Livre blanc

Télétravail & BYOD avec Wisper 360

Wisper

Contactez-nous facilement !

29%

des salariés français télétravaillent au moins une fois par semaine.
(source : Statista)

+90%

des incidents de sécurité impliquant des appareils perdus ou volés ont entraîné une violation non autorisée des données.
(source : JumpCloud)

80%

des organisations utilisent le BYOD aujourd'hui.
(source : JumpCloud)

Table des matières

Introduction 4

Défis actuels 9

Fonctionnement de Wisper 360 12

Cas d'usages Wisper 360 15

Conclusion 16

Contactez-nous facilement !

Introduction

Contexte

Le télétravail a connu une croissance notable en France ces dernières années. Selon une étude de Statista, en 2024, ***29 % des salariés français télétravaillent au moins une fois par semaine****. (source : Statista)*

Cette adoption est particulièrement marquée dans les grandes entreprises. En 2021, 47,5 % des entreprises de plus de 500 salariés ont mis en place le télétravail. (source : Statista)

Le télétravail aujourd'hui

Cette tendance s'est **accélérée avec la pandémie de COVID-19**, qui a contraint de nombreuses entreprises à adopter le télétravail pour **assurer la continuité de leurs activités.** Selon une étude de Statista, le taux de télétravail a atteint un pic de 41 % en 2020, avant de se stabiliser à 36 % en janvier 2024. Statista

Le télétravail est également influencé par l'âge des salariés. En 2024, **les employés âgés de 25 à 34 ans représentaient la plus grande proportion de télétravailleurs en France**. *(source : Statista)*

Cette évolution du télétravail reflète une transformation des modes de travail en France, avec une adoption croissante de pratiques flexibles adaptées aux besoins des salariés et des entreprises.

Les enjeux du BYOD

Le BYOD, ou “Bring Your Own Device”, désigne la pratique dans laquelle **les employés utilisent leurs équipements personnels, tels que leurs ordinateurs personnels, tablettes ou smartphones**. Ceci dans un cadre professionnel.

+90%

DES INCIDENTS DE SÉCURITÉ

impliquant des appareils perdus ou volés ont entraîné une violation non autorisée des données. (source : JumpCloud)

Cette pratique, de plus en plus courante, permet aux employés de travailler avec leurs propres appareils, offrant ainsi davantage de flexibilité. Selon une étude de JumpCloud, **plus de 80 % des organisations utilisent le BYOD aujourd’hui**, et 68 % rapportent une amélioration de la productivité des employés grâce à la mise en place de politiques BYOD. *(source : JumpCloud)*

Cependant, cette tendance engendre des défis majeurs en matière de sécurité. En effet, **30 % des responsables informatiques considèrent la sécurité de l’information comme le principal obstacle à l’adoption du BYOD**. *(source : JumpCloud)*

De plus, **plus de 90 % des incidents de sécurité impliquant des appareils perdus ou volés ont entraîné une violation non autorisée des données**. *(source : JumpCloud)*

Parmi les risques associés au BYOD figurent **le vol et la perte de données, l’infection par des logiciels malveillants et la fuite de données due au shadow IT***. (source : Keeper® Password Manager & Digital Vault)

Ces défis soulignent la nécessité pour les entreprises de mettre en place des politiques et des solutions de sécurité robustes pour protéger les données sensibles tout en permettant la flexibilité offerte par le BYOD.

**Le Shadow IT désigne l’utilisation de logiciels, d’applications ou de services informatiques au sein d’une organisation sans l’approbation ou le contrôle du département informatique.*

Enjeux principaux

L'adoption croissante du télétravail et des politiques de BYOD (Bring Your Own Device) présente plusieurs défis majeurs pour les entreprises, notamment en matière de sécurité des données, de gestion des accès et de support utilisateur.

Sécurité des données

La multiplication des points d'accès externes, tels que les réseaux domestiques et les appareils personnels, **augmente le risque de cyberattaques et de fuites d'informations sensibles**. Selon le Financial Times, **53 % des entreprises ont subi des compromissions liées aux appareils mobiles en 2024**, soulignant la vulnérabilité accrue associée à ces pratiques.
(source : Financial Times)

Support utilisateur

Fournir une assistance efficace à distance nécessite des outils adaptés pour résoudre les problèmes techniques sur une variété d'appareils personnels. La mise en place de **solutions d'accès sécurisé à distance est essentielle pour maintenir la productivité des employés** tout en garantissant la sécurité des données. (*source : Data Legal Drive)*

Gestion des accès

Assurer que seuls les utilisateurs autorisés puissent accéder aux ressources de l'entreprise devient complexe avec la diversité des appareils et des lieux de connexion. La CNIL recommande de **mettre en place des politiques de sécurité strictes pour le télétravail, incluant des directives claires sur l'utilisation des réseaux et des appareils personnels**. *(source : CNIL)*

53%

DES ENTREPRISES
ont subi des compromissions liées aux appareils mobiles

Problématiques spécifiques

Conformité réglementaire (RGPD)

La conformité au RGPD est essentielle pour garantir la protection des données personnelles, en particulier lorsque celles-ci sont accessibles via des appareils personnels dans le cadre du télétravail. **Le télétravail, combiné à la pratique du BYOD, où les employés utilisent leurs propres équipements pour des tâches professionnelles, présente des défis uniques en matière de sécurité des données**.

L'utilisation d'appareils personnels pour accéder aux ressources de l'entreprise peut entraîner des risques accrus, notamment la perte de contrôle sur les appareils, la sécurité des données et la séparation des données professionnelles et personnelles.

Pour assurer la conformité au RGPD, les entreprises doivent adopter des mesures de sécurité robustes, incluant l'évaluation des risques, **le contrôle d'accès, le chiffrement, la formation, la surveillance et un plan de réponse aux incidents**.

Grâce à Wisper 360, les entreprises peuvent mieux gérer les risques associés au télétravail et au BYOD, assurant ainsi la protection des données personnelles et le respect des exigences du RGPD. (*source : Cloudflare)*

Gestion des mises à jour logicielles

La gestion des mises à jour logicielles est essentielle pour maintenir la sécurité et la performance des systèmes informatiques, en particulier dans un environnement où les employés utilisent une variété d'appareils personnels dans le cadre du télétravail et du BYOD.
Maintenir à jour les logiciels sur une multitude d'appareils hétérogènes est une tâche ardue mais nécessaire pour prévenir les vulnérabilités.

L'utilisation d'outils de gestion des appareils mobiles (MDM) est recommandée pour répondre aux besoins informatiques des employés, qu'ils travaillent au bureau ou à domicile. Ces outils permettent de déployer, de gérer et de sécuriser les applications et les données sur les appareils mobiles, assurant ainsi que tous les dispositifs utilisés par les employés sont conformes aux politiques de sécurité de l'entreprise.

Avec Wisper 360, **les entreprises centralisent le déploiement et la maintenance des environnements de travail, simplifiant ainsi la gestion des mises à jour logicielles**. Cela garantit que tous les appareils des employés restent à jour et conformes aux politiques de sécurité de l'entreprise.

Collaboration à distance

Faciliter une communication fluide et efficace entre les équipes dispersées géographiquement est crucial pour maintenir la productivité. La mise en place de solutions de collaboration sécurisées permet de préserver la cohésion et l'efficacité des équipes en télétravail. Des outils tels que Microsoft Teams, Slack et Zoom offrent des fonctionnalités de messagerie instantanée, de vidéoconférence et de partage de fichiers, permettant aux équipes de travailler ensemble en temps réel, quel que soit leur emplacement. Ces plateformes intègrent des mesures de sécurité avancées, telles que le chiffrement des données et le contrôle des accès, garantissant la confidentialité des informations échangées. (*source : AyraDe)*

Cependant, pour garantir une collaboration optimale, il est essentiel de disposer d'un environnement de travail sécurisé et homogène. C'est là que Wisper 360 intervient.

En combinant Wisper 360 avec des solutions de collaboration comme Microsoft Teams ou Slack, les entreprises peuvent offrir à leurs équipes un environnement de travail sécurisé, flexible et propice à une collaboration efficace, quel que soit le lieu de travail.

Défis actuels

Gestion des périphériques

1

Risques liés à la perte ou au vol d'appareils

L'utilisation d'appareils personnels, tels que smartphones, ordinateurs portables ou tablettes, dans un environnement professionnel expose l'entreprise à des risques significatifs. La perte ou le vol de ces dispositifs peut entraîner une violation de données sensibles, notamment si des informations critiques comme des fichiers clients, des données financières ou des informations confidentielles sont stockées sur ces appareils. Selon une étude menée par **Ponemon Institute**, 57% des entreprises ont déjà connu la perte ou le vol d'un appareil mobile, et près de 50% de ces appareils contenaient des données sensibles pour l'entreprise.
(source : *Blog-IT Canada*)

2

Difficultés de contrôle des applications installées

En ce qui concerne le contrôle des applications installées sur les appareils personnels, les entreprises rencontrent des difficultés pour maintenir une visibilité claire sur les logiciels utilisés. Cela pose des risques d'introduction de logiciels malveillants, qui peuvent compromettre la sécurité des données d'entreprise. D'après une enquête réalisée par **Ponemon Institute**, 66% des employés ont téléchargé des applications mobiles sans autorisation, augmentant ainsi le risque de cyberattaques et de vulnérabilités au sein du réseau professionnel.
(source : *Ponemon Institute*)

Compatibilité des environnements de travail

Hétérogénéité des systèmes d'exploitation et des configurations

La diversité des systèmes d'exploitation et des configurations matérielles complique l'intégration des périphériques personnels au sein des systèmes d'entreprise. Par exemple, une entreprise ayant des employés utilisant à la fois Windows et Linux rencontre des défis importants pour maintenir une compatibilité avec les outils collaboratifs ou les solutions de gestion de contenu.

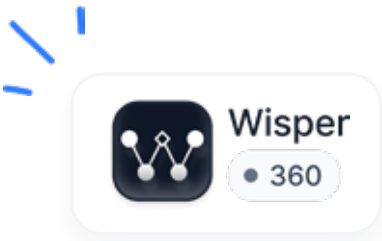
Difficultés d'intégration avec les outils de l'entreprise

Les entreprises sont confrontées à des défis majeurs pour intégrer les périphériques personnels dans leurs systèmes internes. Par exemple, un employé utilisant une application cloud spécialisée sur son appareil personnel peut rencontrer des difficultés pour synchroniser efficacement ces données avec les solutions de gestion des relations clients (CRM) ou les systèmes ERP déployés par l'entreprise.

Une étude menée par **Cisco** souligne que 69 % des entreprises ont constaté une augmentation des incidents de sécurité liés à l'utilisation de périphériques personnels non sécurisés. (*source : Cisco)*

De plus, une enquête de Kingston Technology indique que **le manque de supervision est l'un des principaux problèmes liés à la mise en œuvre du BYOD**. Les entreprises ont besoin d'un personnel d'assistance informatique en nombre suffisant pour permettre aux employés de s'équiper, avec une assistance et un suivi continus. (*source : Cisco)*

Ces données illustrent les défis auxquels les entreprises sont confrontées pour intégrer efficacement les périphériques personnels dans leurs systèmes internes, malgré les avantages potentiels en termes de flexibilité et de productivité.



Sécurisation des données

Risques liés aux accès non autorisés et aux fuites de données

L'accès distant aux données sensibles par le biais de dispositifs personnels expose ces informations à des menaces accrues d'accès non autorisé et de fuite de données. Une étude réalisée par le Ponemon Institute révèle que **78 % des répondants ont indiqué que leur organisation a connu une violation de données en raison d'employés négligents ou malveillants**. (*source : Ponemon Institute)*

Complexité de la mise en place de mesures de sécurité efficaces

La mise en place de mesures de sécurité robustes pour protéger les données sensibles est un défi majeur, en particulier lorsqu'il s'agit de dispositifs personnels utilisés à des fins professionnelles. Des solutions telles que l'authentification multifactorielle (MFA) et le chiffrement des données sont essentielles pour renforcer la sécurité. Cependant, leur déploiement peut s'avérer complexe, notamment lorsque les utilisateurs accèdent à des applications depuis divers types d'appareils et de systèmes.

Selon une étude menée par le Ponemon Institute, **47 % des petites entreprises ne savent pas comment se protéger contre les cyberattaques**, ce qui souligne la difficulté d'harmoniser les politiques de sécurité pour les périphériques personnels. (*source : Sénat)*

De plus, une enquête réalisée par Kingston Technology indique que le manque de supervision est l'un des principaux problèmes liés à la mise en œuvre du BYOD (Bring Your Own Device). Les entreprises ont besoin d'un personnel d'assistance informatique en nombre suffisant pour permettre aux employés de s'équiper, avec une assistance et un suivi continus. (*source : Kingston Technology Company)*

Ces données illustrent les défis auxquels les entreprises sont confrontées pour harmoniser et renforcer leurs politiques de sécurité en matière de périphériques personnels, malgré l'importance cruciale de ces mesures pour prévenir les risques de violation de données.

Fonctionnement de Wisper 360

Wisper 360 *est une solution complète de gestion des environnements de travail, qui centralise le pilotage des postes utilisateurs et machines virtuelles, qu'ils soient utilisés sur site ou à distance. Elle s'appuie sur un système d'exploitation propriétaire sécurisé et un modèle de déploiement basé sur des "Masters" – des templates de machines préconfigurées.*

1

Pilotage centralisé et simplifié

Grâce à **Wisper Manager**, les équipes IT disposent d'un tableau de bord unique pour piloter à distance l'ensemble du parc informatique : postes de travail, utilisateurs, VMs. L'interface offre une vision unifiée sur tous les environnements utilisateurs et permet :

- La création, le déploiement et la mise à jour des Masters en quelques clics,
- Le déploiement automatisé sur des groupes de postes définis,
- L'attribution de rôles, la gestion granulaire des droits d'accès et des ressources,
- La suppression ou le blocage à distance d'un environnement si nécessaire,
- Le suivi des connexions et la géolocalisation des postes.

2

Déploiement flexible et évolutif basé sur des Masters versionnés

Wisper permet de construire des environnements de travail à partir de Masters versionnés, intégrant l'OS client (Linux ou Windows), les applications, les paramètres système et les drivers.

Une fois le Master prêt, vous pouvez :

- le mettre à jour (versioning),
- valider les modifications via un environnement de préproduction,
- et déployer la nouvelle version vers les groupes de postes concernés.

Cette approche centralisée garantit une cohérence renforcée, une sécurité accrue et une forte réduction des tâches manuelles. Elle permet un déploiement rapide, reproductible et pilotable à grande échelle, tout en s'adaptant aux besoins spécifiques des équipes IT.

3 Un écosystème sécurisé par design

La sécurité est au cœur de l'architecture de Wisper 360. L'environnement repose sur un **OS hermétique et chiffré**, garantissant l'isolation totale entre l'environnement professionnel et l'environnement personnel, notamment dans les scénarios BYOD ou télétravail.

Les principales fonctionnalités de sécurité incluent :

- **Blocage du copier-coller** entre environnements pour prévenir toute fuite de données,
- **Séparation stricte** des usages pro/perso sur les appareils,
- **Gestion granulaire des accès** et des autorisations (applications, ressources, connexions),
- **Blocage d'adresses IP non autorisées**,
- **Géolocalisation** des terminaux pour un contrôle renforcé,
- **Suppression ou restriction d'un environnement à distance** via le Manager en cas de perte, vol ou usage suspect.

4 Visibilité et conformité continues

Wisper 360 permet aux DSI de garder un contrôle permanent sur le parc informatique, avec une conformité assurée grâce à :

- Des VMs standardisées et validées,
- Des logiciels maîtrisés,
- Des droits restreints selon les profils utilisateurs,
- Un historique des connexions facilement exploitable pour les audits.

Même si la configuration Dual Boot – permettant de passer d'une machine entreprise à un Boot entreprise ou personnel – reste rare, **Wisper 360** intègre des solutions d'authentification renforcée pour sécuriser cette option. En effet, le Dual Boot offre une isolation complète entre les espaces professionnels et personnels, garantissant une séparation stricte des données et des applications. Associé à une authentification renforcée, ce mode de fonctionnement permet d'assurer une sécurité accrue tout en offrant une flexibilité optimale aux utilisateurs qui souhaitent conserver leur propre équipement.

Réduction des coûts matériels et énergétiques

- **Pas de coût d'infrastructure serveur** : Wisper 360 fonctionne via une virtualisation locale des postes et un Manager SaaS, supprimant la nécessité d'une infrastructure serveur dédiée. Cela se traduit par une économie annuelle estimée entre **50 000 € et 100 000 € pour 100 utilisateurs** (soit **500 à 1 000 € par utilisateur**).

- **Compatibilité avec Windows 11 et TPM** : Wisper 360 assure la compatibilité avec **Windows 11 et TPM**, évitant ainsi le remplacement des PC non conformes. Pour le télétravail, cela simplifie l'utilisation des équipements personnels (BYOD) et optimise la gestion des flottes de PC portables, générant **des économies estimées entre 50 000 € et 100 000 €**.

Différenciateurs de Wisper 360

Wisper 360 se distingue par :

- **Résilience élevée** : indépendance totale vis-à-vis des incidents réseau, cloud ou DataCenter, garantissant une continuité d'activité.

- **Simplicité d'intégration** : compatibilité avec les outils existants pour une transition fluide. Son mode alternative VPN se distingue par sa simplicité, établissant la connexion en 1 ou 2 étapes – bien plus rapide que les 4 à 5 étapes requises par les solutions AVD.

- **Sécurité avancée** : isolation complète des environnements et interdiction des transferts de données entre espaces, éliminant les risques de compromission.

En combinant Wisper 360 avec des solutions de collaboration comme Microsoft Teams ou Slack, les entreprises peuvent offrir à leurs équipes un environnement de travail sécurisé, flexible et propice à une collaboration efficace, quel que soit le lieu de travail.

Cas d’usages Wisper 360

Sécurisation des informations sensibles

Wisper 360 crée un environnement isolé qui **sécurise l’accès aux informations confidentielles**. Grâce à son OS hermétique **Wisper Core**, l’ensemble des données sensibles (informations financières, dossiers clients, documents stratégiques, etc.) est protégé, même sur un appareil personnel. Les restrictions sur les transferts de données, telles que la désactivation du copier-coller, limitent les risques de fuite. La gestion centralisée permet en outre une surveillance continue et une réaction rapide en cas d’incident, renforçant ainsi la sécurité globale des opérations.

Gestion centralisée des applications professionnelles

La solution **offre un accès unifié aux applications métiers**, qu’il s’agisse de CRM ou d’autres outils de travail. En centralisant ces applications dans un environnement virtualisé, **Wisper 360 assure une interface homogène et sécurisée** pour tous les utilisateurs, quelle que soit la configuration de leur appareil. Cette approche simplifie les mises à jour et l’intégration des logiciels, réduisant les incompatibilités et améliorant la productivité tout en garantissant le respect des politiques de sécurité de l’entreprise.

Optimisation et sécurité pour les agents BPO

Les agents de Business Process Outsourcing (BPO) traitent un volume important de données et nécessitent un accès sécurisé et fiable à leurs outils de travail, même à distance. Avec Wisper 360, **ces agents bénéficient d’un environnement virtualisé étanche**, qui assure non seulement une haute performance, mais aussi une gestion centralisée des accès et des mises à jour. Cette solution facilite le déploiement rapide de correctifs et le suivi des incidents, tout en garantissant une continuité d’activité même en cas de défaillance de l’infrastructure réseau traditionnelle. Ainsi, les agents BPO peuvent se concentrer sur leur cœur de métier dans un cadre sécurisé et optimisé.

Conclusion

Synthèse des bénéfices de Wisper pour le télétravail et le BYOD

Wisper 360 constitue une solution incontournable pour les **entreprises souhaitant intégrer le télétravail et le BYOD** de manière efficace. Sa capacité à offrir une infrastructure sécurisée, performante et simple à administrer permet de répondre aux enjeux actuels. Parmi les principaux avantages figurent une réduction significative des c**oûts opérationnels et matériels**, une **amélioration de la productivité** des collaborateurs et **une protection renforcée des données sensibles**.

Vision d'avenir du télétravail et du BYOD

Avec l'évolution rapide des modes de travail, le télétravail et le BYOD s'imposent comme des piliers des organisations modernes. La flexibilité attendue par les employés et les impératifs de sécurité des entreprises nécessitent des solutions technologiques capables de s'adapter à un environnement toujours plus connecté et décentralisé. À l'avenir, ces pratiques deviendront encore plus stratégiques, exigeant des outils capables de combiner simplicité, performance et scalabilité.

Comment Wisper accompagne ces changements ?

En proposant des fonctionnalités avancées telles que la virtualisation locale, une gestion centralisée et des outils intégrés de sécurité, Wisper 360 accompagne les entreprises dans cette transformation. Sa capacité à réduire les coûts, à simplifier l'administration et à optimiser l'expérience utilisateur en fait un allié essentiel pour relever les défis des environnements de **travail hybrides et mobiles**. Wisper anticipe également les besoins futurs des organisations en proposant une solution évolutive et innovante, parfaitement adaptée aux réalités d'aujourd'hui et de demain.

Wisper

Révolutionnez votre management IT avec simplicité, sécurité et économies

11 Rue Dumont d'Urville, 76000 Rouen

Membre de French Tech Grand Paris | Normandy

Contactez-nous facilement !