

Gestion moderne des appareils : Transformer l'agilité, la confiance et la productivité dans une économie pilotée par l'IA



Découvrez comment une gestion moderne des appareils, optimisée par l'IA et profondément intégrée à l'écosystème Microsoft, peut révolutionner votre organisation.

Renforcez votre résilience opérationnelle, accélérez votre agilité métier et instaurez une confiance numérique durable grâce à des insights exploitables. Transformez la gestion des endpoints en levier stratégique générateur de résultats mesurables pour la performance de l'entreprise.

Résumé exécutif

Le lieu de travail numérique atteint un point d'inflexion majeur. Les entreprises ne se contentent plus d'accompagner le changement : elles redéfinissent activement les modalités, les espaces et les technologies du travail. D'après le Microsoft Work Trend Index 2023, « 73 % des salariés souhaitent maintenir une flexibilité dans le travail à distance ». À mesure que le travail hybride, l'intégration de l'IA et les opérations distribuées deviennent la norme, la gestion des terminaux doit passer d'une simple configuration IT tactique à un levier stratégique d'autonomisation des collaborateurs.

La gestion moderne des appareils s'impose aujourd'hui comme un pilier fondamental de la résilience d'entreprise, de l'agilité opérationnelle et de la confiance numérique. Les DSI doivent garantir que chaque terminal — qu'il soit détenu par l'entreprise, utilisé à titre personnel ou assisté par l'IA — soit sécurisé, conforme, productif et gouverné intelligemment. Cela nécessite de dépasser les outils hérités et les modèles cloisonnés au profit d'un écosystème unifié, intelligent et proactif.

Ce livre blanc décrypte les mutations profondes qui redéfinissent la stratégie de gestion des terminaux : évolution des attentes collaborateur, nouvelles exigences en matière de conformité, transformation du profil de risque et impératifs de durabilité. Il présente l'architecture Microsoft de gestion moderne des appareils et en détaille les bénéfices concrets : amélioration de l'expérience utilisateur, renforcement de la sécurité, conformité réglementaire et gouvernance de l'IA à grande échelle.

Cette feuille de route, résolument tournée vers l'avenir et conçue pour les DSI, CTO et dirigeants technologiques engagés dans la transformation digitale, s'appuie sur des projets menés à l'échelle mondiale avec des partenaires tels que

NTT DATA, qui aident les entreprises à moderniser leur infrastructure de terminaux, à réduire leurs coûts d'exploitation et à obtenir des résultats tangibles.

L'enjeu est clair : les organisations qui intègrent une gestion adaptative et sécurisée des appareils au cœur de leur ADN numérique gagneront en agilité, en efficacité, en attractivité et en préparation réglementaire. Le défi ? Comblar les écarts opérationnels par une trajectoire progressive alignant l'évolution technologique sur l'ambition business. Ce livre blanc fournit cette trajectoire.

Introduction

L'entreprise moderne traverse une transformation structurelle et comportementale de grande ampleur. Ses opérations ne sont plus confinées à des bureaux physiques, à des infrastructures fixes ni à des horaires traditionnels. La main-d'œuvre est désormais dynamique, géographiquement dispersée, numériquement agile et dépendante d'un accès instantané aux données et aux services. Parallèlement, les comités de direction évoluent dans un environnement macroéconomique volatil, marqué par l'escalade des cybermenaces, les tensions géopolitiques, la complexité croissante des obligations réglementaires et une pression constante pour « faire plus avec moins ».

Cette convergence entre les individus, les risques et la technologie a hissé la gestion des appareils au rang de levier stratégique dans les décisions d'entreprise. Longtemps considérée comme une fonction technique en back office, la stratégie autour des terminaux est aujourd'hui directement liée à la résilience organisationnelle, à la maîtrise des risques, à la performance des équipes et à l'innovation digitale.

Les implications sont claires : un retard d'onboarding n'est plus une simple difficulté opérationnelle — c'est une perte de productivité et une expérience collaborateur dégradée. Des appareils obsolètes ou des correctifs de sécurité incohérents exposent l'entreprise à des risques à la fois opérationnels et réputationnels. L'absence de visibilité sur la conformité des terminaux fragilise la capacité à adopter l'IA de manière responsable, ou à répondre aux exigences croissantes de transparence ESG.

Dans cette nouvelle réalité, les DSI ne sont plus seulement des gestionnaires d'infrastructure — ils sont devenus des architectes de la transformation numérique. Leur mandat s'élargit pour inclure la création d'environnements de travail sécurisés, cohérents et intelligents, capables de prendre en charge le travail hybride, de favoriser l'innovation et d'instaurer une confiance numérique à grande échelle. Ce livre blanc explore comment l'écosystème moderne de Microsoft — composé de Microsoft Intune, Autopilot, Entra ID, Defender, Purview et Copilot — constitue un socle robuste pour bâtir des environnements de travail évolutifs, sécurisés et prêts à accueillir l'IA.

Les entreprises qui s'appuient sur des intégrateurs expérimentés tels que NTT DATA exploitent déjà ces plateformes pour accélérer la productivité, renforcer la gouvernance de l'IA et aligner les opérations liées aux terminaux sur leurs priorités stratégiques.

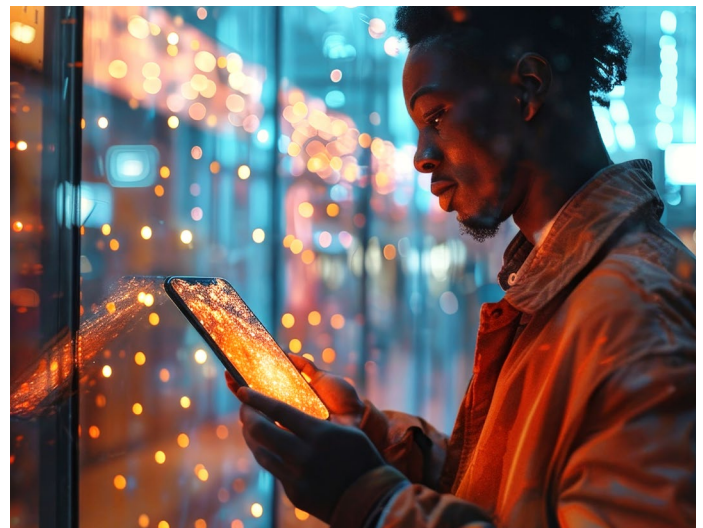
Comment la main-d'œuvre évolue

La composition et les attentes des collaborateurs ont profondément changé, sous l'effet combiné de la disruption technologique, des mutations démographiques et de l'évolution des normes professionnelles. Aujourd'hui, les employés évoluent dans une trame numérique étendue — bureaux à domicile, espaces de coworking, aéroports, sites clients, usines — avec l'attente d'un accès fluide, sécurisé et instantané aux applications critiques et aux données d'entreprise. Cette ubiquité du travail a rendu obsolètes les modèles IT fondés sur un périmètre réseau fixe.

Parallèlement, l'essor de l'IA générative introduit de nouveaux paradigmes en matière de productivité, d'accès à la connaissance et de collaboration homme-machine. Des outils comme Microsoft 365 Copilot ou Copilot dans Intune s'intègrent progressivement aux workflows métiers. Ils aident les collaborateurs à prendre de meilleures décisions, automatiser des tâches répétitives et augmenter la productivité individuelle et collective.

Sur le plan générationnel, les employés Millennials et Gen Z, désormais majoritaires, attendent des expériences numériques semblables à celles des plateformes qu'ils utilisent au quotidien : fluidité, personnalisation, autonomie. Les travailleurs de première ligne, quant à eux, ont besoin d'appareils robustes, adaptés à leur contexte, capables de soutenir des opérations critiques sans latence. Les cadres dirigeants exigent des solutions de collaboration mobile sécurisées pour prendre des décisions d'impact en temps réel.

Cette diversité croissante des usages, des attentes et des styles de travail oblige les DSI à concevoir une infrastructure numérique inclusive, réactive et conforme aux standards de sécurité les plus exigeants. La gestion moderne des appareils, enrichie d'une architecture IA-compatible et centrée sur la conformité, devient le pilier de cette transformation à grande échelle.



Enjeux métier et nouveaux impératifs pour les directions IT

Tous secteurs confondus, les organisations sont confrontées à une accumulation de défis stratégiques et opérationnels : multiplication des cybermenaces, montée en puissance des attentes clients, pression réglementaire accrue, sans oublier l'impératif de performance dans un contexte de rareté des talents. Le lieu de travail est désormais au croisement de ces dynamiques disruptives.

Les stratégies traditionnelles de gestion des terminaux — centrées sur des contrôles statiques, un provisionnement manuel et des outils fragmentés — ne sont plus adaptées à cet environnement. Elles exposent l'entreprise à des risques opérationnels, augmentent le coût total de possession et nuisent à la confiance comme à l'engagement des collaborateurs.

Face à cette réalité, le rôle des responsables IT évolue rapidement. Les DSI et CTO ne sont plus seulement garants de la disponibilité des services. Ils doivent concevoir des environnements numériques résilients, sécurisés et intelligents, capables de générer des résultats concrets pour le business. Cela implique de déployer un provisionnement à grande échelle, de maintenir une visibilité en temps réel sur la conformité des terminaux, de garantir un usage sécurisé de l'IA et d'offrir une expérience numérique cohérente et fluide aux collaborateurs.

Le message est clair : l'IT doit s'affirmer comme un levier stratégique au service de la productivité, de l'innovation et de la confiance. Le déploiement de solutions modernes, sécurisées dès leur conception, évolutives par défaut et centrées sur l'humain constitue l'assise technologique nécessaire à cette transformation durable.

Les grandes tendances qui redéfinissent la gestion moderne des appareils

Les grandes entreprises opèrent dans un environnement marqué par une dépendance numérique accrue, des menaces de sécurité en constante évolution, des attentes croissantes de la part des collaborateurs et un durcissement des exigences réglementaires. Ces forces transversales transforment la gestion des terminaux, la faisant passer d'une fonction IT tactique à un pilier stratégique de la performance business. Sept tendances clés redéfinissent les priorités des directions IT dans ce nouveau paradigme.

Généralisation du travail hybride et accès indépendant du lieu

Selon le rapport Gartner Future of Work Trends Post-COVID-19, 2022 — « Plus de 70 % des travailleurs du savoir attendent désormais des modalités de travail flexibles. » Le travail hybride n'est plus une réponse conjoncturelle : il constitue désormais l'architecture de référence des opérations modernes. Le travail est devenu fluide, sans frontières ni contraintes horaires. Les collaborateurs attendent un accès sécurisé, rapide et fluide aux applications critiques, quel que soit le terminal ou l'emplacement. Cette évolution pousse les DSI à repenser les périmètres réseau traditionnels et à investir dans des plateformes capables d'offrir un accès ubiquitaire, avec un niveau de sécurité et de gouvernance digne d'une infrastructure d'entreprise.

La gestion moderne des appareils de Microsoft, lorsqu'elle est déployée par des partenaires de confiance comme NTT DATA, permet un onboarding fluide, une application centralisée des politiques et une assistance en temps réel pour des équipes dispersées, tant sur le plan géographique que fonctionnel. Les opérations indépendantes du lieu deviennent un avantage concurrentiel, nécessitant des terminaux provisionnés, sécurisés et gouvernés comme des extensions dynamiques de l'infrastructure.



Adoption croissante du cadre de sécurité Zero Trust

Selon l'étude Gartner – Market Guide for Zero Trust Network Access, 2022 — « D'ici 2025, 60 % des organisations auront adopté le Zero Trust comme fondement de leur stratégie de cybersécurité. » Les cybermenaces se multiplient à un rythme sans précédent, rendant les défenses périmétriques traditionnelles obsolètes. Le cadre Zero Trust s'est imposé comme la norme de référence pour sécuriser une main-d'œuvre distribuée et un parc de terminaux en pleine expansion.

Ce modèle repose sur un principe fondamental : aucune entité — utilisateur, appareil ou connexion — ne doit être considérée comme fiable par défaut.

La gestion moderne des appareils de Microsoft joue un rôle central dans cette approche Zero Trust. Chaque utilisateur, chaque terminal et chaque requête d'accès font l'objet d'une vérification continue. L'état du terminal est évalué, les configurations de conformité sont appliquées, et tout écart est surveillé en temps réel — garantissant des décisions d'accès contextualisées et dynamiquement appliquées.

Intégration de l'IA pour renforcer la productivité et optimiser les coûts

L'IA transforme les modèles opératoires de l'entreprise. Des assistants génératifs à l'automatisation intelligente, les organisations intègrent l'intelligence artificielle dans les workflows, les processus et les plateformes pour gagner en efficacité, en scalabilité et en avantage concurrentiel. Selon le Microsoft Copilot Early Access Report, 2023 : « Microsoft 365 Copilot permettrait jusqu'à 29 % de gain de productivité sur l'exécution des tâches et la qualité rédactionnelle. »

Microsoft Intune transforme la gestion des terminaux et fait progresser l'innovation en IA pour l'IT, avec l'introduction des agents Security Copilot. Ces agents permettent aux organisations de renforcer leur posture de sécurité, d'accroître leur productivité et de simplifier les opérations IT — tout en aidant les équipes informatiques et de cybersécurité à faire face à la pression constante liée à la gestion d'environnements de terminaux complexes et à l'évolution rapide des menaces.

Une étude Microsoft Randomized Controlled Trials for Security Copilot for IT Administrators, 2024, révèle que « les professionnels IT utilisant Security Copilot étaient 35 % plus précis dans l'exécution des tâches. » Désormais, Copilot dans Intune étend ses capacités grâce à l'intégration des agents de Security Copilot. Ces agents apportent une automatisation adaptative et puissante aux équipes IT et de sécurité — rationalisant les tâches critiques et leur permettant d'agir plus rapidement et avec une plus grande assurance. Le premier d'entre eux — l'agent de remédiation des vulnérabilités — sera disponible en préversion publique dès mai 2025. Il marque une avancée majeure dans la gestion des terminaux, en intégrant une automatisation des mesures correctives pilotée par l'IA.

Cependant, l'adoption de l'IA engendre aussi de nouvelles exigences en matière de performance des appareils, d'accès aux données, de contrôle des politiques et de gouvernance. Grâce à son savoir-faire, NTT DATA garantit une préparation optimale à l'IA : elle assure le provisionnement d'appareils conformes, sécurise les accès privilégiés aux données sensibles et supervise l'usage de l'IA selon les rôles et fonctions métiers. Cette approche concilie productivité, intégrité des données et gouvernance rigoureuse.

Prise en charge élargie du BYOD et de la diversité du parc de terminaux

La main-d'œuvre actuelle interagit avec un ensemble hétérogène d'appareils : ordinateurs d'entreprise, smartphones personnels, tablettes ou équipements spécialisés durcis. Les modèles BYOD (Bring Your Own Device) et COPE (Corporate-Owned, Personally Enabled) traduisent une approche centrée sur l'utilisateur. Mais cette diversité opérationnelle complexifie la visibilité, le support et la conformité des terminaux.

Les plateformes modernes comme Microsoft Intune assurent une expérience fluide, quels que soient l'environnement ou le mode de propriété. Grâce à l'accompagnement de NTT DATA, les entreprises sont en mesure de piloter efficacement un écosystème de terminaux diversifiés, devenu essentiel pour garantir satisfaction, performance et sécurité à tous les niveaux de l'organisation.

Alignement sur les objectifs de durabilité et les engagements ESG

Selon l'étude NTT DATA ESG and IT Asset Study, 2022 — « Prolonger la durée de vie d'un appareil d'un an peut réduire son empreinte carbone jusqu'à 30 %. » La durabilité est aujourd'hui un impératif stratégique, portée par la pression des investisseurs, les attentes des parties prenantes et les réglementations mondiales. Les entreprises sont désormais tenues de rendre des comptes sur leur impact environnemental — y compris en ce qui concerne leurs actifs IT, leur consommation énergétique et leurs déchets électroniques.

La gestion moderne des appareils contribue à ces engagements ESG en permettant des configurations économes en énergie, en prolongeant la durée de vie des terminaux grâce à la maintenance prédictive et en offrant une visibilité granulaire sur leur utilisation effective. Ces leviers permettent de réduire les déchets électroniques, d'optimiser les cycles de renouvellement et d'inscrire la durabilité dans la stratégie numérique globale. L'expérience mondiale de NTT DATA dans l'alignement des projets de modernisation IT avec les engagements ESG en fait un partenaire clé pour accélérer l'impact, grâce à des insights activables et des modèles éprouvés.

Priorisation renforcée de la conformité et de la gouvernance des données

Avec la prolifération des réglementations sur la protection des données, la conformité n'est plus une simple obligation légale — elle devient une priorité stratégique inscrite à l'agenda des conseils d'administration. Selon l'IDC Future of Trust Survey, 2023 : « Plus de 76 % des dirigeants mondiaux considèrent la gouvernance des données comme un élément critique de leur stratégie d'entreprise. » Les organisations doivent aujourd'hui faire preuve de responsabilité, de transparence et de maîtrise quant à la manière dont les données sont consultées, traitées et stockées — sur les terminaux comme dans les environnements cloud.

La gestion moderne des appareils, lorsqu'elle est intégrée à Microsoft Purview, renforce la protection des données, prévient les menaces internes et assure une traçabilité complète à des fins d'audit. Elle garantit ainsi une conformité continue, évolutive et juridiquement défendable, y compris dans les secteurs hautement réglementés ou soumis à des cadres stricts comme le RGPD ou l'HIPAA.

L'expérience numérique collaborateur (DEX) comme indicateur clé de performance

D'après le Qualtrics X-Data and Gartner Workforce Trends, 2023 : « Les entreprises qui investissent dans la DEX enregistrent 22 % de rétention en plus et 17 % de gains de productivité. » NTT DATA considère que l'expérience numérique collaborateur est devenue un KPI stratégique — directement lié à l'engagement, à la performance et à la fidélisation des talents. Dans un environnement centré sur le numérique, la qualité de l'interaction entre l'utilisateur et son terminal influence directement la perception qu'il a de son entreprise.

Les plateformes modernes de gestion des appareils permettent de mesurer, suivre et améliorer cette expérience, en réduisant les points de friction, en automatisant l'assistance, et en favorisant la personnalisation. Lorsque l'IT devient fluide, intuitive et invisible, elle devient un véritable catalyseur de performance. L'IT ne se contente plus de supporter les opérations : elle devient un moteur de la réussite des collaborateurs.

Comblent le fossé de maturité

Malgré une prise de conscience généralisée quant à la nécessité d'adopter une gestion moderne des appareils, de nombreuses entreprises demeurent prisonnières d'outils obsolètes, d'équipes cloisonnées et de processus réactifs — autant de pratiques qui ne sont plus viables à l'ère du travail hybride, de l'IA généralisée et des cybermenaces persistantes.

Les services IT évoluent souvent dans des environnements fragmentés, où ils doivent gérer plusieurs plateformes avec des politiques incohérentes et peu d'automatisation. Ce manque d'unification expose l'entreprise à des risques multiples : vulnérabilités de sécurité, augmentation des coûts de support, perte de talents, dégradation de la satisfaction collaborateur, erreurs de conformité et prolifération d'usages non contrôlés de l'IA.

Dans les organisations dépourvues de gestion unifiée et automatisée des terminaux, un simple processus d'onboarding peut prendre plusieurs jours, nécessitant des configurations manuelles et des validations redondantes. Les applications stratégiques ne sont pas déployées à temps, les mises à jour de sécurité sont irrégulières, et la visibilité sur la conformité des appareils est inexistante. Ces frictions alimentent l'émergence du shadow IT, multipliant les risques non surveillés et affaiblissant le contrôle global de l'IT. En l'absence d'analytique intégrée, les DSI ne peuvent ni évaluer l'expérience utilisateur, ni anticiper les défaillances, ni démontrer la valeur ajoutée de leurs services.

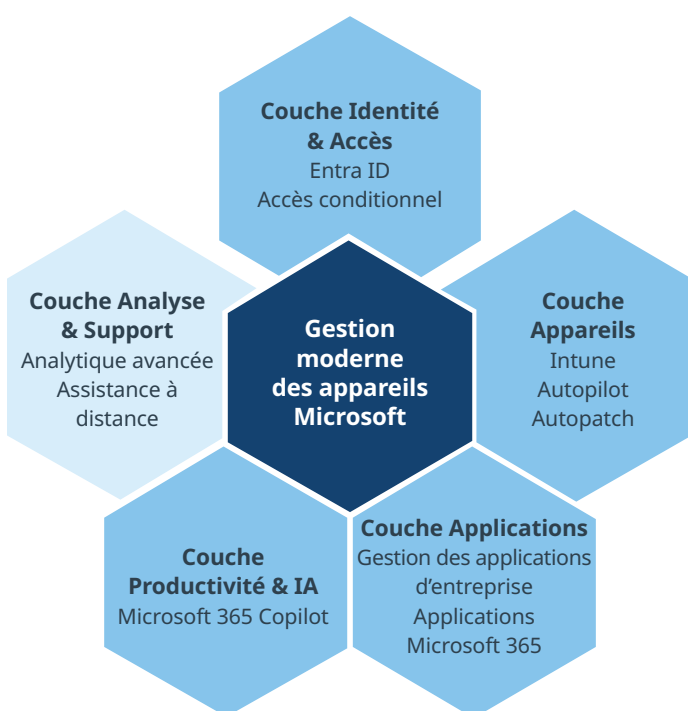
NTT DATA, en partenariat avec Microsoft, a permis à de nombreuses entreprises de franchir ce cap. En déployant une gestion unifiée des endpoints, en instaurant des indicateurs DEX et en réduisant les délais d'intégration de plus de 50 % dans certains déploiements à grande échelle, ces organisations ont pu transformer en profondeur leur environnement de travail.

Exemple concret : NTT DATA a accompagné l'un des plus grands transporteurs aériens mondiaux dans une transformation radicale vers un environnement numérique modernisé, en déployant les solutions Microsoft de gestion des appareils — notamment Intune et Autopilot. L'initiative a permis de moderniser et d'unifier la gestion des terminaux et des services de mobilité sur plus de 30 000 appareils répartis sur 400 sites dans le monde. Résultat : une réduction de 24 % des appels au support, traduisant des gains mesurables en satisfaction collaborateur et en efficacité opérationnelle. Cette collaboration a permis au client d'aligner dynamiquement ses opérations IT sur les priorités business — gestion des pics saisonniers, support des sites critiques et maintenance proactive.

En somme, combler le fossé technologique ne se limite pas à une mise à jour d'outils. Cela implique une refonte en profondeur de la manière dont les appareils sont déployés, gouvernés, maintenus et mesurés tout au long du cycle de vie collaborateur. Cela exige également que les DSI élèvent la gestion des appareils au rang de discipline stratégique — intégrée à la stratégie RH, à la posture de risque, à l'architecture de conformité et à la feuille de route numérique de l'organisation.

La solution : générer un impact business immédiat avec Microsoft Modern Device Management

Le portefeuille Microsoft Modern Device Management constitue une base unifiée, complète et cloud-native, conçue pour répondre à un double impératif : productivité et sécurité. Fondée sur les principes du Zero Trust, pensée pour les environnements hybrides et alignée avec les exigences de continuité d'activité, cette stack technologique intègre le provisionnement, la gestion, la protection, la gouvernance, la productivité et l'automatisation dans un modèle opérationnel unifié. Cela permet aux responsables IT de passer d'outils fragmentés et d'une gestion réactive des incidents à une prestation de services proactive et à un rôle d'activation stratégique.



Grâce à Microsoft Intune, Autopilot, Autopatch, Defender, Purview et 365 Copilot, les entreprises peuvent automatiser l'onboarding à grande échelle, gérer les configurations, faire respecter des politiques de sécurité dynamiques, adopter l'IA de manière responsable et intégrer la conformité dans leurs opérations — tout en renforçant l'expérience numérique des collaborateurs. Le résultat : un environnement de travail plus agile, plus sécurisé et véritablement prêt pour l'avenir.

Fonctionnalités clés :

- 1. Microsoft Entra ID** constitue la base d'une gestion sécurisée des identités dans un environnement hybride ou cloud-native. Il représente souvent la première étape vers une stratégie Zero Trust, en activant l'accès conditionnel, des contrôles fondés sur des politiques, ainsi qu'une authentification fluide sur l'ensemble des appareils et applications.

2. Microsoft Intune offre une visibilité centralisée, cloud-native, sur l'ensemble des terminaux — ordinateurs de bureau, portables, appareils mobiles et environnements virtuels — en distribuant les applications professionnelles et de productivité au bon moment, en garantissant une posture de sécurité cohérente grâce à des configurations de référence, en appliquant la conformité, en configurant les paramètres à distance et en orchestrant les politiques globales.

3. Windows Autopilot permet un provisioning sans intervention manuelle, réduisant considérablement le temps d'onboarding tout en garantissant une expérience utilisateur standardisée, quel que soit le rôle ou la localisation — un atout optimal pour les environnements de travail hybrides.

4. Microsoft Defender xDR fournit une protection avancée contre les menaces et une réponse en temps réel, en s'appuyant sur des analyses pilotées par l'IA pour détecter et neutraliser les attaques aux niveaux des appareils, des e-mails, des applications et des identités.

5. Microsoft 365 Copilot intègre l'intelligence artificielle directement dans les flux de travail afin d'amplifier la productivité des employés, tandis que la gestion des appareils garantit un accès sécurisé et conforme aux sources de données requises.

6. Microsoft Purview applique des politiques de gouvernance, protège les données, sécurise les ressources sensibles de l'entreprise contre les menaces internes, empêche l'exfiltration de données et facilite la conformité à des cadres réglementaires tels que le RGPD, l'HIPAA ou le NIST AI RFM, grâce à des fonctions intégrées de classification et d'audit.

7. Windows Autopatch automatise la gestion des correctifs, garantissant que les appareils restent continuellement à jour, sans nuire à la productivité des utilisateurs ni nécessiter d'intervention manuelle. Cela permet aux équipes IT de se concentrer sur des initiatives stratégiques plutôt que sur la maintenance courante.

Ensemble, ces solutions permettent aux responsables IT de générer des résultats mesurables : réduction des coûts de support, amélioration de la posture de sécurité, accélération de l'onboarding et hausse de la satisfaction des collaborateurs. L'approche plateforme de Microsoft réduit la prolifération des outils, simplifie la conformité et aligne la gestion des terminaux sur les stratégies plus larges de transformation numérique.

L'expertise de NTT DATA dans le déploiement de la stack de gestion moderne Microsoft dans des environnements complexes garantit que ces bénéfices soient rapidement réalisés, et à grande échelle. De la conception de la feuille de route à la gestion du changement, NTT DATA apporte une exécution fiable de la modernisation des terminaux, générant des résultats tangibles tels que la productivité des collaborateurs, l'optimisation des coûts, la continuité d'activité, la sécurisation des opérations, l'alignement réglementaire et la préparation à l'IA.

Feuille de route de mise en œuvre pour les DSI basée sur le modèle de maturité Microsoft

L'adoption d'une stratégie de gestion moderne des appareils n'est pas un événement ponctuel, mais un parcours évolutif structuré en étapes. Le modèle de maturité Microsoft fournit un cadre de référence qui aide les DSI à évaluer leur situation actuelle, à identifier les écarts de capacité et à planifier une trajectoire claire vers un environnement de gestion des terminaux pleinement intégré et optimisé. Chaque phase génère une valeur tangible, tout en construisant progressivement une résilience accrue, une sécurité renforcée et une productivité durable des collaborateurs. Ce modèle aide les DSI à passer d'une logique de maintenance des appareils à une dynamique d'activation numérique.

Étape 1 : Traditionnel — opérations fragmentées, faible visibilité et exposition aux risques

La plupart des organisations démarrent avec un modèle hérité de gestion des appareils, marqué par des outils cloisonnés, des politiques statiques et un provisionnement manuel. L'accès aux ressources de l'entreprise nécessite souvent une présence physique, la visibilité sur la conformité ou les menaces est très limitée. Les politiques de sécurité sont appliquées de façon incohérente, l'expérience utilisateur est non mesurée, et les processus d'intégration sont longs et lourds.

Réalité organisationnelle : coûts de support élevés, délais d'intégration longs, sécurité inconstante, expérience utilisateur insatisfaisante.

Mandat IT : cette phase vise à établir un diagnostic complet de l'écosystème d'appareils existant, à aligner les parties prenantes et à poser les bases de la gouvernance nécessaire à la transformation. Les DSI doivent mener une analyse de l'état actuel — inventaire des terminaux, outils d'administration, posture de sécurité, processus de conformité. L'objectif est d'élaborer une feuille de route préparant la transition vers une gestion centralisée, en phase avec les besoins du personnel et les ambitions de l'entreprise.

Étape 2 : Avancé — standardisé, gouverné et maîtrisé, mais encore réactif

Les entreprises à ce stade amorcent leur modernisation. Une fois le diagnostic et l'architecture de gouvernance en place, elles commencent à standardiser les politiques de gestion des endpoints, à consolider leurs outils et à activer les principales solutions de gestion Microsoft. Intune est déployé pour offrir un contrôle centralisé, Autopilot est configuré pour permettre un provisionnement sans contact,

et Defender est mis en service pour la détection et la réponse aux menaces. L'identité hybride et les accès conditionnels régissent les interactions entre utilisateurs, terminaux et ressources.

Initiatives stratégiques :

- Déploiement d'une identité hybride cloud-native avec Microsoft Entra ID
- Centralisation de la gestion des terminaux via Intune : distribution des applications et configurations
- Lancement du provisionnement sans contact grâce à Windows Autopilot
- Application du cadre Zero Trust via les accès conditionnels
- Détection et réponse aux menaces avec Defender

Résultats métier : amélioration de l'expérience utilisateur sur l'ensemble des appareils, meilleure maîtrise opérationnelle, accélération des intégrations, réduction de la surface d'attaque, atténuation proactive des menaces et premiers gains en optimisation des coûts.

Étape 3 : Optimisé — intégré, automatisé et piloté par la donnée

Le niveau optimal marque une transition décisive : on ne se contente plus de respecter les politiques — on les dépasse grâce à l'optimisation proactive. Les signaux de télémétrie, les données d'usage et les indicateurs de sécurité sont intégrés dans des moteurs analytiques qui déclenchent des actions prédictives. Windows Autopatch assure une gestion automatisée des correctifs et de la conformité. Microsoft Purview permet la protection et la gouvernance intelligentes des données.

Capacités déployées :

- Windows Autopatch pour une gestion automatisée des mises à jour
- Analytique avancée, avec surveillance proactive de la télémétrie des appareils
- Classification et chiffrement des données sensibles, avec politiques DLP via Microsoft Purview

Résultats métier : quasi absence d'interruptions, sécurisation du tissu informationnel et gouvernance prête pour l'audit.

Étape 4 : Stratégique — évolutif, intelligent et aligné sur les objectifs business

À ce stade, la gestion des appareils est entièrement intégrée au modèle économique et à l'architecture numérique de l'entreprise. Le cadre Zero Trust est institutionnalisé à tous les niveaux — appareils, identités, données, applications et réseaux. Microsoft 365 Copilot infuse la productivité au cœur des workflows, tandis que la gouvernance de l'IA garantit une utilisation éthique et responsable de ces outils intelligents. Les contrôles appliqués aux terminaux s'intègrent désormais aux rapports ESG, et les indicateurs DEX (expérience numérique collaborateur) influencent les politiques RH et de planification des effectifs. Les stratégies de gestion des endpoints s'étendent de façon fluide aux opérations de fusion-acquisition, au recrutement international et à l'adoption de nouveaux modèles économiques.

Capacités déployées :

- Cadre Zero Trust à l'échelle de l'entreprise
- Microsoft 365 Copilot, intégré aux processus métier
- Cadres de gouvernance de l'IA avec Microsoft Purview

Transformation organisationnelle :

- Stratégie terminaux alignée avec les enjeux business
- Les métriques endpoints nourrissent les rapports DEX et ESG
- La conformité, la sécurité Zero Trust et la préparation à l'IA deviennent des normes d'entreprise

NTT DATA accompagne les entreprises dans le déploiement et l'opérationnalisation de ces capacités, en s'appuyant sur le modèle de maturité Microsoft. En alignant stratégie, outils et exécution, les DSI passent d'un rôle technique à un véritable pilotage stratégique d'environnements numériques résilients, sécurisés et optimisés pour l'IA — créateurs de valeur tangible pour l'entreprise.

Étape	Opérations	Posture des appareils et opérations :	Gouvernance et insights :	Capacités déployées :	Impact métier :
Traditionnel	Fragmenté	Provisionnement manuel, outils et politiques cloisonnés	Aucune gouvernance, suivi d'inventaire de base	Outils legacy sur site	Coûts élevés, faible visibilité, forte exposition aux risques
Avancé	Réactif	Provisionnement sans contact, onboarding automatisé, identité cloud/hybride, déploiement accéléré des applications et des configurations, accès conditionnel dynamique, contrôle des politiques standardisé, protection et réponse aux menaces	Gestion de la conformité et inventaire unifié	Entra ID, Intune, Autopilot, accès conditionnel, Defender xDR	Productivité accrue des collaborateurs, sécurité renforcée — avec un effet immédiat sur la réduction des coûts
Optimisé	Proactif	Correctifs automatisés, sécurité des données, télémétrie pilotée par l'IA	Analytique avancée, scoring des risques, gouvernance prête pour l'audit	Autopatch, Purview, analytique avancée	Expérience collaborateur renforcée et sécurisation des données — facteurs clés de fidélisation des talents et de réduction quasi totale des interruptions
Stratégique	Intelligent, automatisé, piloté par l'IA	Appareils Zero Trust auto-réparateurs, prêts pour l'IA	Indicateurs DEX, objectifs ESG, cadres de gouvernance de l'IA	Gouvernance IA avec Purview, Microsoft 365 Copilot, cadre Zero Trust	La gestion des terminaux s'aligne sur la stratégie d'entreprise

Repositionner la gestion des appareils comme levier stratégique d'agilité et de confiance pour l'entreprise

La gestion moderne des appareils n'est plus une fonction IT de second plan — elle est désormais au cœur de la stratégie business. Dans un monde façonné par le travail hybride, la productivité augmentée par l'IA et la montée des cybermenaces, la manière dont une entreprise gère ses terminaux influence directement la performance des collaborateurs, les coûts d'exploitation, le niveau de risque et la vitesse d'exécution.

La plateforme Microsoft de gestion des appareils permet aux DSI de passer d'une gestion fragmentée et réactive à une gestion sécurisée, automatisée et intelligente des endpoints, reposant sur le cadre Zero Trust. Résultat : un onboarding plus rapide, une sécurité renforcée, un usage de l'IA conforme et intelligent, et une expérience numérique cohérente — le tout à grande échelle.

Ces avancées ne sont pas que des réussites techniques. Elles se traduisent en résultats business tangibles : baisse des coûts de support, accélération du délai de productivité, satisfaction accrue des collaborateurs, meilleure préparation aux audits et à la conformité. Ce sont les indicateurs qui comptent aujourd'hui pour les décideurs.

Dans le paysage actuel, la dextérité numérique n'est pas simplement un enjeu technologique — c'est un facteur de différenciation concurrentielle. Ce livre blanc propose un plan d'action clair aux DSI confrontés à cette complexité. Il décrypte les nouvelles attentes des collaborateurs, les tendances macro qui redéfinissent les stratégies endpoints, et les écarts opérationnels qui freinent l'exécution métier. Surtout, il démontre comment l'écosystème Microsoft de gestion moderne des appareils permet aux entreprises de transformer leurs terminaux — longtemps considérés comme un poste de coût — en un moteur d'agilité, de confiance et d'engagement des talents.

NTT DATA et Microsoft partagent une même vision : offrir aux entreprises des environnements de terminaux sécurisés, indépendants du lieu et adaptés à la diversité des usages, générant un impact business mesurable. Leur approche stratégique conjointe repose sur une expérience utilisateur fluide, une sécurité proactive et des opérations IT évolutives, ancrées dans le cadre Zero Trust et prêtes pour l'IA. Ce positionnement partagé garantit que les entreprises puissent moderniser leur environnement de travail avec confiance, en conciliant contrôle et flexibilité, performance et maîtrise des coûts.



À propos de NTT DATA et Microsoft

Selon le rapport NTT DATA Global Partnership de 2023 — « NTT DATA est reconnue comme l'un des principaux intégrateurs de systèmes mondiaux de Microsoft (GSI), fournissant des solutions sécurisées pour le lieu de travail numérique dans plus de 50 pays. »

NTT DATA et Microsoft entretiennent un partenariat stratégique mondial de longue date, avec une collaboration étroite pour accompagner les entreprises dans la modernisation de leurs environnements IT et l'accélération de leurs résultats business. En combinant les plateformes cloud et de sécurité de pointe de Microsoft avec l'expertise sectorielle approfondie et les capacités de livraison mondiale de NTT DATA, les organisations accèdent à des solutions de transformation numérique fiables et complètes.

NTT DATA apporte des décennies d'expérience dans la conception, le déploiement et la gestion d'écosystèmes alimentés par Microsoft dans des environnements complexes et fortement réglementés. Qu'il s'agisse de déploiements à l'échelle de l'entreprise de Microsoft Intune et Microsoft Defender, de l'activation sécurisée de Microsoft 365 Copilot ou de la gouvernance des terminaux avec Microsoft Purview, NTT DATA veille à ce que la modernisation soit alignée sur la sécurité, la conformité et la stratégie commerciale à long terme.

Ensemble, NTT DATA et Microsoft apportent l'expertise, la technologie et la puissance opérationnelle nécessaires pour aider les entreprises à bâtir des environnements de travail numériques sécurisés, intelligents et productifs — adaptés aux enjeux d'aujourd'hui et préparés aux transformations de demain.

Annexe – Données de référence

- **Les collaborateurs plébiscitent le travail flexible** : « Plus de 70 % des travailleurs du savoir dans le monde ont adopté un modèle de travail hybride ou souhaitent en bénéficier après la pandémie. » — Gartner, « Future of Work Trends Post-COVID-19 », 2022
- **La gestion moderne des appareils réduit les coûts** : « Les organisations qui unifient la gestion de leurs endpoints constatent une baisse de 30 % de leurs coûts opérationnels et une réduction de 25 % des incidents de sécurité. » — Forrester Total Economic Impact™ Study of Microsoft Endpoint Manager, 2021
- **Le travail hybride est devenu la norme** : « 73 % des employés souhaitent conserver des options de télétravail flexibles. » — Microsoft Work Trend Index, 2023
- **Le Zero Trust devient une norme stratégique** : « D'ici 2025, 60 % des organisations adopteront le Zero Trust comme point de départ de leur stratégie de sécurité. » — Gartner, Market Guide for Zero Trust Network Access, 2022
- **L'IA booste la productivité des collaborateurs** : « Microsoft 365 Copilot améliore la productivité de 29 % pour l'exécution des tâches et la qualité de la rédaction. » — Microsoft Copilot Early Access Report, 2023
- **La conformité devient une priorité au plus haut niveau** : « Plus de 76 % des dirigeants mondiaux considèrent la gouvernance des données comme une composante stratégique. » — IDC Future of Trust Survey, 2023
- **La DEX impacte directement la rétention** : « Les entreprises qui investissent dans l'expérience numérique des collaborateurs affichent 22 % de rétention en plus et 17 % de productivité supplémentaire. » — Qualtrics X-Data and Gartner Workforce Trends, 2023
- **La durabilité passe aussi par les terminaux** : « Allonger la durée de vie d'un appareil d'un an permet de réduire de 30 % son empreinte carbone. » — NTT DATA ESG and IT Asset Study, 2022
- **Partenariat stratégique NTT DATA + Microsoft** : « NTT DATA est reconnu comme l'un des principaux intégrateurs Microsoft à l'échelle mondiale (GSI), avec des déploiements dans plus de 50 pays. » — NTT DATA Global Partnership Report, 2023

En savoir plus sur NTT DATA

Visitez le site nttdata.com

NTT DATA est un innovateur mondial de confiance en services de conseil et technologies, qui aide ses clients à innover, optimiser et se transformer pour réussir. En tant que Global Top Employer, nous réunissons des experts dans plus de 50 pays et bénéficions d'un solide écosystème de partenaires. En savoir plus sur NTT DATA

