un monde mobile orienté cloud

Gestion des identités

Sécurité liée aux identités dans le cloud

la sécurité liée aux identités sur site

Gestion des appareils

Protection des informations

Défis administratifs

4

Comment les clients utilisent-ils EMS

La sécurité liée aux identités.

La productivité mobile gérée ;

La protection des informations de bout en bout ;

Déploiement et gestion simplifiés

Résumé

Synthèse

Une évolution de taille peut être observée en matière d'IT à mesure que les sociétés adoptent une stratégie en faveur de la mobilité et du cloud. Cela a des conséquences considérables sur la manière dont l'IT considère la sécurité.

Ce qui se limitait autrefois à un monde physique sur site s'étend maintenant au cloud et à une myriade d'appareils mobiles. Les interactions des collaborateurs avec d'autres utilisateurs, appareils, applications et données sont devenues de plus en plus complexes, ce qui crée de nouveaux points faibles pour l'IT. La sophistication des vecteurs d'attaques continue de se développer. En outre, de nombreuses sociétés tentent de maintenir des solutions traditionnelles isolées. Les budgets non extensibles ne facilitent pas les choses.

Comment des solutions sur site existantes, utilisées pour la gestion des identités et des appareils, ainsi que pour la protection des informations, peuvent-elles répondre efficacement aux exigences de ce monde moderne ? La réponse est simple : elles en sont incapables. Il faut que le contrôle de tous ces services passe, au fil du temps, de votre propre datacenter au cloud. Procéder comme tel vous donne le contrôle que votre entreprise nécessite, sans sacrifier l'aspect familier de l'expérience mobile et de bureau souhaité par vos collaborateurs.

Il s'agit du principe élémentaire associé à Microsoft Enterprise Mobility + Security (EMS) : la seule solution de mobilité complète désignée pour favoriser la gestion et la protection des utilisateurs, appareils, applications et données dans un monde mobile orienté cloud.

Avec EMS, nous commençons par une identité commune protégée pour sécuriser l'accès à toutes les ressources d'entreprise. Nous protégeons ensuite ces données grâce à des technologies de sécurité innovantes, notamment l'apprentissage automatique, pour protéger les données contre les menaces nouvelles et changeantes en matière de cybersécurité. Par ailleurs, comme EMS est une solution basée dans le cloud, la configuration est simple et rapide. En outre, une certaine évolutivité et des mises à jour garantissent que votre investissement est prêt pour l'avenir.

EMS fonctionne également très bien avec vos investissements actuels sur site. Azure Active Directory Premium se connecte à votre Active Directory existant, tandis que Microsoft Intune se connecte au Gestionnaire de configuration System Center de manière à fonctionner avec tous les appareils de vos clients. Utilisées conjointement, ces technologies intégrées sur le Cloud et sur site permettent de protéger et de gérer vos identités et vos données sur tous vos appareils, où qu'ils se trouvent.

Le monde de l'informatique est (à nouveau) en plein changement, et chaque responsable du service informatique doit suivre le mouvement. Microsoft EMS va vous aider à vivre cette transition.

Prochaine étape : le contrôle dans le cloud

L'un des plus grands défis pour les responsables du service informatique est de reconnaître les changements technologiques majeurs, puis d'adapter leur organisation pour en tirer profit. De nos jours, nombre de ces changements sont à l'initiative des employés, des partenaires et des clients qui souhaitent utiliser les appareils qu'ils affectionnent en les associant à la puissance du Cloud.

Ce phénomène prend toute sa dimension dans la manière dont nous gérons et protégeons les identités, les appareils et les données. Avant l'apparition du Cloud, les technologies utilisées étaient exécutées uniquement dans un environnement sur site (figure 1). Existait-il une autre solution ? Avant l'avènement du Cloud, il n'y en avait aucune.

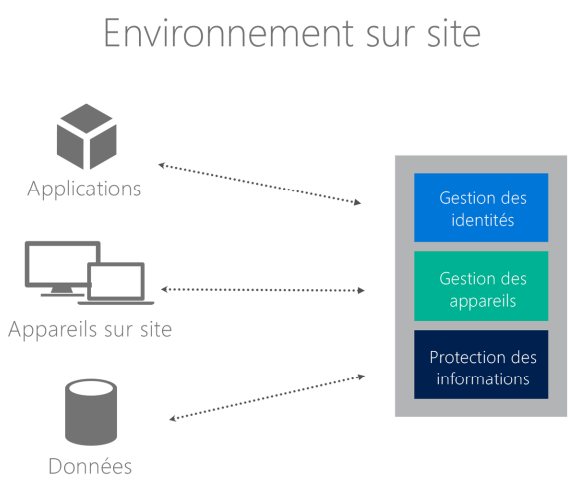

Figure 1 : la gestion des identités et des appareils, ainsi que la protection des données étaient entièrement réalisées dans un environnement sur site.

Les choses étaient beaucoup plus simples. Les préoccupations se limitaient à ce qui se trouvait dans le périmètre du réseau, qui était globalement sous votre contrôle.

C'est de l'histoire ancienne. Aujourd'hui, chaque responsable du service informatique est confronté à beaucoup plus de complexité. Les traditionnels clients et serveurs côtoient désormais des appareils mobiles, des plateformes cloud, des applications SaaS, etc. (figure 2).

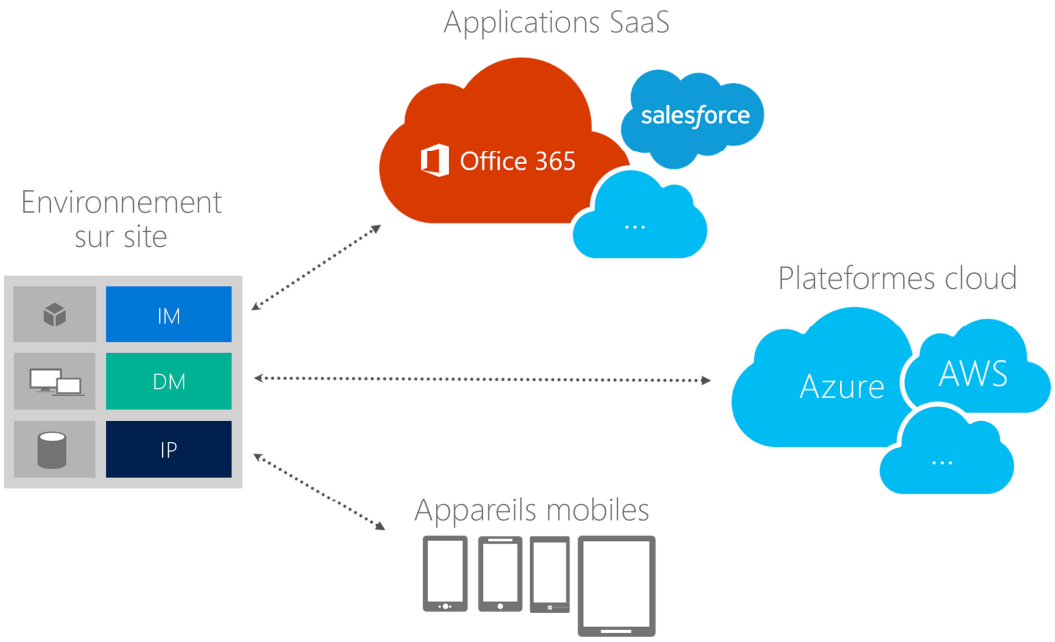

Figure 2 : l'IT en entreprise comprend aujourd'hui des applications SaaS, des plateformes cloud, des appareils mobiles, etc.

En matière d'identité, les exigences sont désormais beaucoup plus élevées. Les appareils à gérer sont divers et souvent hors du périmètre du réseau. Les informations que vous devez protéger ne se trouvent plus uniquement dans l'enceinte d'un pare-feu, mais également accessibles sur ces appareils et dans le cloud.

Dans le même temps, les attaques de cybersécurité qui menacent votre infrastructure dans son ensemble gagnent en sophistication mais évoluent aussi au quotidien et nécessitent des outils et des stratégies de sécurité de plus en plus évoluées.

L'approche traditionnelle, qui s'appuyait uniquement sur des technologies sur site, n'est plus adaptée. L'organisation doit passer à une solution plus flexible basée dans le cloud (figure 3).

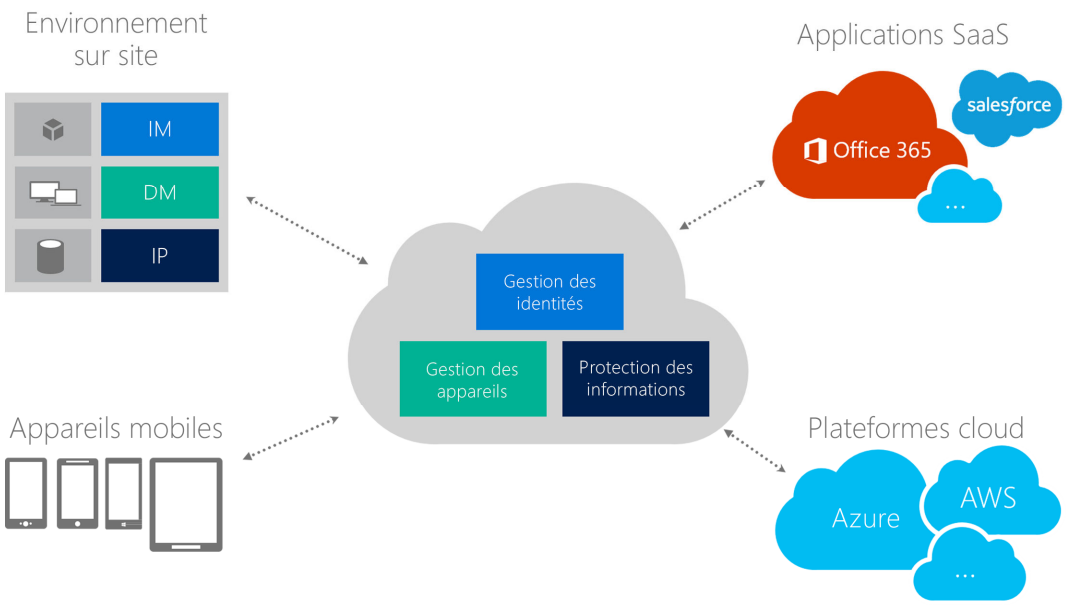

Figure 3 : les technologies principales de gestion des identités (IM), de gestion des appareils (DM) et de protection des informations (IP) doivent désormais être exécutées dans le cloud.

Les technologies existantes sur site de gestion des identités, des appareils et des informations conservent leur importance et ne sont pas appelées à disparaître. Mais sans solution cloud, il est simplement impossible de relever les problèmes du monde moderne. C'est pour cette raison que vous devez vous attendre à passer d'une approche sur site, peut-être d'actualité dans votre organisation, à un nouveau monde de possibilités dans le cloud.

De manière à vous aider face à ce changement, Microsoft a créé Enterprise Mobility + Security (EMS). Chaque composant d'EMS fournit des solutions cloud pour la gestion des identités et des appareils, ainsi que pour la protection des informations. Utilisées ensemble, ces technologies sont encore plus efficaces, ce qui vous apporte des bénéfices, tels que la sécurité basée sur les identités, une approche exhaustive qui répond aux défis complexes du nouveau paysage d'attaques actuel. Par ailleurs, comme ces technologies sont étroitement intégrées à des outils de productivité (comme Office et Office 365) que vos collaborateurs utilisent chaque jour, vous profitez d'un meilleur contrôle et d'une sécurité supérieure, sans devoir imposer des processus complexes ni modifier les comportements de travail.

Il n'appartient qu'à vous de décider de la vitesse à laquelle vos solutions d'identité et de gestion seront déplacées dans le cloud. Ce qui compte désormais est de réaliser pourquoi ce changement se produit, puis de comprendre ce dont vous avez besoin pour en tirer profit. Microsoft EMS prend en charge cette transition, et c'est ce que décrit ce qui suit.

Relever les défis relatifs à un monde mobile orienté cloud

La gestion des identités et des appareils, la protection des informations et la prise en charge d'une nouvelle attaque ne sont pas chose aisée. Fonctionner dans notre monde orienté cloud et mobile, avec des budgets et ressources limités ainsi que de nombreux défis est de plus en plus complexe. Pour mieux comprendre ces problèmes et les prendre à bras le corps ainsi que pour découvrir pourquoi l'association de solutions dans le cloud et sur site est essentiel, il est nécessaire de considérer chaque cas de manière individuelle. Il est également important d'étudier la manière dont les composants d'EMS abordent chacun de ces domaines.

Gestion des identités

Chaque utilisateur souhaite bénéficier de l'authentification unique (SSO) pour différentes applications. Personne n'apprécie de devoir se souvenir de plusieurs noms et mots de passe de connexion. C'est pourquoi les organisations utilisent depuis longtemps des technologies sur site de gestion des identités, telles que Microsoft Active Directory.

Cependant, avec l'augmentation de la popularité des applications SaaS, il ne suffit plus de s'appuyer uniquement sur la gestion sur site des identités. La raison est simple : de manière à proposer l'authentification unique (SSO), une technologie sur site telle qu'Active Directory doit se connecter à chacune des applications auxquelles l'utilisateur veut accéder. Si toutes ces applications se trouvent sur vos serveurs physiques, il n'existe aucune difficulté : chaque application se connecte à son instance locale d'Active Directory. Les problèmes surviennent à mesure que le nombre d'applications Cloud augmente. Si chaque application SaaS se connecte directement à chaque technologie sur site de gestion des identités de l'entreprise, c'est l'anarchie (figure 4). C'est exactement la situation dans laquelle de nombreuses organisations se trouvent aujourd'hui.

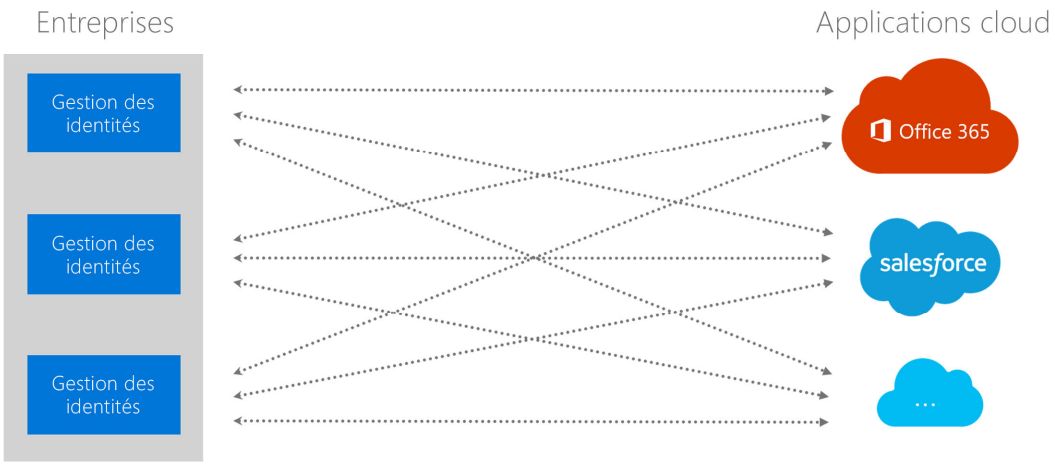

Figure 4 : la création d'une connexion directe entre chaque solution de gestion des identités et chaque application SaaS de l'entreprise deviendrait rapidement trop compliquée à gérer.

Il est plus simple de gérer les identités à l'aide d'une solution cloud : Azure Active Directory (AD) Premium. Votre service d'annuaire sur site conserve son importance, mais se connecte désormais uniquement à Azure AD. Azure AD peut ensuite se connecter directement à chaque application SaaS (figure 5).

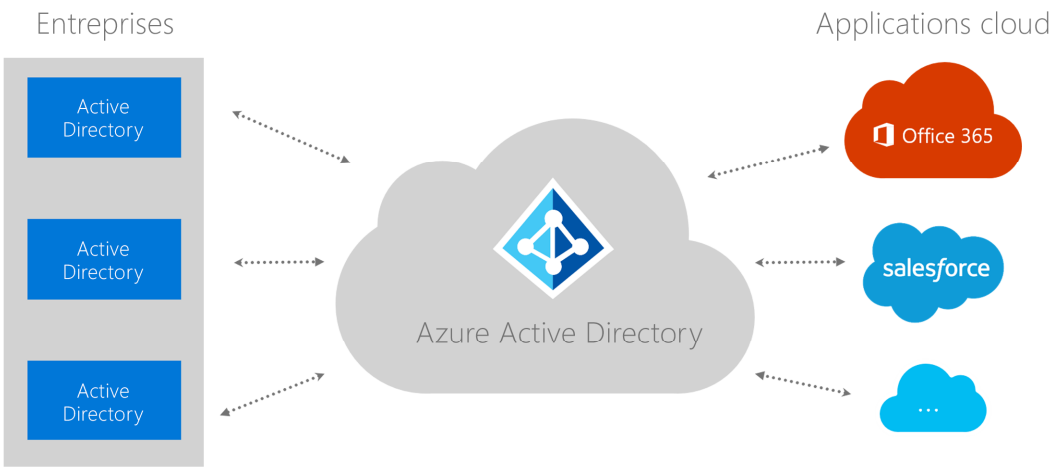

Figure 5 : il est beaucoup plus simple de gérer des identités dans le cloud à l'aide d'Azure Active Directory que de gérer chaque connexion à des applications SaaS.

Résultat : l'authentification unique (SSO) sans l'anarchie. Il demeure possible d'utiliser des identités d'utilisateurs provenant de votre propre service d'annuaire (vous gardez le contrôle), mais l'exploitation de la puissance du cloud vous permet de leur fournir un accès aisé aux applications locales comme aux SaaS, à l'aide d'une seule connexion. Tout le monde en tire profit : vos utilisateurs comme vos administrateurs informatiques.

Azure AD fournit actuellement l'authentification unique (SSO) à plus de 2 000 applications dans le cloud, dont Office 365, Salesforce.com, Box et ServiceNow. Ce service offre plus qu'une authentification unique :

Plus de 80 % des collaborateurs reconnaissent utiliser des applications SaaS non autorisées dans le cadre de leur travail.

– Stratecast, décembre 2013

- **Un accès conditionnel basé sur les risques :** qui peut limiter le risque d'accès non autorisé. L'accès conditionnel propose une évaluation intelligente de l'octroi ou du blocage d'accès ainsi que de l'application d'authentification multifacteur basée sur des facteurs tels que l'adhésion au groupe, la sensibilité de l'application, l'état de l'appareil, l'emplacement et le risque lié à la connexion.
- **Authentification multifacteur intégrée :** pour une couche de sécurité supplémentaire permettant une authentification plus sécurisée. Grâce à l'authentification multifacteur, vous pouvez exiger de vos utilisateurs qu'ils fournissent à la fois un mot de passe et un autre élément d'identification, comme un code envoyé sur leur téléphone mobile, pour se connecter.
- **Gestion privilégiée des identités :** permet un contrôle supplémentaire sur les identités qui exigent un accès privilégié, ainsi que la possibilité de détecter ces accès, de les restreindre et de les contrôler, puis d'octroyer un accès administratif ponctuel aux utilisateurs éligibles.
- **Sécurisation de l'accès distant :** permet de sécuriser l'accès à des applications sur site publiées avec Azure AD sans qu'un réseau privé virtuel soit nécessaire. Azure Active Directory Premium comprend l'authentification multifacteur ; un contrôle d'accès basé sur l'état de l'appareil, l'emplacement de l'utilisateur et l'identité ; ainsi que des rapports de sécurité exhaustifs, des audits et des alertes
- **Collaboration entre les entreprises :** permet de faciliter l'octroi à des fournisseurs, sous-traitants et partenaires d'un accès sans risque à des ressources internes grâce à la collaboration B2B que propose Azure AD.

Sécurité liée aux identités dans le cloud

Non seulement les solutions de sécurité héritées ne permettent pas de garantir un accès efficace à vos applications cloud, mais elles ne sont pas non plus conçues pour protéger les données de ces applications.

Plusieurs facteurs peuvent l'expliquer. Les solutions de sécurité réseau traditionnelle, telles que les pare-feu et le système de prévention des intrusions, ne permettent pas de visualiser les transactions uniques à chaque application ni la manière dont les données sont utilisées et stockées. Par ailleurs, les contrôles classiques ne surveillent qu'un sous-ensemble réduit du trafic dans le cloud et n'ont qu'une perception limitée des activités au niveau de l'application.

Aussi comment pouvez-vous préserver la visibilité, le contrôle et la protection de vos applications dans le cloud ? Grâce à EMS, vous disposez de Microsoft Cloud App Security (CAS), un service complet qui garantit une meilleure visibilité, des contrôles plus complets ainsi qu'une protection améliorée de vos applications dans le cloud. CAS est conçu pour vous aider à développer votre visibilité, vos capacités d'audit ainsi que le contrôle sur site de vos applications dans le cloud (Figure 6).

> Plus de 80 % des collaborateurs admettent qu'ils utilisent des applications SaaS non approuvées à des fins professionnelles.
>
> *– Stratecast, décembre 2013*

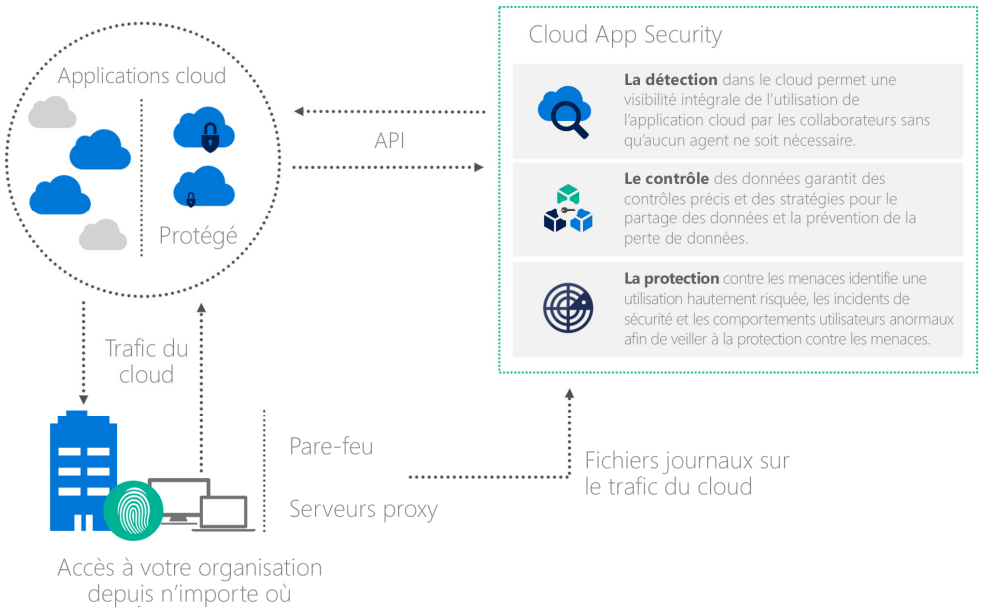

Figure 6 : Cloud App Security garantit une visibilité complète de l'utilisation d'applications dans le cloud par les collaborateurs et un contrôle exhaustif du « shadow IT », ce qui assure une détection des risques en continu et des contrôles précis.

CAS peut identifier plus de 13 000 applications dans le cloud. Aucun agent n'est requis. Au lieu de cela, des informations sont collectées depuis vos pare-feu et serveurs proxy, ce qui permet une visibilité complexe et fournit un contexte exhaustif pour l'utilisation du cloud et le « shadow IT ». Une visibilité accrue des applications, appareils et activités liées aux données permet de déceler des activités suspectes, des erreurs de la part des utilisateurs, ainsi que des menaces potentielles avant que celles-ci ne se concrétisent. Par ailleurs, grâce à l'analyse comportementale, à l'apprentissage automatique et aux renseignements de Microsoft sur la sécurité, vous pouvez sécuriser vos fichiers et données d'entreprise, tout en permettant à vos collaborateurs d'être productifs lors de leurs déplacements.

la sécurité liée aux identités sur site

Bien qu'EMS propose des mises à jour de sécurité efficaces, cela ne vous épargne pas la sécurisation de votre environnement sur site. Microsoft en est consciente ; c'est pourquoi EMS intègre également Advanced Threat Analytics (ATA).

ATA ne s'exécute pas dans le cloud, mais bel et bien dans votre organisation. Son objectif est de vous aider à identifier les activités suspectes avant qu'elles n'aient des conséquences néfastes. Pour atteindre cet objectif, une carte des applications auxquelles vos utilisateurs ont fréquemment accès est générée. Cela implique également un suivi des appareils couramment utilisés, des heures d'accès et plus encore. Si un utilisateur accède de manière inattendue à des applications atypiques à partir d'appareils différents et à des horaires inhabituels, il y a de fortes chances que cet utilisateur ait été piraté. Un utilisateur a deviné son identité, probablement suite au vol de ses nom d'utilisateur et mot de passe.

ATA détecte ce type de menace. Lorsque des anomalies se présentent, ATA avertira votre personnel de sécurité afin qu'une action puisse être prise immédiatement. Plutôt que d'attendre qu'un utilisateur malveillant endommage votre organisation, utilisez ATA pour détecter et stopper ses attaques. Si ATA s'exécute sur site, elle peut faire l'objet d'une licence en tant qu'élément d'EMS (Figure 7).

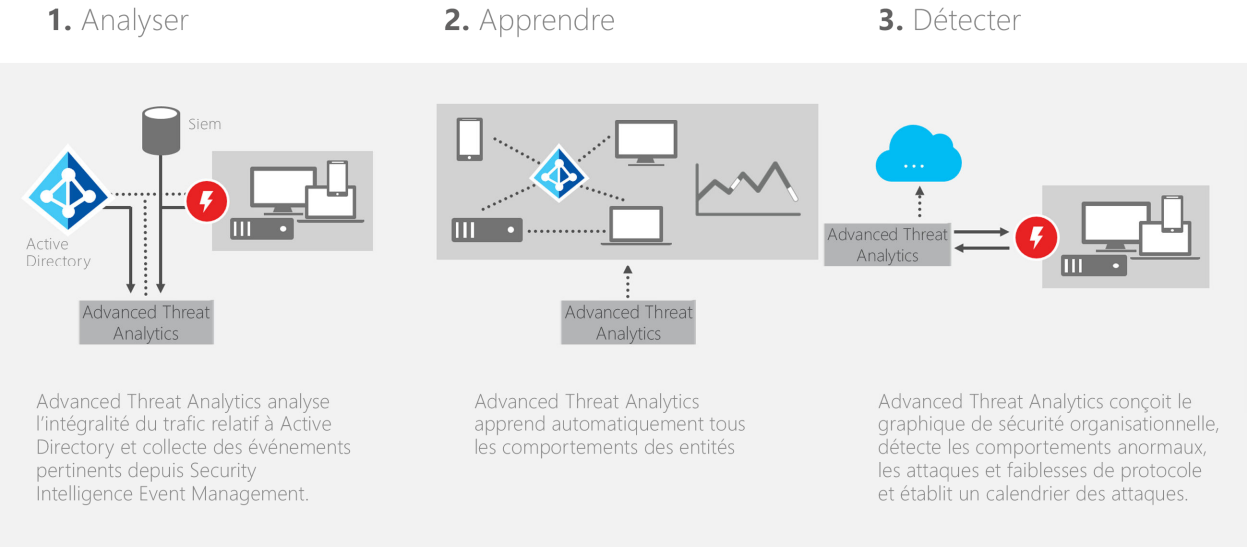

Figure 7 : Microsoft Advanced Threat Analytics (ATA) permet de protéger votre entreprise contre les attaques ciblées avancées en analysant, considérant et identifiant automatiquement tout comportement normal et anormal d'une entité (utilisateur, appareils et ressources)

Advanced Threat Analytics offre également d'autres avantages. En voici quelques-uns :

- **Adaptation à la nature variable de menaces de cybersécurité.** ATA apprend en permanence des entités organisationnelles (utilisateurs, appareils et ressources) et s'adapte afin de refléter les modifications dans votre entreprise en constante évolution. Étant donné que les tactiques des utilisateurs malveillants deviennent de plus en plus sophistiquées, ATA vous aide à vous adapter à la nature évolutive des menaces de cybersécurité à l'aide d'une analyse comportementale continuellement mise à jour.

- **Concentrez-vous sur ce qui est important à l'aide d'une chronologie simple des attaques.** Les outils de sécurité traditionnels génèrent constamment des rapports. Leur analyse pour localiser les alertes importantes et pertinentes peut se révéler épuisante. La chronologie des attaques est un flux clair, efficace et pratique qui met en évidence les éléments pertinents dans un historique, ce qui vous permet d'identifier clairement le qui, le quoi, le quand et le comment. ATA fournit également des recommandations pour l'investigation et la correction de chaque activité suspecte.
- **Réduisez la lassitude liée aux « faux positifs ».** Les outils de sécurité IT traditionnels sont rarement équipés de manière à pouvoir gérer la quantité croissante de données et distribuent ainsi des indicateurs rouges non justifiés, ce qui vous détourne des menaces réelles. Avec ATA, ces alertes ne surviennent qu'une fois les activités suspectes regroupées de manière contextuelle pour vérifier leur comportement, ainsi que celui des autres entités dans le chemin d'interaction. En outre, le moteur de détection vous guide automatiquement tout au long du processus, en vous posant des questions simples afin d'adapter le processus de détection en fonction de vos réponses.

Gestion des appareils

La mobilité est devenue la norme. Pour cette raison, la gestion des appareils mobiles, tels que des téléphones et des tablettes, est désormais essentielle pour la plupart des organisations. La gestion des appareils eux-mêmes, généralement appelée gestion des appareils mobiles (MDM), est importante. Il en est de même pour celle des applications présentes sur ces appareils. Il s'agit de la gestion des applications mobiles (MAM).

Les appareils mobiles n'ont pas attendu le cloud pour être convoités. Par conséquent, les solutions traditionnelles MDM et MAM sont exécutées sur site. Cela s'avérait pertinent tant que les appareils à distance servaient à accéder à des applications également exécutées sur site. De nos jours, ces applications à distance ont toutefois autant de chance d'être exécutées dans le cloud. Si votre solution de gestion des appareils est toujours exécutée sur site, vous devez fréquemment router les communications entre appareils et applications via des serveurs sur site (figure 8).

> 70 % des 10 appareils les plus couramment utilisés présentent de sévères vulnérabilités (HP 2014)
>
> ***– HP***

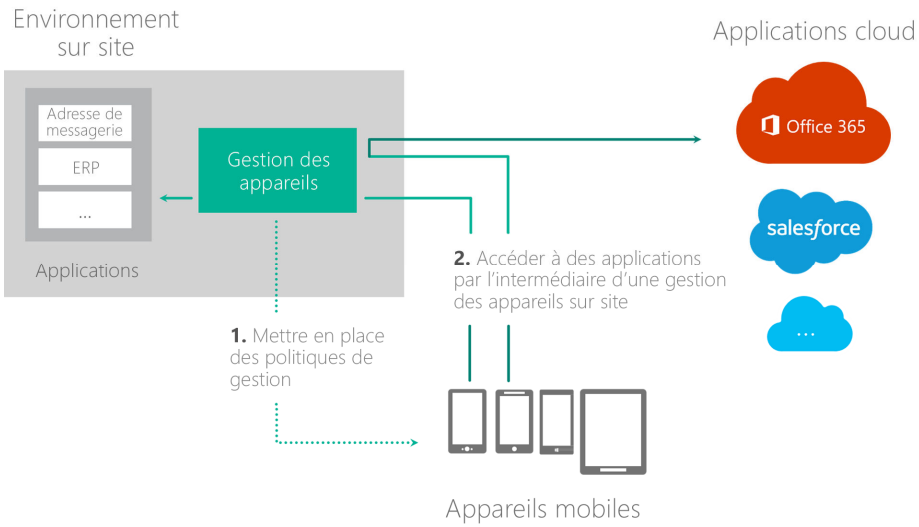

Figure 8 : les solutions traditionnelles de gestion MDM et MAM exigent souvent que la communication entre les appareils mobiles et les applications dans le cloud passe par un goulot d'étranglement sur site.

Comme le montre la figure, une solution de gestion d'appareils déploie généralement les stratégies de gestion vers les appareils gérés (étape 1). Une fois les stratégies appliquées, les applications présentes sur les appareils gérés peuvent accéder aux applications sur site et SaaS. L'ensemble des communications, même celles vers les applications SaaS, est généralement routé via la solution de gestion d'appareils sur site.

Cette approche soulève quelques problématiques évidentes, comme celles liées à la performance et au redimensionnement. Pourquoi limiter la vitesse d'interaction entre appareils et applications sur le Cloud à ce qu'une solution de gestion d'appareils sur site peut offrir ? Pourquoi exiger de votre organisation informatique qu'elle se redimensionne pour y parvenir ? Il est beaucoup plus logique de déplacer la gestion des appareils (MDM comme MAM) dans le cloud (figure 9).

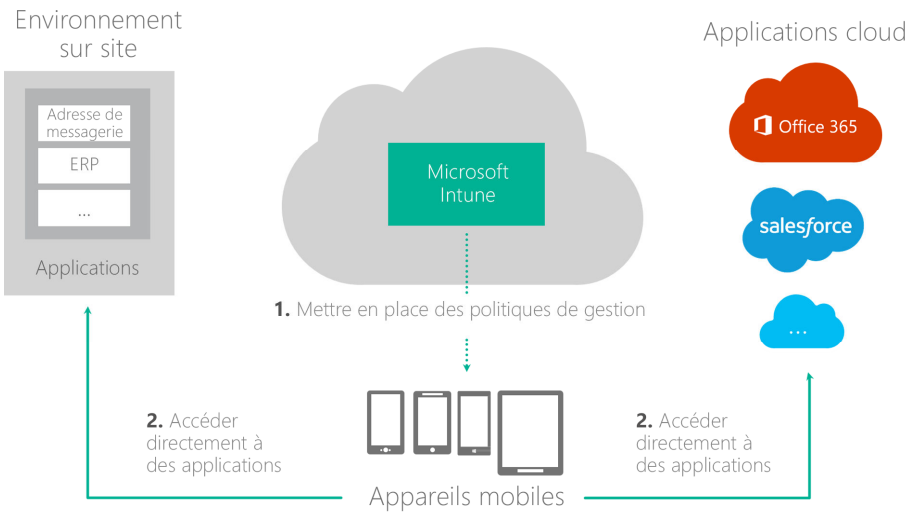

Figure 9 : en offrant la gestion MDM et MAM en tant que service cloud, Microsoft Intune propose une approche plus simple et plus sensée.

Grâce à cette approche, dont Microsoft Intune est un bel exemple, les appareils mobiles continuent de recevoir les stratégies déployées par la solution de gestion des appareils (étape 1). Une fois ces stratégies appliquées, les applications présentes sur ces appareils peuvent communiquer directement avec les applications sur site comme sur le Cloud (étape 2). Le goulot d'étranglement sur site n'a plus de raison d'être.

Le passage de la gestion d'appareils dans le Cloud présente d'autres avantages. Par exemple, Microsoft Intune vous épargne l'exécution et la gestion de vos propres serveurs et logiciels pour la gestion des appareils en le faisant à votre place. La mise à jour des logiciels de gestion des appareils représente un véritable défi. iOS, Android et Windows 10 sont régulièrement mis à jour, et souvent de telle sorte que cela a des conséquences sur les appareils gérés. Le logiciel de gestion des appareils doit être mis à jour pour tirer profit de ces nouvelles fonctionnalités. Avec la gestion d'appareils sur site, les fournisseurs de gestion MDM et MAM doivent fournir de nouveaux correctifs à chaque client, ce qui prend du temps. Chaque client (y compris vous-même) doit ensuite installer et tester ces correctifs, ce qui prend plus de temps. Multipliez ceci par le nombre de systèmes d'exploitation mobiles que vous prenez en charge et le résultat est clair : vous ne serez probablement jamais à jour.

La gestion des appareils dans le Cloud élimine ce problème. Lors de la sortie d'une nouvelle version d'iOS, par exemple, Microsoft met elle-même à jour Intune de manière à prendre en charge toute modification liée à cette mise à jour. Vous êtes toujours à jour, sans être préoccupé par l'installation de correctifs.

Microsoft Intune offre d'autres avantages et fonctionnalités. En voici quelques-uns :

- **Gestion des applications mobiles sans inscription :** vous donne toute la flexibilité nécessaire pour contrôler Office Mobile et d'autres applications sur les appareils iOS, Android et Windows de vos utilisateurs, sans qu'ils doivent inscrire l'appareil sur Intune (ce point sera détaillé plus loin).
- **La gestion de plusieurs identités :** permet à des utilisateurs d'accéder à leurs comptes personnel et professionnel à l'aide des mêmes applications Office mobiles tout en appliquant les stratégies MAM à leur compte professionnel, ce qui garantit une expérience idéale pour les collaborateurs lors de leurs déplacements.
- **Effacement sélectif de données d'entreprise :** supprime à distance des applications, des e-mails, des données, des stratégies de gestion et des profils réseau, tout en veillant à l'intégrité des données personnelles.
- **Une solution unifiée de gestion des points de terminaison :** vous permet de gérer les appareils mobiles et les ordinateurs de bureau de votre organisation à partir du même environnement d'administration (ceci s'appuie sur l'intégration que Microsoft a créée entre Intune et le gestionnaire de configuration System Center). Cela est rendu possible grâce à l'intégration étroite que Microsoft a instaurée entre Intune et System Center Configuration Manager.
- **Fonctionnalités en libre-service :** donne aux utilisateurs la possibilité d'exécuter des tâches telles que la mise à jour de mots de passe, ainsi que l'adhésion à des groupes et leur gestion via un portail unique, ce qui permet d'alléger le travail du helpdesk IT et de réduire le budget associé. Cela s'applique à tous les appareils iOS, Android et Windows de votre écosystème mobile.

Protection des informations

Qui est autorisé à accéder à un document donné ? Quel type d'accès est autorisé ? En lecture, en écriture ou autre ? Comment s'assurer que les données sont protégées depuis leur création et tout au long de leur parcours ? Ce type de contrôle s'est avéré important bien avant l'avènement des appareils mobiles et du Cloud. Dans un monde régi par la mobilité et le Cloud, avec des utilisateurs et des applications disséminés dans le monde, c'est encore plus important.

Ce style de protection des informations était jusqu'ici fourni par des solutions sur site. Par exemple, cela fait un certain nombre d'années que Microsoft propose les services AD RMS (Active Directory Rights Management Services).

Toutefois, proposer ce type de protection à l'aide d'une solution sur site présente des limites (figure 10).

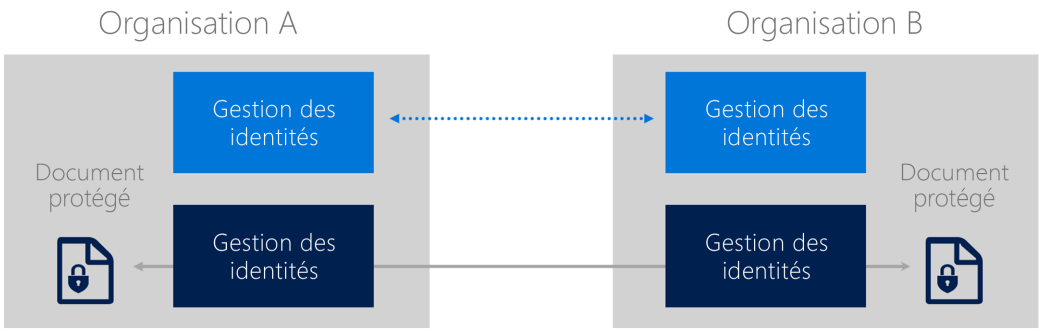

Figure 10 : le fait de s'appuyer sur une technologie sur site pour la protection des informations nécessite la configuration manuelle de connexions point à point entre chaque organisation pour la gestion des identités.

Imaginez que deux organisations, A et B, souhaitent partager un document protégé. Peut-être que seul un groupe de personnes dans chaque entreprise est autorisé à le lire. Par conséquent, toute tentative d'ouverture du document doit être vérifiée par un service de protection des informations. Ce problème peut être résolu à l'aide d'une technologie de protection des informations sur site, mais y parvenir nécessite la configuration de relations point à point entre les solutions de gestion des identités sur lesquelles les technologies de protection des informations s'appuient.

Cela représente beaucoup de travail pour le seul partage de documents protégés. La sécurité dans pareille situation laisse à désirer. Toutefois, grâce à la nouvelle solution Azure Information Protection exécutée depuis le cloud, il est bien plus simple d'y parvenir (Figure 11).

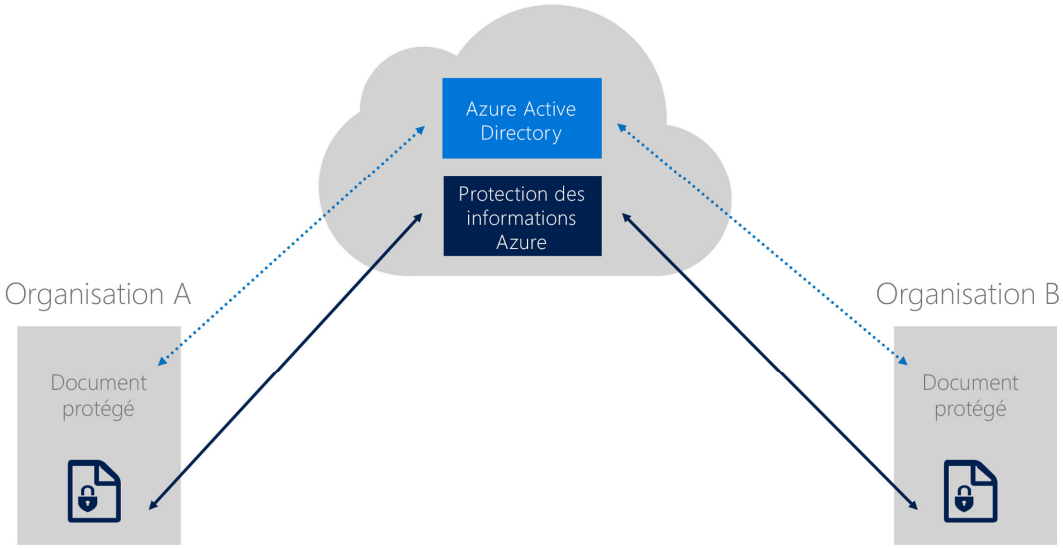

Figure 11 : l'utilisation d'une solution cloud partagée pour la gestion des identités et la protection des informations simplifie grandement le contrôle d'accès aux documents.

Comme le montre la figure, les deux organisations n'ont plus besoin de configurer de connexion directe de l'une à l'autre. Il leur suffit désormais de se connecter une seule fois aux services de cloud (Azure AD et Azure Information Protection). Peu importe le nombre d'organisations avec lesquelles vous partagez des documents, toutes n'ont besoin de se connecter qu'une seule fois aux services de cloud. Grâce à ce modèle, terminée la complexité liée au partage de documents protégés entre organisations.

Azure Information Protection offre d'autres avantages, tels que la possibilité de :

- **Classer, d'étiqueter et de protéger des données :** au moment de la création ou de la modification. Utiliser des polices pour classer et étiqueter des données de manière intuitive, sur la base de la source, du contexte et du contenu des données. La classification peut être totalement automatique, générée par les utilisateurs ou basée sur une recommandation. Une fois que les données sont classées et étiquetées, la protection peut être appliquée automatiquement sur cette base.
- **Fournir aux utilisateurs des contrôles simples et intuitifs :** pour protéger les données tout en restant productif. La classification et la protection des données sont intégrées à Office et à des applications courantes. Elles permettent de sécuriser en un clic les données sur lesquelles des utilisateurs travaillent. Les notifications internes au produit fournissent des recommandations qui permettent aux utilisateurs de prendre des décisions adaptées.
- **Gagner en visibilité et d'augmenter votre contrôle sur les données partagées :** les propriétaires de documents peuvent suivre les activités sur des données partagées et supprimer l'accès si nécessaire. L'IT peut utiliser des fichiers journaux et des rapports pour contrôler, analyser et exploiter des données partagées.
- **Protégez les données à l'endroit où elles sont stockées dans le cloud ou sur site** et choisissez comment vos clés de chiffrement sont gérées à l'aide d'options Bring Your Own Key.

Défis administratifs

Tandis que des sociétés s'efforcent de fonctionner dans un monde mobile orienté cloud, nombreuses sont celles qui disposent encore de trop de solutions ponctuelles et sont dépourvues de ressources permettant de les gérer. Les produits sont souvent trop difficiles à configurer, à intégrer et à conserver. Par ailleurs, dans un paysage d'attaques qui évolue constamment, un système de protection peut rapidement devenir obsolète. Par ailleurs, les budgets limités en matière d'IT n'aident pas à relever ces défis. La priorisation de ces budgets pour faire face à de nouveaux défis de sécurité n'est pas une tâche aisée pour nombre de nos clients.

EMS offre un ensemble intégré de solutions conçues pour fonctionner parfaitement ensemble grâce à vos investissements sur site, ce qui permet d'éviter des efforts d'intégration onéreux et compliqués entre les fonctionnalités. Pour faciliter un peu plus le déploiement, EMS est proposé avec FastTrack, un service Microsoft qui inclut des pratiques idéales, outils, ressources et informations d'experts qui feront de votre expérience avec EMS un succès. En tant que solution cloud, EMS facilite également la mise à l'échelle, la maintenance et l'application de mises à jour.

Scénarios : ce qu'EMS peut offrir

Si chaque domaine (gestion des identités, protection des informations et gestion des appareils) est envisagé individuellement, il existe un argument incontestable justifiant son passage au cloud. Mais l'argument est encore plus fort lorsque ces services cloud sont utilisés conjointement, comme dans EMS. Pour en démontrer la pertinence, observons quatre scénarios :

1. la sécurité liée aux identités.
2. la protection des informations de bout en bout ;
3. la productivité mobile gérée ;
4. Déploiement et gestion simplifiés

la sécurité liée aux identités.

Comme nous l'avons vu, l'identité est au cœur de l'action d'EMS. Mais que se passe-t-il si un utilisateur malveillant s'approprie l'identité d'Anne ? Imaginons qu'elle choisisse un mot de passe facile à deviner ou que ses informations d'identification lui soient dérobées par piratage psychologique. C'est exactement le type d'attaque utilisé dans plusieurs violations récentes sophistiquées. La menace est réelle.

La détection de ce type de menace exige une sécurité en matière d'identité, ce qu'EMS offre de plusieurs manières. Commençons par un exemple de sécurisation de l'accès principal. Par exemple, Azure AD est capable de détecter des connexions potentiellement non valides, puis d'avertir l'équipe de sécurité (figure 12).

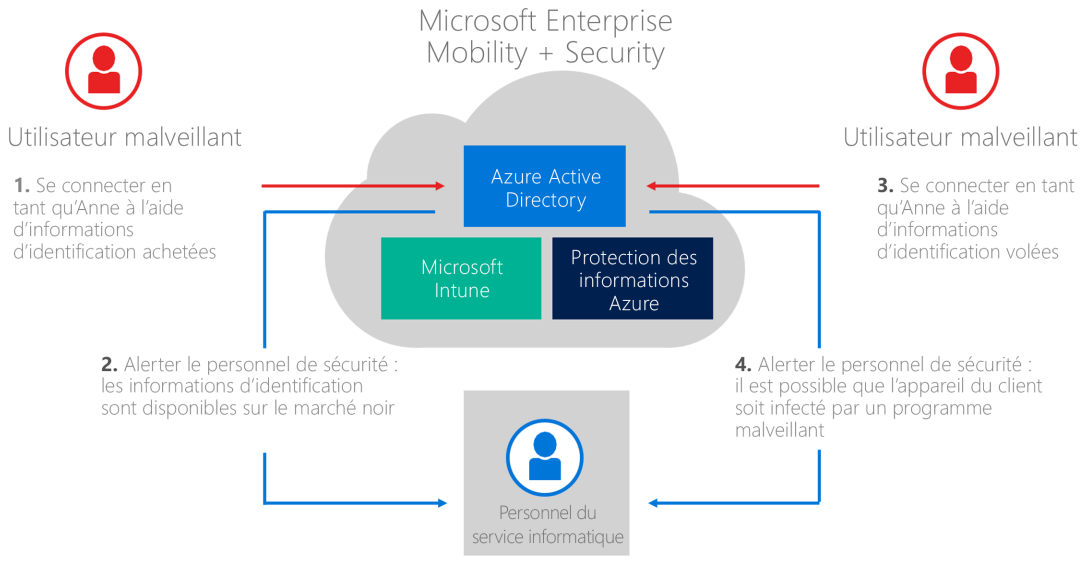

Figure 12 : Azure AD peut prévenir plusieurs types de connexions effectuées par des utilisateurs malveillants.

Imaginons qu'un utilisateur malveillant achète le nom et le mot de passe de connexion d'Anne sur un site pirate, puis les utilise pour se connecter à votre organisation (étape 1). Microsoft surveillant ces sites, Azure AD détecte la présence des informations d'identification d'Anne sur le marché noir. Lorsqu'Azure AD perçoit cette connexion, l'équipe de sécurité est avertie de la situation (étape 2). Imaginons qu'un autre utilisateur malveillant se connecte à l'aide des informations d'identification d'Anne, mais que l'appareil client sur lequel cette connexion est effectuée soit infecté par un logiciel malveillant (étape 3). Azure AD prévient également l'équipe de sécurité (étape 4).

> 63 % des violations de données avérées impliquent une faiblesse, une défectuosité ou la subtilisation de mots de passe
>
> ***– Rapport sur les atteintes à la sécurité des données Verizon 2016***

La capacité à détecter ces menaces liées à la connexion est propre à Azure AD et dépend des ressources étendues de Microsoft dans le cloud. Les informations que Microsoft obtient suite aux attaques de ses différentes offres de Cloud (Office 365, Azure, Xbox, etc.) sont fournies à Azure AD pour rendre votre entreprise plus sécurisée. Il est également possible d'agir lorsque ce type de problème est détecté. À titre d'exemple, lorsque votre équipe de sécurité apprend que les identifiants d'Anne ont été volés, il se peut que celle-ci doive modifier son mot de passe, puis utiliser l'authentification multifacteur dès qu'elle se connecte.

Azure AD signale également d'autres comportements inhabituels. Si Anne se connecte à son compte depuis Los Angeles, en Californie, puis de Lima au Pérou, cinq minutes plus tard, cela signifie qu'il y a un problème. Azure AD le signalera. D'autres comportements inhabituels seront également signalés. Il peut s'agir, par exemple, de l'utilisation d'une tablette Android, alors qu'Anne utilise normalement un iPad. Évidemment, Azure AD signale les problèmes habituels, comme le dépassement d'un nombre défini de tentatives de connexion.

Imaginons qu'un utilisateur malveillant parvienne néanmoins à passer outre toutes ces barrières. Comment détecter ce type d'attaque après que la connexion a réussi ? La réponse dépend de la capacité à reconnaître le comportement d'un utilisateur malveillant utilisant une identité volée. Il sera différent de celui du propriétaire légitime de cette dernière. ATA peut détecter ces différences, puis prévenir l'équipe de sécurité (figure 13).

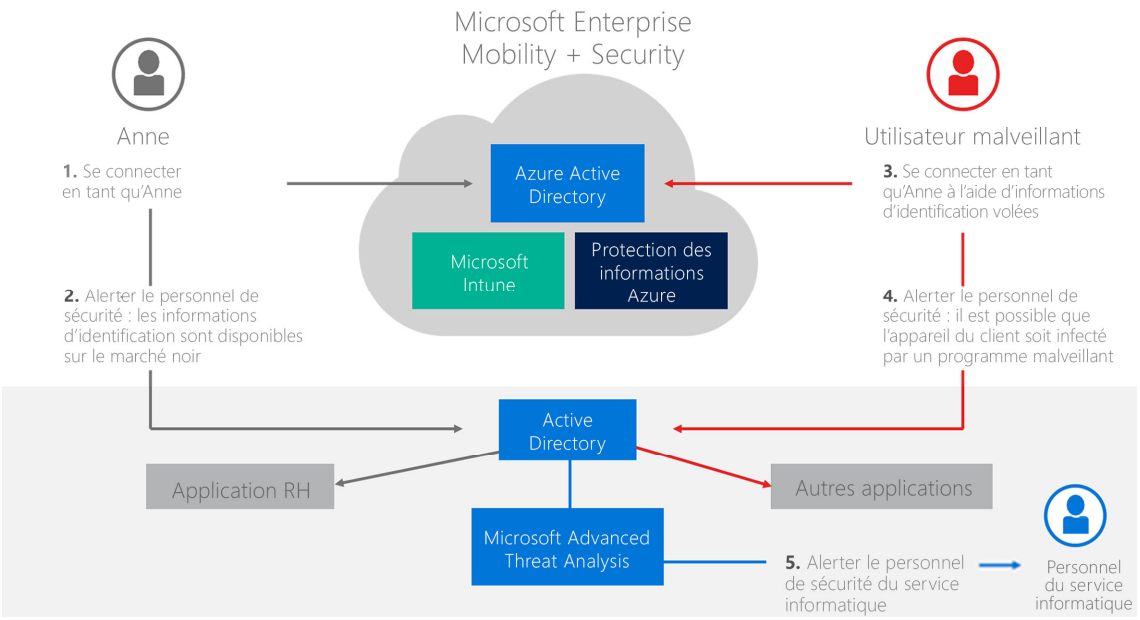

Figure 13 : grâce à ATA, EMS peut détecter et signaler l'activité suspecte à l'équipe de sécurité lorsqu'un compte menace d'être compromis.

Imaginons qu'Anne se connecte à Azure Active Directory (étape 1), puis travaille selon ses horaires habituels. Anne fait partie du service des ressources humaines. Elle accède donc principalement aux applications et aux données RH de l'organisation (étape 2). Supposons maintenant qu'un utilisateur malveillant se connecte à l'aide des informations d'identification volées d'Anne (étape 3). Accédera-t-il également aux ressources RH pendant les horaires de travail de celle-ci ? Il est presque certain que cela ne sera pas le cas ; il accédera plutôt à d'autres applications et types de données. Il est également probable qu'il le fasse à des heures différentes, car il peut se trouver dans un autre fuseau horaire, à l'autre bout du monde (étape 4).

ATA peut détecter cette variation du comportement. En surveillant le trafic vers et depuis Active Directory sur site, puis en utilisant la technologie d'apprentissage machine pour l'analyser, ATA peut rapidement apprendre les habitudes d'accès des utilisateurs. Lorsque l'un d'entre eux se comporte différemment, comme c'est le cas pour Anne, ATA peut prévenir l'équipe de sécurité d'une possible violation de sécurité (étape 5).

Après qu'un utilisateur malveillant a accédé à une organisation, il s'y cache généralement pendant des mois dans l'attente d'opportunités. Il ne sera souvent pas détecté tant qu'il n'aura pas exploité ces opportunités (et pourrait même le rester si c'était le cas). L'utilisation conjointe d'ATA et des services de création de rapports fournis par Azure AD peuvent vous aider à détecter et à mettre fin à ces attaques avant qu'elles ne soient néfastes à votre entreprise. Avec Azure AD dans le cloud et ATA sur site, EMS offre une solution complète de sécurité de l'identité.

Bien entendu, il existe d'autres scénarios où une violation de sécurité n'est pas malveillante mais résulte d'une action accidentelle de la part d'un utilisateur interne. C'est à ce niveau que des technologies EMS, telles que Cloud App Security, interviennent pour protéger les données. À titre d'exemple, grâce à CAS, vous pouvez définir des stratégies qui analysent automatiquement les applications dans le cloud auxquelles vos utilisateurs ont accès, afin de protéger du contenu sensible tel que des numéros de carte de crédit ou des dossiers médicaux. Lorsque CAS trouve ces données, vous avez la possibilité d'identifier qui a téléchargé les données ou y a accédé ainsi que d'entreprendre des actions, telles que la suppression des autorisations, la mise en quarantaine de l'utilisateur concerné, etc.

Dans la section suivante, nous envisagerons d'autres cas de figure dans lesquels EMS permet de protéger les données avant même qu'elles aient été divulguées par erreur à des applications ou utilisateurs non autorisés.

Protection des informations de bout en bout

Une fois qu'Anne a accès à Exchange Online, elle commence à recevoir ses e-mails professionnels. Même si elle utilise son iPad (que ce soit depuis le salon d'un aéroport ou tout autre lieu public), sa messagerie contient des informations qui doivent être protégées. Il est nécessaire de parvenir à l'empêcher d'envoyer ces informations (accidentellement ou volontairement) à n'importe qui, que ce soit par e-mail ou en copiant du contenu dans des applications non approuvées. La protection des informations de bout en bout est indispensable. EMS le permet par l'intermédiaire du fonctionnement conjoint d'Azure AD, d'Intune et d'Azure Information Protection (figure 14).

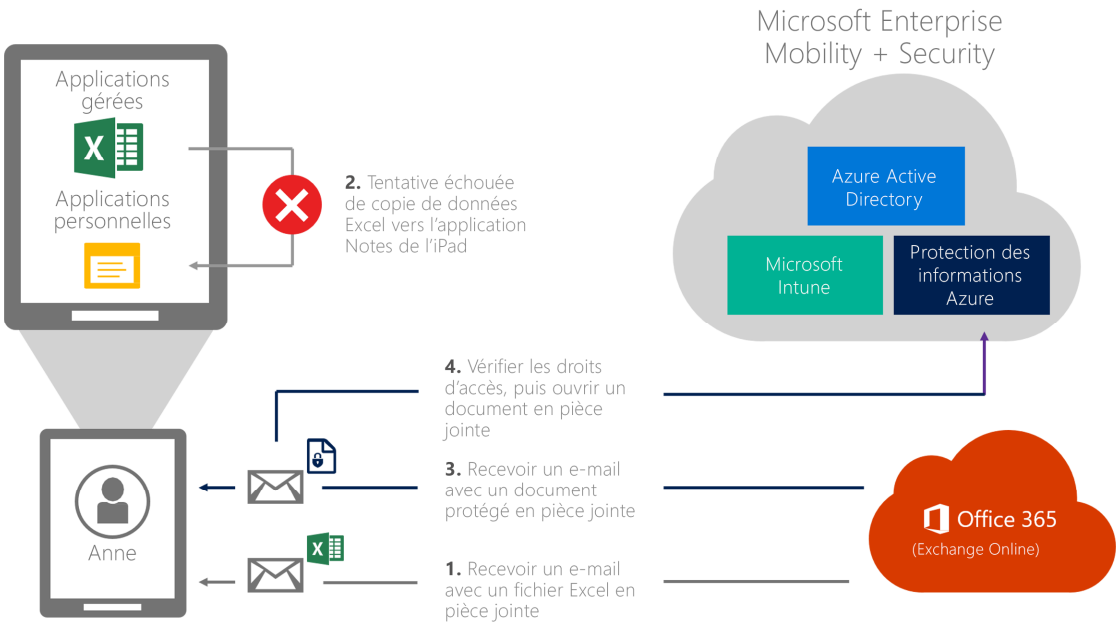

Figure 14 : EMS protège les informations professionnelles en autorisant leur utilisation et leur copie uniquement dans un environnement géré, et en incorporant des contrôles d'accès directement dans des fichiers chiffrés.

Imaginons qu'Anne reçoive une feuille de calcul Excel en pièce jointe d'un e-mail professionnel (étape 1). Elle ouvre la pièce jointe à l'aide de l'application mobile Excel sur son iPad, puis tente de copier-coller des données de la feuille de calcul dans l'application Notes intégrée à l'iPad. Si EMS est installé, cette tentative échouera (étape 2).

> 33 % des violations par un utilisateur ont lieu par erreur.
> ***–VansonBourne, février 2014***

Cet échec s'explique par le fait qu'Intune sépare les applications gérées de ses applications personnelles présentes sur son iPad. Comme le montre la figure, les applications mobiles Office d'Anne sont toutes marquées comme gérées. Cela signifie qu'il est impossible de copier les données pour les coller dans des applications non gérées. Dans cet exemple, l'option Coller n'apparaît pas lorsqu'elle tente de déplacer des données de la feuille de calcul Excel vers l'application Notes d'iOS. Elle est libre de déplacer des informations d'une application gérée à l'autre, comme d'une feuille de calcul Excel à un document Word. C'est tout. Même si la figure ne le montre pas, les applications gérées peuvent également être obtenues auprès d'autres fournisseurs de logiciels ou être créées par votre organisation. Vous n'êtes pas obligé d'utiliser les applications Microsoft.

Microsoft offre ce type de protection des informations pour les applications mobiles Office sur iPad et sur les appareils Android ; les autres fournisseurs de gestion MAM ne le peuvent pas. Anne peut tout à fait utiliser les applications mobiles Office à des fins professionnelles et personnelles. Il lui suffit de se connecter à l'aide d'une autre identité. Intune garantit que les stratégies de l'entreprise sont appliquées aux données professionnelles, mais ne se soucie pas des données personnelles.

La protection des informations offerte par Intune pour les appareils mobiles est cruciale, mais insuffisante. Imaginons qu'Anne reçoive par e-mail une autre pièce jointe contenant des données professionnelles confidentielles (étape 3). Il est possible qu'elle ne l'ouvre jamais sur son iPad, mais imaginons qu'elle le transfère accidentellement à un tiers : que se passera-t-il ? Et si l'envoi de la pièce jointe à Anne était une erreur et qu'elle n'était pas supposée y avoir accès ? La protection des informations de bout en bout nécessite de traiter ces problématiques.

Azure Information Protection a été créée pour les résoudre. Protégée par Azure Information Protection, la pièce jointe qu'Anne a reçue est chiffrée. Cela signifie qu'aucun logiciel ne peut l'ouvrir sans préalablement contacter le service de cloud (étape 4). Azure Information Protection utilise l'identité d'Anne, fournie via Azure AD, ainsi que des informations présentes dans le document protégé pour déterminer les droits d'accès dont elle dispose. Ses droits pourraient la limiter à la seule lecture du document ou l'autoriser à le lire et à le modifier. En fonction de ce que le créateur du document permettrait, elle pourrait réaliser d'autres tâches.

En plus de contrôler les données auxquelles Anne a accès, Azure Information Protection peut également contrôler ce qu'Anne peut transférer, ce qui constitue un outil efficace supplémentaire permettant d'empêcher la fuite de données. À titre d'exemple, les administrateurs peuvent créer des stratégies qui détectent automatiquement des données sensibles (telles que des informations relatives à une carte de crédit) et appliquent automatiquement une protection empêchant tout transfert. Dans le même temps, Azure Information Protection permet aux utilisateurs d'appliquer aisément leur propre protection, grâce à un contrôle intégré directement au ruban Office.

Azure Information Protection veille à la protection des données où que se trouvent les documents. Intune protège les informations consultées sur des appareils mobiles. Ces deux composants, ainsi que les informations d'identité fournies par Azure AD, permettent à EMS de proposer une protection des informations de bout en bout.

la productivité mobile gérée ;

Vos collaborateurs utilisent des appareils mobiles pour des tâches personnelles et professionnelles. Tout en veillant à la productivité de vos collaborateurs, vous souhaitez également prévenir toute perte de données, qu'elle soit intentionnelle ou non. En outre, vous devez pouvoir protéger les données de la société auxquelles il est possible d'accéder via des appareils, même dans l'hypothèse où ces données ne seraient pas gérées par vos soins.

Vous pouvez utiliser des stratégies de gestion des applications mobiles Intune pour protéger les données de votre société. Du fait que les stratégies MAM d'Intune peuvent être utilisées indépendamment de toute solution de gestion des appareils mobiles, vous pouvez les utiliser pour protéger les données de votre société avec ou sans inscription d'appareils dans une solution de gestion des appareils. De cette manière, EMS vous donne la flexibilité de gérer des appareils ou applications, voire une association des deux.

Pour avoir comment Microsoft EMS peut y parvenir, nous allons tout d'abord nous pencher sur un scénario d'appareils gérés. Dans ce cas de figure, commençons par étudier un exemple. Une utilisatrice, prénommée Anne, ajoute un nouvel iPad au réseau de votre entreprise (figure 15).

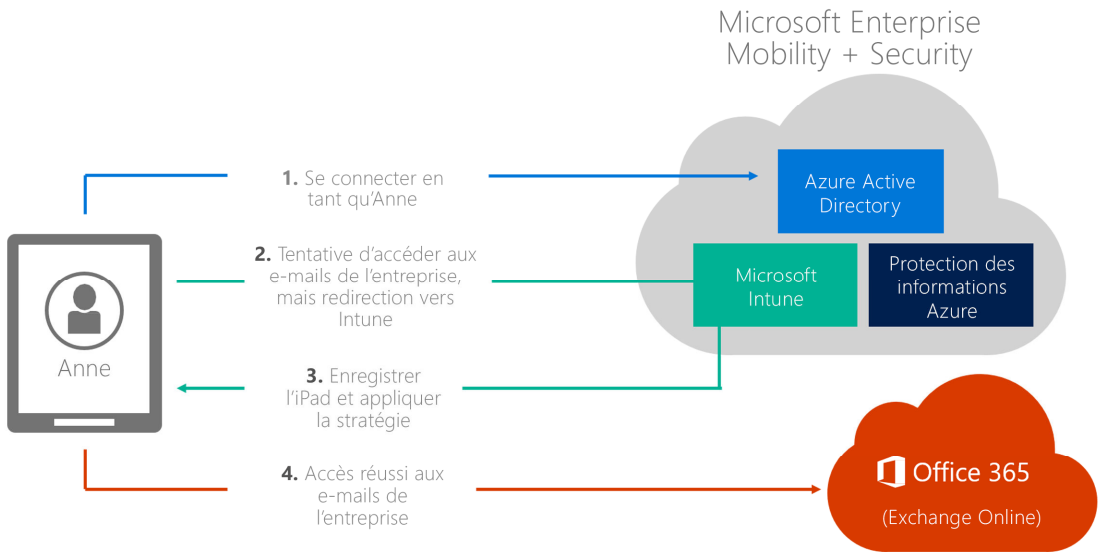

Figure 15 : EMS peut inscrire automatiquement un appareil, puis appliquer des stratégies d'accès aux applications.

L'identité est la base de tout le reste. Par conséquent, le processus commence par la connexion d'Anne à Azure AD (étape 1). L'iPad qu'elle utilise peut être le sien ou celui fourni par votre organisation. Dans les deux cas, la première chose qu'elle fait après s'être connectée est d'accéder à une application SaaS. Dans cet exemple, il s'agit de l'application Exchange Online, qui fait partie d'Office 365 : Anne souhaite accéder à sa messagerie professionnelle. Comme son nouvel iPad n'est pas encore géré, la requête est redirigée vers Intune (étape 2).

Intune établit ensuite une relation de gestion avec l'iPad d'Anne (avec son autorisation, bien évidemment) pour autoriser la gestion de cet appareil. Pour ce faire, Intune applique toutes les stratégies définies pour iPad (étape 3). Par exemple, il est possible que vos administrateurs aient spécifié que pour faire partie de l'environnement de votre entreprise un iPad doit disposer d'un jeu de mots de passe de déverrouillage, chiffrer les données professionnelles qu'il stocke et être équipé d'une messagerie gérée. La définition et l'application de ces stratégies reposent à la fois sur Azure AD et sur Intune.

Son appareil étant désormais géré, Anne peut accéder à sa messagerie professionnelle (étape 4). Préalablement, Azure AD et Intune fonctionnent de concert pour vérifier qu'Anne respecte une autre stratégie : celle définie pour l'application en question. Par exemple, l'une des stratégies liées à Exchange Online peut exiger que les demandes proviennent d'appareils gérés par Intune et qui sont parfaitement à jour. Il s'agit d'un exemple d'accès conditionnel : l'utilisateur est autorisé à effectuer une tâche à la condition de respecter plusieurs critères. Ces derniers peuvent être liés à l'identité, au type d'appareil présentant certaines caractéristiques, etc. L'accès conditionnel est une fonctionnalité puissante qui n'est utilisable que lorsque plusieurs services fonctionnent conjointement, comme dans EMS. Cette synergie constitue un point essentiel (et un avantage évident) de toute solution cloud unifiée.

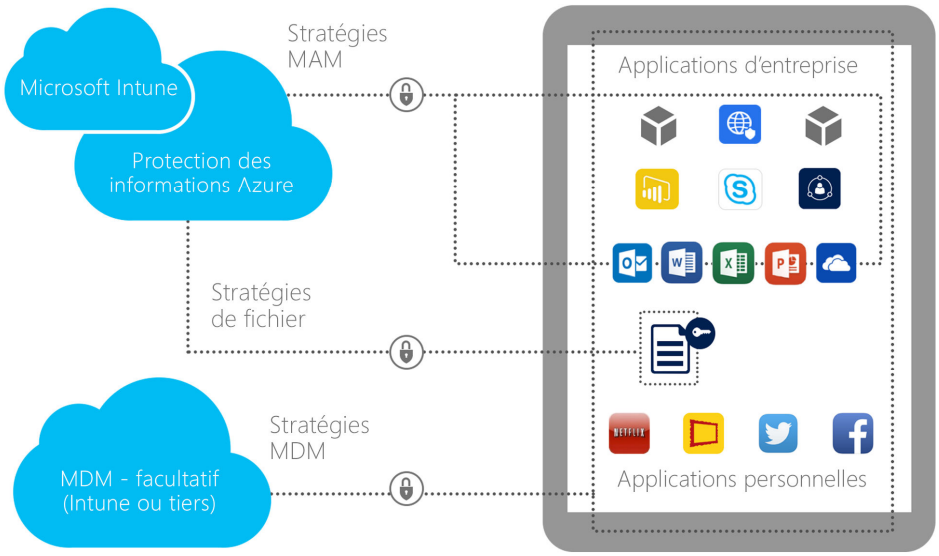

Figure 16 : EMS permet également de gérer avec flexibilité la gestion des applications mobiles sans inscription.

Tandis que de nombreuses organisations voudront gérer tous les appareils utilisés par des collaborateurs, dans de nombreux cas de figure, ces derniers souhaitent utiliser leurs propres appareils non gérés tout en tirant parti d'applications d'entreprise. Ainsi, quelle protection des données d'applications Office offre EMS ? En utilisant la stratégie MAM d'Intune sans la fonctionnalité d'inscription, les organisations peuvent sécuriser des données sur des appareils à l'aide d'Office pour mobiles et d'autres applications installées, sans qu'il soit nécessaire d'inscrire ces appareils dans Intune MDM (Figure 16).

Cela signifie également que, pour les clients qui disposent déjà d'un fournisseur MDM ou qui ne souhaitent pas gérer les appareils de leurs utilisateurs via MDM, ils peuvent continuer de protéger l'accès à Office et aux données de la société. Cela inclut des restrictions des fonctionnalités couper/copier/coller, une désactivation de la fonction « Enregistrer sous », la détection d'attaques jailbreak, des exigences relatives aux codes PIN et la possibilité de supprimer à distance des données protégées par la stratégie MAM.

Déploiement et gestion simplifiés

Dans ce document, nous avons vu à quel point l'architecture basée dans le cloud d'EMS simplifiait la configuration et la gestion de solutions, même dans les cas de figure les plus complexes liés à la mobilité. Nous voulions toutefois faciliter davantage l'administration en ajoutant un service appelé FastTrack.

FastTrack est un avantage proposé par les ingénieurs Microsoft pour vous permettre de commencer rapidement votre déploiement EMS. À titre d'exemple, ces ingénieurs peuvent créer des comptes d'utilisateurs, déplacer des identités dans le cloud, configurer des applications tests ainsi qu'un système libre-service dans le site MyApps. Ils peuvent configurer des groupes d'utilisateurs et activer la gestion des droits pour les utilisateurs, y compris des modèles de test. Ils peuvent également intégrer System Center Configuration Manager sur site avec Intune pour un contrôle complet des PC et des appareils mobiles.

Outre un déploiement plus rapide, FastTrack permet également à votre partenaire Microsoft de disposer de plus de temps pour se consacrer à des services à haute valeur ajoutée relatifs à EMS, notamment la personnalisation, la correction, la configuration des appareils à l'échelle de l'entreprise, l'augmentation du nombre d'utilisateurs, la gestion et l'amélioration de la solution dans son ensemble.

Cette possibilité de proposer une solution complète est la véritable richesse d'EMS. Contrairement à des solutions ponctuelles proposées par d'autres fournisseurs, EMS inclut tout ce dont vous avez besoin dans une solution unique intégrée, et notamment une équipe de compte ainsi qu'une structure d'octroi de licences simplifiée. Par ailleurs, du fait qu'EMS est exécuté dans le cloud, vous devez acheter et gérer moins de matériel sur site, ce qui implique bien des économies.

Résumé

Microsoft Enterprise Mobility + Security permet à votre personnel d'être productif sur les appareils qu'il affectionne, tout en protégeant les ressources de votre entreprise. En déplaçant les applications sur site vers le cloud, EMS aide votre organisation à être plus productive, mieux gérée et plus sécurisée dans un monde où mobilité et cloud sont les maîtres mots. En intégrant ces services les uns aux autres, ainsi qu'à leurs cousins sur site, EMS offre une solution complète sans comparaison sur le marché actuel. En déployant EMS, facilitez la vie de vos employés, de vos partenaires commerciaux et de vos clients.