



Jamf et Google – Gérer et sécuriser les appareils Apple pour les organisations natives clou

*Dans les organisations qui offrent le choix des appareils et des modèles de travail flexibles, le défi pour les décideurs technologiques consiste à assurer l'**efficacité**, la **sécurité** et l'**évolutivité des opérations**, sans compromettre l'expérience de l'utilisateur final.*



Proposer des appareils Apple en entreprise devrait être une décision stratégique, et non un compromis. Lorsque les organisations proposent des terminaux Apple à leurs équipes, elles ont besoin d'outils spécialement conçus pour cette plateforme. Les outils de productivité multiplateformes comme Google Workspace ont leur intérêt, mais lorsqu'il s'agit de la gestion et de la sécurité des appareils, une expertise approfondie de la plateforme s'avère indispensable.

Utiliser des outils multiplateformes ou conçus sur Windows pour prendre en charge des appareils Apple introduit souvent des frictions, de la complexité et des angles morts :

1. Les agents dégradent les performances des points de terminaison.
2. Les VPN traditionnels augmentent la surface d'attaque et frustrer les utilisateurs.
3. La gestion des points de terminaison macOS et iOS est insuffisante et n'offrent qu'une faible visibilité.

En revanche, une solution adaptée à une plateforme offre un socle éprouvé pour le succès à long terme des programmes d'appareils. En remplaçant les logiciels de gestion traditionnels par des solutions dédiées à Apple, vous allez donner davantage d'autonomie aux utilisateurs et concrétiser le potentiel de vos investissements dans l'écosystème Google.

Jamf propose la seule solution dédiée à Apple qui s'intègre étroitement à Google Workspace, Chrome Enterprise, Google Cloud Identity et Google Security Operations. Le résultat ? Un écosystème « zero trust » unifié, conçu pour les équipes informatiques et de sécurité des organisations tournées vers le cloud.

Google et Jamf coopèrent pour permettre aux organisations de toutes tailles de communiquer, créer, collaborer et travailler en toute sécurité.

Ensemble, Jamf et Google offrent productivité et collaboration à vos équipes Apple, avec la sécurité d'un système « zero trust » basé sur l'identité pour Apple en entreprise.

Les organisations savent que seuls les utilisateurs autorisés, équipés d'appareils inscrits et sécurisés, peuvent accéder aux applications et aux données professionnelles. Ces appareils sont protégés par une gestion robuste, des contrôles réseau étroits et une sécurité dédiée aux points de terminaison. Tout le trafic est régi par l'accès réseau « zero trust » (ZTNA) pour des connexions à distance sécurisées à grande échelle.

Jamf et Google partagent depuis longtemps la même vision : remplacer les VPN traditionnels par des solutions de sécurité modernes multicouches. Ensemble, nous offrons une expérience

« zero trust » simple et fluide, spécialement conçue pour Apple et pour les besoins des entreprises hybrides d'aujourd'hui.

Grâce à Google Workspace, qui facilite la collaboration et la productivité, et à Chrome, qui offre une navigation sécurisée et conforme sur Mac et sur mobile, les organisations peuvent offrir en toute confiance une gestion et une sécurité de référence à leurs utilisateurs Apple.

Jamf se combine aux outils de productivité orientés cloud et à la navigation sécurisée de Google afin de jeter les bases d'une stratégie « zero trust » pensée pour Apple. Cette approche intégrée a un double avantage : protéger les utilisateurs et les données, mais aussi donner aux employés les moyens de travailler de manière flexible, sécurisée et productive, où qu'ils se trouvent.

Sécurité « zero trust » intégrée avec Jamf and Google



Présentation de l'intégration	Description	Documentation produit ou référence Marketplace	Produits Jamf	Produit Google
LDAP sécurisé 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 avec le LDAP sécurisé de Google	Jamf Pro Jamf School	Google Workspace, Google Cloud Identity
Intégrations de l'accès sensible au contexte de Google	L'intégration permet aux appareils mobiles et Mac de communiquer à BeyondCorp l'état de conformité déterminé par Jamf. Restreindre l'accès aux applications protégées par les règles contextuelles	Google BeyondCorp Entreprise	Jamf Pro, Jamf Connect	Google Workspace, Google Cloud Identity, Google Cloud
Utilisation de Chrome Enterprise Core et Premium	Chrome Entreprise possède des avantages et des fonctionnalités de grande envergure pour les organisations. Jamf Pro et Jamf School peuvent permettre de profiter pleinement des fonctionnalités d'entreprise de Google Chrome.	Inscrire des navigateurs sur macOS avec Jamf Pro Inscrire des navigateurs sur mobile avec Jamf Pro	Jamf Pro, Jamf School	Chrome Entreprise
SSO pour l'identité cloud	Cette intégration permet aux administrateurs d'une organisation d'utiliser leurs identifiants Google pour se connecter à leur instance Jamf Pro, au portail Jamf macOS Security Cloud et au portail Jamf Security Cloud.	Configuration de la SSO avec Google Workspace	Compte Jamf	Google Workspace, Google Cloud Identity
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 Google. L'expérience est identique à celle des utilisateurs de Chromebook ou de Windows avec GCPW.	Intégration avec Google Identity	Jamf Connect	Google Workspace, Google Cloud Identity
Jamf Protect Parsers pour Google Security Operations	L'intégration de Google Protect et de Google Security Operations permet de transmettre aux SecOps les données détaillées d'événements, d'alertes et de journalisation unifiée que capture Jamf Protect.	Google Security Operations	Jamf Protect	Google Security Operations
Jamf Pro Parsers pour Google Security Operations	Les informations d'inventaire de Jamf Pro sont lisibles par Google Security Operations	Google Security Operations	Jamf Pro	Google Security Operations
Inscription par l'utilisateur basée sur le compte avec Google Identity pour iOS en BYOD	Mettez en place une gestion des appareils respectueuse de la vie privée des utilisateurs sur leurs appareils mobiles personnels. Les utilisateurs n'ont qu'à s'inscrire à la gestion via l'application Réglages avec leurs identifiants Google pour recevoir des profils et des applications.	Inscription des utilisateurs en BYOD	Jamf Pro, Jamf School	Google Workspace, Google Cloud Identity



www.jamf.com/fr

© 2002–2026 Jamf, LLC. Tous droits réservés.

Pour en savoir plus sur le partenariat entre Google et Jamf, consultez notre page sur les [intégrations Google](#). Pour vous lancer, [demandez une version d'essai](#).