jamf

Jamf et Microsoft – **gérer** et **sécuriser** Apple en entreprise

À l'heure où le télétravail et la mobilité se généralisent dans l'entreprise, les décideurs de l'**informatique** et de la **sécurité** doivent relever plusieurs défis d'envergure :

- Comment gérer et sécuriser un réseau d'appareils et d'utilisateurs dont les données sensibles sont accessibles à partir de multiples emplacements ?
- Comment consolider les outils et faire plus avec moins, tout en augmentant les capacités de gestion et de sécurité ?

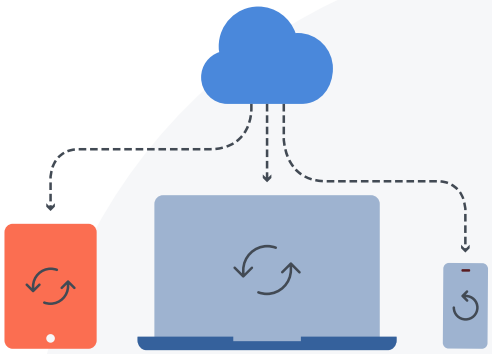
De nombreuses technologies de pointe ont été développées pour répondre à ces défis modernes. Pour autant, beaucoup d'organisations ont encore du mal à assurer la sécurité des utilisateurs et des données, malgré l'arsenal censé simplifier la transition vers les environnements de travail à distance.

Les conséquences sont lourdes :

- Complexité inutile lors de la configuration d'une sécurité complète
- Une expérience utilisateur médiocre, qui ajoute une charge administrative supplémentaire à la gestion.
- Une sécurité lacunaire qui ne couvre pas tous les appareils de l'infrastructure.
- L'absence de contrôles cohérents sur les ressources et les données sensibles de l'entreprise

Member of Microsoft Intelligent Security Association

Microsoft



Quels autres défis faut-il encore relever ?

La protection des données et des applications les plus sensibles d'une organisation implique aujourd'hui un ensemble complexe de variables :

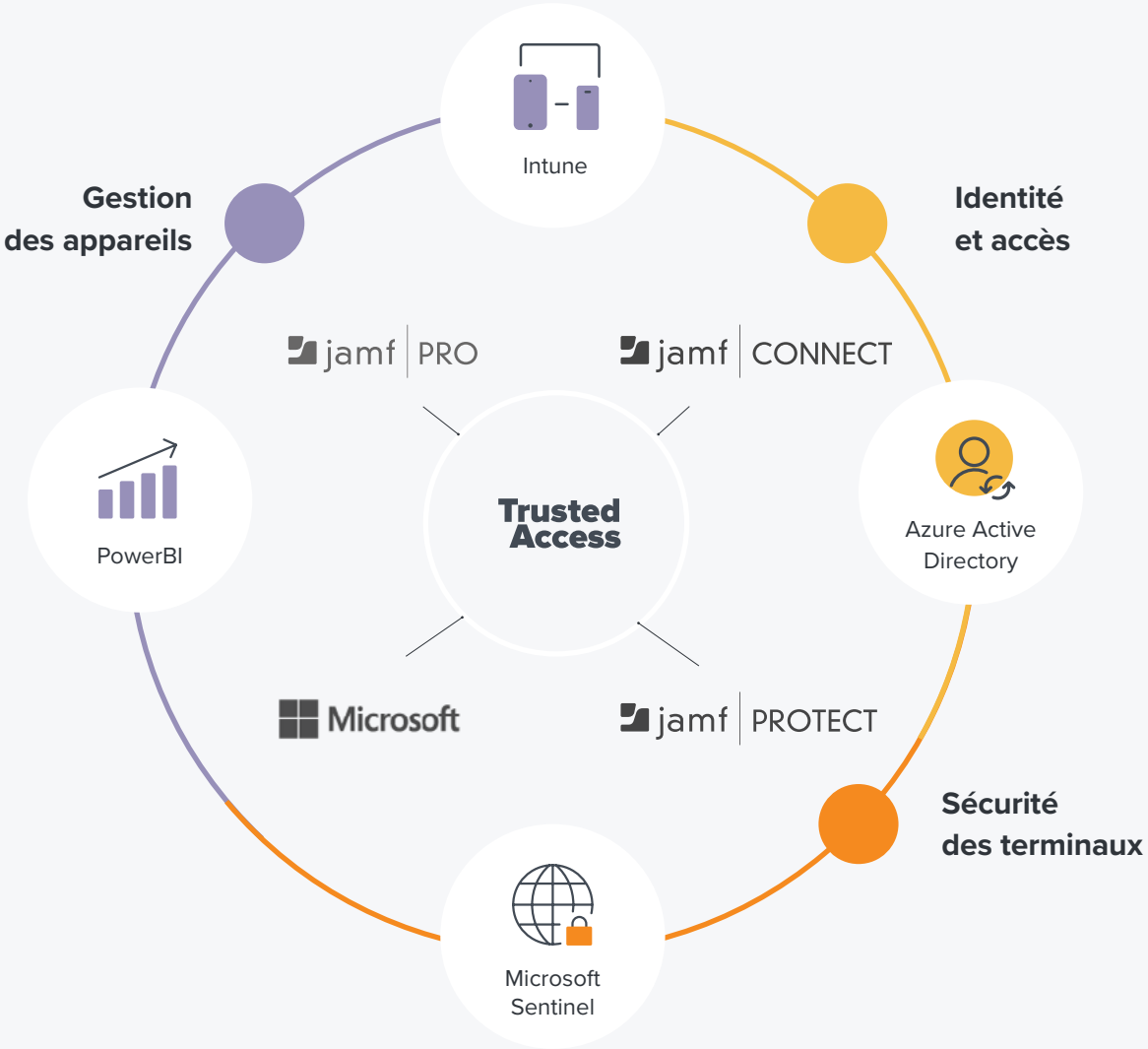
- Les programmes de choix des employés, les appareils mobiles et le BYOD créent de nouvelles contraintes pour la gestion et la sécurisation des appareils
- Les plateformes modernes ont besoin de solutions à la hauteur pour vérifier l'identité des utilisateurs et les connecter aux données en toute sécurité.
- Les nouveaux appareils et l'évolution des cas d'utilisation et des exigences réglementaires introduisent de nouvelles catégories de risques.

La réponse de Jamf + Microsoft

Parce que Jamf peut réunir ce qui se fait de mieux en matière de gestion des appareils Apple, de gestion des identités et de protection des terminaux, la société a toutes les cartes en main pour délivrer son approche Trusted Access en toute transparence avec Microsoft. Avec Trusted Access, les organisations savent que seuls les utilisateurs autorisés, équipés d'appareils inscrits et sécurisés, peuvent se connecter aux applications et aux données professionnelles. Trusted Access repose sur une intégration avec un fournisseur d'identité cloud (IdP) : l'association de Jamf et Microsoft est donc parfaitement naturelle. Tous les appareils inscrits sont sécurisés par la gestion et la protection des terminaux. Quant au trafic, il est contrôlé par l'accès réseau Zero-Trust (ZTNA) qui sécurise les connexions à distance. Cette nouvelle approche pensée pour le paysage des menaces modernes corrige les défauts des VPN traditionnels.

L'intégration de Jamf et de Microsoft concrétise le paradigme du Trusted Access, indispensable dans les organisations dont l'infrastructure repose sur la plateforme Microsoft et qui veulent réussir avec Apple.

Jamf jette un pont entre l'offre d'Apple et les besoins des entreprises. Découvrez les intégrations de Jamf et Microsoft qui simplifient Apple dans votre organisation.



Intégrations à la gestion des appareils	Description	Documentation produit ou référence Marketplace	Produits Jamf	Produit Microsoft	Citation client
LDAP pour l'interrogation des utilisateurs et des groupes	Informations sur les utilisateurs d'une organisation (nom, e-mail, rôle, etc.). Ces informations permettent d'attribuer les bonnes applications et les bons réglages aux utilisateurs finaux. L'administrateur peut consulter ces informations sans avoir à les recréer manuellement.	**Intégration aux services d'annuaire LDAP**	**Jamf Pro**	AD On Prem	
Fournisseur d'identité cloud pour l'interrogation des utilisateurs et des groupes	Informations sur les utilisateurs d'une organisation (nom, e-mail, rôle, etc.). Ces informations permettent d'attribuer les bonnes applications et les bons réglages aux utilisateurs finaux. L'administrateur peut consulter ces informations sans avoir à les recréer manuellement.	**Intégration Azure AD**	**Jamf Pro**	Microsoft Azure AD et InTune (Microsoft Endpoint Manager)	**Intégration en toute simplicité entre Jamf Pro et Azure AD** « Une documentation facile à suivre, fournie à la fois par Jamf et par Microsoft. L'intégration la plus simple à laquelle j'ai jamais participé. » I. Borota
Rapports d'inventaire des appareils	Les administrateurs rêvent souvent d'une « fenêtre unique » sur leur flotte, surtout si elle combine des appareils Windows et Apple. Cette intégration permet à Jamf Pro d'envoyer une sélection de données macOS à InTune pour apporter de la visibilité sur les flottes mixtes dans un outil central.	**Accès conditionnel**	**Jamf Pro**	Microsoft InTune (Microsoft Endpoint Manager)	« InTune simplifie l'inscription des appareils macOS à des fins d'inventaire pour donner un maximum de visibilité et faciliter la maintenance. L'intégration permet de configurer rapidement une règle de conformité supplémentaire : c'est très pratique, il suffit de connaître un peu InTune pour l'appliquer, et cela allège la charge des équipes des opérations de sécurité. Une excellente expérience dans l'ensemble. » DominicVasquez
Tableaux de bord et rapports analytiques	Transformez les données en renseignements en quelques minutes avec Power BI Desktop. Obtenez gratuitement tout ce dont vous avez besoin pour créer et enregistrer un nombre illimité de rapports interactifs. Utilisez l'application Jamf Pro Power BI pour approfondir l'analyse des données de votre déploiement Jamf. Enrichissez les fonctions de rapports de Jamf Pro et intégrez-les à votre architecture Power BI. Données • Ordinateurs et appareils mobiles • Détails • Applications • Attributs d'extension • Groupes	**Power BI**	**Jamf Pro**	Microsoft Power BI	**Power BI avec Jamf Pro** « Power BI s'intègre parfaitement à Jamf Pro pour délivrer des rapports détaillés sur tous les aspects de votre instance Jamf Pro. Vous créez des rapports sur les versions de macOS, les versions de définitions de virus, le nombre d'appareils par bâtiment, etc. J'adore cet outil : il nous fournit des données qui nous permettent d'agir. » C. McBride

Intégrations des identités et des accès	Description	Documentation produit ou référence Marketplace	Produits Jamf	Produit Microsoft	Citation client
Conformité des appareils macOS/iOS	Les organisations doivent vérifier que les utilisateurs sont fiables et équipés d'un appareil conforme (OS à jour, code activé) avant de les autoriser à accéder aux ressources. Avec cette intégration, Jamf Pro vérifie si un appareil est conforme et transmet son statut à Microsoft. *Cette intégration remplace l'accès conditionnel dans Jamf Pro 10.43	**Conformité des appareils**	**Jamf Pro**	Microsoft Azure AD et InTune (Microsoft Endpoint Manager)	« Une intégration qui veille à ce que l'accès aux données du bureau soit réservé aux appareils conformes. L'intégration transparente de Jamf et Microsoft Azure AD répond à cette exigence de sécurité. Une solution incontournable sur le plan de la sécurité. » Samstar777
Accès conditionnel pour MacOS	Les organisations doivent vérifier que les utilisateurs sont fiables et équipés d'un appareil conforme (OS à jour, code activé) avant de les autoriser à accéder aux ressources. Cette intégration transmet une sélection d'attributs d'inventaire de Jamf Pro à Microsoft Intune afin de déterminer si l'utilisateur peut accéder à l'application demandée. *Cette intégration est obsolète : elle a été remplacée par Conformité des appareils dans Jamf Pro 10.43 (nous continuerons à prendre en charge cette intégration pendant un an après l'abandon de l'API par Microsoft).	**Accès conditionnel**	**Jamf Pro**	Microsoft Azure AD et InTune (Microsoft Endpoint Manager)	**macOS dans l'environnement Windows** « En tant qu'intégrateur Mac, je suis souvent impliqué dans des projets consistant à intégrer macOS dans des environnements Windows. Et cette approche repose essentiellement sur Jamf Pro et Azure Active Directory. L'accès conditionnel et la conformité de macOS n'ont jamais été aussi efficaces. » N. Lecchi
SSO pour l'identité cloud	Cette intégration permet aux administrateurs d'une organisation d'utiliser leurs identifiants Azure pour se connecter à leur instance Jamf Pro, au portail Jamf macOS Security Cloud et au portail Jamf Security Cloud.	**Configuration de l'authentification unique avec les services de fédération d'Active Directory**	**Jamf Pro**	Microsoft Azure AD et InTune (Microsoft Endpoint Manager)	**Meilleure intégration des IdP** « Azure AD s'intègre à tous nos outils qui prennent en charge un IdP externe. Avec la prise en charge des fournisseurs d'identité Cloud pour le SSO dans Jamf Pro et l'intégration pour Jamf Protect, vous pouvez utiliser vos identités d'entreprise avec vos produits Jamf et vos services tiers en toute simplicité. » T. Ellis
Identité cloud pour Mac	Cet outil permet aux utilisateurs finaux d'une organisation de se connecter à leur Mac à l'aide de leurs identifiants Azure.	**Intégration à Microsoft Azure AD**	**Jamf Connect**	Microsoft Azure AD et InTune (Microsoft Endpoint Manager)	« Les instructions que nous avons reçues ont beaucoup facilité la mise en œuvre. Le SSO change la vie. » Tyler Verlato

Intégrations de sécurité des terminaux	Description	Documentation produit ou référence Marketplace	Produits Jamf	Produit Microsoft	Citation client
Jamf Protect pour Microsoft Sentinel	La solution Jamf Protect pour Microsoft Sentinel crée des données d'événements détaillées à partir des terminaux macOS puis les envoie à un espace de travail Microsoft Sentinel via un workflow très simple. Elle apporte une visibilité complète sur la sécurité des terminaux Apple de l'entreprise en s'appuyant sur les workbooks et les règles analytiques. Ceux-ci contiennent à la fois des événements d'**alerte** et de **journal unifié** capturés par Jamf Protect, mais aussi les **événements de sécurité intégrés à macOS**.	**Jamf Protect pour Microsoft Sentinel**	**Jamf Protect**	Microsoft Sentinel	« **Sentinel Security fonctionne très bien avec Jamf.** Associée à Jamf Protect, cette application optimise les workflows et vous rend le contrôle des opérations de sécurité, tout simplement. Elle accroît votre productivité et apporte une vision détaillée de la posture de sécurité de votre flotte d'appareils. Nous recommandons chaudement. » DominicVasquez
Transmission de la télémétrie des terminaux	Par défaut, les Mac collectent toutes sortes de données sur leurs performances et leurs applications. Cela représente une grande quantité d'informations, mais nous les filtrons avec Jamf Protect pour envoyer uniquement les renseignements pertinents aux outils de sécurité qui savent les exploiter.	**Intégration de Jamf Protect à Microsoft Sentinel**	**Jamf Protect**	Microsoft Sentinel	« Un nouvel exemple de la qualité de l'intégration de Jamf et Azure ! » User-MrCcStilBF
Transfert des événements du flux de menaces réseau	Le flux de trafic réseau permet aux organisations d'importer, d'enregistrer et d'examiner toute l'activité du réseau traitée par l'infrastructure du service, au moyen d'agrégateurs de journaux et d'outils d'analyse tiers. Les événements sont envoyés en temps réel dans un syslog codé au format CEF (Common Event Format) via TLS (sécurité de la couche de transport) pour garantir la sécurité des données en transit. Le flux d'événements de menace peut envoyer des événements en temps réel sous forme de syslogs au format CEF ou d'événements HTTP au format JSON. Les deux flux peuvent être intégrés dans Microsoft Sentinel.	**Flux de trafic réseau** **Flux d'événements de menaces**	**Jamf Protect** et **Jamf Connect**	Microsoft Sentinel	« Excellente intégration avec Azure et Sentinel. Le lien avec Jamf Protect est particulièrement utile. » Catherine Breese

Pour en savoir plus sur le partenariat entre Microsoft et Jamf, consultez notre page sur les intégrations Microsoft.