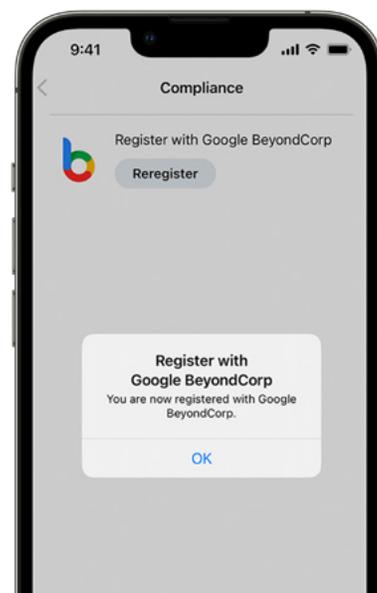




BeyondCorp Enterprise

Sécuriser les entreprises avec l'accès contextuel



Utilisez **Jamf Pro** et **BeyondCorp Enterprise** pour doter votre entreprise d'une solution zero-trust complète basée sur le cloud.

Le télétravail s'est considérablement développé au cours des dernières années. Dans ce contexte, les entreprises ont besoin d'un cadre de conformité et de sécurité axé sur les appareils des utilisateurs finaux plutôt que sur le périmètre d'un réseau.

Vous pouvez désormais utiliser l'outil de référence pour la gestion des appareils Apple tout en renforçant votre sécurité Google grâce à l'**intégration BeyondCorp Context Aware Access** de Jamf. Grâce à cette intégration, les entreprises peuvent confier à Jamf la gestion de leurs appareils Apple tout en continuant à s'appuyer sur le cadre zero-trust de Google.

Ainsi, seuls les utilisateurs de confiance utilisant des appareils macOS, iOS ou iPadOS sécurisés peuvent accéder aux ressources protégées par Google.



La vision Google de la sécurité en entreprise

Google Workspace est en passe de devenir la référence pour les organisations en quête d'espaces de collaboration flexibles en ligne. En effet, en mars 2023, [Google Workspace a franchi la barre des 9 millions de clients payants](#).

Avec [BeyondCorp](#), Google réinvente l'architecture de sécurité, en créant des workflows d'authentification et d'autorisation basés sur l'utilisateur et l'appareil. Cette approche abandonne la segmentation du réseau comme moyen de protéger les ressources sensibles. Dans ce modèle zero-trust, l'accès aux ressources doit être soumis à des contrôles de sécurité, mais il est possible quel que soit le réseau sur lequel se trouve l'utilisateur. L'accès est accordé sur la base d'informations contextuelles concernant l'utilisateur et l'appareil, fournies par Jamf Pro.



BeyondCorp Enterprise

Comprendre l'intégration de BeyondCorp à Jamf Pro

Avec cette intégration, les appareils mobiles et Mac peuvent :



Partager avec BeyondCorp leur état de conformité déterminé par Jamf



Restreindre l'accès aux applications protégées par les règles contextuelles de BeyondCorp Enterprise

Prenons pour exemple le workflow d'onboarding des nouveaux employés :

- Les administrateurs définissent des règles de sécurité flexibles et utilisent les groupes intelligents de Jamf pour définir des états de conformité.
- Les nouveaux employés suivent le processus d'onboarding défini par les administrateurs.
- Les utilisateurs inscrivent leur appareil mobile et leur portable, qu'ils appartiennent à l'entreprise ou qu'ils soient en BYOD
- Ils s'inscrivent ensuite auprès de BeyondCorp via Jamf Self Service ou Google Chrome, selon la plateforme.
- Les règles d'accès contextuelles de Google déterminent l'accès en fonction des informations fournies par Jamf sur l'utilisateur et l'état de conformité de l'appareil.

Les intégrations Google de Jamf ouvrent de nouvelles perspectives

Cette intégration n'est qu'un aspects de nos efforts constants pour [simplifier et améliorer la connectivité entre les écosystèmes d'Apple et de Google](#).



www.jamf.com/fr

© 2002–2023 Jamf, LLC. Tous droits réservés.

Mis à jour en février 2022

Découvrez comment combiner les meilleurs atouts d'Apple et de Google avec Jamf.