



## **Télétravail : comment protéger les données de votre entreprise ?**



# SÉCURISATION DE VOS DONNÉES EN QUELQUES HEURES

Quelles mesures informatiques peuvent être prises immédiatement ou en quelques heures, localement ou à distance lorsque cela est possible :

## ✓ Un conseil efficace pour une situation inattendue

0. L'ensemble de la situation peut être abordé de manière très efficace, bien que ce soit un peu radical. Vous pouvez simplement « tout refuser » et autoriser les accès et les permissions uniquement à la demande pour certains utilisateurs lorsque cela est nécessaire.

## ✓ Protection de votre accès

1. La configuration appropriée des rôles des utilisateurs, ainsi que de l'accès aux systèmes et aux stockages de données, peut être facilement effectuée via Active Directory (AD).
2. L'activation d'une protection supplémentaire et d'une validation des accès est assurée dans ce cas par l'utilisation d'une authentification multifacteur (généralement à deux facteurs), qui est désormais prise en charge par tous les systèmes informatiques modernes. Cela permet d'authentifier les utilisateurs à l'aide de SMS ou de codes numériques générés, par exemple dans l'application mobile.

## ✓ Connexion à distance à votre réseau

3. Idéalement, un réseau privé virtuel (VPN) actif devrait être déployé. De cette façon, la connexion des ordinateurs à votre réseau et aux systèmes, aux données et aux stockages sensibles, est toujours facilitée par l'utilisation d'un VPN.

## ✓ Protection de vos postes de travail

4. Les disques durs de ces appareils devraient être chiffrés car ils stockent des données de votre entreprise.
5. Parmi vos équipements de travail, les **ordinateurs portables** sont une catégorie assez courante qui comporte des risques particulièrement élevés.
  - a. Chiffrez les disques durs avant de les fournir aux utilisateurs afin de protéger les postes de travail contre les fuites de données en cas de perte ou de vol des appareils.
  - b. Séparez les profils de travail des autres utilisateurs, tels que les travailleurs, afin d'empêcher tout accès indésirable par des utilisateurs non autorisés ; les profils peuvent être séparés au niveau du système d'exploitation et au niveau des navigateurs web.
  - c. Les ordinateurs portables sont souvent équipés de supports de stockage externes personnels ou tiers, ce qui augmente le risque de transmission de logiciels malveillants et ouvre également la voie au vol de données sensibles. Vous pouvez les contrôler à l'aide de solutions de contrôle des périphériques.

# SÉCURISATION DE VOS RESSOURCES EN QUELQUES JOURS

Voici quelques actions plus exigeantes, qui conduisent cependant à une protection plus adéquate de l'environnement de votre entreprise, même en cas de recours au télétravail.

## ✓ Appareils portables

6. Les supports de stockage portables tels que les clés USB, les disques durs externes ou les appareils mobiles sont également une source fréquente de fuites d'informations sensibles, de connaissances, etc. Le chiffrement des supports et des disques durs externes par une méthode physique ou virtuelle est certainement très recommandé.

## ✓ Périmètre sécurisé

7. La mise en place d'un périmètre de travail sécurisé réduit considérablement le risque de fuite d'informations sensibles. Le fait de restreindre les services disponibles contribue grandement à la protection des données et des transferts de données :
  - a. L'utilisation de messageries et de webmails gratuits (tels que yahoo.com ou gmail.com) comporte des risques considérables en cas de communication depuis un poste de travail.
  - b. Il en va de même pour l'utilisation de services de stockage de fichiers bien connus ou de services dans le Cloud librement accessibles (tels que Dropbox, WeTransfer, etc.).
  - c. En général, limitez l'utilisation des appareils externes et leur connexion aux postes de travail.

## ✓ Formation rapide des utilisateurs

8. Expliquez la situation actuelle aux utilisateurs, mettez à jour les politiques de sécurité, communiquez quelques conseils de sécurité très efficaces ; voilà autant d'étapes qui contribueront à protéger les télétravailleurs. Fournissez des recommandations sur l'utilisation des données sensibles avec des outils et des systèmes informatiques.
9. Restez fidèle à votre routine de travail, vos heures de travail et votre emploi du temps. Le télétravail ne signifie pas travailler en freelance, et l'éthique professionnelle ainsi que les contacts fréquents sont également un élément important qui contribue à maintenir un comportement raisonnable et prudent.

## ✓ Accès à distance

10. L'accès à distance comporte également des risques élevés pour la sécurité des données. Il permet aux utilisateurs de se connecter depuis leur propre ordinateur à celui de leur bureau, ce qui leur fournit un accès supplémentaire aux systèmes internes et aux données sensibles. Du point de vue de l'administrateur informatique, c'est un défi de taille que les solutions de DLP peuvent atténuer.
11. Les administrateurs informatiques doivent disposer d'outils de supervision des facteurs de risque et des incidents de sécurité, idéalement avec la possibilité d'envoyer des alertes de sécurité instantanées et/ou des rapports réguliers sur vos données les plus importantes.

# PROTECTION À LONG TERME DE VOS DONNÉES ET ÉQUIPEMENTS

Les grands chantiers conduisant à une protection idéale de votre environnement informatique interne prennent du temps. Préparez-vous dès maintenant pour éviter les situations similaires à l'avenir !

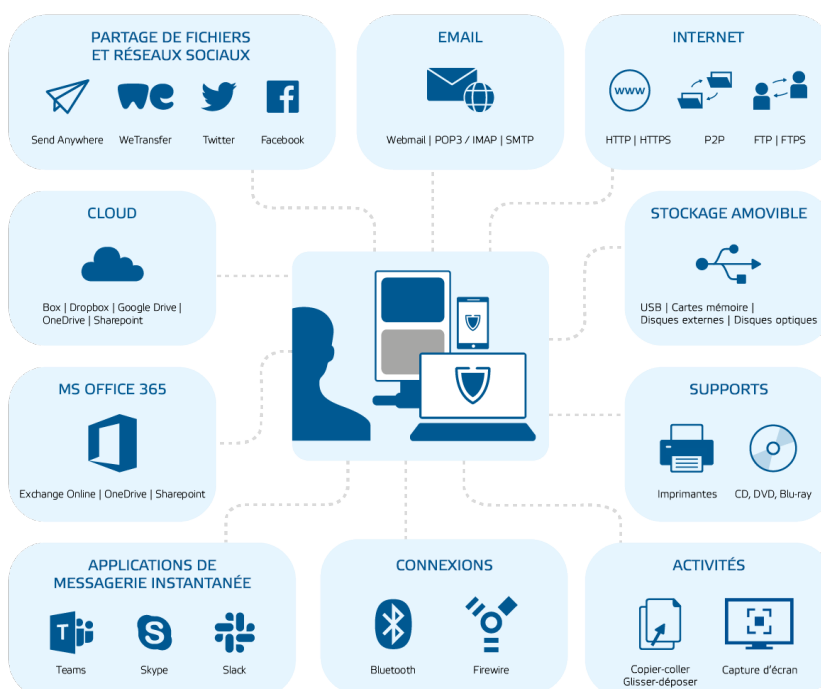
## ✓ Déploiement d'une protection active des données

12. D'après notre longue expérience, nous recommandons aux administrateurs informatiques de différencier les heures de travail officielles des heures non ouvrables pour leurs utilisateurs, et de surveiller étroitement les activités et les incidents de sécurité qui se produisent en dehors des heures de travail. Ils impliquent souvent des tentatives intentionnelles de fuite de données sensibles, ou un accès non autorisé aux systèmes internes.
13. Améliorez la sécurité de vos données et votre expérience utilisateur en utilisant des solutions de DLP (prévention des fuites de données) telles que Safetica.

## ✓ Formation avancée des utilisateurs

14. Le réseau de votre entreprise n'est aussi sûr que le réseau des utilisateurs qui s'y connectent. Sensibilisez vos utilisateurs sur les meilleures pratiques pour configurer leurs ordinateurs, leurs appareils et leurs réseaux personnels :
  - a. Logiciels antivirus et leurs paramètres
  - b. Mise à jour des applications, du système d'exploitation et des composants du réseau
  - c. Utilisation d'applications tierces et téléchargement d'applications à partir des app stores
  - d. Configuration de WPA2 avec mot de passe pour la connexion au réseau Wifi personnel

## DÉCIDEZ DE VOTRE PROPRE « ZONE PROTÉGÉE »



## COMMENT SAFETICA PEUT VOUS AIDER

Safetica assure la protection de vos données sur plusieurs canaux et plateformes, et veille à ce que vos données soient protégées où qu'elles se trouvent.

- ✓ **Protection des données** – protégez les données cruciales de votre entreprise et contrôlez les personnes qui y accèdent.
- ✓ **Analyse du comportement des utilisateurs** – découvrez comment le temps de travail, l'impression ou les logiciels coûteux sont utilisés.
- ✓ **Contrôle des appareils connectés** – déterminez quels appareils portables peuvent être utilisés et empêchez la connexion de supports non autorisés.

---

## SAFETICA

Safetica est un éditeur de logiciels tchèque qui protège les entreprises du monde entier contre les fuites de données sensibles et les menaces internes. Nous fournissons aux petites et moyennes entreprises une solution de protection des données. Nous estimons que chaque entreprise mérite de protéger ses données sensibles.

Safetica s'associe avec les principaux acteurs de la sécurité informatique tels qu'ESET, Microsoft, Fortinet, et des distributeurs leaders dans plus de 110 pays.



La solution Safetica a été récompensée par Gartner, Forrester et Radicati. Elle a remporté le prix TOP 100 Europe du concours Red Herring, le prix European User Award for Security de Computer Weekly, et s'est vue attribuée 5 étoiles par CNET et SC Magazine. Safetica est également signataire du Cybersecurity Tech Accord.



@Safetica



@Safetica



Safetica |

[www.safetica.com](http://www.safetica.com)

03\_2003