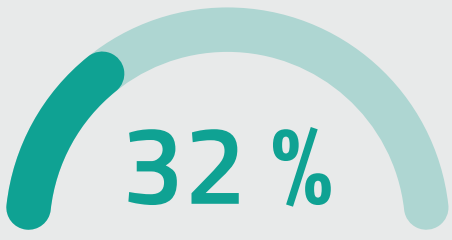
SHADOW IT :
LE DANGER CACHÉ POUR LES ENTREPRISES

Le phénomène du shadow IT, "informatique de l'ombre" ou encore "rogue IT", se réfère à l'utilisation non autorisée par la direction informatique de logiciels, de services et d'applications au sein d'une organisation.

La nouvelle menace secrète des entreprises...

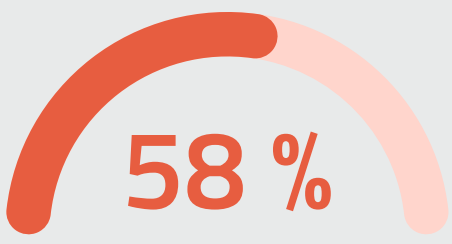
DES INCIDENTS

de sécurité rencontrés par une entreprise sont causés par le Shadow IT en 2021



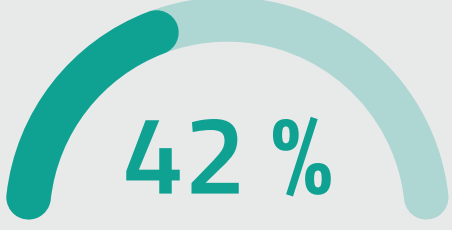
INSATISFAITS

des logiciels et applications proposés par leur entreprise



DES EMPLOYÉS

utilisent des comptes de messagerie non approuvés par les équipes informatiques en 2020



Shadow IT : quels risques pour les entreprises ?

VIOLATIONS DES DONNÉES

Le salarié contourne les protocoles de sécurité de l'entreprises, ainsi les données sensibles sont vulnérables au piratage informatique

PERTE DE PROPRIÉTÉ INTELLECTUELLE

Le salarié peut copier des fichiers sensibles et des courriels contenant des éléments de propriété intellectuelle de grande valeur grâce à un logiciel non autorisé

RISQUES DE CYBER-ATTAQUES

Un échange de fichiers via un e-mail ou un logiciel installé sans approbation sur un ordinateur est un potentiel point d'ouverture pour les cyber-attaques

Comment mettre fin aux pratiques de shadow IT ?

1 SENSIBILISER LES SALARIÉS

Lors de sessions de sensibilisation régulières, exposez des exemples concrets d'incidents de shadow IT et leurs conséquences pour l'entreprise et les individus.

2 AVOIR UNE POLITIQUE INFORMATIQUE

Créez une charte informatique définissant les logiciels, applications, matériel et services cloud approuvés, ainsi que le processus de validation des nouvelles applications.

3 FAVORISER LA COMMUNICATION

Favorisez les échanges entre salariés et DSI via des canaux de communication accessibles à tous, pour encourager les questions et idées, pour optimiser les outils en place.

www.aneol.com aneol team@aneol.com