ENTRUST
SECURING A WORLD IN MOTION

5 Bonnes raisons D'INTÉGRER UN HSM NSHIELD À VOTRE DÉPLOIEMENT AZURE

1 LES DONNÉES DE VOS CLIENTS SONT VOTRE RESPONSABILITÉ

Le mécanisme de responsabilité partagée indique que, quelle que soit la manière dont le service cloud est fourni, les clients restent responsables de leurs données.

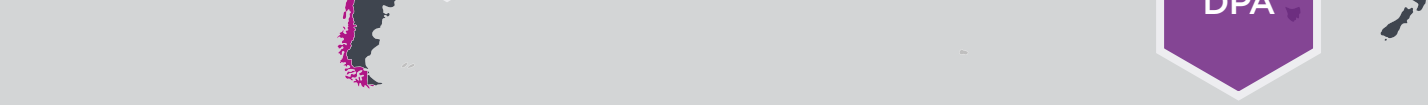
	Infrastructure en tant que Service (IaaS)	Plateforme en tant que Service (PaaS)	Logiciel en tant que Service (SaaS)
Responsabilité du client	Données	Données	Données
	Application	Application	Application
	Temps d'exécution	Temps d'exécution	Temps d'exécution
	Intergiciel	Intergiciel	Intergiciel
	SE	SE	SE
Responsabilité du fournisseur	Virtualisation	Virtualisation	Virtualisation
	Serveurs	Serveurs	Serveurs
	Stockage	Stockage	Stockage
	Mise en réseau	Mise en réseau	Mise en réseau

Source : https://gallery.technet.microsoft.com/Shared-Responsibilities-81d091

2 IL Y A DE PLUS EN PLUS DE FUITES DE DONNÉES

Le nombre connu de données personnelles compromises a considérablement augmenté, passant de 197,6 millions à 446,5 millions en 2018, soit un bond de 126 %. Le nombre total réel de données compromises est probablement encore plus élevé puisque la moitié seulement des fuites signalées en divulguent le nombre.

Forte hausse du nombre de données personnelles compromises en 2018 : +126 %



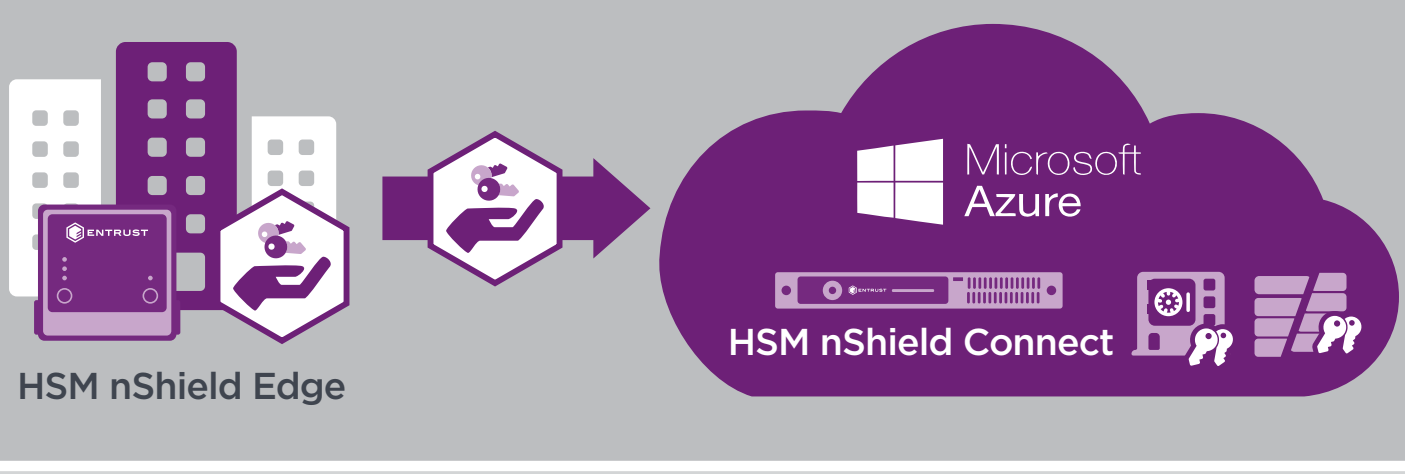
Source : Identity Theft Resource Center www.idtheftcenter.org/2018-data-breaches

3 VOUS DEVEZ RESPECTER LES NORMES EN VIGUEUR EN MATIÈRE DE CONFORMITÉ

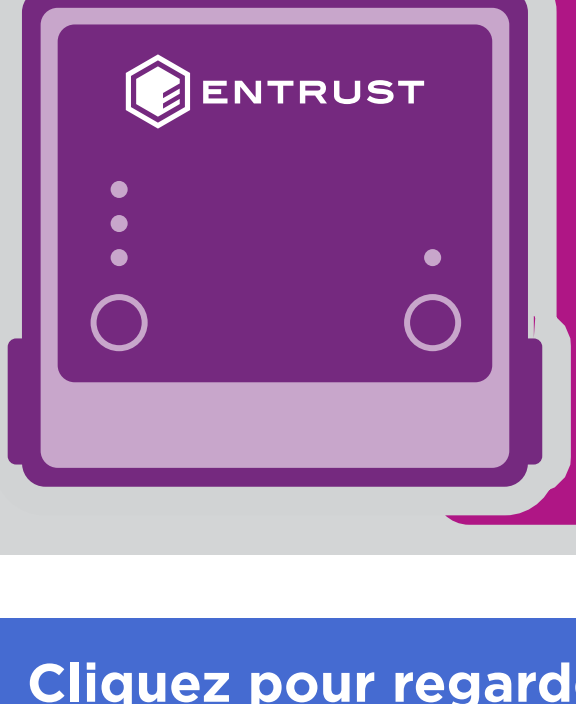
De nouvelles réglementations en matière de protection de la vie privée sont appliquées dans le monde entier, ce qui implique que les entreprises doivent assumer davantage de responsabilité et de transparence, sous peine de se voir infliger des amendes sévères. Respectez toutes ces exigences avec les HSM nShield.®

4 CONSERVEZ LE CONTRÔLE TOTAL SUR VOS CLÉS

Avec Bring Your Own Key (BYOK), vous pouvez surveiller et protéger vos données cloud grâce aux clés de chiffrement. Vous générez vos propres clés sur site, puis elles sont transférées de manière sécurisée vers les HSM dans le cloud, afin qu'Azure les utilise pour sécuriser les applications et les données, sans toutefois pouvoir les voir ou en faire un usage abusif.



5 UNE COUCHE DE PROTECTION SUPPLÉMENTAIRE POUR VOTRE CLOUD



Les HSM fournissent un environnement renforcé et inviolable permettant de réaliser des opérations de chiffrement sécurisé, de protéger les clés et de les gérer. Caractéristiques et fonctionnalités :

- Une couche de sécurité supplémentaire pour la création de plateformes d'application sécurisée
- Isolement des opérations et des clés de chiffrement
- Authentification forte des utilisateurs par carte à puce
- Application de la double vérification et de la séparation des tâches
- Génération de clés performantes et certifiées
- Puissante accélération et décharge du processus de chiffrement
- Certification FIPS 140-2

Cliquez pour regarder notre vidéo sur *Bring Your Own Key avec Entrust et Microsoft Azure*

Découvrez-en plus sur
entrust.com/HSM

ENTRUST
SECURING A WORLD IN MOTION