jamf

LIVRE BLANC

Accès Conditionnel: Protéger au-delà du périmètre de sécurité traditionnel

L'espace de travail moderne et la sécurité nouvelle génération

Depuis des décennies, les entreprises érigent des «murs » autour de leurs locaux et utilisent le périmètre de leur réseau comme première ligne de défense. Mais aujourd'hui, les espaces de travail sont plus fluides et les périmètres de sécurité ont évolué. Il arrive que créer un réseau et le protéger à l'aide d'un pare-feu ne soit plus suffisant. Il est grand temps de repenser le modèle de sécurité traditionnel basé sur le périmètre.

Le temps où les employés arrivaient à 9 h pour repartir à 17 h est révolu. À présent, les employés ne sont plus au bureau du lundi au vendredi.

Ils travaillent à domicile, dans les cafés, dans les halls d'hôtel ou sur divers sites de travail, selon des horaires qui leur conviennent. Face à ces situations, ils auront non seulement besoin d'accéder aux données de l'entreprise, mais aussi d'y accéder en dehors des horaires traditionnels de bureau.

Le nouvel « espace de travail » est une notion fluide, les employés ont désormais besoin d'utiliser des outils et de consommer des données sur plusieurs appareils, à partir de différentes apps et depuis une multitude d'endroits.

C'est là que le cloud entre en jeu.

Les services de cloud protégés par pare-feu constituent le fondement de ce nouvel environnement centré autour de l'employé. De plus, ces services offrent un meilleur accès aux données, car ils permettent aux utilisateurs de se connecter au site ou à l'app qu'ils souhaitent depuis tout type d'appareil pour consulter les informations dont ils ont besoin. Et avec les services de cloud modernes, les entreprises peuvent automatiser leurs opérations pour un coût bien inférieur à ce qu'il était auparavant.

La modification des espaces de travail et l'utilisation de plus en plus répandue du cloud ne sont pas de simples passades, comme l'a expliqué Vladimir Petrosyan, Senior Product Manager de Microsoft lors de sa présentation à la Jamf Nation User Conference de 2017:

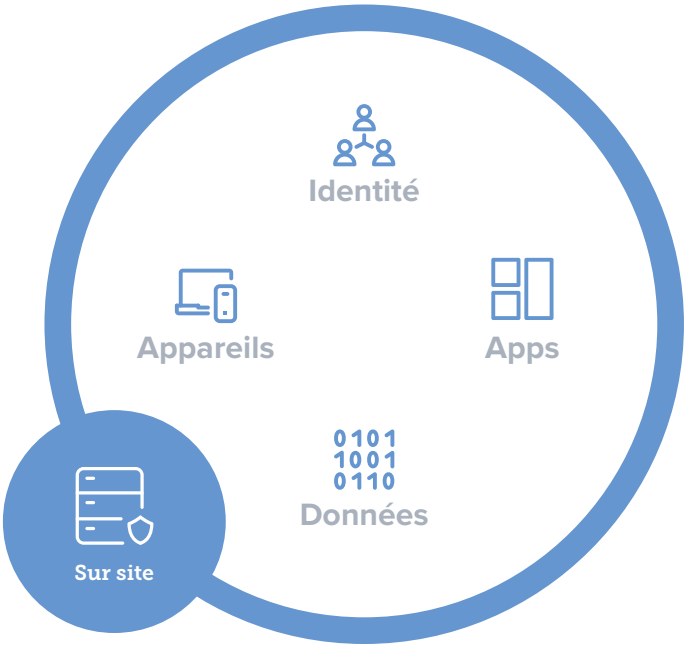
- **85 %** des entreprises conservent des données sensibles dans leur cloud
- **80 %** des employés utilisent des apps SaaS qui ne sont pas approuvées pour l'usage professionnel
- **41 %** des employés estiment que les apps mobiles professionnelles transforment leurs méthodes de travail

Les entreprises étant de plus en plus nombreuses à vouloir s'adapter à l'évolution d'un environnement de travail auparavant dominé par les « shadow IT », il devient crucial de moderniser les paramètres de sécurité et leurs modes de protection des utilisateurs, des appareils et des apps. Bon nombre d'apps et de services essentiels dépendent toujours des infrastructures et des serveurs sur site. Parallèlement à cela, les contenus, plates-formes de collaboration, suites bureautiques dans le cloud et l'utilisation d'appareils mobiles stockant les données en externe favorisent l'utilisation croissante d'outils dans le cloud au sein des entreprises. Dans l'état actuel des choses, les employés travaillent en dehors de la protection du pare-feu, et la plupart des applications et des données auxquelles ils accèdent sont stockées dans le cloud. En outre, nombreux sont ceux qui essayent d'accéder aux ressources de leur entreprise depuis leur appareil personnel. Les entreprises sont aussi de plus en plus nombreuses à commencer à déplacer leur infrastructure vers le cloud, et à souhaiter un accès plus sécurisé à leurs services. Elles recherchent donc des méthodes modernes et plus efficaces pour garantir leur conformité et leur sécurité.

Il s'agit de trouver un équilibre entre donner les moyens aux utilisateurs d'améliorer leur productivité et garantir la sécurité des données de l'entreprise.

LA MODERNISATION DE LA SÉCURITÉ DANS LES ENTREPRISES D'AUJOURD'HUI

Le périmètre de sécurité a changé. La méthode consistant à créer un réseau et à le protéger avec un pare-feu n'est plus aussi pertinente, car les appareils et les données ne sont plus hébergés sur site. Les appareils sont utilisés dans le monde



Modèle de sécurité traditionnel

entier et peuvent directement se connecter aux services dans le cloud, aux applications de messagerie et à d'autres ressources sensibles des entreprises, à tout moment.

Vous pouvez voir ci-dessus un exemple de modèle de sécurité traditionnel, comportant des périmètres de sécurité en aval du pare-feu.

Mais cela ne représente qu'une part infime des contenus auxquels les employés et leurs appareils peuvent maintenant accéder. Le stockage dans le cloud, les apps de productivité et l'utilisation de plusieurs appareils en dehors de la protection du pare-feu sont désormais monnaie courante. Étant donné la nature ouverte du modèle maintenant en vigueur, nous pouvons facilement constater la vulnérabilité à laquelle les entreprises

Modèle de sécurité moderne

s'exposeraient en continuant à appliquer un modèle de sécurité basé sur le périmètre.

Les entreprises ne peuvent plus avoir recours aux outils de gestion des identités internes pour fournir l'accès aux services, car les appareils et les ressources dont ont besoin les utilisateurs sont majoritairement déplacés vers le cloud. Pour atténuer les vulnérabilités potentielles et garantir la productivité des employés, où qu'ils travaillent, il faut repenser le modèle de sécurité traditionnel basé sur le périmètre. L'identité doit désormais être accessible depuis le monde entier, et aussi flexible que les services dans le cloud utilisés.

APPAREIL ET ACCÈS : NIVEAUX DE SÉCURITÉ

Trois facteurs contribuent à la sécurité et à l'authentification. Tous ont leurs avantages et leurs inconvénients:

- Sécurité basée sur l'appareil
- Sécurité basée sur l'utilisateur
- Authentification multifacteur

Sécurité basée sur l'appareil

Cette méthode de sécurité s'applique aux appareils d'entreprise gérés ou aux appareils gérés qui ne sont pas conformes aux règles de sécurité de l'entreprise. Son inconvénient est qu'elle ne permet pas de protéger l'appareil si une personne malveillante capte les identifiants par hameçonnage ou en les devinant. En outre, si l'appareil n'est pas géré, ce qui est assez courant, il n'est ni sécurisé, ni conforme aux normes établies par l'entreprise.

Sécurité basée sur l'utilisateur

Ce niveau de sécurité s'applique aux appareils nécessitant de se connecter avec un nom d'utilisateur et un code d'accès. Toutefois, si un appareil ou un ordinateur non géré ayant accès aux services et aux ressources de l'entreprise est perdu ou volé, ou bien si les identifiants de connexion d'un utilisateur sont récupérés par une personne malveillante, c'est la sécurité de tout le réseau qui est compromise.

Authentification multifacteur

L'authentification multifacteur est un niveau de sécurité consistant à fournir à l'utilisateur un accès à l'appareil et aux ressources de l'entreprise uniquement s'il est en mesure de confirmer son identité en plusieurs étapes. Exemples d'informations permettant de confirmer l'identité:

- Un élément que vous connaissez (mot de passe)
- Un élément dont vous disposez (jeton de sécurité)
- Une preuve d'identité (empreinte digitale)

En demandant un nom d'utilisateur ou un code, ainsi qu'une deuxième méthode d'authentification physique (par exemple, un jeton RSA), les entreprises pensent appliquer un processus de sécurité infaillible. Cependant, il leur manque encore des outils qui leur permettraient d'exploiter la grande variété de contextes dans lesquels peuvent se trouver les appareils, ainsi que des moyens permettant de garantir la sécurité par rapport aux nombreux cas d'utilisation, utilisateurs et emplacements qui découlent des nouvelles méthodes de travail.

Pour résumer, nous pouvons dire que choisir entre l'identification sécurisée et l'authentification physique ne suffit pas toujours. Les entreprises doivent mettre en place ces deux méthodes, et éventuellement les compléter, sans compromettre l'expérience utilisateur.

UN NOUVEAU PÉRIMÈTRE : L'IDENTITÉ

Centrify, Duo Security, Microsoft, Ping Identity, Okta, Sailpoint et Salesforce comptent parmi les nombreux fournisseurs à s'être récemment positionnés sur le marché de la gestion des identités et de l'accès aux services. La plupart des outils qu'ils proposent ne nécessitent pas d'avoir une infrastructure d'authentification existante, comme Active Directory, et étendent ces identités aux services dans le cloud à l'aide de protocoles tels qu'Oauth, SAML et OpenID.

L'identité est le point commun entre tous les appareils d'un utilisateur, et s'applique au-delà de la sécurité basée sur l'utilisateur, l'appareil ou le jeton. Prendre en compte la gestion des identités dans votre processus de gestion de la sécurité est essentiel pour créer un environnement sécurisé au sein d'un univers mobile basé sur le cloud.

« Les attaques auxquelles nous sommes confrontés, leur niveau

de sophistication et la vitesse à laquelle elles se propagent sont tels que l'esprit et la main de l'homme ne sont pas capables de les résoudre seuls », explique Brad Anderson, vice-président de Microsoft.

Les entreprises doivent disposer d'un ensemble de fonctionnalités qui les aident à comprendre les risques relatifs à l'identité, aux appareils et aux applications. À terme, elles devront pouvoir garantir que leurs données ne soient accessibles que par des utilisateurs de confiance, à partir d'applications fiables installées sur des appareils fiables.

> Pour en savoir plus sur EMS rendez vous sur: https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security

Microsoft utilise la sécurité basée sur l'identité pour vérifier les identifiants avec Azure Active Directory (AD) lorsqu'un utilisateur tente d'accéder à Microsoft Office 365. Brad Anderson affirme que cette vérification d'identité est répétée 15 milliards de fois chaque jour.

Active Directory est la source de référence de plus de 90 % des services mondiaux pour la vérification des identités sur site. Pour la plupart d'entre elles, Azure AD est la source de référence pour ce qui est de la vérification des identités dans le cloud. Tous les produits conçus par Microsoft s'appuient sur Azure AD dans le cloud de Microsoft.

UNE SOLUTION AUX FAILLES DE SÉCURITÉ

Pendant la Jamf Nation User Conference de 2017, Brad Anderson a proposé une nouvelle solution pour combler les défauts de sécurité des systèmes actuels.

« Jamf Pro utilise la fonctionnalité "Microsoft Workplace Join" intégrée à Azure Active Directory pour connecter les Mac enrôlés via Jamf au reste des appareils, qu'ils appartiennent à l'entreprise ou aux utilisateurs. Une fois le processus Workplace Join effectué, Intune peut créer des rapports sur eux de la même manière qu'il en crée sur les appareils enrôlés via Intune. » Il a ensuite précisé : « Cela signifie que les entreprises peuvent donner l'accès à leurs ressources sur la base non seulement des identifiants de l'utilisateur, mais aussi de la conformité du Mac. C'est ce que nous appelons l'accès conditionnel. » Jamf Pro, la solution la plus utilisée pour la gestion d'appareils Apple, peut appliquer des règles aux appareils afin de leur donner accès à Office 365, en tirant profit de l'accès conditionnel d'EMS. Les Mac gérés par Jamf accèdent désormais au cloud de Microsoft via Workplace Join, sous réserve qu'ils répondent aux règles de conformité des appareils d'Intune, qui peuvent être adaptées aux besoins de toutes les entreprises. Une fois les données de l'ordinateur transférées dans le cloud, Microsoft Intune et Enterprise Mobility + Security (EMS) peuvent s'intégrer totalement à Jamf pour gérer ces appareils.

Si un Mac non géré demande accès aux e-mails ou à d'autres services dans le cloud, le service informatique peut autoriser une procédure d'enrôlement par l'utilisateur depuis Jamf Pro, et vérifier que les appareils non sécurisés ou non gérés passent sous gestion avant de leur accorder l'accès.

Les règles applicables au Mac, comme les conditions requises en matière de mot de passe, peuvent être définies avec Intune. Le service informatique peut alors les appliquer à l'intégralité du système. La collaboration entre Jamf et Microsoft est unique en ce qu'elle permet d'étendre les possibilités offertes par la structure de gestion des appareils mobiles (MDM) d'Apple, en donnant accès à des outils locaux. Un administrateur peut par exemple créer un profil de configuration qui applique les mots de passe et valide leur complexité. Cela permet de faire coïncider les règles de l'entreprise avec les capacités immédiatement accessibles, à travers des options pour le Mac provenant d'une solution MDM traditionnelle.

Lorsque Microsoft vérifie les identifiants de l'utilisateur et Jamf ceux de l'appareil, une analyse des risques relatifs à l'utilisateur, à l'appareil (est-il ou non conforme aux règles de l'entreprise) et à l'application (quelle app est utilisée) est exécutée en temps réel, afin de déterminer si l'accès aux ressources stockées dans le cloud doit être accordé ou refusé.

Lorsque l'authentification multifacteur s'avère insuffisante du fait qu'elle s'attache principalement à l'utilisateur, cette nouvelle méthode étend la vérification à la manière dont ce dernier interagit avec les informations. Ainsi, l'identité de confiance correspond à un utilisateur authentifié sur un appareil conforme.

Désormais, les entreprises disposent d'une authentification multifacteur étendue par le biais d'une vérification de la conformité : 1) nom d'utilisateur et mot de passe, 2) code et jeton et 3) conformité de l'appareil. De plus, les entreprises peuvent maintenant fournir l'accès approprié, de manière contextuelle et dynamique, en se basant l'utilisateur, l'appareil et le contexte du cas d'utilisation, offrant par là même le périmètre adaptatif et flexible nécessaire aux employés modernes, qui utilisent plusieurs appareils et se connectent depuis différents endroits.

ACCÈS CONDITIONNEL SANS PROXY

L'Accès conditionnel d'EMS est un élément essentiel de ce niveau de sécurité. C'est aussi lui qui donne la possibilité de vérifier automatiquement tout risque potentiel associé à l'identité, à l'appareil et à l'application.

Le service informatique est donc en mesure de définir les conditions dans lesquelles les utilisateurs pourront accéder à vos ressources.

La plupart des fournisseurs de solutions de gestion de la mobilité en entreprise (EMM) disposent de solutions prenant en charge l'accès conditionnel à travers un serveur proxy afin de permettre aux appareils distants de s'authentifier pour accéder aux ressources stockées dans le périmètre du réseau de l'entreprise. Un serveur proxy est un serveur qui sert d'intermédiaire pour traiter les requêtes des utilisateurs lorsqu'ils cherchent des ressources stockées sur d'autres serveurs. Il peut s'agir de trafic entrant sur un réseau, ou en sortant. La collaboration entre Jamf et Microsoft élimine le besoin de proxy. Grâce à ce partenariat, tout est directement intégré à Azure Active Directory, qui devient la source unique d'informations. La conformité des appareils devient un attribut pouvant servir de prérequis pour se voir autoriser l'accès à divers services. Cela signifie qu'il n'existe aucun intermédiaire (par exemple, un serveur proxy) nécessitant une configuration réseau pour déterminer l'accès ou faire office de nouvel élément d'infrastructure réseau dont il faudra assurer la maintenance. Cela permet d'intégrer une procédure d'authentification enrichie directement à Azure Active Directory et à Intune, tout en éliminant un point de défaillance éventuel.

Les entreprises ont reconnu et pris en compte le taux d'adoption rapide des Mac. C'est la raison pour laquelle elles exigent une solution capable d'assurer leur sécurité au-delà du périmètre habituel, comme pour leurs autres appareils. En d'autres termes, avant de pouvoir faire confiance à un utilisateur, c'est l'appareil sur lequel il s'identifie qui doit être validé.

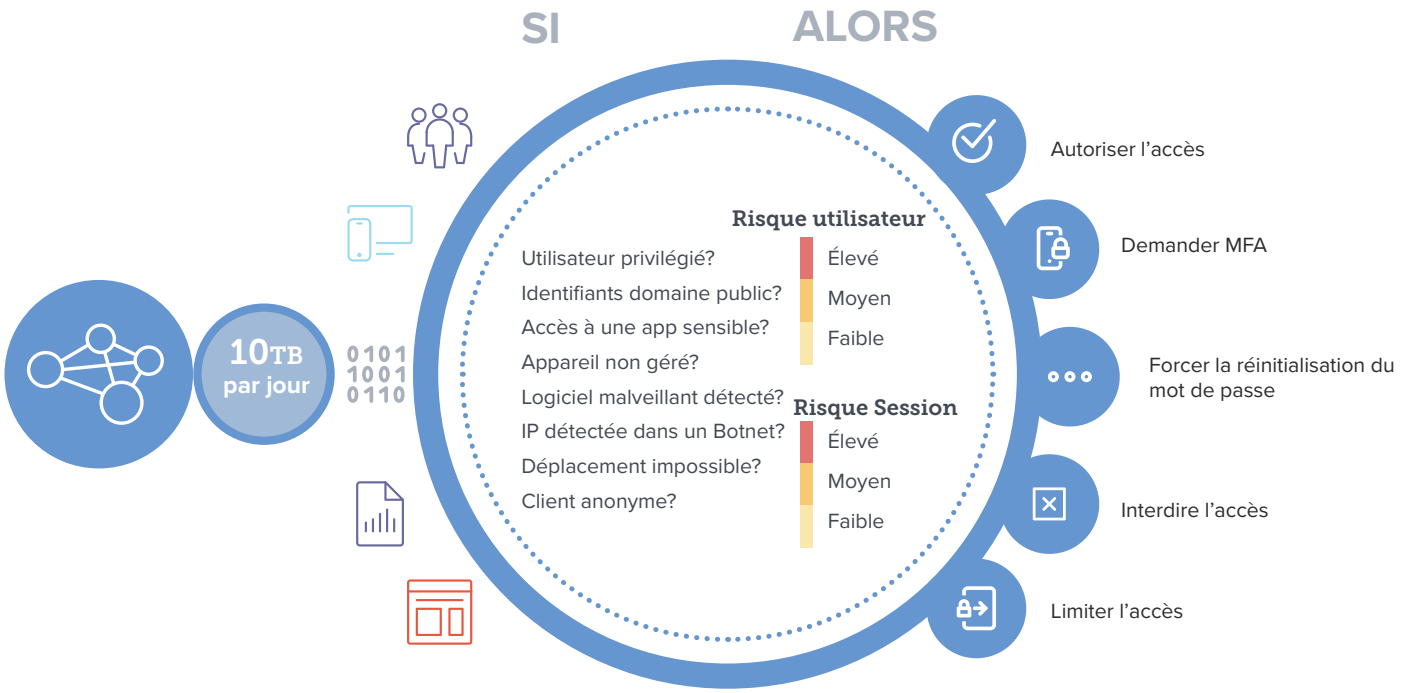
Microsoft et Jamf ont collaboré pour mettre au point une solution conçue dans ce sens. Elle s'intègre totalement aux technologies d'Azure Active Directory et d'Intune afin de garder intacte l'expérience utilisateur native et tire profit des points forts de Jamf et d'Intune. Il en résulte une solution bien plus performante que ce que l'une ou l'autre entreprise seule pourrait créer.

PARTENERIAT MICROSOFT ET JAMF

Le partenariat entre Jamf et Microsoft EMS a donné naissance à une solution automatisée de gestion de la conformité pour les ordinateurs Mac qui accèdent à des applications configurées avec l'authentification Azure AD. Cette collaboration tire parti de l'accès conditionnel pour garantir que seuls les utilisateurs de confiance, qui travaillent sur des appareils conformes dotés d'apps approuvées peuvent accéder aux données de l'entreprise.

Ensemble, Jamf et EMS empêchent les utilisateurs non autorisés d'utiliser un appareil pour accéder à des ressources spécifiques fournies par l'entreprise. Il peut s'agir d'appareils personnels, non gérés ou d'appareils d'entreprise gérés qui ne sont pas conformes aux règles de sécurité, et donc plus vulnérables aux tentatives frauduleuses d'accès aux données de l'entreprise. Pour cela, ils imposent à l'utilisateur d'enregistrer les appareils dont il souhaite se servir pour accéder à Microsoft Office 365 et à d'autres applications validées par Azure AD.

Il s'agit d'un processus unique par rapport aux autres solutions qui sollicitent un accès conditionnel puisque les appareils ne sont pas obligés de passer par un proxy. En évitant le proxy,



Accès Conditionnel EMS

les entreprises bénéficient d'une approche simplifiée de la protection des appareils.

Qu'en est-il de l'expérience utilisateur ? Elle est simple et pédagogique. Si un utilisateur se connecte à partir d'un appareil non conforme pour s'identifier et accéder aux données de l'entreprise, il recevra un message sur l'appareil lui spécifiant que celui-ci ne remplit pas toutes les conditions requises pour se voir autoriser l'accès. L'utilisateur peut alors cliquer sur ce message et suivre les étapes qui lui sont proposées pour résoudre le problème de conformité.

Le message informe l'utilisateur de la situation et explique pourquoi l'appareil n'est pas conforme. S'il s'agit d'un problème de mot de passe, il n'aura qu'à cliquer sur « Resolve Issues » (Résoudre les problèmes) et à modifier son mot de passe pour rendre l'appareil conforme et avoir accès aux données de l'entreprise.

Les données que Jamf communique à Microsoft permettent de renforcer la sécurité en la rendant plus intelligente, ce qui se traduit par une solution de gestion plus efficace et offrant une expérience utilisateur fluide.

BRAD ANDERSON : « APPRÉCIÉE DES UTILISATEURS, SUSCITE LA CONFIANCE DES INFORMATICIENS »

Pour offrir une expérience moderne, responsabilisante et sécurisée, les processus de gestion doivent s'adapter à la manière dont les employés travaillent, à l'endroit d'où ils le font et aux outils qu'ils utilisent. Le service informatique doit intégrer ses protocoles de protection de manière transparente et définir des consignes précises afin que les utilisateurs ne répondant pas aux critères de sécurité puissent être réhabilités sans exposer les données de l'entreprise à des risques.

Ensemble, Jamf et Microsoft permettent aux services informatiques d'y parvenir grâce à la sécurité basée sur l'identité. Avec celle-ci, les utilisateurs bénéficient d'un accès permanent, en tout lieu, et sans passer par un proxy.

Pendant des décennies, les entreprises ont érigé des « murs » autour de leurs locaux et ont fait des périmètres réseau leur première ligne de défense, laissant le problème de la sécurité interne de côté. Or les données se sont déplacées et le monde a évolué. Ces solutions modernes répondent aux problèmes posés par ces changements.

Découvrez comment améliorer vos pratiques de sécurité pour que votre service informatique ait tous les outils dont il a besoin, et pour que vos utilisateurs puissent améliorer leur productivité en toute sécurité, depuis l'appareil de leur choix.

L'amélioration de la sécurité commence ici

jamf

www.jamf.com

Pour en savoir plus sur les atouts de Jamf Pro pour la gestion de vos Mac et appareils iOS, rendez-vous sur **jamf.com/fr/produits/jamf-pro**