# Les dangers du BYOD (Bring Your Own Device)

La pratique n'est pas nouvelle. Déjà en 2009, le cabinet Gartner constatait que 43 % des cadres des grandes entreprises américaines utilisaient leur propre matériel – portable, smartphone et désormais tablette – pour leur travail. Le **BYOD** (*Bring Your Own Device*, apporter son propre terminal) séduit tout autant les employés qui s'équipent du matériel qu'ils choisissent eux mêmes, que les entreprises qui peuvent ainsi satisfaire une des demandes récurrentes de leurs employés ; disposer immédiatement de la dernière technologie IT en vogue. On appelle également cela la **consummérisation de l'IT** !

Cette tendance s'accompagne en revanche d'un alourdissement de la problématique sécuritaire de l'entreprise. Dans une récente étude, le constructeur de solutions réseaux Netgear pointait les trois éléments principaux qui doivent être maîtrisés pour adopter le BYOD : la sécurité du système d'information vis-à-vis du terminal (contrôle des accès, contrôle des flux, etc.) ; la sécurité du terminal lui-même (antivirus, authentification, chiffrement des données) ; et la gestion du parc de terminaux mobiles. Et d'indiquer que la plupart des grandes entreprises ont pris la mesure de la difficulté et mis en place de nouvelles procédures, voire adopté des solutions de gestion centralisée de terminaux mobiles (MDM).

## La PME en danger

La problématique du BYOD devient plus sensible lorsque l'on évoque les PME. En effet, si l'étude de Netgear révèle que cette pratique concerne désormais 87 % des employés dans les PME américaines, et probablement autant en France, le risque est le même que pour les grandes entreprises mais la conscience du problème et le déploiement de solutions de sécurité adaptées sont très en retrait.

Manquant de personnel qualifié et de moyens pour gérer les terminaux et éventuellement déployer une solution de MDM, les PME qui pratiquent le BYOD affichent un indice de risque très élevé. « *Et qui reste peu pris en compte par les solutions de sécurité disponibles et à la portée des PME* », indique **Frédéric Dubois**, directeur régional de Netgear France. « *La grande majorité des services informatiques des PME interrogées ont simplement renoncé à contrôler le nombre toujours croissant de terminaux mobiles personnels utilisés par leurs employés.* »

## Limiter les risques

Les petites entreprises disposent pourtant de moyens pour limiter les risques. Comme l'usage du BYOD s'accompagne souvent d'une prise en charge d'une partie du budget d'équipement de l'utilisateur, sous la forme du paiement de l'abonnement ou d'un avantage en nature, l'entreprise peut par exemple imposer à son salarié d'installer un antivirus et de le mettre à jour, ou encore de supporter un VPN. Elle doit surtout le sensibiliser à la problématique sécuritaire, pour elle comme pour le salarié, et déployer des règles et usages à respecter.

Frédéric Dubois conseille également aux PME de s'équiper systématiquement de boîtiers de sécurité de type UTM, qui associent firewall, antivirus et filtrage d'URL, afin de filtrer tous les flux entrants vers les terminaux personnels. Des solutions qui complètent et renforcent les logiciels de sécurité installés sur les postes de travail.