ZIMPERIUM®
MOBILE THREAT DEFENSE

# GDPR & appareil mobile

## FAIT #1 : LE GDPR INCLUT LE MOBILE DEPUIS SON ENTRÉE EN VIGUEUR EN 2018

À l'heure actuelle, toute personne qui exerce des activités commerciales au sein de l'Union européenne devrait connaître le GDPR. Le cadre juridique fixe des lignes directrices pour la collecte et le traitement des informations personnelles des individus au sein de l'Union européenne (UE). Chaque pays qui fait des affaires dans l'UE doit se conformer aux normes du GDPR.

Ce qui n'est peut-être pas connu de tous, c'est que les exigences du GDPR s'appliquent aux appareils mobiles. En fait, à peine trois semaines après l'entrée en vigueur du règlement le 25 mai 2018, une publication informatique de premier plan attirait l'attention sur l'applicabilité du GDPR aux appareils mobiles et sur le fait que la plupart des entreprises négligeaient complètement le mobile.

Les recherches ont montré que la plupart des entreprises ne pouvaient pas dire avec certitude quelles données leurs employés possédaient sur des appareils mobiles. Ce manque de visibilité des données sur les appareils mobiles (appartenant à l'entreprise ou aux employés), combiné à un manque de gouvernance et de protection de ces appareils, constitue « un défi direct à la conformité au GDPR ».

En d'autres termes, si vos mesures de conformité au GDPR n'incluent pas encore les appareils mobiles, vous n'êtes pas en conformité.

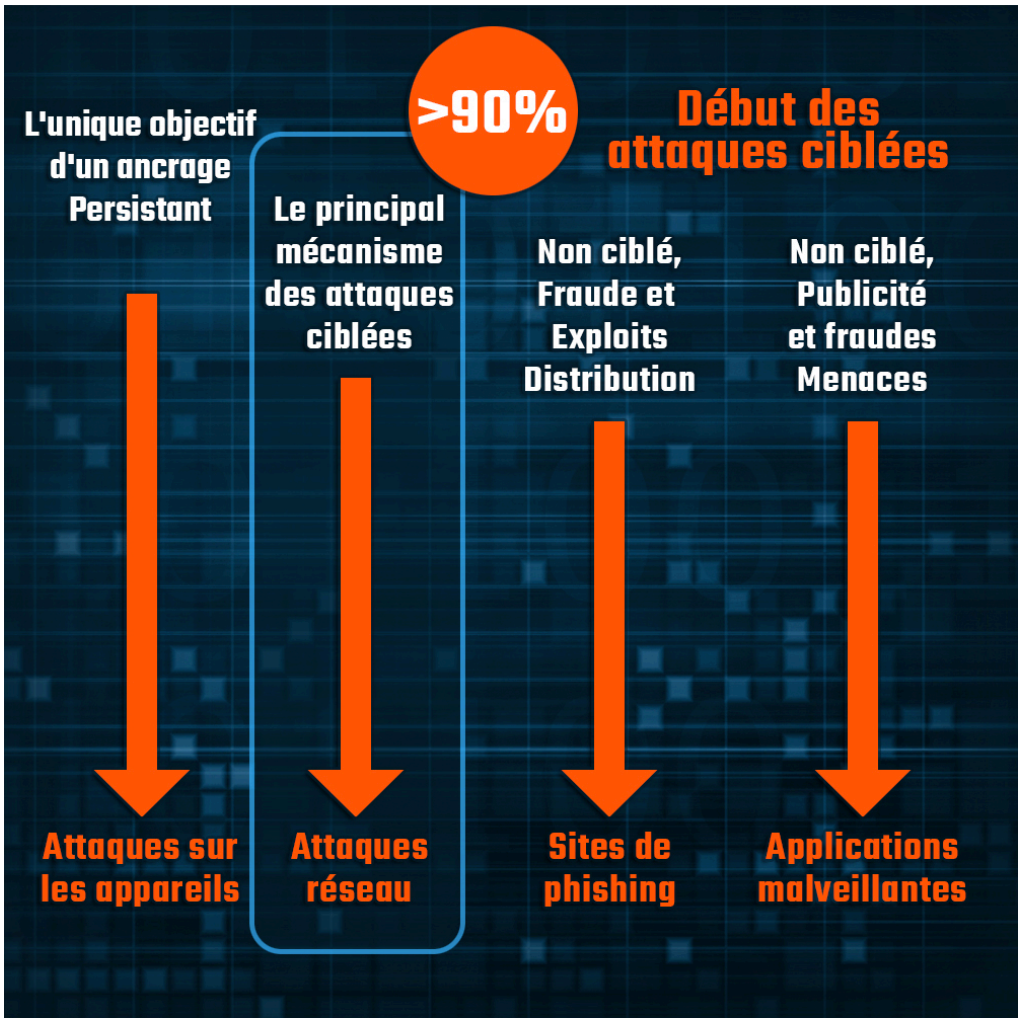
## FAIT #2 : LES APPAREILS MOBILES REPRÉSENTENT 60 % DES ENDPOINTS COUVERTS PAR LE GDPR

L'infographie de la Commission européenne a montré qu'en janvier 2019, les amendes pour les violations du GDPR avaient dépassé les 50 millions d'euros. Il n'est donc pas surprenant que la plupart des entreprises soumises au règlement aient investi des ressources importantes pour s'y conformer. Le problème survient lorsque les entreprises se concentrent sur la protection des endpoints sans se rendre compte que les appareils mobiles sont des endpoints, tant en ce qui concerne le GDPR qu'en général.

Les appareils mobiles sont désormais la plate-forme de facto de la productivité en entreprise. Cela signifie que les dispositifs informatiques traditionnels (par exemple, les serveurs, les ordinateurs de bureau et les ordinateurs portables) sur lesquels les entreprises ont concentré leurs efforts en matière de sécurité et de conformité ne représentent qu'environ 40 % des endpoints de leur entreprise. Les autres 60 % des appareils qui se connectent à votre réseau d'entreprise - les appareils mobiles - doivent également être mis en conformité avec le GDPR.

## FAIT #3 : LES ENDPOINTS MOBILES SONT ATTAQUÉS

Une différence essentielle entre les appareils mobiles et les autres types d'endpoints est la variété des vecteurs d'attaque auxquels les appareils mobiles sont exposés. Garantir l'intégrité des appareils mobiles nécessite de les protéger contre toutes ces formes d'attaque.



## FAIT #4 : LES EXIGENCES DU GDPR EN MATIÈRE DE MOBILE SONT EXPLICITES

Les exigences du GDPR s'appliquent explicitement aux appareils mobiles et autres s'ils détiennent des données à caractère personnel (DCP) sur des sujets de l'UE, ou des données sensibles si elles sont liées à des DCP. Les appareils mobiles étant au cœur de la productivité de l'entreprise moderne, ils interagiront inévitablement avec les systèmes stockant les DCP. À titre d'exemple, pensez au nombre d'E-mails qu'un employé typique d'une entreprise envoie chaque jour, et considérez que les adresses E-mails constituent des DCP.

L'article 5, Principes relatifs au traitement des données à caractère personnel, stipule que « (1) Les données à caractère personnel sont : (f) traitées de manière à garantir une sécurité appropriée des données à caractère personnel » En bref, les appareils mobiles de votre entreprise doivent être protégés.

De même, l'article 25, Protection des données dès la conception et par défaut, indique au paragraphe 1 que les entreprises soumises au GDPR « ... mettent en œuvre les principes de protection des données ... afin de satisfaire aux exigences du présent règlement et de protéger les droits des personnes concernées ». Cela signifie que les appareils mobiles de votre entreprise doivent être protégés dès la conception. L'article 25 exige également, au paragraphe 2, « que les entreprises soient responsables et puissent démontrer qu'elles sont conformes au paragraphe 1 ».

## FAIT #5 : ZIMPERIUM EST LA SOLUTION POUR LA CONFORMITÉ MOBILE AU GDPR

Étant donné que les solutions de Zimperium détectent les menaces sur l'appareil plutôt que d'envoyer des informations sur un cloud, elles peuvent protéger les appareils mobiles sans qu'il soit nécessaire de collecter ou de traiter des données à caractère personnel (DCP). Il s'agit de la configuration de Zimperium pour GDPR. En ne collectant ni ne rapportant aucune DCP, Zimperium permet aux entreprises de recevoir toutes les détections de risques mobiles et de menaces actives de Zimperium de manière totalement conforme au GDPR.

Zimperium s'appuie sur un moteur breveté basé sur l'apprentissage automatique, z9, pour détecter en temps réel les attaques contre les appareils mobiles, le réseau, le phishing et les applications, offrant ainsi la protection la plus complète disponible pour les appareils mobiles et les données qu'ils contiennent.

À ce jour, le moteur z9 a détecté 100 % des exploits zero-day sur les appareils sans nécessiter de mise à jour ni souffrir des retards et des limites de la détection basée sur le cloud ou des architectures de sécurité existantes, ce qui rend Zimperium particulièrement apte à répondre aux exigences mobiles du GDPR.

En outre, Zimperium permet aux entreprises de sécuriser les applications mobiles qu'elles créent grâce au SDK zIAP (In-App Protection). Plutôt que d'utiliser l'IMEI, zIAP utilise un identifiant unique créé par Zimperium qui n'a aucun lien avec les DCP et n'y a pas accès.

## CONTACTEZ ZIMPERIUM POUR LA CONFORMITÉ MOBILE AU GDPR

Lorsque vous êtes prêt à assurer la conformité aux exigences mobiles du GDPR, veuillez nous contacter pour une évaluation personnalisée.

ZIMPERIUM®