FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Microsoft Intune — Gestion de flotte moderne

Guide Intune / PME

Intune unifie la gestion de vos PC Windows, Mac, smartphones et tablettes en mode cloud. Ce guide pose les bases d'un déploiement réussi : enrôlement, conformité, applications, Conditional Access avec Entra ID.

Scannez pour acceder a la version en ligne

contact@flashmodz.be | +32 471 87 87 07

https://flashmodz.be

L'essentiel en 5 minutes

Intune transforme une flotte invisible et hétérogène en infrastructure pilotée. Inclus dans M365 Business Premium et E3+.

1

Intune est probablement déjà payé

Microsoft 365 Business Premium (~22 €/user) et Microsoft 365 E3+ incluent Intune. La majorité des PME M365 n'ont pas activé Intune malgré sa souscription. C'est un gain immédiat : pas de coût supplémentaire, juste de la mise en œuvre.

2

Autopilot révolutionne le provisionnement PC

Avec Autopilot, un PC neuf est expédié directement au collaborateur (livraison à domicile possible). Il le démarre, se connecte avec ses identifiants Entra ID, et le PC se configure tout seul en 30 minutes (apps, politiques, profils). Le technicien ne touche plus la machine, et l'expérience utilisateur est meilleure.

3

Conditional Access "Compliant Device" = Zero Trust

La combinaison Intune (Compliance Policy) + Conditional Access (Compliant Device Required) est la pierre angulaire du Zero Trust pour endpoints : seuls les appareils enrôlés et conformes ont accès aux données. C'est un saut majeur de sécurité par rapport au "MFA seul".

4

Le BYOD se gère sans intrusion personnelle

App Protection Policies (Intune) protègent les données pro sur smartphones personnels SANS enrôlement complet de l'appareil. Container Outlook chiffré, copier-coller restreint, wipe sélectif au départ. Le collaborateur garde sa vie privée intacte, l'employeur a la maîtrise.

5

Compatible Windows + Mac + iOS + Android

Intune gère les 4 grandes plateformes. Pour des PME mixtes Windows + Mac jusqu'à ~50 Mac, Intune suffit. Au-delà ou pour des besoins très spécialisés (déploiement créatif, automatisation Bash), un MDM dédié Apple comme Jamf complète Intune (ou le remplace pour la partie Mac).

Et maintenant ?

Les pages qui suivent détaillent chacun de ces points avec exemples, chiffres et actions concrètes.

Document conçu pour PME — MDM Microsoft Intune · Lecture : ~15-20 min · Édition 2026

© 2026 FlashModz Enterprise — https://flashmodz.be

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

© 2026 FlashModz Enterprise — https://flashmodz.be

Le marché belge en chiffres

Chapitre 1

4 OS

Windows, macOS, iOS/iPadOS et Android gérés depuis une seule console (Linux Ubuntu également pris en charge)

Sources : textes officiels (NIS2, RGPD, DORA) et publications des éditeurs cités

0 serveur

à installer ou maintenir : Intune est un service 100% cloud

3-6 semaines

durée typique d'un projet Intune pour 50 postes

inclus

Intune fait partie de Microsoft 365 Business Premium et E3+

Contexte & enjeux

En 2026, gérer une flotte d'appareils en PME sans MDM est devenu intenable. Vos collaborateurs ont des PC Windows (parfois Mac), des smartphones (iOS et Android), parfois des tablettes. Certains travaillent au bureau, d'autres en télétravail, d'autres en clientèle. Chaque appareil est une porte d'entrée potentielle vers vos données et systèmes.

Sans MDM, voici ce qui se passe typiquement : une partie du parc échappe complètement à l'IT, les patches Windows sont irréguliers, les antivirus sont désactivés sur certains postes, les disques ne sont pas chiffrés, les applications sont installées à la main par les techniciens (parfois pas du tout), un appareil perdu reste un trou de sécurité ouvert pendant des semaines, et le BYOD se fait sans aucune séparation entre données pro et perso.

Microsoft Intune (anciennement "Microsoft Endpoint Manager") est la solution MDM intégrée à Microsoft 365 Business Premium et aux SKUs E3+. C'est un produit cloud-native, sans infrastructure à maintenir, qui gère Windows 10/11, macOS, iOS/iPadOS et Android. Il s'intègre nativement avec Entra ID, Conditional Access et Defender. L'inscription automatique au moment de la jonction Entra ID (licence Entra ID P1 requise) rend même l'enrôlement transparent pour l'utilisateur. C'est l'écosystème de référence pour une PME en environnement Microsoft.

Bien déployé, Intune transforme la gestion de flotte en un processus structuré : un nouveau collaborateur reçoit un PC neuf en provenance directe du fournisseur (Autopilot), il le démarre, se connecte avec ses credentials Entra ID, et le PC se configure tout seul (apps, politiques, profils). En cas de perte ou de départ, l'IT peut effacer l'appareil à distance. La compliance des appareils devient une condition d'accès via Conditional Access. Compter 3-6 semaines de projet pour 50 postes, hors apps métier complexes.

© 2026 FlashModz Entreprise — https://flashmodz.be

> *"En 2026, ne pas avoir de MDM dans une PME, c'est piloter sans tableau de bord. Intune n'est plus optionnel : c'est l'infrastructure de base de la sécurité des endpoints."*
>
> — Jérémy Manet, FlashModz Enterprise

Pourquoi votre flotte d'appareils est ingérable aujourd'hui

Chapitre 2

Les conséquences invisibles d'une absence de MDM en 2026.

Vous ne savez pas qui a quoi

Sans MDM, l'inventaire des appareils est tenu dans un Excel à jour partiel. Combien de PC sous Windows 10 vs 11 ? Combien de Mac ? Quels smartphones reçoivent les emails M365 ? Personne ne sait précisément. C'est un risque opérationnel ET un risque RGPD (qui accède à quoi).

Les patches Windows sont irréguliers

Sans MDM, la politique de patchs repose sur les utilisateurs. Certains PC sont patchés mensuellement, d'autres tournent encore en Windows 10 21H2. La surface d'attaque s'élargit chaque mois sans visibilité. Avec Intune Update Rings, vous pilotez les patches comme dans un grand compte.

Le BYOD est ingérable

Vos collaborateurs accèdent à leurs emails M365 sur leur smartphone perso. En cas de départ ou de vol, vous ne pouvez ni effacer les données pro, ni vérifier que le téléphone a un code PIN. C'est un trou RGPD et NIS2 béant que la plupart des PME ignorent.

Les disques ne sont pas chiffrés

BitLocker (Windows) et FileVault (Mac) sont des fonctionnalités gratuites incluses, mais leur activation et la gestion centralisée des clés de récupération demandent un MDM. Sans MDM, une partie du parc n'est jamais chiffrée et personne ne le voit. Un PC perdu non chiffré, c'est une fuite de données potentielle à déclarer à l'APD.

Le provisionnement d'un nouveau PC prend 3 jours

Sans Autopilot, votre technicien IT déballe le PC, fait le setup Windows, joint le domaine, installe Office, déploie les apps métier, configure les imprimantes, etc. 4 à 8 heures par PC, étalées sur 2-3 jours. Avec Intune Autopilot, le PC arrive pré-configuré et l'utilisateur le configure lui-même en 30 minutes.

© 2026 FlashModz Enterprise — https://flashmodz.be

Conditional Access sans appareils gérés est aveugle

Vous avez peut-être activé Conditional Access dans Entra ID. Mais sans Intune et sans politique "Compliant Device Required", n'importe quel appareil peut se connecter dès que MFA passe. Avec Intune + Compliance Policy, seuls les appareils enrôlés et conformes (chiffrés, à jour, antivirus actif) ont accès aux données.

Mythes vs Réalité

Chapitre 3

Six idées reçues qui empêchent d'agir — et ce qu'en disent les chiffres.

01

ON ENTEND SOUVENT

Intune nous force à tout enrôler, perte de liberté pour les utilisateurs.

EN RÉALITÉ — *Niveau d'enrôlement = choix*

Vous choisissez le niveau d'enrôlement par persona. App Protection (BYOD) protège juste les apps pro sans enrôler l'appareil. Full enrollment (corporate) gère l'appareil entier. C'est modulable et explicable aux utilisateurs.

02

ON ENTEND SOUVENT

Intune c'est complexe, c'est pour les grands comptes.

EN RÉALITÉ — *3-6 semaines, 80% des cas couverts*

Intune a une courbe d'apprentissage, oui. Mais une PME peut couvrir 80% de ses besoins avec 5 Compliance Policies, 3 profils de configuration et Autopilot. 3-6 semaines de projet, ce n'est pas SAP.

03

ON ENTEND SOUVENT

On a un Active Directory et des GPO, pas besoin d'Intune.

EN RÉALITÉ — *GPO ⅋ Intune (complémentaires)*

GPO fonctionne SEULEMENT sur les PC joints au domaine et au bureau (ou via VPN). En 2026, télétravail + Mac + smartphones rendent GPO insuffisant. Intune fonctionne partout, sur tous les OS, sans VPN.

04

ON ENTEND SOUVENT

Intune coûte cher en plus de M365.

EN RÉALITÉ — *Inclus dans Business Premium*

Intune est inclus dans Microsoft 365 Business Premium (~22 €/utilisateur) et E3 (~32 €/utilisateur). Pour les structures sur Business Standard (~12,50 €), passer à Business Premium ajoute environ 10 €/utilisateur pour Intune + Defender for Office 365 P1 + Conditional Access. L'écart se justifie dès le premier incident évité.

© 2026 FlashModz Enterprise — https://flashmodz.be

05

ON ENTEND SOUVENT

Notre partenaire IT externe gère nos PC, on n'a pas besoin d'Intune.

EN RÉALITÉ

RMM ≠ Intune, expertise spécifique

Beaucoup de partenaires IT PME travaillent avec des outils RMM classiques (ConnectWise, NinjaOne). Ils peuvent gérer Intune en MSP, mais c'est loin d'être systématique. Demandez explicitement : "avez-vous une certification Microsoft Endpoint Administrator (examen MD-102) dans l'équipe ?". La réponse est révélatrice.

06

ON ENTEND SOUVENT

On verra Intune au prochain renouvellement matériel dans 2-3 ans.

EN RÉALITÉ

Enrôlement = pas de réinstall

Intune ne nécessite pas de renouvellement matériel. Les PC existants Windows 10/11 se laissent enrôler sans réinstallation. C'est un déploiement logique, pas physique. Attendre 2-3 ans, c'est laisser un vide de sécurité béant.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

Cabinet d'avocats namurois (45 collaborateurs)

Contexte: 38 PC Windows, 12 iPhones, 4 iPads. Pas de MDM. Inventaire dans un Excel. BYOD pour les emails sur smartphone perso. Plusieurs cas de vol de PC dans les 18 derniers mois.

Impact: Suite à un audit ITAA, projet Intune en 5 semaines : Autopilot pour les nouveaux PC, BitLocker forcé via Conditional Access, App Protection Policies pour les emails pro sur les smartphones perso (sans enrôlement complet du téléphone). Coût total 18 K€. Aucun incident de vol non maîtrisé depuis.

Leçon: Pour un cabinet juridique, Intune n'est pas un nice-to-have, c'est une hygiène de base du secret professionnel. L'investissement est rentabilisé dès le premier vol évité (ou correctement géré).

Agence créative bruxelloise (28 collaborateurs)

Contexte: Mix Windows + Mac (60/40). Croissance rapide, recrutement de 8 personnes en 6 mois. L'IT manager passe son temps à provisionner des PC.

Impact: Déploiement Intune avec Autopilot pour Windows et ABM/DEP pour les Mac. Nouvelle arrivée : le PC ou Mac est livré directement chez le collaborateur, qui se connecte avec ses credentials, l'appareil se configure en 30 min. Temps IT économisé : 4 jours/mois. Pour les Mac complexes, complément Jamf Now ponctuel.

Leçon: Intune gère Mac et Windows. Pour une PME 100% Microsoft + Mac, Intune suffit largement et évite la complexité de gérer 2 MDM. La frontière avec Jamf se discute au-delà de 50 Mac ou de besoins macOS très spécialisés.

PME industrielle wallonne (90 collaborateurs)

Contexte: 70 PC Windows (production + bureaux + commerciaux), 25 smartphones Android et iOS. Intune licencié dans M365 E3 mais jamais activé. Patches Windows aléatoires.

Impact: Activation Intune en mode pilote (15 PC pendant 3 semaines), puis rollout progressif sur 8 semaines. Mise en place Update Rings (Pilot, Broad, Critical), App Protection Policies pour le BYOD, BitLocker forcé. Score de conformité au-dessus de 90% en 3 mois.

Leçon: Intune était déjà payé dans la licence M365 E3. Il suffisait de l'activer. Cas extrêmement fréquent en PME : les fonctionnalités sont souscrites mais dorment. Faire un audit licence avant d'acheter de nouveaux outils.

Avant / Après — la différence concrète

Chapitre 5

Ce qui change quand on passe d'une posture artisanale à une posture maîtrisée.

	Flotte sans MDM	Flotte gérée par Intune
01	**INVENTAIRE APPAREILS**	
	Excel partiel, jamais à jour, appareils invisibles.	Console Intune temps réel, tous les appareils enrôlés.
02	**PROVISIONNEMENT PC NEUF**	
	4-8h par technicien IT, étalées sur 2-3 jours.	Autopilot : 30 min, par l'utilisateur final, sans technicien.
03	**PATCHES WINDOWS**	
	Aléatoires. Certains PC en Windows 10 21H2 en 2026.	Update Rings pilotées : Pilot, Broad, Critical. Déploiement contrôlé, parc homogène.
04	**BITLOCKER / FILEVAULT**	
	Activation aléatoire selon les postes. Clés de récupération perdues.	Forcé par Compliance. Parc entièrement chiffré. Clés déposées dans Entra ID.
05	**BYOD SMARTPHONE**	
	Aucune protection. Mail M365 sur device perso non maîtrisé.	App Protection : container chiffré, wipe sélectif, sans enrôlement complet.
06	**VOL DE PC**	
	Trou de sécurité ouvert plusieurs semaines. Notification APD souvent nécessaire.	Wipe à distance dans la journée. PC chiffré = pas de notification APD.
07	**ANTIVIRUS**	
	Désactivé sur certains postes. Aucune visibilité centrale.	Defender for Endpoint pilotage Intune. Visibilité, alertes, isolation automatique.

© 2026 FlashModz Enterprise — https://flashmodz.be

08 CONDITIONAL ACCESS

- Aveugle aux endpoints. MFA seul.
- Compliant Device Required. Zero Trust opérationnel.

Auto-évaluation de maturité

Chapitre 6

Faites le point en 5 minutes : où en êtes-vous vraiment ?

Pour chaque question, cochez la case qui correspond le mieux à votre situation actuelle.

SITUATION	NON	PARTIEL	OUI
1. Tous les PC Windows et Mac de l'entreprise sont enrôlés dans Intune (corporate-owned).	☐	☐	☐
2. Une Compliance Policy de base est appliquée : OS à jour, chiffrement actif, antivirus actif.	☐	☐	☐
3. Conditional Access exige "Compliant Device" pour les apps M365 sensibles (Outlook, SharePoint, Teams).	☐	☐	☐
4. Windows Autopilot est en place pour les nouveaux PC (commande pré-enrôlée).	☐	☐	☐
5. Les patches Windows sont pilotés via Update Rings (Pilot, Broad, Critical).	☐	☐	☐
6. BitLocker (Windows) et FileVault (Mac) sont forcés par Compliance Policy.	☐	☐	☐
7. Les apps métier sont déployées via Intune (pas installées manuellement).	☐	☐	☐
8. Pour le BYOD : App Protection Policies protègent les données pro sur smartphones perso.	☐	☐	☐
9. Une procédure de départ collaborateur déclenche un wipe sélectif ou complet de l'appareil.	☐	☐	☐
10. La conformité de la flotte est à > 90% sur le tableau de bord Intune.	☐	☐	☐
11. Les nouvelles versions d'OS (Windows, macOS, iOS) sont anticipées et testées en pilote.	☐	☐	☐
12. L'antivirus Defender for Endpoint est piloté par Intune (si licence E5 ou add-on).	☐	☐	☐

SCORING : Non = 0 pt • Partiel = 1 pt • Oui = 2 pts

< 40% : Critique • 40-70% : À renforcer • > 70% : Bonne posture

Ce qu'on met en place avec vous

Chapitre 7

Du cadrage au pilote, jusqu'au rollout généralisé. Sans imposer de contraintes inutiles aux utilisateurs.

Cadrage & dimensionnement Intune (3 jours)

Inventaire des appareils, identification des cas d'usage (corporate-owned, BYOD, Mac, mobile), choix de licence, conception de l'architecture cible. Livrable : architecture, plan de déploiement, ROI. Sans engagement.

Pilote Intune (10-15 appareils, 2-3 semaines)

Activation Intune, enrôlement d'un panel pilote (1-2 PC par profil utilisateur), configuration des Compliance Policies, Conditional Access "Compliant Device Required", BitLocker, antivirus Defender. Validation avant rollout général.

Rollout général + Autopilot

Enrôlement progressif de la flotte existante, mise en place Autopilot pour les nouveaux PC (commande directe chez Lenovo/Dell/HP avec pré-enregistrement), configuration des profils Windows 10/11, déploiement des apps métier via Intune. Pour 30-150 appareils.

BYOD et App Protection

Politique BYOD pour smartphones personnels : protection des données M365 sans enrôlement complet de l'appareil (App Protection Policies). Container chiffré, copier-coller restreint, wipe sélectif au départ. Conforme RGPD et NIS2.

Intégration Defender for Endpoint

Pour les PME en E5 ou avec add-on : intégration Intune + Defender for Endpoint. Compliance Policy basée sur le risque Defender, alertes EDR centralisées, isolation automatique d'un poste compromis. Niveau de protection grand compte.

© 2026 FlashModz Enterprise — https://flashmodz.be

macOS via Intune

Configuration Intune pour gérer macOS : enrôlement via ABM/DEP, FileVault, configurations système, déploiement d'apps Mac. Alternative à Jamf pour les flottes Mac < 50 appareils. Cohabitation possible avec Jamf si besoins avancés.

Run & maintien (option mensuelle)

Revue mensuelle de la conformité, gestion des nouvelles arrivées/départs, mises à jour des politiques (nouveau Windows, nouvel iOS), troubleshooting niveau 3. Forfait 1-3 jours/mois selon taille.

Notre façon de travailler

Une méthode en 4 étapes, progressive, pensée pour votre réalité. Pas de slides : des livrables concrets à chaque étape.

1

VOIR CLAIR

AUDIT

On commence par comprendre votre contexte : cartographie de l'existant, entretiens avec les équipes, identification des vrais risques. Pas de diagnostic à distance, pas d'hypothèses. On part de ce qui existe chez vous.

2

PRIORISER ENSEMBLE

PLAN

Qu'est-ce qui est urgent, qu'est-ce qui peut attendre ? On construit le plan avec vous, pas à votre place. Chaque action est pondérée par son impact, son effort et votre budget. Vous gardez la main sur les décisions.

3

STABILISER

ACTION

On corrige, on durcit, on protège. Des actions concrètes et mesurables, livrées par jalons. À chaque étape, vous validez avant qu'on avance. Pas de surprise, pas de dérive budgétaire.

4

TRANSMETTRE

AUTONOMIE

On documente tout ce qu'on fait, on forme vos équipes, on vous laisse les clés. Notre succès se mesure à votre capacité à continuer sans nous. Pas de dépendance, du transfert de compétences.

Feuille de route en phases

Chapitre 8

Un chemin balisé, du diagnostic à la maturité — étape par étape.

1	2	3	4	5
SEMAINE 1	SEMAINE 2-4	SEMAINE 4-6	SEMAINE 5-7	CONTINU
Cadrage	**Pilote**	**Rollout PC**	**Mobile & BYOD**	**Maintien**
• Inventaire • Personas • Architecture cible • Choix licence	• 10-15 appareils • Compliance Policies • Conditional Access • Validation usage	• Enrôlement flotte • Autopilot • Apps déployées • Patches via Update Rings	• App Protection • Mail mobile sécurisé • Wipe sélectif • Documentation user	• Revue mensuelle • Nouvelles versions OS • Ajustement policies • Onboarding/offboarding

Conseil méthodo

Chaque phase est un livrable autonome. Vous pouvez vous arrêter à n'importe quelle étape ou ralentir le rythme selon votre budget et votre charge interne. L'important n'est pas la vitesse — c'est de ne pas reculer.

Articulation Intune avec NIS2, RGPD, ISO 27001

Chapitre 9

Comment Intune sert directement plusieurs exigences réglementaires.

Gestion des actifs et accès

NIS2 art. 21

NIS2 exige un inventaire des actifs IT et un contrôle des accès basé sur le contexte. Intune fournit l'inventaire automatisé, les Compliance Policies définissent l'état attendu, Conditional Access conditionne l'accès au respect de cette compliance.

BÉNÉFICE CACHÉ :

Sans MDM, une PME part de loin sur ces exigences. Avec Intune correctement déployé, l'inventaire et le contrôle d'accès sont couverts, et le reste s'enchaîne logiquement.

Sécurité des appareils

RGPD art. 32

RGPD impose des mesures techniques pour protéger les données personnelles, dont chiffrement et gestion des appareils. Intune force BitLocker/FileVault, supervise l'antivirus, permet le wipe à distance en cas de perte.

BÉNÉFICE CACHÉ :

En cas de PC volé, prouver qu'il était chiffré (BitLocker forcé par MDM) évite en règle générale la notification aux personnes concernées. Vous évitez le stress, les coûts d'investigation et l'impact réputationnel.

Asset management

ISO 27001 A.8

Annex A d'ISO 27001:2022 exige une gestion des actifs (A.5.9) et un retour des actifs en fin de contrat (A.5.11). Intune répond aux deux points : inventaire automatisé + wipe au départ d'un collaborateur.

BÉNÉFICE CACHÉ :

Sur un audit ISO 27001, montrer la console Intune et faire la démonstration d'un wipe à distance valide ces points sans débat.

Zero Trust pour les endpoints

Conditional Access + Compliance

Combiner Conditional Access (Entra ID) avec une Compliance Policy (Intune) implémente la pierre angulaire du Zero Trust : "vérifier explicitement chaque accès, en fonction du contexte". Pas d'accès aux données si l'appareil n'est pas conforme.

BÉNÉFICE CACHÉ :

Le Zero Trust est promu par NIST, Microsoft et le CCB. Intune + Conditional Access est l'implémentation Microsoft de référence, accessible aux PME.

Checklist détachable — vos actions prioritaires

Imprimez cette page, cochez au fur et à mesure. Les colonnes EFFORT et IMPACT vous aident à séquencer.

		EFFORT	IMPACT	DÉLAI
☐	Vérifier que Intune est inclus dans votre licence M365 actuelle.	1	4	1 semaine
☐	Inventaire complet des appareils existants (Windows, Mac, iOS, Android).	2	3	2 semaines
☐	Pilote sur 10-15 appareils avec Compliance + Conditional Access.	3	5	4 semaines
☐	Forcer BitLocker/FileVault via Compliance Policy.	2	5	4 semaines
☐	Activer Conditional Access "Compliant Device Required" sur Outlook + SharePoint + Teams.	2	5	4 semaines
☐	Configurer Windows Autopilot avec votre fournisseur PC habituel.	3	4	6 semaines
☐	Mettre en place Update Rings (Pilot, Broad, Critical) pour Windows.	2	4	6 semaines
☐	Déployer App Protection Policies pour Outlook/Teams sur smartphones perso.	3	5	6 semaines
☐	Cataloguer et déployer les apps métier via Intune.	4	4	8 semaines
☐	Procédure de départ collaborateur : wipe automatisé.	2	4	6 semaines
☐	Documentation utilisateur : enrôlement, support, FAQ.	2	3	4 semaines

© 2026 FlashModz Enterprise — https://flashmodz.be

	EFFORT	IMPACT	DÉLAI
☐ Revue mensuelle conformité + ajustement policies.	● ○ ○ ○ ○	● ● ● ○ ○	Continu

CONSEIL : Commencez par les actions à fort impact ET faible effort (les "quick wins").

Si vous bloquez sur une action, contactez-nous : on vous oriente gratuitement.

© 2026 FlashModz Enterprise — https://flashmodz.be

Questions fréquentes

Chapitre 10

Les questions que nos clients posent le plus souvent — et nos réponses sans détour.

Q1. Quelle licence Microsoft pour avoir Intune ?

Intune est inclus dans : Microsoft 365 Business Premium (~22 €/utilisateur, jusqu'à 300 utilisateurs), Microsoft 365 E3 (~32 €/utilisateur), Microsoft 365 E5 (~52 €/utilisateur). Aussi disponible en standalone (Intune Plan 1, ~8 €/utilisateur) si vous n'avez pas M365. Pour la majorité des PME, Business Premium est la bonne porte d'entrée.

Q2. Combien d'appareils peut-on enrôler par utilisateur ?

Par défaut 5 appareils par utilisateur (configurable dans Entra ID Device Settings). Largement suffisant pour la plupart des PME (1 PC + 1 smartphone + 1 tablette). À ajuster pour les profils particuliers (ex : développeurs avec PC + Mac + 2 smartphones de test).

Q3. Intune gère-t-il vraiment macOS ?

Oui, Intune gère macOS via enrôlement ABM/DEP (recommandé) ou User Approved MDM. Fonctionnalités principales : profils de configuration, déploiement d'apps (.pkg), FileVault, antivirus, Compliance. Pour les flottes Mac < 50 appareils, Intune suffit. Au-delà ou pour des besoins très avancés (scripts complexes, packaging Munki), Jamf reste la référence.

Q4. Faut-il abandonner Active Directory pour Intune ?

Non, les deux cohabitent. Architecture typique PME : Active Directory on-prem (apps legacy, partages) + Hybrid Join Entra ID + Intune (gestion moderne). Pour les parcs déjà gérés par Configuration Manager, la co-gestion (co-management) permet de basculer les charges de travail (conformité, Windows Update, Endpoint Protection) vers Intune progressivement, sans big bang. Tendance long terme : Entra ID-only avec Intune pour les nouveaux postes, et conservation de l'AD pour les apps legacy le temps de la transition.

Q5. Que faire si un utilisateur refuse l'enrôlement BYOD ?

C'est son droit. Trois options possibles : (1) il fournit un appareil corporate dédié (gestion complète possible), (2) il utilise les emails uniquement via webmail navigateur (sans App Protection), (3) il n'a pas accès aux emails sur mobile. La politique BYOD doit être écrite, signée à l'embauche, et alignée avec la convention collective.

Q6. Quelle différence entre Intune et Microsoft 365 MDM Basic ?

Microsoft 365 MDM Basic est une version allégée incluse dans toutes les licences M365 (sans Intune). Couvre l'essentiel (PIN, chiffrement, wipe à distance) pour mobiles. Intune va beaucoup plus loin : Compliance Policies, App Protection, Configuration Profiles, Apps déployées, Autopilot. Si vous avez Business Premium ou E3+, vous avez Intune : utilisez-le.

Q7. Comment gérer les PC qui ne sont pas chez Microsoft (sur site, kiosks) ?

Intune gère parfaitement les modes "shared device" (PC partagés en kiosk, en magasin, en atelier) et les Windows IoT. Configuration via Profile Configuration "Shared multi-user device" ou "Kiosk". Idéal pour des cas spécifiques (caisse, borne d'accueil, atelier industriel).

© 2026 FlashModz Enterprise — https://flashmodz.be

Q8. Combien de temps pour un projet Intune en PME ?

50 utilisateurs : 3-4 semaines incluant pilote. 100-150 utilisateurs : 5-6 semaines. Au-delà : ajouter ~1 semaine par tranche de 50 utilisateurs supplémentaires + complexité des apps métier. Le pilote (10-15 appareils, 2-3 semaines) est crucial : il valide les politiques et limite les surprises au rollout.

Glossaire

Chapitre 11

Tous les termes techniques de ce guide, expliqués en français clair.

ABM

Apple Business Manager. Portail Apple pour entreprises permettant l'achat groupé d'apps, l'enrôlement automatisé d'appareils Apple via DEP/ADE, et la gestion des Managed Apple ID.

Autopilot

Service Microsoft de provisionnement zero-touch d'appareils Windows. L'utilisateur reçoit un PC neuf, le démarre, se connecte avec ses credentials, le PC se configure tout seul.

Azure Policy

Service Azure qui applique automatiquement des règles de gouvernance (régions autorisées, tags obligatoires, taille VM max, configurations de sécurité).

BYOD

Bring Your Own Device. Modèle où les collaborateurs utilisent leur appareil personnel pour le travail. Pose des défis de séparation données pro/perso.

Compliance Policy

Règle MDM (Intune, Jamf) qui définit ce qui est attendu d'un appareil pour être considéré conforme : OS à jour, chiffrement actif, MFA, antivirus actif.

Conditional Access

Fonctionnalité Entra ID (ex Azure AD) qui applique des règles d'accès en fonction du contexte : utilisateur, appareil, localisation, application, niveau de risque.

COPE

Corporate-Owned, Personally Enabled. Appareil fourni par l'entreprise mais utilisable à des fins personnelles. Compromis BYOD/COBO.

Defender for Office 365

Suite anti-phishing et anti-malware Microsoft pour M365 : Safe Links, Safe Attachments, protection anti-usurpation. Plan 1 inclus dans Business Premium, Plan 2 (investigation, simulation d'attaques) dans E5.

DEP / ADE

Device Enrollment Program / Automated Device Enrollment. Enrôlement automatique d'appareils Apple achetés chez un revendeur agréé. Le device s'enrôle dès le premier démarrage.

DLP

Data Loss Prevention. Protection contre la fuite de données sensibles (PII, financières, propriété intellectuelle) via politiques automatisées sur emails, fichiers, partages.

© 2026 FlashModz Enterprise — https://flashmodz.be

Entra ID

Nouveau nom d'Azure Active Directory depuis 2023. Annuaire d'identités cloud Microsoft. Le plan P1 (Conditional Access) est inclus dans Business Premium et E3, le plan P2 (PIM, Identity Protection) dans E5.

FileVault

Chiffrement disque natif de macOS, basé sur XTS-AES-128 avec clé de 256 bits. Activable par MDM, avec dépôt centralisé de la clé de récupération (Jamf, Intune, Mosyle).

Hub-Spoke

Topologie réseau Azure classique : un VNet "hub" centralise les services partagés (firewall, DNS, identité), des VNets "spokes" hébergent les workloads.

IaaS

Infrastructure as a Service. Ressources cloud bas niveau (VM, stockage, réseau) que vous configurez vous-même. Exemples : Azure VM, AWS EC2, Google Compute Engine.

Landing Zone

Architecture Azure de référence (Cloud Adoption Framework). Fondation conçue pour scaler de façon cohérente : networking, identités, gouvernance, sécurité.

Management Group

Niveau Azure au-dessus des subscriptions, permettant d'appliquer des policies et accès en cascade. Hiérarchie : Tenant Root > MG > Subscription > Resource Group > Resource.

MDM

Mobile Device Management. Solution de gestion centralisée d'un parc d'appareils (Windows, Mac, iOS, Android). Permet déploiement, configuration, sécurité, conformité.

MFA

Multi-Factor Authentication. Authentification à plusieurs facteurs (mot de passe + appli mobile, clé physique ou SMS). Selon Microsoft, bloque plus de 99% des attaques par compromission de compte.

PaaS

Platform as a Service. Environnement cloud géré pour exécuter des applications sans gérer l'OS sous-jacent. Exemples : Azure App Service, AWS Elastic Beanstalk.

SaaS

Software as a Service. Application livrée en mode cloud, accessible par navigateur, mise à jour automatique. Exemples : M365, Salesforce, Slack.

Sensitivity Labels

Étiquettes de classification dans M365 (Public, Interne, Confidentiel, Très confidentiel) qui appliquent automatiquement chiffrement, watermark, restrictions de partage.

© 2026 FlashModz Enterprise — https://flashmodz.be

Subscription Azure

Conteneur de facturation Azure. Une organisation a typiquement plusieurs subscriptions (prod, dev, test, sandbox) pour isoler workloads et budgets.

Tenant

Instance dédiée d'un service cloud (M365, Azure, Salesforce, etc.) propre à une organisation. Identifiée par un domaine et un GUID unique.

Zero Trust

Modèle de sécurité où aucun utilisateur, appareil ou réseau n'est implicitement de confiance. Vérification continue, accès minimal, segmentation forte. Promu par NIST, Microsoft, Google.

Ressources externes

Chapitre 12

Sites officiels, outils gratuits et lectures recommandées pour aller plus loin.

Microsoft Learn

learn.microsoft.com

Documentation officielle Microsoft, gratuite, exhaustive. Tutoriels, parcours certifications, références pour M365, Azure, Intune, Defender, Entra.

Microsoft Cloud Adoption Framework

aka.ms/caf

Référentiel officiel Microsoft pour adopter Azure de façon structurée. Méthodologie, modèles, guides Landing Zone.

Microsoft Security Score

security.microsoft.com

Tableau de bord intégré M365 qui note votre sécurité sur 100 et propose les actions prioritaires. Premier outil à consulter sur tout tenant.

Apple Business Manager

business.apple.com

Portail Apple pour entreprises. Gestion achats groupés, enrôlement zero-touch (DEP/ADE), Managed Apple ID. Gratuit.

Apple Platform Deployment

support.apple.com/guide/deployment

Documentation officielle Apple pour le déploiement entreprise (macOS, iOS, iPadOS, tvOS). Référence pour configurations MDM.

Jamf Nation Community

community.jamf.com

Communauté Jamf : forums, scripts partagés, retours d'expérience admins MDM Apple en entreprise. Très actif.

NIST SP 800-124

csrc.nist.gov/publications/detail/sp/800-124/rev-2/final

Standard NIST pour la gestion des mobiles en entreprise. Référentiel reconnu pour les politiques MDM.

CIS Microsoft 365 Benchmark

cisecurity.org/benchmark/microsoft_365

Référentiel de hardening M365 par le Center for Internet Security. Recommandations gratuites, niveau 1 et 2.

CIS Microsoft Azure Foundations Benchmark

cisecurity.org/benchmark/azure

Référentiel CIS pour sécuriser une fondation Azure. Politiques applicables via Azure Policy ou Defender for Cloud.

© 2026 FlashModz Enterprise — https://flashmodz.be

CCB — Centre pour la Cybersécurité Belgique ccb.belgium.be

Recommandations cyber publiques pour les entités belges. Guides M365, durcissement, gestion des accès, ransomware.

À propos de FlashModz Enterprise

FlashModz Enterprise est un cabinet d'expertise IT opérationnelle, fondé par Jérémy Manet et basé à Farciennes, dans la région de Charleroi. Conseil et mise en œuvre concrète : sécurité, audit et pentest, automatisation Linux/DevOps et formations — pour les particuliers comme pour les entreprises, en Belgique et à l'international. Notre conviction : les ressources, les connaissances pointues et les outils des grandes entreprises doivent être accessibles aux PME et aux indépendants. À leur échelle. À leur budget. Avec la même rigueur.

CE QUE NOUS FAISONS

- Audit sécurité
- Pentest & rapport
- Sprint de stabilisation
- Team Lead fractionnel
- Formations Linux / DevOps

CERTIFICATIONS & RÉFÉRENTIELS

- CWNA · Ruckus
- Cisco Meraki
- Fortinet NSE
- Veeam
- Jamf · Apple
- OWASP / PTES
- NIS2
- ISO 27001
- RGPD

Jérémy Manet

Fondateur · Ingénieur & architecte système/réseau

Plus de 15 ans en architecture et ingénierie système/réseau : infrastructure, Wi-Fi d'entreprise, sécurité et virtualisation. Également management (people & technique) et gouvernance IT en tant que Process Owner COBIT, DORA et NIS2. Certifié CWNA, Cisco Meraki, Fortinet, Veeam, Jamf, Apple. Technologies : Aruba, HPE, Cisco, FortiGate, Nutanix.

Spécialités : Architecture · Réseau · Wi-Fi · Sécurité · Virtualisation · Gouvernance · NIS2 · DORA

De l’expertise IT pour ce qui compte vraiment.

contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

LinkedIn Facebook TikTok Avis Google

© 2026 FlashModz Enterprise — https://flashmodz.be

IDENTITÉ LÉGALE

FlashModz Enterprise

DÉNOMINATION	FlashModz Enterprise
FONDATEUR	Jérémy Manet
SIÈGE SOCIAL	Rue du Wainage 18, 6240 Farciennes (Belgique)
BCE / TVA	1035.510.038 · BE 1035.510.038
EU VAT	2.386.268.987
ZONES DESSERVIES	Charleroi et alentours (B2C) · Belgique & international (B2B)
CONTACT	contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

FlashModz

Construisons votre projet Intune

Chaque entreprise est unique. Chaque idée a ses contraintes,
son contexte et ses priorités.

C'est pourquoi nous ne proposons pas de grille tarifaire figée.
Nous préférons échanger avec vous, comprendre votre situation
et construire une réponse adaptée à vos vrais besoins.

Parlons de votre situation

EMAIL

contact@flashmodz.be

TELEPHONE

+32 471 87 87 07

WEB

flashmodz.be

RETROUVEZ-NOUS

LinkedIn · Facebook · TikTok · Avis Google

Scannez pour accéder
à ce document

BCE 1035.510.038 | Charleroi · Belgique & international