Développez les capacités de gestion et de sécurité d'Office 365 grâce à EMS

Microsoft

Microsoft Enterprise Mobility + Security

“Le principe directeur de la transformation numérique est la mobilité de l'expérience humaine. »

Satya Nadella

Accès sécurisé

Gestion mobile

Sécurité avancée

Accélérez votre transformation numérique

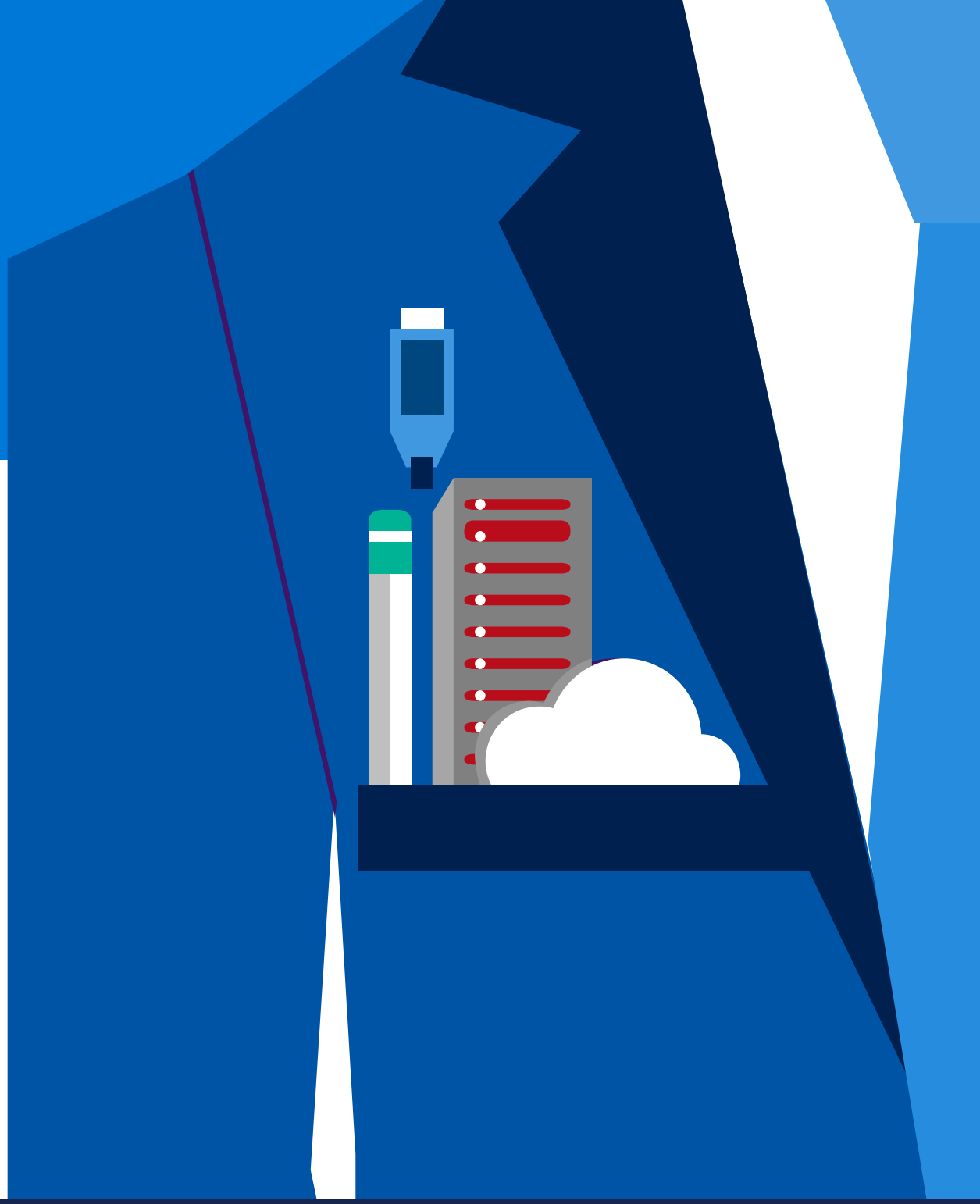
Office 365 est une plateforme puissante et représente une étape cruciale de la transformation numérique de votre entreprise. Vous pouvez dériver une grande valeur commerciale à partir d'une productivité sans compromis grâce à des outils basés sur le cloud qui donnent à vos utilisateurs la liberté de travailler de n'importe où, sur n'importe quel appareil. Les **capacités fondamentales en matière de gestion et de sécurité** intégrées à Office 365 sont conçues pour vous apporter un contrôle complet sur les opérations sans perturber l'expérience de l'utilisateur final. Lorsque vous déployez Office 365, vous devez étendre ces capacités de gestion et de sécurité à votre écosystème numérique au sens large pour aboutir à une stratégie de sécurité exhaustive et globale.

Avec **Microsoft Enterprise Mobility + Security** (EMS), vous pouvez utiliser votre déploiement Office 365 pour donner un coup d'accélérateur aux priorités spécifiques de votre entreprise à chaque étape de votre transformation numérique. EMS offre un niveau de sécurité supplémentaire pour Office 365 et développe vos capacités pour **fournir en toute sécurité votre portefeuille élargi d'applications, basées sur ou compatibles avec le cloud**, à n'importe quel appareil et sauvegarder les ressources essentielles de votre entreprise à tous les niveaux. En outre, EMS **protège votre portefeuille global d'applications** et l'infrastructure informatique des utilisateurs finaux contre les menaces à la fois **sur site et dans le cloud**.

EMS fournit des capacités stratégiques pour vous aider à mettre en œuvre la transformation numérique : accès sécurisé, gestion mobile et sécurité avancée.

Section 1

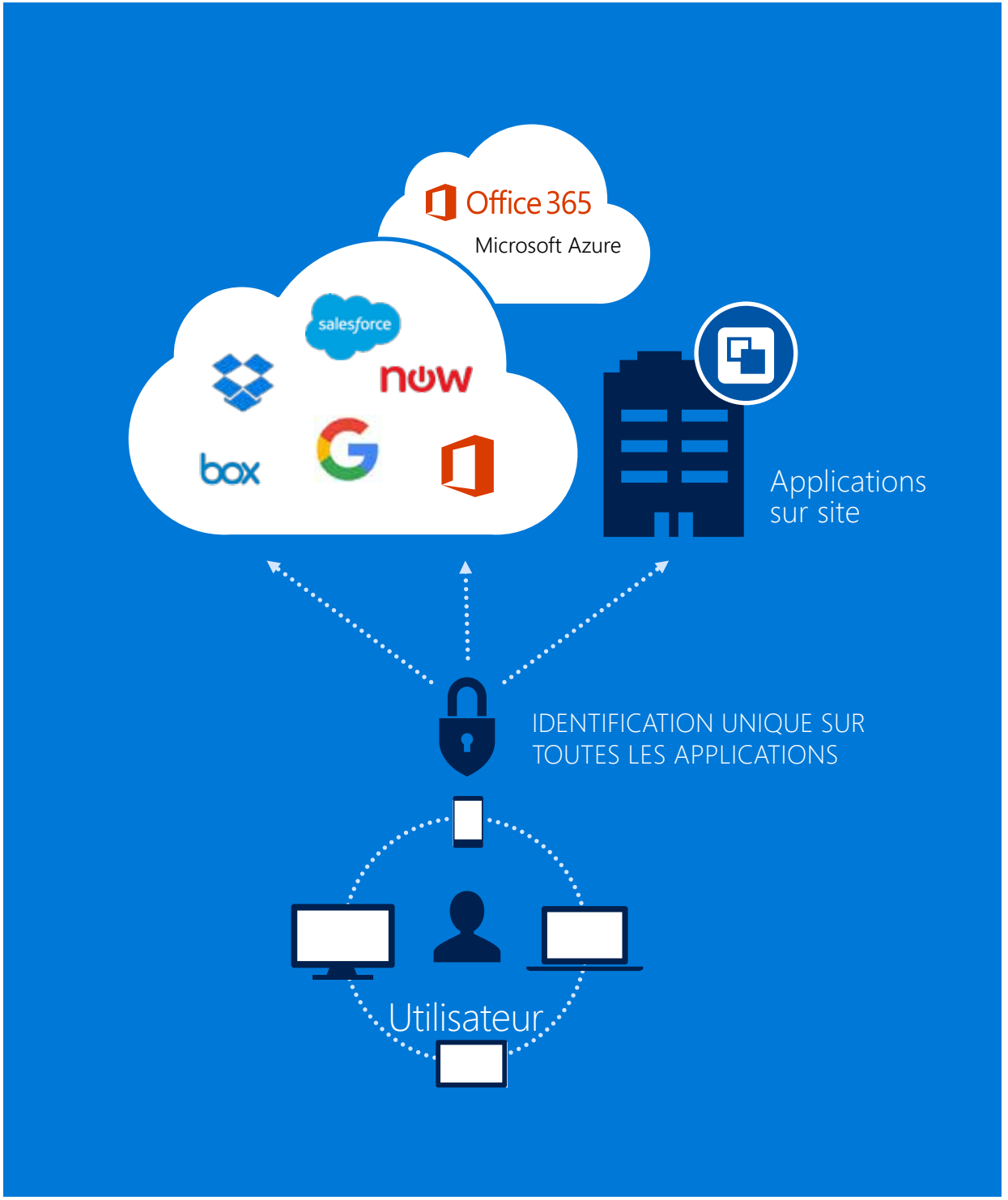
Accès sécurisé



En partie, la transformation numérique promet une infrastructure qui garantit une productivité sans compromis pour l'intégralité de votre main-d'œuvre. À cette fin, Office 365 fournit un accès sécurisé et transparent à ses applications depuis n'importe quel appareil et n'importe quel emplacement. Mais les applications Office Mobile ne seront pas les seules applications de votre portefeuille d'applications orientées cloud, tandis que vous développez votre stratégie de cloud et que vous y déplacez toujours plus d'applications métier. Au fur et à mesure que vous continuez à diversifier votre écosystème numérique, vous aurez besoin d'une solution exhaustive pour gérer et sécuriser l'accès à tous les éléments. **Il est absolument essentiel d'offrir une identité unique et unifiée pour chaque utilisateur**. EMS vous permet de **connecter vos investissements actuels en matière d'identité sur site** à vos scénarios d'usage SaaS et sur site et d'établir une identité unique pour chacun de vos utilisateurs. Une identité unique vous permet d'ancrer la sécurité et la productivité pour l'intégralité de votre portefeuille d'applications.

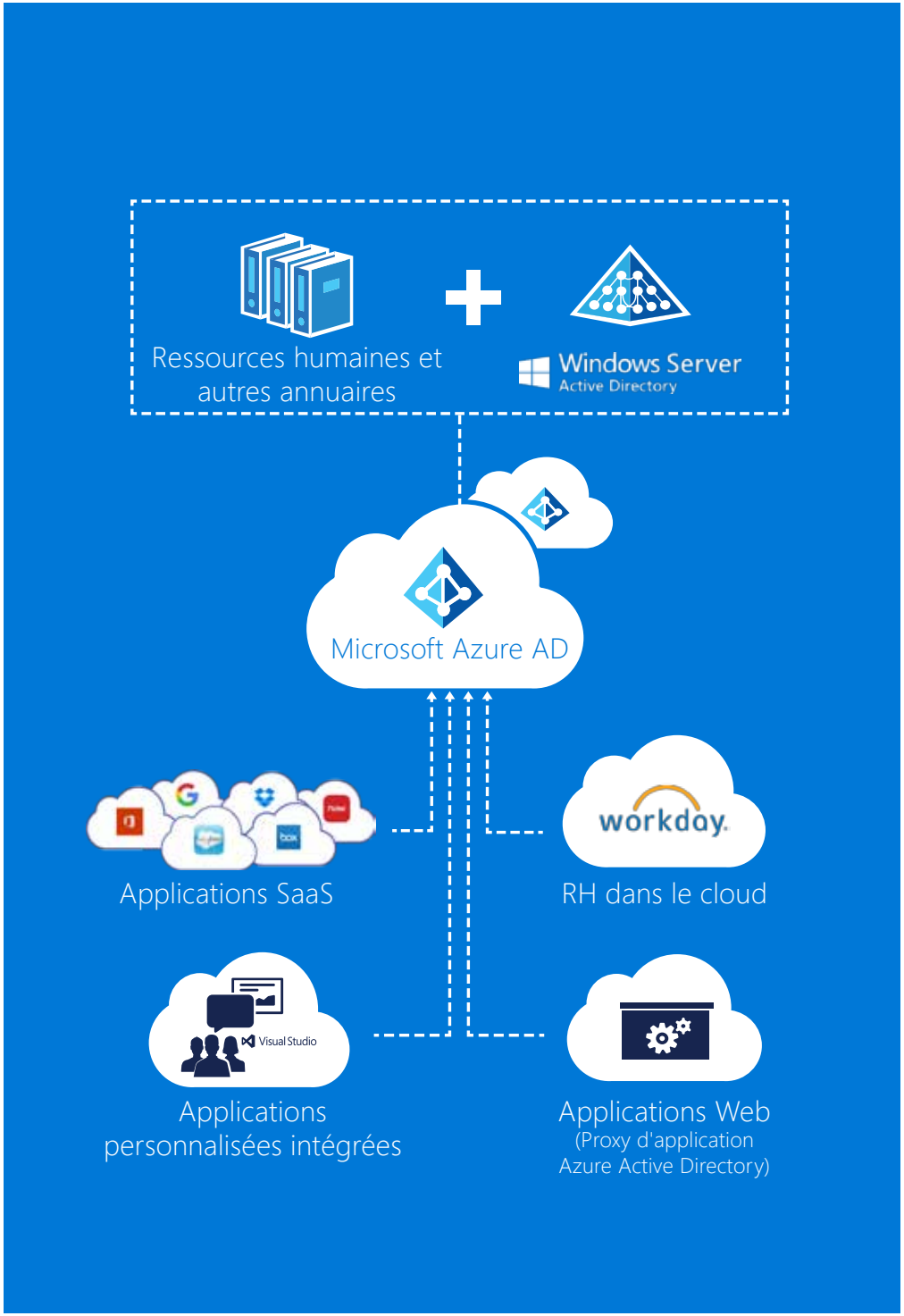
Commencez par configurer l'authentification unique sur Office 365 et toutes vos applications

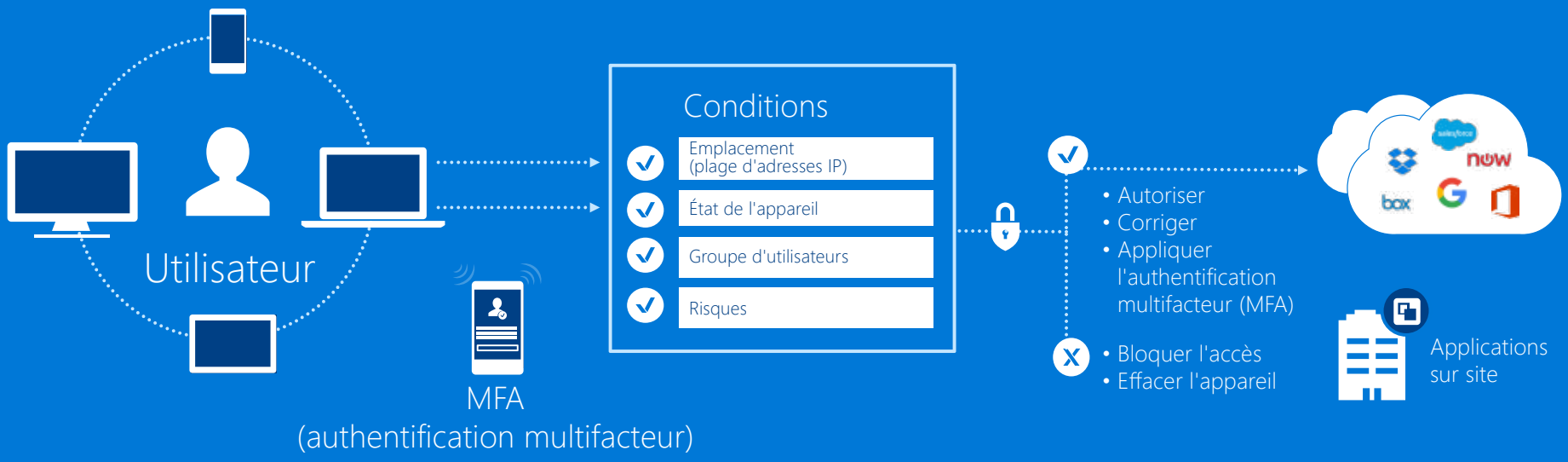
Les collaborateurs sont plus productifs lorsqu'ils n'ont qu'un seul nom d'utilisateur et un seul mot de passe à retenir. Avec Office 365, vos utilisateurs bénéficient de la simplicité fonctionnelle de l'authentification unique sur Office 365, pour une expérience utilisateur cohérente et fluide sur n'importe quel appareil. **EMS étend cette fonctionnalité à des milliers d'applications Web sur site et dans le cloud**, le tout avec une identification unique et sécurisée. Pour favoriser davantage la productivité, EMS fournit des capacités en libre-service aux utilisateurs finaux, telles que la réinitialisation des mots de passe oubliés ou les demandes d'accès à une application, ce qui permet de réduire considérablement les demandes imposées à votre service de support informatique.



Assurez-vous de protéger et de gérer les identités dotées de privilèges

Une fois que vous avez établi une seule identité unifiée par utilisateur, la gestion des différents privilèges pour vos utilisateurs est un moyen important de vous prémunir contre les vulnérabilités potentielles. Grâce à EMS, vous bénéficiez de capacités de **surveillance et de contrôle sur tous les niveaux des privilèges utilisateurs**. Vous pouvez découvrir les administrateurs permanents au sein de votre entreprise et utiliser l'accès administratif ponctuel, tel quel ou en l'exigeant sur demande, de sorte que les privilèges accrus soient uniquement disponibles pour certains utilisateurs en fonction des besoins. L'assistant Sécurité EMS simplifie la conversion des administrateurs permanents en administrateurs éligibles, de sorte à faciliter la gestion et la mise en œuvre des privilèges à la demande. Les rapports d'audit et les révisions d'accès permettent de déterminer qui a encore besoin de droits d'administration, et EMS vous signalera les rôles inactifs afin que vous puissiez réduire ou éliminer les privilèges inutilisés.





Ajoutez un accès conditionnel basé sur les risques et informé par un ensemble élargi de conditions

Office 365 inclut un accès conditionnel basé sur l'état de l'appareil, de sorte que vous pouvez empêcher les utilisateurs d'accéder aux ressources Office à partir d'appareils vulnérables ou compromis. EMS **développe vos capacités en matière d'accès conditionnel** afin de fournir **un contrôle plus complet sur plusieurs niveaux** : identité, appareil, application et fichier. Grâce à EMS, vous pouvez définir des conditions d'accès qui incluent :

Utilisateur

Affectez plusieurs conditions (d'après l'emplacement, l'application, l'appareil et les niveaux de risque) à tous les utilisateurs ou à plusieurs groupes de sécurité. Vous pouvez également exclure expressément certains groupes afin qu'ils ne soient pas affectés par les politiques d'accès conditionnel.

Emplacement

Définissez un ensemble d'adresses IP de confiance de sorte à autoriser l'accès uniquement à partir de celles-ci. Si un utilisateur tente d'accéder aux ressources de l'entreprise à partir d'un réseau inconnu, définissez des contrôles spécifiques qui soit exigent de l'utilisateur qu'il fournisse une **authentification multifacteur** (MFA), soit bloquent complètement l'accès. Vous pouvez également appliquer des politiques à des groupes d'utilisateurs.

Application

Élaborez une politique qui définit les conditions d'accès à une application en fonction de la sensibilité que vous spécifiez. Par exemple, vous pouvez bloquer l'accès à une application à partir d'emplacements inconnus, ou exiger une authentification multifacteur (MFA) pour une application, soit lors de chaque accès à cette application, soit en fonction de l'emplacement à partir duquel l'accès s'effectue. Vous pouvez appliquer ces politiques à n'importe quelle application dans le cloud (SaaS) ou sur site protégée par Azure Active Directory, y compris pour sa clientèle étendue, mobile ou basée sur un navigateur.

Risque

Évaluez les risques en temps réel. Dans le graphique de sécurité intelligent de Microsoft, l'apprentissage automatique exploite des milliards de signaux quotidiens, est capable de **détecter les comportements suspects** et applique un accès conditionnel basé sur les risques qui protège vos applications et vos données d'entreprise stratégiques en temps réel. Lorsque les conditions changent, cela déclenche des contrôles qui autorisent ou bloquent les utilisateurs, ou encore exigent d'eux l'utilisation de l'authentification multifacteur, l'inscription de leur appareil ou un changement de mot de passe.

Section 2

Gestion mobile

Une fois que vous avez activé un accès sécurisé et géré, l'étape suivante consiste à protéger vos données. Les applications, telles que vos applications Office Mobile, représentent le point d'accès le plus probable à vos ressources d'entreprise, une sorte de « porte d'entrée » donnant accès à votre environnement et à ses données. Cela fait de la gestion des applications un aspect essentiel de votre stratégie de sécurité, surtout au vu de la complexité et du nombre d'appareils, applications, préférences et comportements des utilisateurs. Grâce à EMS, vous pouvez gérer les données au sein des applications Office Mobile, ainsi qu'au sein de vos applications métier et tierces. **Des solutions souples pour la gestion mobile** vous permettent de décider exactement de ce qu'il advient de vos données une fois l'accès avéré.

Protégez les applications avec ou sans inscription des appareils

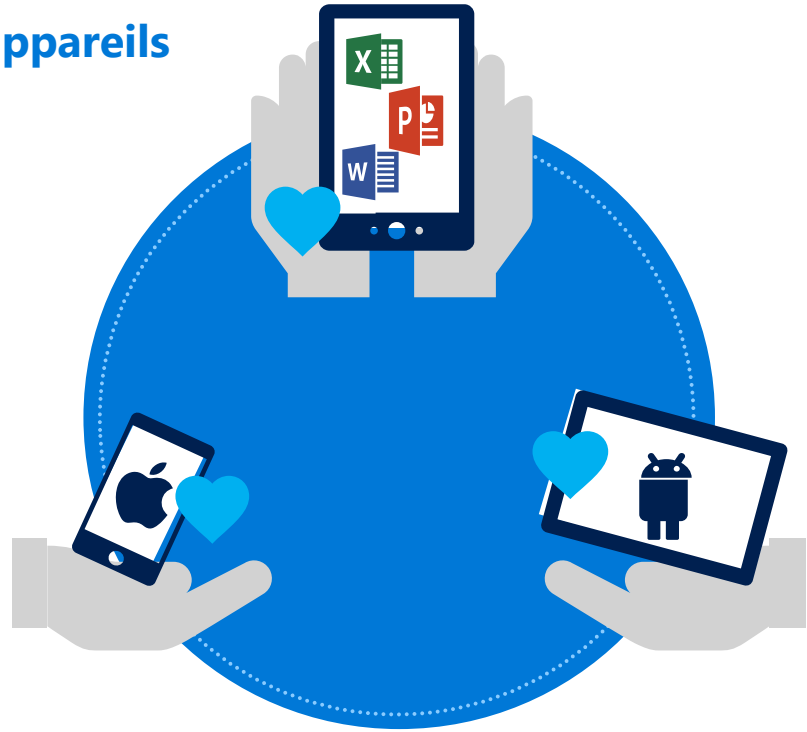
En sus de la complexité de votre main-d'œuvre, votre cercle de collaboration s'étend au-delà de votre propre entreprise pour inclure d'autres partenaires commerciaux et sous-traitants. Les nuances de votre écosystème mobile peuvent exiger une certaine souplesse en matière de gestion des appareils et des applications. Dans ce domaine, EMS vous donne le choix.

Vous pouvez bénéficier de capacités de gestion complètes des appareils appartenant à l'entreprise ou aux utilisateurs par l'intermédiaire de l'inscription à la **gestion des appareils mobiles (MDM) avec EMS**. Une fois un appareil inscrit, le service informatique peut définir et appliquer la conformité aux politiques de sécurité, automatiquement livrer des applications, définir des restrictions des fonctionnalités couper/copier/coller/enregistrer sous, détecter des attaques de type jailbreak, appliquer des exigences relatives aux codes PIN et supprimer à distance des données protégées sur n'importe lequel de vos appareils ou applications gérés par EMS.

Dans certaines situations, il est nécessaire de fournir aux utilisateurs l'accès aux ressources d'entreprise à partir d'appareils qu'il est impossible ou déconseillé d'inscrire à la gestion des appareils mobiles (MDM). La gestion des politiques d'application sans passer par l'inscription à la gestion des appareils mobiles (MDM) vous donne, ainsi qu'à vos utilisateurs, la souplesse nécessaire pour déployer des applications Office Mobile sur les appareils de types iOS, Android et Windows **sans exiger une inscription via EMS**. Vous pouvez également utiliser une solution de gestion des appareils mobiles (MDM) externe à Microsoft. Dans ce cas, vous pouvez choisir d'utiliser votre solution actuelle de gestion des appareils mobiles (MDM) ou décider de vous passer de ce type de gestion tout en continuant de protéger l'accès à Office 365 et aux données de votre entreprise.

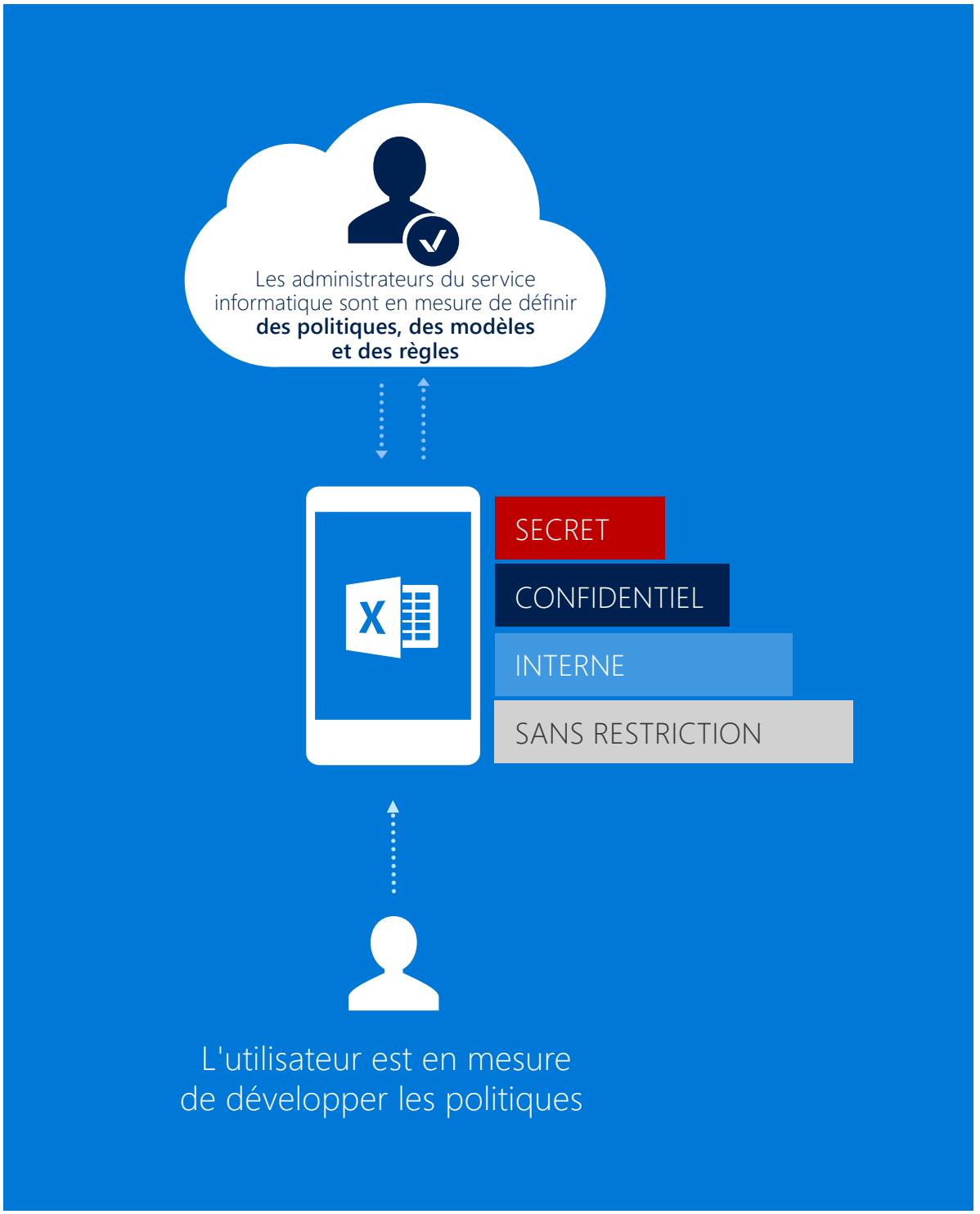
Les politiques de protection des applications EMS protègent vos données au niveau des applications sans nécessiter l'inscription d'aucun appareil. Les capacités de sécurité incluent le chiffrement des applications au repos, le contrôle d'accès aux applications exigeant un code PIN ou des informations d'identification, une navigation sur le Web sécurisée et un affichage sécurisé des fichiers PDF, des images et des vidéos. Même sans recourir à l'inscription d'appareils, vous pouvez toujours définir des restrictions des fonctions couper/copier/coller/enregistrer sous et une suppression sélective au niveau des applications lorsque cela est nécessaire.

Vous disposerez d'une visibilité et d'un contrôle complets de vos applications métier et d'un ensemble sans cesse croissant d'applications tierces auxquelles vos utilisateurs accèdent à partir d'une grande variété d'appareils. EMS ajoute une gestion détaillée des applications de sorte que le service informatique puisse apporter un équilibre parfait entre productivité et protection, pour ouvrir la voie à une collaboration sécurisée.



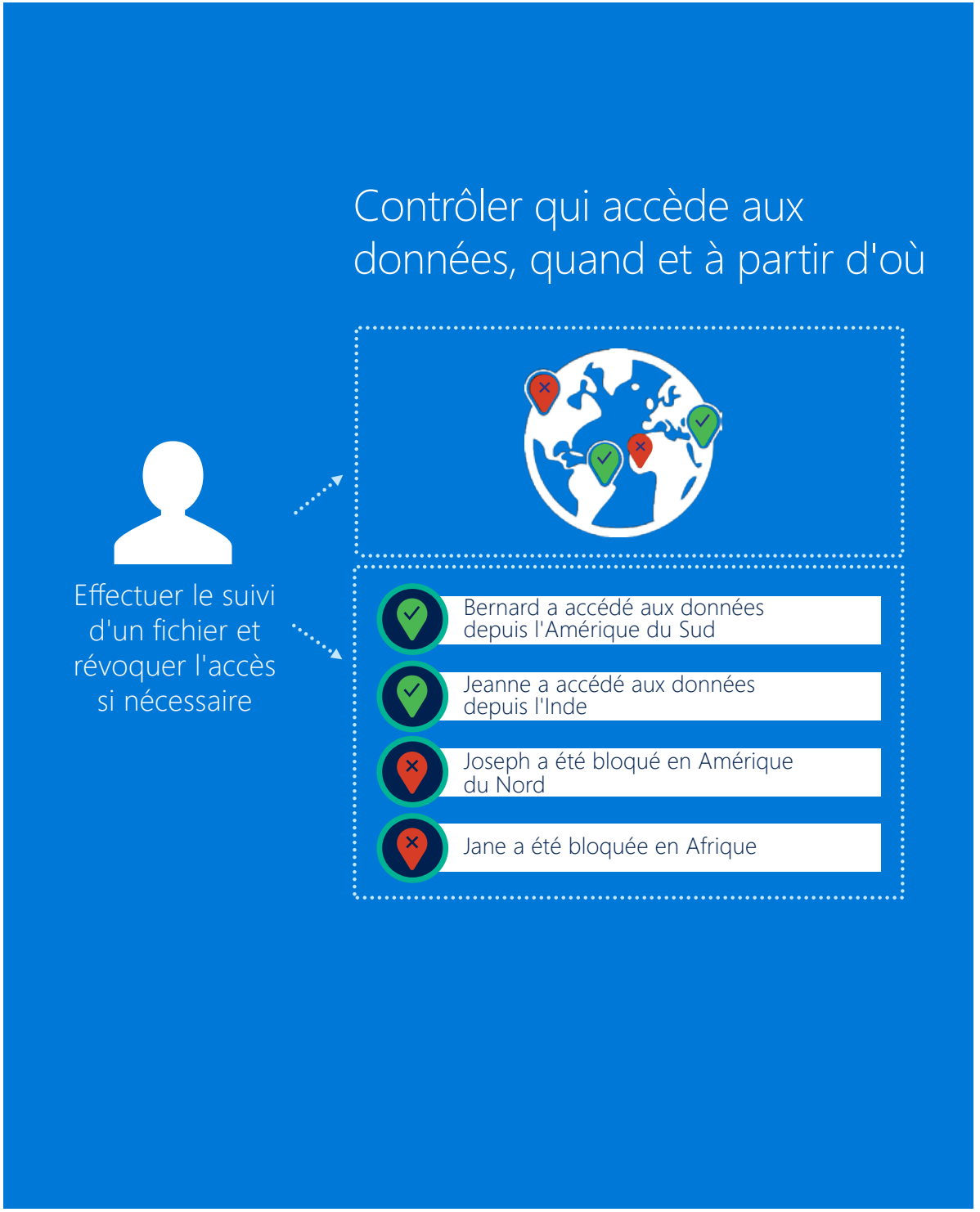
Étendez la gestion des droits dans Office 365 pour la collaboration

Vos utilisateurs peuvent appliquer une protection en continu en matière de gestion des droits aux fichiers Office via Office 365 afin que les données soient protégées lorsqu'elles sont partagées. **EMS étend la protection en continu des données** à tout type de fichier afin que vos utilisateurs puissent collaborer en toute sécurité au sein et en dehors de votre entreprise. Pour bénéficier des plus grands avantages de la protection au niveau des fichiers, EMS inclut une classification automatique des données basée sur la sensibilité, ce qui permet de protéger vos données d'éventuelles vulnérabilités provenant d'incohérences de classification. Vous pouvez définir des politiques qui classent et étiquettent automatiquement les données au moment de la création ou de la modification, en fonction de la source, du contexte et du contenu lui-même.



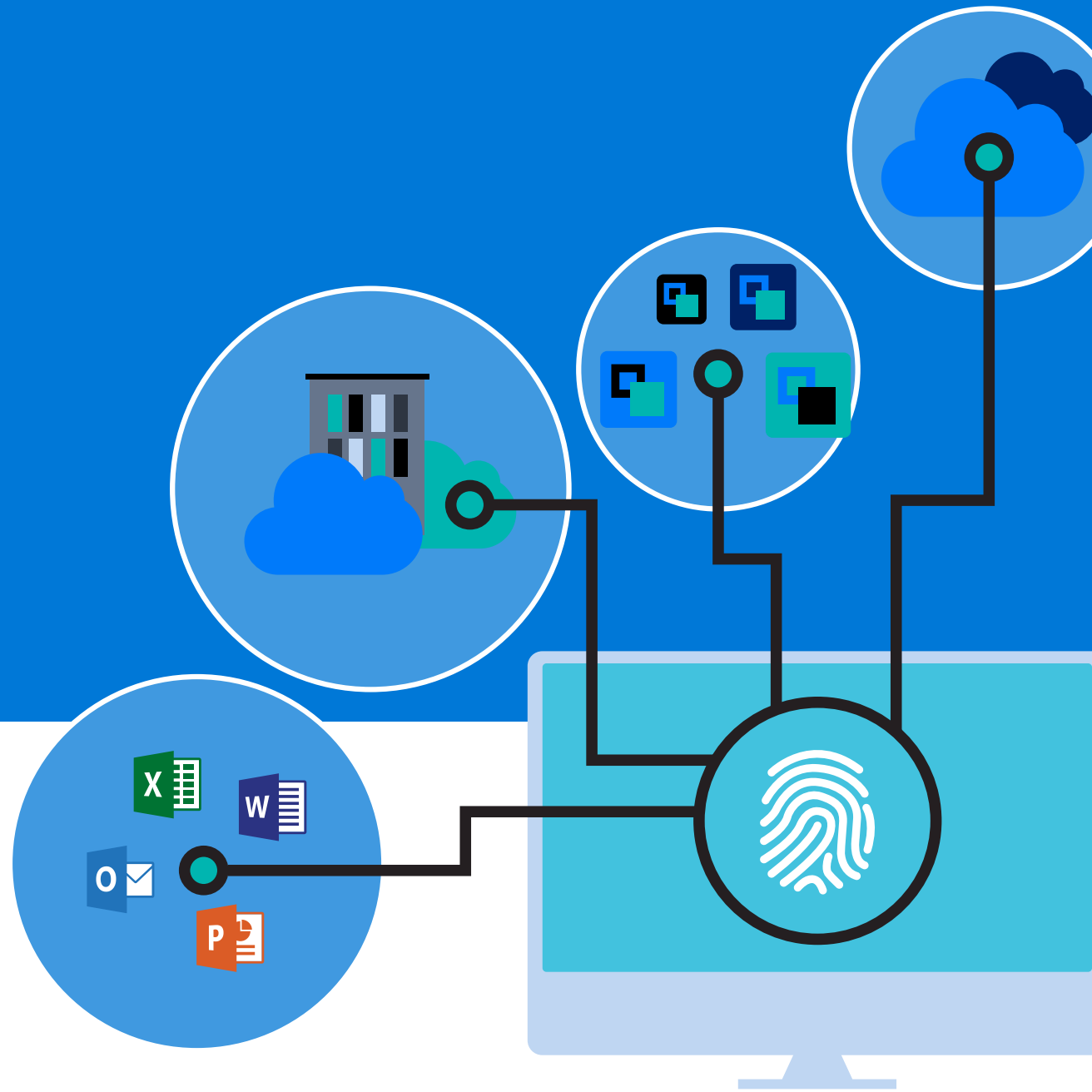
Gérez la collaboration avec le suivi des fichiers et la révocation

Pour encore davantage de **visibilité et de contrôle sur la collaboration interne et externe**, vous pouvez surveiller les fichiers partagés et réagir à d'éventuelles fuites via EMS. Le service informatique et les utilisateurs peuvent effectuer le suivi des fichiers partagés de sorte à surveiller l'activité en fonction des collaborateurs autorisés, révoquer l'accès si nécessaire et réviser la classification. Votre équipe informatique peut utiliser des fichiers journaux et des rapports efficaces sur les fichiers partagés afin de contrôler, analyser et exploiter les données. Grâce à la protection en continu des informations via EMS, vous pouvez mettre en œuvre une collaboration sécurisée pour n'importe quel fichier, sur n'importe quel appareil, à partir de n'importe quel emplacement.



Section 3

Sécurité avancée



Office 365 offre une productivité sans compromis, n'importe où et à n'importe quel moment. L'ajout de l'accès sécurisé et de la gestion mobile via EMS contribue à renforcer l'infrastructure qui vous aidera à protéger votre entreprise à la fois sur site et dans le cloud. EMS utilise **les identités gérées et protégées en tant que clé de voûte de la sécurité avancée** qui permet de détecter les menaces internes grâce à une analyse comportementale et à des technologies de détection d'anomalies de pointe. Grâce à EMS, vous pouvez découvrir toute activité suspecte et identifier précisément les menaces sur l'ensemble de votre écosystème sur site et dans le cloud.

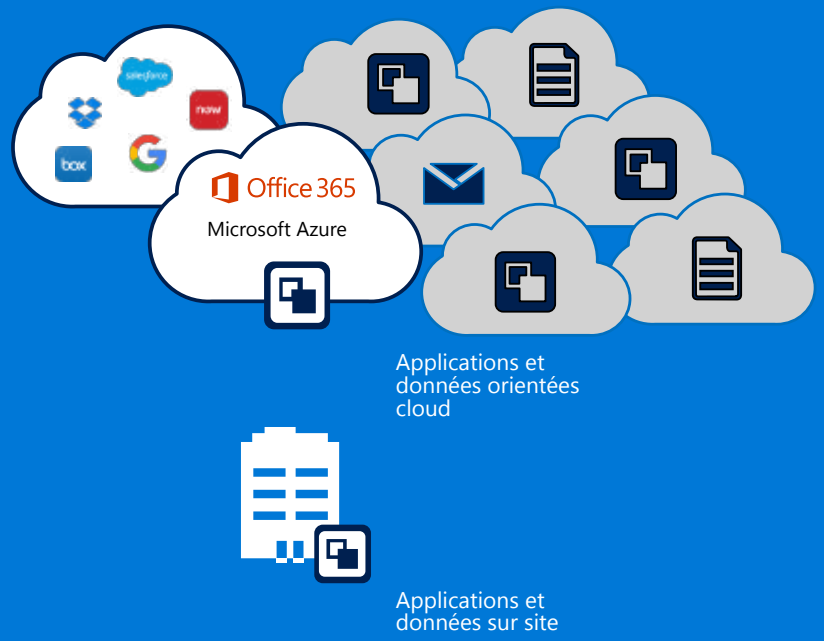
Advanced Threat Analytics

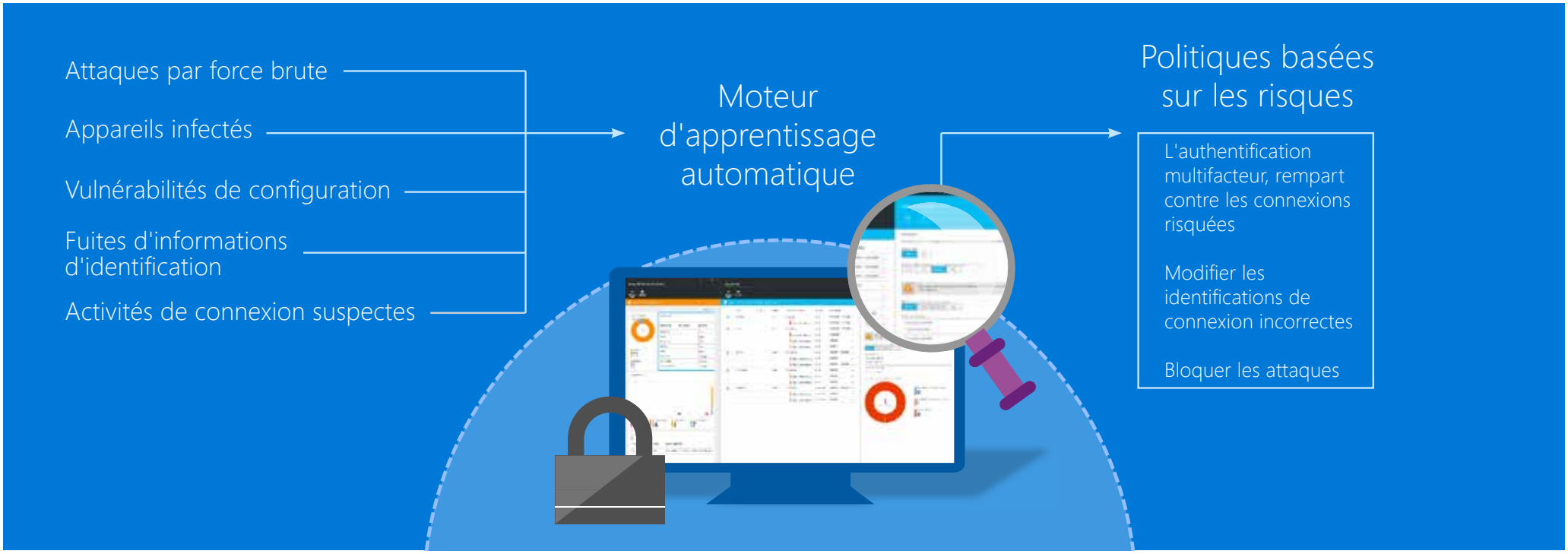
Par l'intermédiaire de l'apprentissage automatique et des journaux d'événements, **EMS identifie les menaces avancées persistantes** sur site et détecte les attaques malveillantes connues presque instantanément dès qu'elles surviennent. Grâce à des informations claires et pertinentes fournies par l'intermédiaire d'une

Développez Office 365 Advanced Security Management avec Cloud App Security

Votre investissement Office 365 vous fournit une excellente base pour la sécurisation de vos applications Office Mobile contre les menaces basées sur le cloud. Pour mettre en œuvre une sécurité complète des applications cloud qui préserve l'ensemble de vos applications, EMS inclut une grande efficacité en matière de visibilité, de détection des menaces, de prévention des attaques et une détection approfondie de l'informatique fantôme. Vous pouvez surveiller le comportement des utilisateurs et les caractéristiques des flux de données pour bénéficier d'un aperçu détaillé de la façon dont vos utilisateurs travaillent avec les applications orientées cloud. **Les capacités de sécurité d'EMS en matière d'applications cloud** s'associent également à vos mécanismes d'intervention existants afin que vous puissiez continuer à développer vos investissements actuels.

Efficacité en matière de visibilité, de détection des menaces, de prévention des attaques et détection approfondie de l'informatique fantôme





Surveillez, évaluez et prenez des décisions basées sur les estimations des risques en temps réel

Avec Office 365 et EMS, vous pouvez adopter des **mesures de sécurité plus éclairées, souples et complètes** en ce qui concerne le paysage complexe et en constante évolution de la sécurité des identités. Même les attaques les plus sophistiquées laissent derrière elles des traces qui forment des motifs détectables. Chaque mois, Microsoft traite un volume prodigieux de tels signaux. En outre, nous mettons à jour plus d'un milliard de PC, traitons plus de 450 milliards d'authentifications et analysons plus de 200 milliards de courriers électroniques, à la recherche de logiciels malveillants et de sites Web suspects.

Les systèmes Microsoft de renseignements sur les menaces observent quasiment tous les types d'attaques et dirigent les données collectées directement vers notre **graphique de sécurité intelligent Microsoft**.

Le graphique de sécurité intelligent rassemble les données de télémétrie et les signaux des centaines de services cloud gérés par Microsoft, les résultats de recherches exhaustives menées en continu qui identifient les vecteurs d'attaque émergents et les logiciels malveillants, ainsi que les données provenant de partenariats avec les leaders du secteur et les organismes responsables de l'application de la loi. Nous appliquons l'apprentissage automatique et l'analyse de données afin d'identifier les activités anormales et suspectes qui caractérisent les attaques avancées et persistantes. Le graphique permet à Microsoft de fournir des recommandations et des actions automatisées qui aident à se prémunir contre les attaques et à les contrer. En fonction des données recueillies, nous calculons et attribuons un niveau de risque (faible, moyen ou élevé) à chaque activité de connexion et à chaque compte utilisateur. Nous attribuons également un score de risque aux éventuelles vulnérabilités de configuration, comme des administrateurs dotés d'options d'authentification faibles, ou l'absence d'une configuration initiale d'authentification multifacteur pour les utilisateurs finaux.

À travers Office 365 et EMS, le graphique de sécurité intelligent Microsoft fait partie de votre stratégie de sécurité avancée.

Élaborez une stratégie efficace pour votre entreprise

Votre transformation numérique est en marche. Le déploiement d'Office 365 peut être l'une des premières étapes effectuées par votre entreprise vers sa transformation. Poursuivez ce développement en vous appuyant sur les capacités de gestion et de sécurité Office 365, afin d'avancer dans cette voie avec une confiance accrue. Tandis que vous mettez en œuvre le déploiement Office 365 et Enterprise Mobility + Security dans l'ensemble de votre entreprise, commencez à envisager un portefeuille étendu d'applications SaaS, tout en élargissant votre cercle de collaboration au sein et en dehors de votre entreprise.

Évaluez votre stratégie de mobilité

Évaluez votre contexte de mobilité grâce à l'**évaluation EMS**, permettant d'identifier les points forts et de découvrir les lacunes cachées dans votre stratégie de mobilité en entreprise.

Outil d'évaluation

Essayez EMS avec votre déploiement Office 365 gratuitement dès aujourd'hui

En savoir plus sur les solutions **Enterprise Mobility + Security** et les façons dont votre entreprise peut exploiter votre investissement Office 365 initial.

Explorez les solutions Microsoft pour **gérer la productivité mobile.**

Préservez vos ressources d'entreprise en gérant les accès avec **la sécurité basée sur les identités.**

Commencez votre **essai gratuit** et bénéficiez d'**instructions de déploiement détaillées.**

Commencez dès aujourd'hui !

Activez **l'accès conditionnel** et sécurisez les données d'entreprise tout en permettant aux collaborateurs d'être productifs sur n'importe quel appareil.

Maximisez la productivité des collaborateurs en leur donnant accès aux ressources d'entreprise sur leurs applications mobiles Office 365 préférées. Configurez une **politique de protection des applications** à partir de votre console de gestion Office 365.

Protégez vos applications Web sur site grâce à un **accès à distance sécurisé.**

Avantages d'EMS pour les clients Office 365

	Gestion des identités et des accès	Sécurité basée sur les identités	Productivité mobile gérée	Protection des informations
Enterprise Mobility + Security	**Azure Active Directory** • Accès conditionnel basé sur les risques • Rapports de sécurité avancés • Authentification unique pour toutes les applications • Authentification multifacteur (MFA) avancée • Groupes dynamiques, attribution de licences basée sur les groupes • Gestion des identités dotées de privilèges	**Cloud App Security** • Visibilité et contrôle pour toutes les applications orientées cloud **Advanced Threat Analytics** • Identifier les menaces avancées sur les identités en local	**Intune** • Gestion des applications mobiles • Gestion des utilisateurs en libre-service • Fourniture de certificat • Gestion des ordinateurs	**Azure Information Protection** • Classification intelligente et étiquetage des données automatisées • Suivi et notifications pour les documents partagés • Protection des partages de fichiers Windows Server en local
Office 365	**Gestion des identités de base via Active Directory Azure pour Office 365 :** • Authentification unique pour Office 365 • Authentification multifacteur (MFA) de base pour Office 365	**Advanced Security Management** • Aperçu des activités suspectes dans Office 365	**Gestion de base des appareils mobiles via MDM pour Office 365** • Gestion des paramètres des appareils • Effacement sélectif • Intégration à la console de gestion Office 365	**Protection RMS via RMS pour Office 365** • Protection du contenu stocké dans Office (sur site ou Office 365) • Accès au kit de développement logiciel RMS • Apportez votre propre clé

3T TECHNOLOGY TRANSFER & TRAINING SA

ET MICROSOFT

VOTRE PARTENAIRE MICROSOFT EMS

3T Technology Transfer & Training

Vous manifestez un intérêt pour EMS ? Contactez-nous:

3T Technology Transfer & Training

Email: ttt@ttt.ch

Tél: +41 (0)22 994 90 90

Adresse: Av. du Mont-Blanc 31, 1196 Gland

www.ttt.ch