FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

# Sécurisation de Microsoft 365 / Office 365

Guide M365 / PME

Microsoft 365 est puissant mais livré ouvert par défaut. Ce guide donne les configurations de sécurité que Microsoft ne vous impose pas et que la majorité des PME omettent : MFA, Conditional Access, Defender, DLP, partage externe.

Scannez pour acceder a la version en ligne

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

https://flashmodz.be

# L'essentiel en 5 minutes

*Microsoft 365 est puissant mais livré ouvert. 2 semaines de durcissement structurent durablement votre sécurité collaborative.*

### 1 MFA universelle : la mesure qui rapporte le plus

Activer MFA pour tous les utilisateurs (pas juste les admins) est la mesure n°1 pour un tenant M365. Selon Microsoft, elle bloque plus de 99% des attaques par compromission de compte. L'argument "ça gêne les utilisateurs" ne tient plus en 2026 : Microsoft Authenticator et Windows Hello rendent l'authentification fluide. Un seul incident BEC coûte plus cher que des années de licences et le projet de durcissement réunis.

### 2 Conditional Access remplace les politiques rigides

Au lieu de "MFA partout, tout le temps", Conditional Access permet une approche contextuelle : MFA seulement hors du bureau, MFA renforcée pour les admins, blocage des connexions impossibles, exigence d'appareil conforme pour les apps sensibles. C'est plus sécurisé ET plus fluide pour l'utilisateur.

### 3 Defender for Office 365 doit être configuré, pas juste acheté

Microsoft 365 Business Premium inclut Defender for Office 365 P1, qui filtre l'essentiel du phishing à condition d'être configuré. Anti-Phishing, Safe Links, Safe Attachments et Spoof Intelligence ne sont pas activés par défaut : comptez 1-2 jours de configuration, puis un tuning trimestriel.

### 4 Le partage externe est un risque RGPD majeur

Les liens "Anyone with the link" SharePoint/OneDrive s'accumulent de façon invisible. Une PME de 50 personnes en accumule typiquement des milliers. Auditer et restreindre ce partage est un chantier RGPD à part entière, pas un détail technique.

### 5 CIS Benchmark = référentiel gratuit, recommandations concrètes

Le CIS Microsoft 365 Foundations Benchmark détaille des dizaines de contrôles avec scripts PowerShell prêts à l'emploi. Aligner votre tenant sur CIS Niveau 1 vous place très au-dessus de la moyenne des tenants PME. C'est un objectif réaliste, gratuit et reconnu par les auditeurs.

**Et maintenant ?**

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

*Document conçu pour Indépendants & PME — Microsoft 365 / Office 365 · Lecture : ~15-20 min · Édition 2026*

# Table des matières

*Naviguez rapidement vers les sections qui vous concernent.*

# Le marché belge en chiffres

Chapitre 1

**99,9%**

des attaques par compromission de compte bloquées par MFA, selon Microsoft

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

**2019**

depuis octobre 2019, Microsoft active Security Defaults sur les nouveaux tenants. Les tenants plus anciens restent souvent ouverts

**180 jours**

rétention des journaux d'audit en Purview Audit Standard. 1 an avec Audit Premium (E5)

**2 semaines**

durée typique d'un projet de durcissement M365 pour 50 utilisateurs

## Contexte & enjeux

Microsoft 365 est un produit puissant, et complexe à sécuriser correctement. Le tenant que vous a livré votre revendeur Microsoft est le plus souvent configuré "par défaut", c'est-à-dire ouvert au maximum pour ne pas gêner l'usage. C'est cohérent côté Microsoft. C'est dangereux côté entreprise.

Les attaquants le savent. Compromettre un tenant M365 est l'un des vecteurs d'intrusion les plus rentables : une fois dans Exchange Online, ils accèdent à des années d'emails, exfiltrent des fichiers OneDrive et SharePoint, posent des règles de transfert d'inbox pour persister, puis lancent des attaques BEC (Business Email Compromise) ciblées sur vos clients et fournisseurs. Le Verizon Data Breach Investigations Report chiffre le montant médian détourné par attaque BEC en dizaines de milliers de dollars. Pour une PME, un seul incident suffit à plomber l'année.

La bonne nouvelle : Microsoft 365 contient déjà les briques nécessaires. Il faut les activer et les configurer. MFA obligatoire, Conditional Access, blocage de l'authentification héritée (POP, IMAP, SMTP basique), Defender for Office 365, DKIM et DMARC sur vos domaines, DLP, Sensitivity Labels, journaux d'audit, restrictions de partage externe, Privileged Identity Management. La quasi-totalité est incluse dans Microsoft 365 Business Premium (~22 €/utilisateur/mois) ou dans E3/E5 pour les structures plus grandes.

Ce guide vous donne la liste des configurations à appliquer, dans l'ordre, en expliquant pourquoi et avec quel impact utilisateur. L'objectif : un Secure Score en forte hausse sans dégrader la productivité de vos collaborateurs. Compter 2 semaines de projet pour 50 utilisateurs si vous suivez la méthode.

> *"Sécuriser un tenant M365 n'est pas un projet IT, c'est une hygiène de base. Tant qu'on traite ça comme un sujet technique optionnel, des PME continueront de payer le prix fort pour une simple compromission BEC."*
>
> — Jérémy Manet, FlashModz Enterprise

# Ce que la majorité des PME laisse ouvert dans M365

Chapitre 2

*Les configurations par défaut de Microsoft sont permissives. Voici les angles morts les plus exploités.*

### MFA non généralisée — la faille n°1

Microsoft active "Security Defaults" sur les nouveaux tenants depuis octobre 2019, ce qui force MFA. Mais les tenants antérieurs et beaucoup de tenants migrés via revendeur n'ont PAS MFA active sur les utilisateurs courants. Résultat : un mot de passe leaké suffit pour entrer. Microsoft répète depuis des années que MFA bloque plus de 99% des attaques par compromission de compte. Le déploiement traîne quand même.

### Comptes admins permanents et partagés

Beaucoup de PME n'ont qu'un seul "Global Administrator", utilisé au quotidien pour les emails ET pour les configs admin. Les comptes admin partagés (admin@, it@) sont fréquents. C'est le scénario rêvé pour un attaquant : compromettre un compte sans MFA dont les credentials traînent dans un fichier Excel partagé.

### Partage externe SharePoint/OneDrive sans contrôle

Par défaut, M365 autorise le partage public de fichiers SharePoint/OneDrive avec n'importe quelle adresse email. Les utilisateurs créent des liens "Anyone with the link" qui restent valides indéfiniment. Auditer ces liens dans une PME de 50 personnes révèle typiquement des milliers de partages actifs, dont une partie porte des données sensibles ou personnelles.

### Defender for Office 365 acheté mais non configuré

Vous avez peut-être Microsoft 365 Business Premium, qui inclut Defender for Office 365 P1. Mais il faut le configurer : Anti-Phishing, Safe Links, Safe Attachments, Spoof Intelligence. Sans configuration, c'est un produit dormant. Avec configuration, la grande majorité des phishings est bloquée avant la boîte de réception.

### Aucune journalisation utile en cas d'incident

Quand un compte est compromis, retracer l'activité (emails envoyés, fichiers consultés, règles inbox créées) demande un Audit Log activé ET des rapports configurés. Purview Audit Standard conserve 180 jours de logs, Audit Premium (E5) un an. Beaucoup de PME découvrent en pleine crise que leur audit log était désactivé ou trop court. Impossible alors de mesurer l'impact.

## Apps consenties par les utilisateurs sans validation admin

Par défaut, vos utilisateurs peuvent autoriser des apps tierces à accéder à leurs emails et fichiers en cliquant "Accepter" sur un consentement OAuth. Les attaquants envoient des phishings consent-grant qui font passer une app malveillante pour un service légitime. Une fois accordé, l'attaquant a accès même sans mot de passe et même avec MFA. Désactivation indispensable.

# Mythes vs Réalité

Chapitre 3

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

01

ON ENTEND SOUVENT

*M365 est sécurisé out-of-the-box, Microsoft s'en occupe.*

EN RÉALITÉ — *Shared Responsibility — la moitié vous incombe*

Microsoft sécurise l'infrastructure (datacenters, plateforme). Vous êtes responsable de la configuration de VOTRE tenant : MFA, Conditional Access, partage, DLP. C'est le "Shared Responsibility Model" et il est non-négociable.

02

ON ENTEND SOUVENT

*Si on impose MFA, les utilisateurs vont se révolter et demander de revenir en arrière.*

EN RÉALITÉ — *MFA en 2026 = friction quasi nulle*

Avec Microsoft Authenticator (push notification) ou Windows Hello (biométrie), MFA prend 1-2 secondes. La friction est faible. Les utilisateurs s'y adaptent en 1 semaine. La résistance est principalement managériale, pas utilisateur.

03

ON ENTEND SOUVENT

*On a Defender for Office 365, on est protégés.*

EN RÉALITÉ — *Defender configuré ≠ Defender installé*

Defender doit être CONFIGURÉ. Sans configuration des Anti-Phishing, Safe Links, Safe Attachments, c'est un produit dormant. Avec configuration, l'essentiel du phishing est bloqué en amont. La nuance fait toute la différence.

04

ON ENTEND SOUVENT

*L'antivirus sur les postes utilisateurs nous protège des phishings M365.*

EN RÉALITÉ — *Phishing 2026 ≠ malware classique*

Les phishings M365 modernes ne déposent pas de malware : ils volent des credentials sur de faux portails Office 365 ou demandent un consent OAuth malveillant. L'antivirus poste est aveugle. La protection se joue côté email (Defender) et côté identité (Conditional Access).

05

ON ENTEND SOUVENT

*Notre revendeur Microsoft a configuré le tenant, on doit être bons.*

EN RÉALITÉ

*Revendeur ≠ expert sécurité*

Les revendeurs Microsoft sont d'excellents commerciaux et licenseurs. Leur métier, c'est la vente de licences. Le durcissement du tenant reste à votre charge, et il est rarement fait en sortie d'usine. Vérifiez votre Secure Score : il donne la réponse en 5 minutes.

06

ON ENTEND SOUVENT

*Microsoft 365 Business Premium coûte plus cher, on reste sur Business Standard.*

EN RÉALITÉ

*+10 €/mois = tout le socle sécurité*

L'écart entre Business Standard (~12,50 €) et Business Premium (~22 €) est d'environ 10 €/utilisateur/mois, soit 6 000 €/an pour 50 utilisateurs. Pour ce prix, vous obtenez Conditional Access, Intune, Defender for Office 365 P1 et les Sensitivity Labels. Un seul incident BEC coûte plus cher que des années de cet écart.

# Cas concrets en Belgique

Chapitre 4

*Trois scénarios types, inspirés de situations réelles et anonymisés.*

## Cabinet juridique liégeois (35 collaborateurs)

**Contexte:** Tenant M365 historique, Security Defaults désactivés lors d'une migration en 2022. MFA seulement sur le Global Admin. Pas de Defender configuré.

**Impact:** Phishing ciblé sur l'associé senior, mot de passe entré sur un faux portail Office 365. Inbox forwarding rule créée discrètement vers un email criminel. Pendant 6 semaines, tous les emails de l'associé sortaient en double. Découverte fortuite par un client qui a noté un mail "bizarre". Coût : des dizaines de milliers d'euros d'investigation, plus la perte d'un dossier client.

**Leçon:** MFA seul aurait évité le scénario. Le surcoût annuel (Microsoft 365 Business Premium pour 35 users = ~9 200 €) est dérisoire face au coût d'un seul incident.

## PME industrielle namuroise (110 collaborateurs)

**Contexte:** M365 E3, MFA active. Mais partage externe activé sans contrainte sur SharePoint. Les commerciaux partagent des dossiers clients via "Anyone with the link".

**Impact:** Audit suite à une revue RGPD : plusieurs milliers de liens de partage actifs, dont des centaines sur des dossiers clients confidentiels. Plusieurs liens datent de 2022, jamais révoqués, encore utilisés par d'anciens commerciaux. Résultat : un chantier de mise en conformité RGPD à part entière.

**Leçon:** La sécurité ne s'arrête pas au login. Le partage externe est un sujet à part entière, qui demande politique, configuration tenant et formation utilisateurs. Le service ITAA et l'APD prennent ces sujets très au sérieux.

## Cabinet d'architecture bruxellois (22 collaborateurs)

**Contexte:** M365 Business Premium souscrit auprès d'un revendeur. Tenant "out of the box" jamais durci. Defender for Office 365 inclus mais non configuré.

**Impact:** Audit Security Score : 28/100. Plan de durcissement en 8 jours d'intervention répartis sur 3 semaines. Activation MFA + Conditional Access + Defender + DLP + restrictions partage. Score final : 78/100. Aucun ticket utilisateur post-déploiement.

**Leçon:** Un tenant correctement durci coûte une dizaine de jours-homme une fois pour toutes. L'usage utilisateur n'est pas dégradé si la conduite du changement est faite (notif + MFA setup + courte formation).

# Avant / Après — la différence concrète

Chapitre 5

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

| Tenant M365 par défaut | Tenant M365 durci CIS Niveau 1 |
|---|---|
| **01 AUTHENTIFICATION** | |
| Mot de passe seul. Quelques utilisateurs ont activé MFA volontairement. | MFA forcée pour 100% des utilisateurs. Conditional Access contextuel. |
| **02 COMPTES ADMIN** | |
| 1 Global Administrator utilisé au quotidien pour les emails. Mot de passe dans un Excel partagé. | Comptes admin dédiés, MFA token physique, activation just-in-time via PIM. |
| **03 PHISHINGS ENTRANTS** | |
| Filtrage EOP de base uniquement. Les phishings ciblés passent. | Defender for Office 365 configuré : Anti-Phishing, Safe Links, Safe Attachments. La grande majorité bloquée avant la boîte. |
| **04 PARTAGE EXTERNE** | |
| Liens "Anyone with the link" sans expiration. Utilisateurs créent ce qu'ils veulent. | Politique formelle : domaines autorisés, expiration 90 jours, classification obligatoire. |
| **05 AUDIT LOGS** | |
| Désactivés ou rétention 30 jours. Investigation incident impossible. | Activés, rétention étendue, alertes sur événements sensibles, exports SIEM. |
| **06 APPS TIERCES (OAUTH)** | |
| Utilisateurs consentent librement. Apps malveillantes peuvent être autorisées. | Admin consent obligatoire. Catalogue d'apps validées. Surveillance des consentements. |

## 07 CLASSIFICATION DONNÉES

- Aucune. Toutes les données sont au même niveau.
- Sensitivity Labels (Public, Interne, Confidentiel, Très confidentiel) avec actions automatiques.

## 08 SECURITY SCORE

- 30-40 / 100 typique.
- 70-85 / 100 après projet.

# 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. MFA est forcée pour 100% des utilisateurs (pas juste les admins). | ☐ | ☐ | ☐ |
| 2. Au moins une politique Conditional Access bloque l'authentification legacy (POP, IMAP, SMTP basic). | ☐ | ☐ | ☐ |
| 3. Les comptes Global Administrator sont dédiés (pas utilisés pour les emails au quotidien). | ☐ | ☐ | ☐ |
| 4. Les comptes admin sont protégés par MFA forte (Authenticator number-matching ou clé physique). | ☐ | ☐ | ☐ |
| 5. Defender for Office 365 est configuré : Anti-Phishing, Safe Links, Safe Attachments actifs. | ☐ | ☐ | ☐ |
| 6. Le partage externe SharePoint/OneDrive est limité par politique (domaines autorisés, expiration). | ☐ | ☐ | ☐ |
| 7. Le consentement utilisateur aux apps OAuth tierces est désactivé (admin consent obligatoire). | ☐ | ☐ | ☐ |
| 8. Audit Log Search est activé et la rétention est étendue (>90 jours). | ☐ | ☐ | ☐ |
| 9. Des alertes admin sont configurées sur les événements sensibles (inbox rules, élévations, MFA fails). | ☐ | ☐ | ☐ |
| 10. Au moins 3 Sensitivity Labels sont déployés (Public, Interne, Confidentiel ou équivalents). | ☐ | ☐ | ☐ |
| 11. Une politique DLP basique est active (au minimum sur PII : emails et carte bancaire). | ☐ | ☐ | ☐ |
| 12. Un Security Score > = 70/100 est maintenu et revu trimestriellement. | ☐ | ☐ | ☐ |

**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

*Audit, durcissement, formation. Sans dégrader l'expérience utilisateur.*

## Audit Security Score & gap analysis

Analyse de votre tenant M365 sur 80 points de contrôle (CIS Benchmark + recommandations Microsoft). Livrable : Security Score actuel, top 15 actions prioritaires, estimation effort. Forfait 3 jours, sans engagement de suite.

## Durcissement complet en 2 semaines

Activation MFA pour tous, mise en place Conditional Access (3-5 policies typiques), configuration Defender for Office 365, DLP basique, restrictions partage externe, audit logs étendus, alertes admin. Pour 25-100 utilisateurs.

## Refonte des comptes admins (PIM)

Création de comptes admins dédiés (séparés des comptes mailbox), mise en place Privileged Identity Management (PIM) pour activation just-in-time des rôles admin avec MFA renforcée. Élimine les comptes admin permanents.

## Politique de partage externe contrôlé

Définition d'une politique partage adaptée à votre métier : qui peut partager, vers quels domaines, durée d'expiration, classification obligatoire. Configuration SharePoint + OneDrive + Teams + Sensitivity Labels.

## Sensitivity Labels & DLP métier

Classification (Public, Interne, Confidentiel, Très confidentiel) avec actions automatiques : chiffrement, watermark, restriction partage. Politiques DLP métier (PII, données financières, propriété intellectuelle). Intégration Outlook + SharePoint + OneDrive.

### Formation utilisateurs (1h en ligne)

Session de sensibilisation pour vos collaborateurs : pourquoi MFA, comment l'activer, comment reconnaître un phishing M365, bonnes pratiques de partage. Format en ligne, replay disponible. Inclus dans le projet de durcissement.

### Surveillance continue (option)

Revue trimestrielle de votre Security Score, alerte sur dérive de configuration, ajustement des Conditional Access selon nouveaux scénarios, analyse des incidents M365. Forfait mensuel ou trimestriel.

## 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 1-2 | SEMAINE 2 | SEMAINE 2-3 | CONTINU |
| **Audit** | **Identités** | **Email & data** | **Visibilité** | **Maintien** |
| • Security Score<br>• Inventaire utilisateurs/admins<br>• Cartographie partage externe<br>• Plan de durcissement | • MFA universelle<br>• Conditional Access<br>• Comptes admin dédiés<br>• PIM (si éligible) | • Defender configuré<br>• Restrictions partage<br>• Sensitivity Labels<br>• DLP basique | • Audit logs étendus<br>• Alertes admin<br>• Tableau de bord<br>• Formation users | • Revue trimestrielle<br>• Score tracking<br>• Ajustements<br>• Sensibilisation |

**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 M365 / NIS2 / RGPD / ISO 27001

Chapitre 9

*Comment un tenant M365 bien configuré sert directement votre conformité.*

### Mesures techniques cyber

NIS2 art. 21

NIS2 exige des mesures techniques proportionnées : MFA, gestion des accès, surveillance, gestion des incidents. Un tenant M365 durci coche directement 6-7 des 10 points de l'article 21.

**BÉNÉFICE CACHÉ :**

*Investir dans la sécurité M365, c'est investir dans NIS2, pas un effort en plus.*

### Sécurité du traitement

RGPD art. 32

RGPD impose des "mesures techniques et organisationnelles appropriées" pour protéger les données personnelles. Pour une PME en M365, cela inclut MFA, chiffrement (BitLocker, EFS, Sensitivity Labels), DLP, audit logs.

**BÉNÉFICE CACHÉ :**

*En cas de contrôle ou d'incident RGPD, prouver un tenant durci CIS-aligné transforme le contrôle en formalité.*

### Contrôles ISO sur M365

ISO 27001 Annex A

L'Annex A d'ISO 27001:2022 contient ~30 contrôles directement applicables à un tenant M365 : A.5.15 (gestion des accès), A.5.17 (authentification), A.8.20 (sécurité réseau), A.8.24 (chiffrement), A.5.10 (utilisation des informations).

**BÉNÉFICE CACHÉ :**

*Un tenant aligné CIS Microsoft 365 Benchmark couvre l'essentiel d'un audit ISO 27001 sur le périmètre cloud collaboratif.*

### Référentiel reconnu et gratuit

CIS Benchmark M365

Le CIS Microsoft 365 Foundations Benchmark publie des dizaines de recommandations détaillées (niveau 1 = essentiel, niveau 2 = avancé). Mis à jour régulièrement. Référence en audit cyber.

**BÉNÉFICE CACHÉ :**

*Aligner votre tenant sur CIS Niveau 1 vous place très au-dessus de la moyenne des tenants PME. Objectif réaliste en 2 semaines de projet.*

# 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 |
|---|---|---|---|
| ☐ Activer MFA pour 100% des utilisateurs (Security Defaults ou Conditional Access). | ●●○○○ | ●●●●● | 1 semaine |
| ☐ Créer des comptes Global Administrator dédiés (séparés des mailboxes). | ●○○○○ | ●●●●● | 1 semaine |
| ☐ Bloquer l'authentification legacy (POP/IMAP/SMTP basic) via Conditional Access. | ●○○○○ | ●●●●○ | 1 semaine |
| ☐ Configurer Defender for Office 365 (Anti-Phishing, Safe Links, Safe Attachments). | ●●○○○ | ●●●●● | 2 semaines |
| ☐ Désactiver le consentement utilisateur aux apps OAuth tierces. | ●○○○○ | ●●●●○ | 1 semaine |
| ☐ Activer Audit Log Search avec rétention étendue. | ●○○○○ | ●●●●○ | 1 semaine |
| ☐ Définir une politique de partage externe (SharePoint + OneDrive). | ●●●○○ | ●●●●● | 3 semaines |
| ☐ Configurer alertes admin sur événements sensibles (inbox rules, élévations). | ●●○○○ | ●●●●○ | 2 semaines |
| ☐ Déployer 3 Sensitivity Labels (Public, Interne, Confidentiel). | ●●●○○ | ●●●●○ | 4 semaines |
| ☐ Mettre en place une politique DLP basique sur PII. | ●●●○○ | ●●●●○ | 4 semaines |
| ☐ Activer Privileged Identity Management (PIM) pour les rôles admin. | ●●●○○ | ●●●●● | 3 semaines |

| | | EFFORT | IMPACT | DÉLAI |
|---|---|---|---|---|
| ☐ | Audit complet utilisateurs + désactivation des comptes inactifs > 90 jours. | ●●○○○ | ●●●○○ | 2 semaines |
| ☐ | Formation utilisateurs (1h en ligne) sur les bonnes pratiques M365. | ●●○○○ | ●●●○○ | 4 semaines |
| ☐ | Revue trimestrielle du Security Score et ajustements. | ●○○○○ | ●●●●○ | 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.*

# Questions fréquentes

Chapitre 10

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

### Q1. Quelle licence M365 minimum pour avoir une sécurité correcte ?

Microsoft 365 Business Premium pour les PME jusqu'à 300 utilisateurs (~22 €/utilisateur/mois). Il ajoute à Business Standard tout le socle sécurité : Entra ID P1 (Conditional Access), Intune, Defender for Office 365 P1, Sensitivity Labels. Business Basic (~6 €, apps web uniquement) et Business Standard (~12,50 €, apps de bureau) n'incluent ni Conditional Access, ni Intune, ni Defender for Office 365. Au-dessus de 300 utilisateurs : E3 + add-on E5 Security, ou directement E5.

### Q2. Combien de temps pour durcir un tenant M365 ?

Pour 25-100 utilisateurs : 8 à 12 jours-homme étalés sur 2-3 semaines. Au-delà : ajouter ~1 jour par tranche de 50 users supplémentaires. Pas linéaire à la taille car le travail est principalement sur la configuration tenant, pas sur les utilisateurs.

### Q3. Faut-il prévenir les utilisateurs avant d'activer MFA ?

Oui, impérativement. Annonce 2 semaines avant, 1 semaine avant, 1 jour avant. Fournir un tutoriel d'enrôlement Microsoft Authenticator (5 min). Idéalement : courte session live (30 min) pour expliquer pourquoi et répondre aux questions. La résistance vient du défaut d'explication, pas du produit.

### Q4. Que faire si on a déjà un partenaire IT externe ?

Deux options : (1) lui demander un audit Security Score documenté et un plan de remédiation, (2) faire un audit indépendant (3 jours) pour valider l'état des lieux et identifier les écarts. Beaucoup de partenaires IT généralistes manquent d'expertise sécurité M365. Ce n'est pas une critique, juste un constat sectoriel.

### Q5. Conditional Access ou Security Defaults : lequel choisir ?

Security Defaults (gratuit, simple) si vous avez moins de 100 utilisateurs et un usage standard. Conditional Access (Entra ID P1, inclus dans Business Premium) dès que vous avez besoin de finesse : exclusions, contextes, scénarios métier. Conditional Access remplace Security Defaults, il ne s'y ajoute pas.

### Q6. Comment gérer les boîtes partagées (Shared Mailboxes) ?

Les boîtes partagées sont des comptes utilisateur sans licence dédiée. Les accès se font via les comptes des utilisateurs, pas via un mot de passe propre. Important : (1) bloquer la connexion directe sur ces comptes (Block sign-in), (2) auditer les accès, (3) ne pas les utiliser comme adresse d'expédition automatique sans validation.

### Q7. Faut-il bloquer les protocoles legacy (POP, IMAP) ?

Oui, sauf cas métier prouvé. Les protocoles legacy ne supportent pas MFA, donc tout compte qui les autorise reste vulnérable malgré MFA partout ailleurs. Désactivation via Conditional Access "Block Legacy Authentication". Vérifier avant que personne n'utilise un client mail antédiluvien (Outlook 2010, Thunderbird sans modern auth).

## Q8. Comment gérer les comptes "service" (apps qui envoient des emails) ?

Microsoft retire progressivement l'authentification basique, y compris SMTP AUTH. Privilégier Graph API avec permissions applicatives (OAuth 2.0) pour l'envoi applicatif, ou un service de relais dédié. Documenter chaque compte de service, le surveiller via les audit logs, et le revoir au moins une fois par an.

# 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.

### 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.

### 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.

**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

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

# Verrouillez votre tenant M365 en 2 semaines

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