Intune et BitLocker 2026 : Gestion et Sécurisation des Endpoints

> Intune BitLocker 2026 — XTS-AES 256, clés Entra ID, Compliance Policies et Zero Trust endpoint pour organisations françaises soumises à NIS 2.

En 2024, lors d'un audit de sécurité d'une collectivité territoriale française de 800 agents, nous avons découvert que 63% des postes de travail Windows 10 et 11 n'avaient aucun chiffrement de disque activé, malgré la présence d'une licence Microsoft Intune incluse dans le contrat Microsoft 365 E3 souscrit trois ans auparavant. La raison était simple : les profils de configuration BitLocker n'avaient jamais été déployés via Intune, et l'ancienne infrastructure MECM coexistait avec Intune sans synchronisation cohérente du workload Endpoint Protection. En cas de vol ou de perte d'un appareil — situation courante dans une collectivité avec des agents terrain et des élus en déplacement fréquent — les données non chiffrées auraient été directement accessibles sans aucune barrière technique. Ce scénario est représentatif de la réalité de nombreuses organisations françaises qui ont adopté Intune sans déployer correctement les politiques de chiffrement des endpoints. Ce guide complet présente l'architecture de déploiement **Intune et BitLocker 2026** pour sécuriser les endpoints Windows dans un environnement Microsoft 365 moderne, couvrant les profils de chiffrement XTS-AES 256 recommandés par l'ANSSI, la gestion centralisée des clés de récupération dans Entra ID, les politiques de conformité Conditional Access qui bloquent l'accès M365 aux appareils non chiffrés, l'intégration **Windows Hello for Business**, et les métriques de couverture via Endpoint Analytics. Nous abordons également la migration depuis MECM vers Intune pour le workload BitLocker, la coexistence des deux outils en phase transitoire, et les pièges à éviter pour garantir une couverture de chiffrement exhaustive et vérifiable avant un audit ANSSI ou une inspection dans le cadre de la directive NIS 2 transposée en droit français en 2024, concernant désormais environ 15 000 organisations françaises dans les secteurs critiques définis par l'annexe de la directive européenne.

À RETENIR

À retenir

• **XTS-AES 256** est le standard de chiffrement BitLocker recommandé par l'ANSSI pour les données sensibles depuis 2022

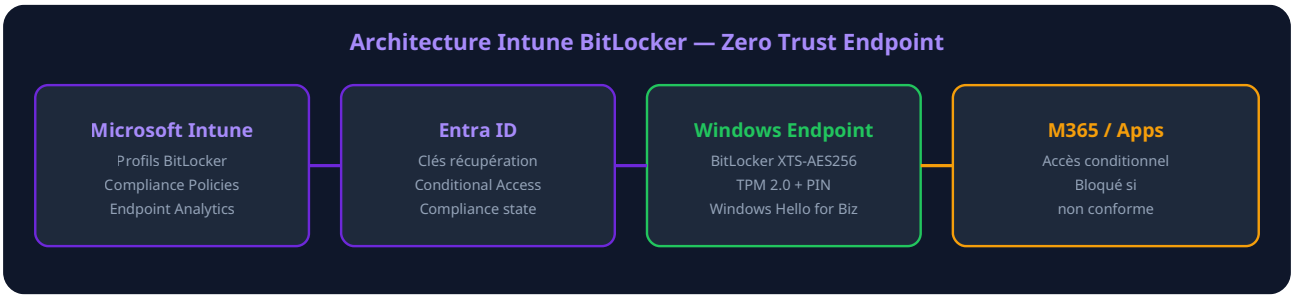
• Les clés de récupération BitLocker doivent être sauvegardées dans **Entra ID** avant activation — jamais uniquement en local

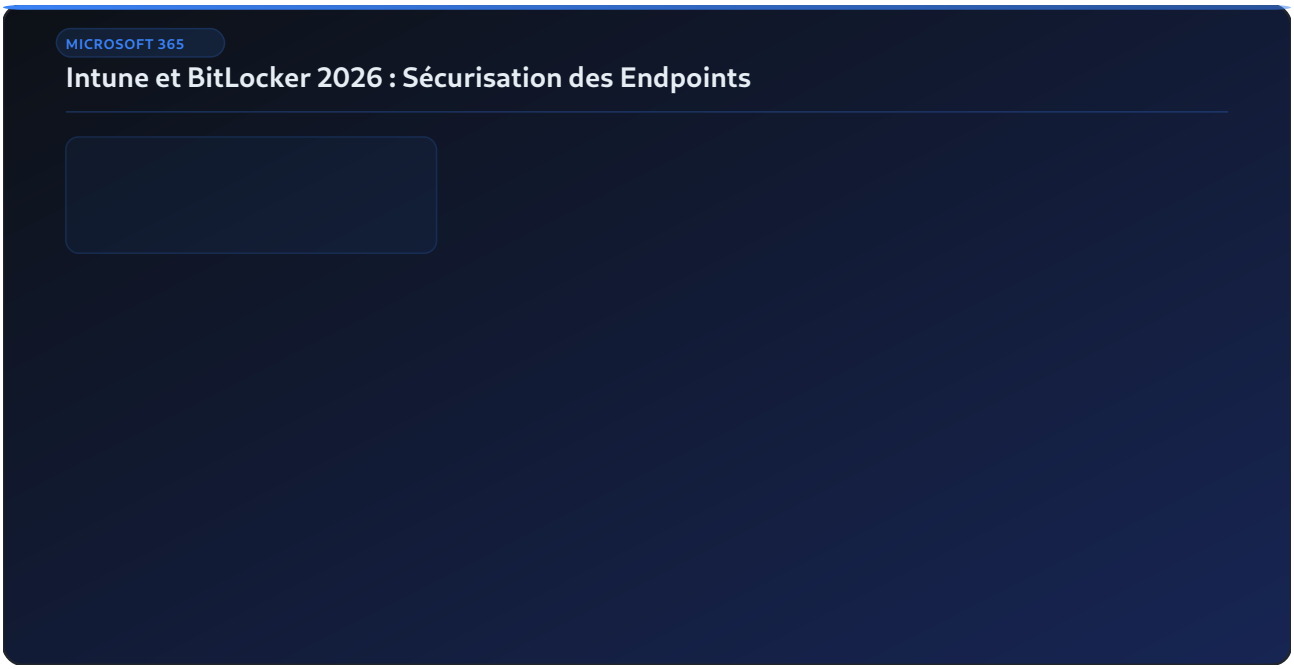
• Intune Conditional Access peut bloquer l'accès M365 depuis les appareils non conformes (non chiffrés) en temps réel automatiquement

• **Windows Hello for Business** remplace les mots de passe par des clés cryptographiques liées au TPM et à BitLocker

• Endpoint Analytics permet de mesurer la couverture de chiffrement et d'identifier les appareils non conformes en temps réel

• La coexistence MECM + Intune (Co-management) nécessite une configuration explicite du workload BitLocker pour éviter les conflits





Microsoft **Intune** (Microsoft Endpoint Manager) est la solution MDM cloud-native incluse dans les licences Microsoft 365 Business Premium et E3/E5, permettant de gérer les appareils Windows, iOS, Android et macOS depuis une interface web unifiée. **MECM (Microsoft Endpoint Configuration Manager)**, anciennement SCCM, est la solution on-premise historique de gestion des postes Windows, en production depuis plus de 10 ans dans de nombreuses organisations françaises. La coexistence des deux outils est gérée via le **Co-management**, une fonctionnalité qui répartit les workloads de gestion entre MECM et Intune selon une configuration explicite par l'administrateur.

Pour BitLocker spécifiquement, il est impératif de définir explicitement quel outil gère le workload Endpoint Protection dans la console Co-management MECM. Si les deux outils tentent simultanément d'appliquer des profils BitLocker, des conflits de configuration peuvent empêcher l'activation du chiffrement ou provoquer des blocages de démarrage sur certains modèles d'appareils. Ce scénario de conflit est le plus fréquent lors des migrations Intune que nous accompagnons chez des clients français, et nécessite systématiquement une validation du workload BitLocker avant tout déploiement large de profils de chiffrement. La migration complète vers Intune pour le workload BitLocker dure généralement 3 à 6 mois selon la

complexité du parc et le nombre d'appareils à enrôler et à valider individuellement. La documentation officielle Microsoft Intune BitLocker détaille les options disponibles selon les versions Windows et les configurations hardware supportées pour chaque mode de chiffrement.

Configurer les profils BitLocker dans Intune : XTS-AES 256 et activation silencieuse

La configuration d'un profil BitLocker dans Intune s'effectue depuis le portail Intune sous Endpoint Security → Disk Encryption → Create Policy → Windows → BitLocker. Les paramètres clés pour un niveau conforme aux recommandations ANSSI sont : méthode de chiffrement **XTS-AES 256 bits** pour les lecteurs système et les lecteurs de données fixes, démarrage avec TPM + PIN (niveau de protection 3) ou TPM seul (niveau 2, acceptable pour les postes à risque modéré dans des locaux sécurisés), et sauvegarde obligatoire de la clé de récupération dans Azure AD (Entra ID) avant l'activation du chiffrement. L'XTS-AES 128 bits n'est acceptable que pour les supports amovibles BitLocker To Go, pour des raisons de compatibilité avec les systèmes tiers qui doivent lire ces supports en dehors de l'organisation.

> ⚡ **Retour terrain**
>
> Dans les environnements Microsoft 365, le Secure Score est une métrique utile mais trompeuse : il donne du crédit pour des actions facilement automatisables (activer MFA, désactiver protocoles legacy) mais ignore des risques critiques comme la gestion des consentements OAuth (applications tierces autorisées par les utilisateurs), les permissions d'accès délégué entre boîtes aux lettres, et les partages OneDrive/SharePoint externes non supervisés. Un score de 70/100 ne garantit pas un environnement sûr.

L'option **BitLocker silent enablement** (activation silencieuse) est la méthode recommandée pour les déploiements à grande échelle car elle active le chiffrement en arrière-plan sans interaction utilisateur, possible uniquement sur les appareils dotés d'un TPM 2.0 fonctionnel et d'une interface UEFI avec Secure Boot activé. Avant de déployer les profils BitLocker en mode silencieux sur le parc complet, un pré-inventaire via Endpoint Analytics identifie les appareils ne satisfaisant pas les prérequis matériels, évitant ainsi les échecs silencieux difficiles à diagnostiquer a posteriori. Ce pré-inventaire est une étape critique que nous recommandons systématiquement comme première phase de tout projet de déploiement BitLocker Intune en France. Les organisations disposant de postes anciens sans TPM 2.0 doivent créer une politique BitLocker distincte avec authentification par mot de passe pré-démarrage pour couvrir ces appareils dans le périmètre de chiffrement global.

Gestion des clés de récupération BitLocker dans Entra ID

La sauvegarde des clés de récupération BitLocker dans **Entra ID** est le fondement de la gestion des clés en entreprise. Lorsqu'un utilisateur oublie son PIN BitLocker, remplace sa carte mère (le TPM est lié au matériel), ou rencontre un problème de démarrage, le service desk peut récupérer la clé de 48 chiffres depuis le portail Entra ID Admin Center sous Devices → All Devices → [appareil] → Recovery Keys, sans intervention physique sur le poste. Ce processus remplace avantageusement MBAM (Microsoft BitLocker Administration and Monitoring), déprécié par Microsoft et qui nécessitait une infrastructure serveur dédiée en plus du contrôleur de domaine Active Directory.

La politique de sauvegarde dans le profil BitLocker Intune doit être configurée avec l'option "Required" pour forcer la sauvegarde avant l'activation du chiffrement. Sans cette configuration, certains appareils peuvent activer BitLocker localement sans sauvegarder la clé dans Entra ID, rendant toute récupération impossible en cas de défaillance matérielle ou d'oubli du PIN. L'ANSSI recommande de vérifier mensuellement que 100% des appareils chiffrés ont leur clé de récupération dans Entra ID, car des appareils migrés depuis un ancien domaine MECM peuvent avoir des clés orphelines non synchronisées. Cette vérification s'automatise via Microsoft Graph API en interrogeant l'endpoint `/informationProtection/bitlocker/recoveryKeys` et en

comparant la liste des deviceId avec l'inventaire Intune complet. Une absence de clé détectée par cet audit automatique doit déclencher immédiatement une remédiation : réactivation du profil BitLocker sur l'appareil concerné et vérification que la sauvegarde de la nouvelle clé dans Entra ID est confirmée avant de clore le ticket de remédiation.

Compliance Policies Intune : définir et mesurer la conformité endpoint

Les **Compliance Policies** Intune définissent les critères qu'un appareil doit respecter pour être considéré conforme : chiffrement BitLocker actif, version minimale du système d'exploitation Windows, antivirus Microsoft Defender à jour avec ses signatures, Secure Boot activé dans l'UEFI, protection en temps réel Defender active, et absence de jailbreak ou root sur les appareils mobiles iOS et Android. La conformité est évaluée en continu par l'agent Intune sur l'appareil toutes les 8 heures par défaut, et transmise à Entra ID qui met à jour l'attribut de conformité utilisé par les règles Conditional Access en temps quasi-réel après la détection d'un changement d'état.

Un appareil non conforme déclenche le flux Conditional Access configuré : blocage immédiat de l'accès M365, notification à l'utilisateur lui indiquant quelle condition manque avec un lien vers la documentation de remédiation, et alerte au service desk si la non-conformité persiste au-delà du délai de grâce défini. Cette automatisation transforme le contrôle de conformité endpoint d'une tâche d'audit annuelle en un processus continu et automatique, conforme aux exigences de contrôle permanent recommandées par les référentiels ISO 27001, NIS 2 et le guide ANSSI sur la sécurisation des systèmes Windows. Le rapport de conformité en temps réel disponible dans Endpoint Analytics constitue une preuve documentaire directement utilisable dans les audits de certification.

Paramètre de conformité	Impact si non conforme	Délai grâce	Priorité
BitLocker actif	Blocage M365 immédiat	0 jour	Critique
Defender AV à jour	Blocage M365	1 jour	Critique
Windows Update (30j)	Notification puis blocage	7 jours	Élevé
Secure Boot activé	Non conforme	3 jours	Élevé
Version OS min (W11 23H2)	Non conforme	30 jours	Moyen
PIN complexité (min 6)	Notification utilisateur	14 jours	Moyen

Conditional Access basé sur la conformité device : Zero Trust endpoint

L'intégration entre les Compliance Policies Intune et **Conditional Access (CAP)** Entra ID est le cœur du modèle **Zero Trust endpoint** de Microsoft. La règle CAP fondamentale à déployer est : exiger que l'appareil soit marqué conforme par Intune pour accéder aux ressources Microsoft 365 et aux applications cloud enregistrées dans Entra ID en SSO. Cette règle unique couvre Exchange Online, SharePoint Online, Teams, OneDrive et toutes les applications SaaS intégrées, créant une barrière d'accès basée sur l'état de sécurité réel de l'appareil en temps réel — bien plus efficace que la seule vérification de l'identité au moment de la connexion initiale, qui ne garantit pas que l'appareil utilisé est sécurisé et conforme aux politiques de l'organisation.

Le déploiement doit être précédé d'une phase de test en mode Report-Only pour identifier les utilisateurs et appareils qui seraient bloqués. Dans notre expérience d'accompagnement de déploiements en France, une organisation qui active cette règle CAP sans phase de test bloque invariablement des appareils légitimes non encore enrôlés dans Intune — notamment les postes partagés, les imprimantes multifonctions avec des clients email embarqués, et les appareils des sous-traitants. La phase Report-Only d'au moins 30 jours est donc non négociable avant l'activation de la règle en mode Enforced, sous peine de paralysie opérationnelle partielle de l'organisation. Pendant cette phase, chaque connexion qui aurait été bloquée est journalisée dans

Entra ID Sign-in logs avec le motif précis de non-conformité, permettant une remédiation ciblée avant l'activation de la règle de blocage effective.

Windows Hello for Business : authentification passwordless liée au TPM

Windows Hello for Business (WHfB) remplace les mots de passe Windows par des credentials cryptographiques asymétriques protégés par le TPM de l'appareil. L'utilisateur s'authentifie avec un PIN local (jamais transmis sur le réseau, protégé par le TPM) ou une biométrie (empreinte digitale, reconnaissance faciale IR), déverrouillant la clé privée stockée dans le TPM pour l'authentification auprès d'Entra ID. Cette architecture élimine les risques de phishing de mots de passe, de credential stuffing depuis des bases compromises, et de pass-the-hash car la clé privée WHfB ne quitte physiquement jamais le TPM de l'appareil légitime.

L'intégration entre WHfB et BitLocker est naturelle : les deux reposent sur le même TPM de l'appareil. BitLocker peut être configuré pour libérer automatiquement ses clés de chiffrement lors d'une authentification WHfB réussie, supprimant la contrainte de saisir un PIN BitLocker au démarrage tout en maintenant un niveau de sécurité élevé basé sur la liaison cryptographique TPM-appareil. Cette configuration — BitLocker sans PIN pré-boot combiné à WHfB pour l'authentification OS — est le compromis optimal entre sécurité et usabilité pour la grande majorité des postes de travail professionnels qui ne traitent pas d'informations classifiées Confidentiel Défense. Les organisations qui déploient WHfB constatent également une réduction significative des tickets de service desk liés aux mots de passe oubliés, avec des économies opérationnelles mesurables en heures de support eliminées.

Déploiement et audit BitLocker via PowerShell et Intune

Avant de déployer les profils BitLocker Intune, un inventaire des prérequis matériels est indispensable : TPM 2.0 présent et activé dans le BIOS/UEFI, espace disque suffisant pour la

partition système BitLocker, et version Windows compatible. Le script PowerShell suivant, exécutable via Intune comme script de remédiation Proactive Remediation ou via MECM, fournit un inventaire rapide de l'état BitLocker et des prérequis matériels de chaque poste, exportable en CSV pour le suivi de déploiement.

```
 # Audit état BitLocker et prérequis TPM pour déploiement Intune
$BitLockerStatus = Get-BitLockerVolume -MountPoint "C:" -ErrorAction SilentlyContinue
$TPM = Get-Tpm -ErrorAction SilentlyContinue

[PSCustomObject]@{
    ComputerName    = $env:COMPUTERNAME
    BitLockerStatus = if($BitLockerStatus) { $BitLockerStatus.ProtectionStatus } else { "No
    EncryptionPct   = if($BitLockerStatus) { $BitLockerStatus.EncryptionPercentage } else {
    TPMPresent      = $TPM.TpmPresent
    TPMEnabled      = $TPM.TpmEnabled
    SecureBoot      = Confirm-SecureBootUEFI -ErrorAction SilentlyContinue
    KeyProtectors   = ($BitLockerStatus.KeyProtector.KeyProtectorType) -join ", "
} | ConvertTo-Json
```

Ce script retourne un objet JSON avec l'état complet de l'appareil, qu'Intune peut collecter via Proactive Remediation et agréger dans Endpoint Analytics pour un tableau de bord de couverture fleet-wide. La colonne KeyProtectors est particulièrement importante : elle indique si la clé de récupération est de type RecoveryPassword (clé 48 chiffres sauvegardeable dans Entra ID) ou d'un autre type non compatible avec la sauvegarde cloud. Ce résultat d'audit doit être exporté vers un tableau de suivi partagé avec le RSSI pour mesurer la progression du déploiement semaine après semaine jusqu'à atteindre l'objectif de 100% de couverture.

Self-service de récupération BitLocker : réduire la charge du service desk

La procédure de récupération BitLocker est l'une des demandes les plus fréquentes adressées aux services desk des organisations ayant déployé le chiffrement obligatoire. Un utilisateur bloqué au démarrage Windows par BitLocker — après une mise à jour BIOS, un oubli de PIN, ou un changement de composant matériel — a besoin de la clé de récupération de 48 chiffres immédiatement pour reprendre son travail. Sans portail self-service, cette demande génère un

ticket au service desk avec un délai de traitement de 15 à 45 minutes selon la disponibilité des agents.

Un portail de **self-service BitLocker** — déployable via une application Power Apps personnalisée connectée à Microsoft Graph, ou via le portail Microsoft My Sign-Ins — permet aux utilisateurs de récupérer leur propre clé après une authentification MFA réussie, réduisant la charge du service desk de 30 à 50% sur les tickets BitLocker. Pour les organisations avec des agences régionales ou un service desk centralisé difficile à joindre hors heures ouvrées, cette fonctionnalité self-service est particulièrement précieuse pour éviter des demi-journées de travail perdues à cause d'un poste bloqué dont la clé est dans Entra ID mais inaccessible à l'utilisateur sans l'aide du service desk. La mise en place du self-service doit être accompagnée d'une communication claire aux utilisateurs sur la procédure à suivre et d'une formation courte expliquant pourquoi leur clé BitLocker est stockée dans le cloud plutôt que sur un papier dans un tiroir, afin de lever les résistances culturelles parfois observées en France.

Endpoint Analytics Intune : mesurer la couverture de chiffrement

Endpoint Analytics est le tableau de bord de monitoring de conformité et performance des endpoints géré par Intune. Il fournit des métriques en temps réel sur la couverture de chiffrement BitLocker par politique, les taux de conformité agrégés par groupe d'appareils, et les motifs détaillés de non-conformité pour chaque appareil non conforme. Pour les RSSI qui doivent reporter la couverture de chiffrement à la direction ou aux auditeurs (ISO 27001, NIS 2, ANSSI), Endpoint Analytics génère des rapports exportables directement utilisables comme preuves de conformité documentaires.

Le rapport spécifique "Device compliance" dans Endpoint Analytics permet de voir le pourcentage d'appareils conformes par politique, avec un drill-down sur les appareils non conformes et leurs motifs de non-conformité précis. Une couverture BitLocker inférieure à 95% déclenche une investigation immédiate pour identifier les appareils récalcitrants — souvent des appareils anciens sans TPM 2.0 qui nécessitent une politique BitLocker distincte avec authentification par mot de passe pré-démarrage, ou des appareils récemment achetés non encore enrôlés dans Intune car le processus d'enrôlement Autopilot n'a pas été configuré pour les

commandes les plus récentes. Le suivi de l'évolution de la couverture sur un graphe hebdomadaire dans Endpoint Analytics est particulièrement utile pour démontrer la progression lors des comités de pilotage sécurité et pour motiver les équipes IT qui conduisent le déploiement sur des centaines d'appareils simultanément.

BitLocker To Go : chiffrement des supports amovibles en entreprise

BitLocker To Go étend le chiffrement BitLocker aux clés USB, disques durs externes et autres supports amovibles. Dans un environnement Intune, la politique BitLocker peut exiger que tous les supports amovibles connectés aux appareils gérés soient chiffrés avec BitLocker To Go avant d'être accessibles en écriture — une mesure de prévention des fuites de données (DLP physique) pertinente pour les organisations traitant des données personnelles RGPD ou des informations sensibles. Le chiffrement des supports amovibles est exigé par certaines normes sectorielles françaises, notamment dans les secteurs de la santé (HDS) et de la défense nationale.

La configuration Intune pour BitLocker To Go propose trois options avec des niveaux de restriction croissants : bloquer l'accès en écriture aux supports non chiffrés (mesure la plus sécurisée mais pouvant générer des frictions opérationnelles), afficher un avertissement à l'utilisateur lui proposant de chiffrer le support avant l'accès en écriture, ou permettre l'accès en lecture seule aux supports non chiffrés. La première option est recommandée pour les environnements traitant des données très sensibles, mais des procédures d'exception doivent être prévues pour les échanges légitimes avec des partenaires et fournisseurs utilisant des clés USB non chiffrées pour partager des fichiers volumieux. Le support BitLocker To Go est natif dans Windows 10 et 11 et ne nécessite pas de logiciel additionnel côté utilisateur pour lire les supports chiffrés sur un poste Windows autorisé.

Audit de couverture BitLocker via Microsoft Graph API

L'API Microsoft Graph fournit un accès programmatique à l'ensemble des clés de récupération BitLocker stockées dans Entra ID, permettant d'auditer automatiquement la couverture de chiffrement fleet-wide sans passer par l'interface graphique Intune. L'endpoint `GET /informationProtection/bitlocker/recoveryKeys` retourne la liste de toutes les clés stockées avec leur `deviceId` associé, que l'on peut comparer avec la liste des appareils Intune pour identifier les appareils sans clé de récupération dans Entra ID.

```
 # Rapport de couverture BitLocker via Microsoft Graph
$token = (Get-AzAccessToken -ResourceUrl "https://graph.microsoft.com").Token
$headers = @{ Authorization = "Bearer $token" }
$devices = (Invoke-RestMethod -Uri "https://graph.microsoft.com/v1.0/deviceManagement/manag
$keys = (Invoke-RestMethod -Uri "https://graph.microsoft.com/v1.0/informationProtection/bit
$devicesWithKeys = $keys | Select-Object -ExpandProperty deviceId -Unique
$coverage = [Math]::Round(($devicesWithKeys.Count / $devices.Count) * 100, 1)
Write-Host "Couverture BitLocker: $coverage% ($($devicesWithKeys.Count)/$($devices.Count))"
$devices | Where-Object { $_.id -notin $devicesWithKeys } | Export-Csv /tmp/missing_bitlock
```

Ce script PowerShell, exécutable depuis une Azure Automation Runbook ou une machine de gestion avec les droits Graph appropriés, produit à la fois une métrique de couverture globale et une liste exportée en CSV de tous les appareils Windows gérés sans clé BitLocker dans Entra ID. Cette liste CSV est la base d'un plan de remédiation ciblé. L'automatisation hebdomadaire de ce script et l'envoi du rapport par email au RSSI via une Azure Logic App constituent un monitoring de couverture BitLocker entièrement automatisé et auditable.

Durcissement avancé : Network Unlock, DMA Protection et Pluton

BitLocker Network Unlock permet de déverrouiller automatiquement les appareils au démarrage lorsqu'ils sont connectés au réseau d'entreprise filaire avec certificat PKI valide, sans PIN à saisir. Cette configuration est idéale pour les postes fixes des opérateurs de systèmes critiques qui doivent redémarrer rapidement après une coupure de courant sans intervention humaine, tout en maintenant le chiffrement complet quand l'appareil est déconnecté du réseau.

La configuration requiert un serveur WDS (Windows Deployment Services) avec le rôle Network Unlock configuré et un certificat PKI dédié déployé par l'AD CS de l'organisation.

La **DMA Protection** (protection contre les attaques Direct Memory Access via Thunderbolt et PCIe) est un complément crucial à BitLocker pour les postes portables de direction. Sans DMA Protection activée, un attaquant ayant accès physique à un poste démarré mais verrouillé peut extraire les clés BitLocker de la RAM via une attaque DMA avec un équipement spécialisé. Le Kernel DMA Protection dans Windows 11, activé via UEFI et vérifié par Intune comme critère de conformité optionnel, bloque ces attaques en isolant les périphériques Thunderbolt. **Microsoft Pluton**, disponible sur certains processeurs depuis 2022, représente la génération suivante de protection hardware en intégrant le TPM directement dans le CPU, éliminant la surface d'attaque du bus CPU-TPM et rendant les attaques de type bus sniffing physiquement impossibles même avec un accès prolongé à l'appareil ouvert.

Résolution des problèmes BitLocker fréquents en déploiement Intune

Le déploiement BitLocker via Intune génère régulièrement des problèmes spécifiques que les déploiements MECM classiques ne présentent pas. Les problèmes les plus fréquents documentés lors de nos accompagnements client : TPM 2.0 présent mais désactivé dans le BIOS UEFI (nécessite une intervention manuelle ou un script de configuration UEFI pour les modèles HP, Dell et Lenovo qui supportent la configuration à distance), Secure Boot désactivé bloquant l'activation automatique de BitLocker en mode silencieux, espace disque insuffisant sur C pour créer la partition système BitLocker sur des postes anciens partitionnés avec peu d'espace libre, et conflits entre les politiques BitLocker Intune et les GPO BitLocker héritées de l'Active Directory on-premise qui ne sont pas désactivées lors de la migration vers Intune.

Le diagnostic de ces problèmes s'effectue via les logs Intune disponibles dans le portail sous Devices → Monitor → Device configuration. Les logs détaillés BitLocker sont accessibles sur l'appareil lui-même sous `C:\Windows\Logs\BitLocker\` et dans l'Observateur d'événements sous Applications and Services Logs → Microsoft → Windows → BitLocker-API. La résolution systématique passe par la vérification séquentielle : TPM actif et validé, Secure Boot activé, politique Co-management configurée, GPO BitLocker désactivée, puis application du profil

Intune avec monitoring de la progression dans Endpoint Analytics. Un runbook de dépannage documenté et maintenu à jour par l'équipe IT est un investissement indispensable pour tout déploiement BitLocker Intune supérieur à 100 appareils, car les mêmes problèmes se répètent sur les mêmes modèles et la solution est toujours identique une fois identifiée.

Analyse TCO : Intune BitLocker versus solutions tierces de chiffrement

La question du choix entre BitLocker natif géré par Intune et des solutions tierces de chiffrement endpoint (Symantec Endpoint Encryption, Sophos SafeGuard, McAfee Complete Data Protection) se pose régulièrement dans les organisations françaises qui avaient investi dans ces solutions avant d'adopter Microsoft 365. L'analyse TCO sur 3 ans penche systématiquement en faveur de BitLocker via Intune pour les organisations sous licence Microsoft 365 E3 ou supérieure, car Intune et BitLocker sont inclus sans surcoût dans ces licences. Le seul coût additionnel est le temps d'implémentation initiale et la formation des équipes IT, estimé entre 5 et 15 jours selon la complexité de l'environnement et le volume d'appareils.

Les solutions tierces offrent parfois des fonctionnalités avancées (chiffrement des partitions système Linux, support des systèmes MacOS plus complet, journalisation détaillée centralisée) qui peuvent justifier leur coût dans des environnements hétérogènes avec de nombreux systèmes non-Windows. Pour les organisations 100% Windows avec Microsoft 365, le passage à BitLocker via Intune offre un retour sur investissement typiquement positif dès la première année, combinant l'élimination des licences tierces, la centralisation de la gestion dans un outil déjà utilisé par les équipes IT, et la garantie d'une intégration native avec Conditional Access et Entra ID sans connecteurs tiers supplémentaires à maintenir. Notre guide des pratiques de sécurité Microsoft 365 détaille les critères de décision entre les différentes options de sécurisation des endpoints dans un environnement Microsoft 365 complet.

Feuille de route de déploiement BitLocker Intune en 4 phases

Un déploiement réussi de BitLocker via Intune dans une organisation française de taille intermédiaire (200 à 2000 appareils) suit généralement quatre phases sur 3 à 6 mois. **Phase 1 — Inventaire** (3-4 semaines) : déploiement du script d'audit PowerShell sur l'ensemble du parc via MECM ou Intune, identification des appareils sans TPM 2.0 ou sans Secure Boot, liste des appareils en Co-management dont le workload BitLocker est encore côté MECM, et audit des GPO BitLocker existantes dans l'Active Directory qui devront être neutralisées. **Phase 2 — Pilote** (4-6 semaines) : déploiement des profils BitLocker Intune sur 50 appareils représentatifs de la diversité du parc, monitoring renforcé des logs BitLocker et Intune, et documentation des problèmes rencontrés et de leurs solutions.

Phase 3 — Déploiement progressif (6-8 semaines) : activation des profils en mode Report-Only d'abord sur l'ensemble du parc pour identifier les non-conformités potentielles, suivi hebdomadaire des métriques Endpoint Analytics, puis bascule en mode Enforced par vagues de 200 appareils avec monitoring renforcé. **Phase 4 — Activation Conditional Access** (2 semaines) : configuration de la règle CAP en mode Report-Only sur 14 jours, analyse des connexions qui auraient été bloquées, correction des exceptions légitimes, puis activation en mode Enforced avec communication claire aux utilisateurs sur le comportement attendu. Notre service de RSSI externalisé accompagne cette feuille de route avec un suivi hebdomadaire et un escalade rapide des problèmes bloquants.

Chiffrement des endpoints non-Windows : FileVault macOS et dm-crypt Linux

L'écosystème Intune ne se limite plus aux appareils Windows. Pour les endpoints **macOS**, Intune déploie et gère **FileVault 2** (le chiffrement disk natif Apple basé sur XTS-AES 128) avec la même logique de sauvegarde des clés de récupération personnelles dans Entra ID. La politique FileVault Intune peut être configurée pour forcer l'activation au premier login de l'utilisateur, avec un workflow d'approbation administrateur si l'utilisateur n'était pas connecté lors du

déploiement de la politique. Pour les appareils Apple Silicon (M1, M2, M3), le chiffrement est activé par défaut au niveau hardware et FileVault ajoute une couche de protection au niveau OS.

Pour les appareils **Linux** gérés via Intune (Ubuntu et RHEL supportés en préversion depuis 2025), le chiffrement LUKS (Linux Unified Key Setup) via dm-crypt peut être configuré via des scripts de remédiation Intune. L'intégration native est moins aboutie que pour Windows et macOS, mais des scripts PowerShell ou Bash déployés via Intune permettent d'automatiser la configuration et la vérification du chiffrement LUKS, et d'exporter les clés de récupération LUKS vers un coffre-fort de clés sécurisé comme Azure Key Vault. Cette extension du périmètre de chiffrement géré aux endpoints non-Windows est essentielle pour les équipes de développement avec des MacBook ou des postes Linux, afin d'éviter des angles morts dans la posture de sécurité globale qui pourraient être détectés lors d'un audit ANSSI ou lors d'une certification ISO 27001 incluant l'inventaire des actifs et des mesures de protection des supports amovibles et des endpoints.

Intégration Patch Tuesday et Windows Update for Business avec Intune

La gestion des mises à jour Windows est indissociable de la sécurité BitLocker : certaines mises à jour du firmware UEFI ou du TPM peuvent invalider les mesures de démarrage sécurisé sur lesquelles BitLocker repose, déclenchant une demande de clé de récupération au prochain démarrage. Ce scénario — redouté par les équipes IT car il génère un pic soudain de tickets service desk — peut être prévenu en activant la fonctionnalité de mise à jour transparente des PCR (Platform Configuration Registers) dans les politiques BitLocker Intune, qui sauvegarde automatiquement les nouvelles valeurs de mesure après une mise à jour validée du firmware ou du TPM.

Windows Update for Business (WUfB) intégré dans Intune permet de contrôler le rythme de déploiement des mises à jour Windows sur le parc, en créant des anneaux de déploiement progressif : groupe pilote (10% du parc), groupe étendu (40%), groupe large (50%), chacun avec un délai différé par rapport à la disponibilité des mises à jour sur Windows Update. Cette approche prévient les déploiements massifs et simultanés qui peuvent générer des problèmes de chiffrement BitLocker à grande échelle si une mise à jour est incompatible avec certains

firmwares. Le suivi des taux de déploiement est disponible dans Endpoint Analytics et le tableau de bord Windows Update for Business Reports dans Microsoft 365 Admin Center. Notre guide sur l'automatisation des audits Microsoft 365 via PowerShell inclut des scripts de surveillance du déploiement des mises à jour et de la conformité BitLocker post-Patch Tuesday.

BitLocker et sécurité physique : défense contre le vol et la perte d'appareils

Le chiffrement BitLocker est la dernière ligne de défense contre l'accès non autorisé aux données en cas de vol ou de perte d'un appareil. Sans BitLocker, un voleur ou un enquêteur hostile peut extraire le disque, le connecter à un autre système, et lire toutes les données sans aucune contrainte d'authentification Windows. Avec BitLocker activé en mode XTS-AES 256 avec TPM + PIN, la donnée est illisible sans la clé de 256 bits stockée dans le TPM, protégée par un PIN que seul l'utilisateur légitime connaît — offrant une protection pratiquement inviolable contre l'accès direct aux données, même avec un accès physique prolongé à l'appareil et des ressources de calcul modernes.

La gestion des appareils perdus ou volés dans Intune doit être intégrée à la politique BitLocker. En cas de signalement de perte ou de vol, la séquence standard est : déclenchement de la commande Remote Wipe depuis le portail Intune pour effacer à distance le contenu de l'appareil lors de sa prochaine connexion réseau, révocation des certificats et tokens d'authentification associés à l'appareil depuis Entra ID, signalement aux autorités compétentes avec le numéro de série et l'IMEI si applicable, et vérification dans Entra ID que la clé de récupération BitLocker de l'appareil perdu est toujours accessible pour documenter que les données sont protégées même si l'effacement à distance n'a pas encore pu s'exécuter faute de connexion réseau. Ce processus doit être documenté dans la politique de sécurité de l'organisation et testé annuellement en conditions réelles pour vérifier que chaque étape fonctionne correctement.

Conformité ANSSI et NIS 2 : exigences de chiffrement des endpoints

Le guide ANSSI "Recommandations relatives à la sécurisation des systèmes d'information" exige le chiffrement des disques dur des postes de travail et des appareils mobiles pour les organisations OIV et OSE traitant des données sensibles. La mesure ESS-6.5 impose l'utilisation d'un algorithme de chiffrement agréé par l'ANSSI — BitLocker XTS-AES 256 satisfait cette exigence. Les publications de l'ANSSI sur la sécurité du poste de travail détaillent les exigences applicables aux différentes catégories de données et de systèmes.

La directive NIS 2, transposée en droit français par la loi du 3 octobre 2024, étend les obligations de sécurité des systèmes d'information à environ 15 000 organisations françaises dans 18 secteurs critiques. Le texte impose explicitement des "mesures techniques et organisationnelles appropriées" pour gérer les risques de sécurité, dont le chiffrement des données en transit et au repos. Le chiffrement complet des disques des endpoints via BitLocker Intune, combiné avec la gestion centralisée des clés dans Entra ID et le monitoring de conformité en continu via les Compliance Policies, constitue une réponse directe et documentable à ces obligations réglementaires. Les rapports Endpoint Analytics et les exports Graph API constituent les preuves documentaires nécessaires pour les audits NIS 2 menés par l'ANSSI. Notre service de conformité NIS 2 accompagne les organisations dans la mise en place de ces mesures de chiffrement et leur documentation.

Intune et BitLocker dans l'architecture Zero Trust globale

Dans l'architecture **Zero Trust** préconisée par l'ANSSI et Microsoft pour les organisations françaises soumises à NIS 2, la sécurisation des endpoints via Intune et BitLocker n'est qu'une composante d'un modèle global de sécurité. Les cinq piliers du Zero Trust — Identité (Entra ID, MFA), Endpoint (Intune, BitLocker), Réseau (segmentation, ZTNA), Applications (CASB, Conditional Access), Données (Purview, sensibilité) — doivent être déployés et coordonnés de manière cohérente pour créer une posture de sécurité sans périmètre de confiance implicite permettant d'accéder aux ressources sans contrôle préalable.

La conformité BitLocker est l'un des signaux de confiance les plus fiables dans ce modèle Zero Trust : un appareil chiffré avec BitLocker, enrôlé dans Intune, avec Secure Boot et HVCI activés, représente un endpoint dont on peut raisonnablement affirmer qu'il n'a pas été compromis au niveau du firmware ou du système d'exploitation. Ce niveau de confiance élevé dans l'endpoint permet d'assouplir d'autres contrôles d'accès (moins de challenges MFA répétés, accès à des ressources plus sensibles) tout en maintenant une sécurité globale élevée — c'est le principe fondamental du Zero Trust : adapter les contrôles au niveau de confiance établi plutôt que de tout bloquer ou tout permettre de manière uniforme. Contactez notre équipe via le diagnostic NIS 2 pour une évaluation de votre maturité Zero Trust endpoint actuelle.

Questions fréquentes

Peut-on utiliser BitLocker sans TPM avec Intune ?

Oui, via une configuration GPO ou un script Intune modifiant la clé de registre `EnableBDEWithNoTPM`. Cette configuration est acceptable pour les appareils anciens sans TPM 2.0, mais offre un niveau de protection inférieur car sans TPM, le chiffrement repose uniquement sur un mot de passe pré-démarrage que l'utilisateur doit saisir à chaque démarrage, sans vérification de l'intégrité de la chaîne de démarrage sécurisé.

Comment migrer les clés BitLocker de MBAM vers Entra ID ?

Via un script PowerShell déployé par Intune ou MECM qui exécute `BackupToAAD-BitLockerKeyProtector` sur chaque appareil avec BitLocker actif. Ce script force la sauvegarde de la clé de récupération existante dans Entra ID sans nécessiter de redémarrage ou de rechiffrement du disque, réduisant l'impact sur les utilisateurs à pratiquement zéro lors de la migration depuis MBAM.

Quelle est la différence entre TPM seul et TPM + PIN pour BitLocker ?

BitLocker avec TPM seul déverrouille automatiquement le disque au démarrage si le matériel est intact. BitLocker avec TPM + PIN exige un PIN numérique au démarrage, ajoutant une couche d'authentification même en cas de vol de l'appareil éteint. L'ANSSI recommande TPM + PIN pour les données sensibles et les postes mobiles, TPM seul pour les postes fixes en locaux sécurisés.

Quels modèles d'appareils posent le plus de problèmes lors du déploiement BitLocker Intune ?

Les appareils les plus problématiques sont les PC anciens avec BIOS legacy (non UEFI) qui ne supportent pas Secure Boot, les appareils avec des versions de firmware TPM obsolètes nécessitant une mise à jour avant déploiement, et certains modèles HP avec des configurations BIOS propriétaires désactivant le TPM par défaut. Un inventaire pré-déploiement avec le script PowerShell fourni permet d'identifier ces appareils avant que les problèmes ne se produisent en production.

Comment Conditional Access vérifie-t-il que BitLocker est actif ?

Conditional Access vérifie l'attribut de conformité de l'appareil dans Entra ID, mis à jour par l'agent Intune toutes les 8 heures. Si BitLocker est désactivé, l'agent Intune détecte la non-conformité et met à jour l'état dans Entra ID, après quoi le CAP bloque automatiquement l'accès M365 depuis cet appareil, sans intervention humaine nécessaire de la part de l'équipe IT.

Peut-on déployer BitLocker sur des VMs Azure avec Intune ?

Les VMs Azure utilisent Azure Disk Encryption (ADE) géré depuis Azure Key Vault plutôt que BitLocker géré par Intune. Pour les Azure AD Joined VMs, les profils BitLocker Intune peuvent s'appliquer mais les clés sont stockées dans Entra ID. La recommandation Microsoft est d'utiliser ADE pour les VMs IaaS et les profils BitLocker Intune pour les appareils physiques et les Windows 365 Cloud PC.

Accompagnement déploiement Intune et BitLocker : retour d'expérience France

La sécurisation des endpoints Windows via Intune et BitLocker est un projet structurant pour la posture de sécurité d'une organisation française, qui combine des aspects techniques (compatibilité matérielle, migration depuis MECM, configuration des profils), organisationnels (change management, formation des utilisateurs, procédures de service desk), et réglementaires (conformité NIS 2, ANSSI, ISO 27001). Notre service RSSI externalisé accompagne les organisations de toutes tailles dans ce projet, depuis l'audit initial de couverture jusqu'à la mise en production et le reporting de conformité mensuel.

Pour les organisations soumises à des obligations réglementaires spécifiques comme NIS 2 ou les exigences ANSSI pour les OIV, nous proposons également un audit de conformité dédié à la sécurité des endpoints, incluant la vérification de la configuration BitLocker, des profils Intune, des politiques Conditional Access, et des procédures de récupération. Cet audit produit un rapport de conformité avec preuves documentaires directement utilisable lors des contrôles ANSSI ou des audits de certification ISO 27001. Contactez-nous via le diagnostic NIS 2 pour une évaluation initiale gratuite de votre couverture de chiffrement actuelle et une estimation du projet de déploiement adapté à votre parc.