

## **StealthZONE d'Imation solution USB du poste de travail ultras curis **

### **Accessoire**

Post  par : JulieM

Publi e le : 3/5/2012 11:30:00

**Imation Corp.**, le sp cialiste des solutions de stockage  volutives et de la s curit  des donn es, annonce la disponibilit  de **StealthZONE, sa solution USB** d'environnement de poste de travail ultra s curis , destin e aux entreprises.

D j  utilis e par les administrations nationales et les services de renseignements pour sa capacit    fournir un poste de travail sur un dispositif haute s curit  de poche, StealthZONE conviendra aux entreprises n cessitant un environnement de travail s curis  et op rationnel sur n'importe quel ordinateur.

### **Une r ponse aux attentes du march **



**Le ph nom ne grandissant du BYOD** (Bring Your Own Device, concept consistant   apporter son propre p riph rique sur le lieu de travail) entra ne des d fis importants en mati re de s curit  pour les entreprises. D'apr s une enqu te men e dans 17 pays par le fournisseur de solutions technologiques Avanade, les employ s, dans 88 % des entreprises, utilisent leurs p riph riques personnels   des fins professionnelles<sup>1</sup>. De plus, une enqu te men e par Harris Interactive pour le compte d'Imation, r v le que 91 % des entreprises interrog es autorisent les p riph riques de stockage amovibles sur leurs r seaux, alors que 34 % appliquent des politiques de chiffrement<sup>2</sup>.

Une autre  tude d'Imation indique que 82 % des professionnels de l'informatique sont tr s pr occup s par les cons quences de l'utilisation de p riph riques personnels sur la s curit  informatique. Ainsi, 36 % des entreprises interdisent l'utilisation d'appareils mobiles personnels. Cela signifie que les inqui tudes des entreprises en mati re de s curit  les emp chent de b n ficier des avantages majeurs du concept BYOD.

### **Un fonctionnement simple et s r**

Les périphériques StealthZONE d'information résolvent les problèmes du BYOD en offrant un environnement de travail sécurisé et cohérent sur tout point d'accès à l'équipement de ports USB. Le choix d'une machine hôte ne revêt ainsi aucune importance et ne présente aucune problématique liées à la sécurité, la faisabilité ou la licence. L'utilisateur branche un périphérique USB StealthZONE à son PC ou ordinateur portable personnel Windows, non sécurisé, et lance Windows depuis le périphérique USB. Après une authentification à trois critères, l'utilisateur peut accéder à un espace de travail Microsoft Windows entièrement isolé. Puisque les activités informatiques ne se déroulent que dans l'environnement sûr du périphérique, les applications et données sont sécurisées du matériel du PC non sécurisé et donc protégées contre toutes menaces. Lorsque le périphérique StealthZONE est débranché de l'ordinateur hôte, il ne laisse aucune trace.

« La solution StealthZONE est idéale pour les entreprises avec un important personnel nomade » déclare **Nick Banks**, directeur EMEA et APAC d'Information Mobile Security. « Permettre à tout ordinateur non fiable de se transformer en un système sécurisé s'avère inestimable pour les travailleurs mobiles. Compte tenu des statistiques troublantes concernant le nombre d'employés télétravaillant dans l'insécurité et utilisant des périphériques de stockage non chiffrés à des fins professionnelles, les entreprises devraient sérieusement considérer la sécurisation de leur personnel nomade. »

[Lisez notre test sur le HDD 200 Biométrique d'Information](#)