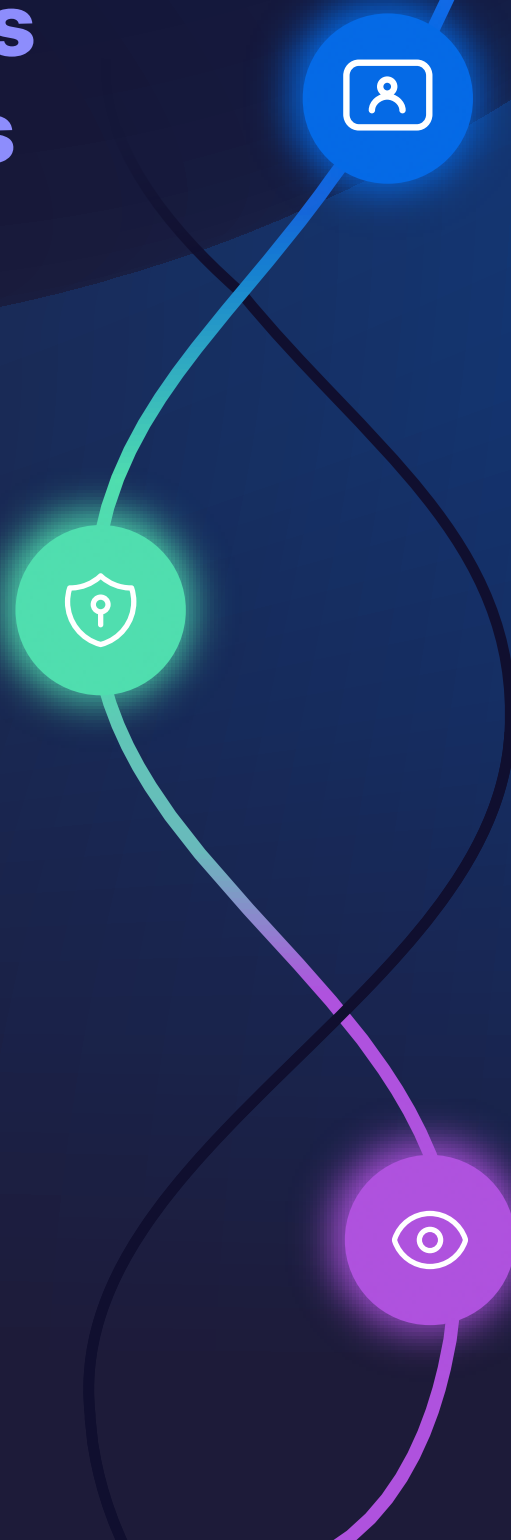


Vous cherchez à intégrer des appareils Apple dans un environnement où les PC sont majoritaires ?

Votre environnement dispose déjà de systèmes matures en matière d'**identité**, de **sécurité** et de **visibilité**.

Vous devez maintenant ajouter des appareils Apple avec un triple objectif : **un déploiement plus rapide, moins d'efforts de personnalisation et une réduction des risques.**

Avec notre auto-évaluation, découvrez à quelle vitesse vous pouvez intégrer Apple à vos systèmes existants sans créer une pile technologique parallèle.



Vérifiez l'accès et la confiance

Les appareils Apple doivent s'intégrer parfaitement à votre modèle d'accès, sans exception à gérer manuellement.

Posez les questions suivantes :

1. Peut-on appliquer des **politiques d'accès** cohérentes et communes aux utilisateurs Mac et Windows ?
2. Peut-on définir une politique basée sur des **groupes d'identités** sans avoir à recréer la structure de l'organisation ?
3. Peut-on lier l'accès à la **conformité de l'appareil** (et pas seulement à une identification basée sur le nom d'utilisateur et le mot de passe) ?



Vérifier la posture, la détection et la réponse



Les appareils Apple ne doivent pas être exclus de votre modèle d'opérations de sécurité ; au contraire, ils doivent y contribuer.

Posez les questions suivantes :

1. Peut-on visualiser le risque Apple dans la **même console** que le risque Windows ?
2. Les **alertes** sont-elles concrètement exploitables ou simplement informatives ?
3. Peut-on **automatiser la réponse** ou faut-il nécessairement procéder manuellement dans le cas d'Apple ?

Vérifiez les actifs et les workflows

Les appareils Apple devraient être pleinement visibles dans vos opérations informatiques et dans le cycle de vie de vos actifs, et vous devez pouvoir disposer de données propres et fiables.

Posez les questions suivantes :

1. Disposons-nous d'un **inventaire complet** (applications, système d'exploitation, état de chiffrement, propriété) ?
2. Est-il possible d'intégrer **les terminaux Apple dans les flux ITSM existants** sans étapes supplémentaires ?
3. Les **intégrations sont-elles bidirectionnelles** (synchronisation et actions) ou uniquement conçues pour exporter des données ?

Préparation à l'intégration

Auto-évaluation

Notez chaque catégorie de 1 à 5, où 5 indique une confiance maximale dans l'affirmation



Identité :

- ☐ Nous pouvons appliquer à Apple un modèle d'accès cohérent et basé sur la fiabilité des appareils.
- ☐ Il est facile d'appliquer des réglages à des groupes définis d'appareils et d'automatiser les étapes du cycle de vie.
- ☐ Les utilisateurs Apple ne nécessitent que des efforts minimes de gestion des exceptions.



Sécurité :

- ☐ Les risques et la posture d'Apple sont visibles dans les flux de nos opérations de sécurité
- ☐ Nous pouvons automatiser les actions de réponse (et pas seulement les alertes) grâce à la gestion déclarative des appareils (DDM) d'Apple.
- ☐ Les rapports sont alignés sur nos contrôles et nos audits internes



Visibilité :

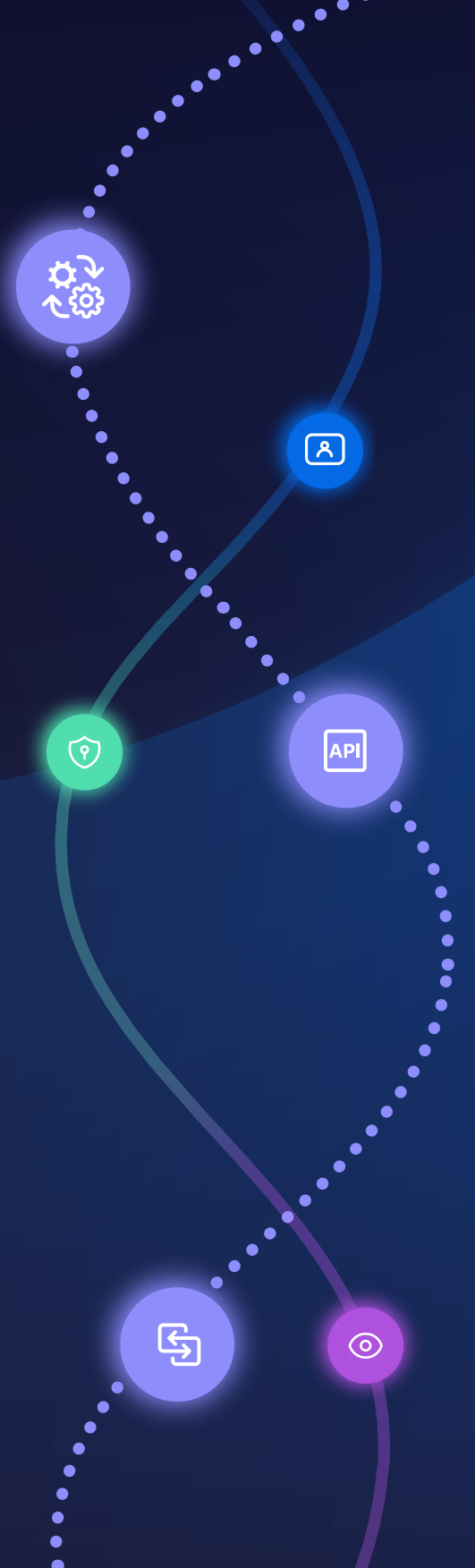
- ☐ L'inventaire du parc Apple est complet, précis et utilisable dans un système CMDB/ITSM.
- ☐ Nous pouvons déclencher des workflows à partir de l'état de l'appareil en temps réel, et non de données stockées dans des feuilles de calcul.
- ☐ Les données restent cohérentes dans le temps sans nettoyage manuel

Si vous avez mis moins de 3 à l'un de ces piliers : vous risquez de devoir mettre en place des solutions de contournement manuelles, d'accumuler une dette d'intégration et de faire face à des problèmes d'évolutivité.



Les entreprises réussissent leurs intégrations avec Jamf

Jamf accélère l'adoption d'Apple grâce à des **intégrations provenant de notre place de marché** et à des **API flexibles** dans les domaines de l'identité, de la sécurité et de la visibilité. Pleinement prises en charge, ces intégrations simplifient les workflows, réduisent la dette d'intégration et aident les équipes à mettre en œuvre et à étendre Apple à l'aide d'outils auxquels elles font déjà confiance.



Ne nous croyez pas sur parole : découvrez pourquoi Jamf a été nommé **Leader** dans l'étude **IDC MarketScape : Évaluation des fournisseurs de logiciels de gestion unifiée des terminaux pour les appareils Apple 2025–2026**.