

2018

# RAPPORT SUR LES MENACES INFORMATIQUES

Tendances en matière de chiffrement  
et de sécurité des données

**ÉDITION MONDIALE**  
RÉSUMÉ OPÉRATIONNEL

#2018DataThreat

## LES POINTS CLÉS

La transformation numérique bouleverse tout. Changez votre façon de protéger vos données – ou faites-vous pirater. Encore.

Pour sa sixième édition, publiée en 2018, le Rapport de Thales sur les menaces informatiques quantifie l'étendue des piratages que subissent les moyennes et grandes entreprises dans le monde entier. En identifiant les risques et en détaillant les plans budgétaires de sécurité, le rapport apporte un éclairage crucial sur la façon dont les organisations peuvent éviter de subir une attaque informatique.

Cette année, nous avons constaté que la transformation digitale soumet les organisations à des changements majeurs. Elle conduit les organisations vers un monde régi par les données : 94 % des organisations utilisent des données sensibles via le cloud, le big data, des objets connectés, des conteneurs ou des environnements mobiles. Ces nouveaux usages sont autant de surfaces d'attaque et représentent de nouveaux risques pour les données. D'où la nécessité de prévoir des contrôles de sécurité en la matière.

### LA TRANSFORMATION NUMÉRIQUE EXIGE DE NOUVELLES APPROCHES



**94 %** des entreprises utilisent des technologies de transformation digitale sur des **données sensibles**.

Les taux élevés d'adoption de ces technologies renforcent le problème.



**100 %**  
des entreprises ont adopté le cloud



**99 %**  
recourent au big data



**94 %**  
mettent en place des solutions d'objets connectés



**91 %**  
utilisent des modes de paiements mobiles ou y travaillent

### LES ORGANISATIONS DOIVENT CHANGER LEUR FAÇON DE PROTÉGER LEURS DONNÉES

#### Entreprises piratées



**67 %** des entreprises ont déjà été piratées par le passé.

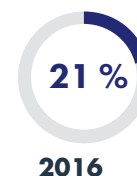
#### Entreprises piratées sur les trois dernières années



**36 %**  
2018



**26 %**  
2017



**21 %**  
2016

Chaque année, de plus en plus d'entreprises sont confrontées au piratage de leurs données.

### COMME SOUVENT : LES TEMPS ONT CHANGÉ, PAS LES STRATÉGIES DE SÉCURITÉ

Les pros de la sécurité informatique savent ce qui fonctionne pour protéger les données – mais ils ne donnent pas la priorité au budget affecté à la sécurité des données stockées.



**Données stockées**



**Réseau**



**Données mobiles**



**Analyse et corrélation**



**Points terminaux et mobiles**



■ Efficacité estimée

■ Augmentation des dépenses

### LE CHIFFREMENT EST LA CLÉ

Chiffrement nécessaire pour favoriser l'utilisation de technologies de transformation digitale :



Les outils de chiffrement arrivent en tête des achats prévus l'année suivante pour la sécurité des données :



**44 %**  
Tokenisation



**43 %**  
Chiffrement avec BYOK



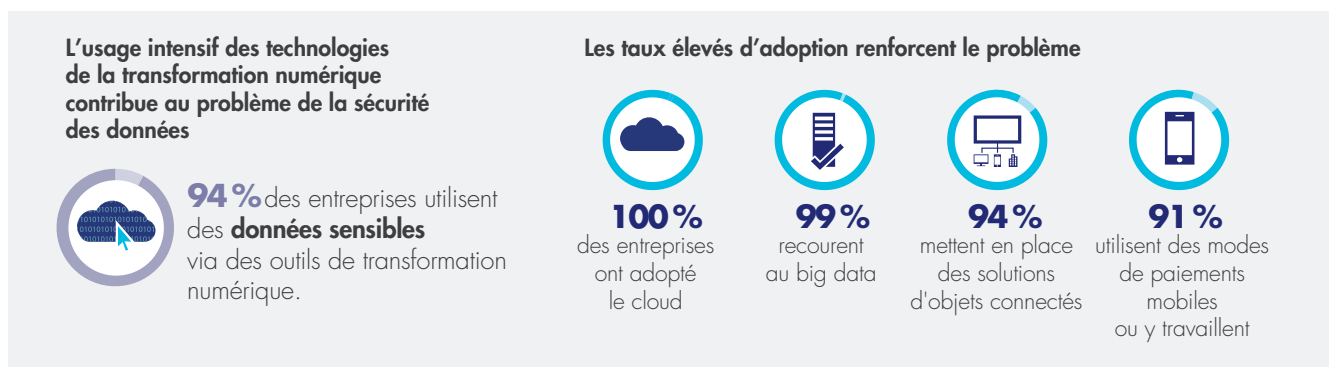
**41 %**  
Modules matériels de sécurité pour un chiffrement sûr

## LES DONNÉES SENSIBLES PLUS VULNÉRABLES QUE JAMAIS

La transformation numérique, outre le bouleversement qu'elle engendre dans le secteur informatique, nécessite de repenser la sécurité des données.

Ce phénomène grandissant redouble l'efficacité et accroît le périmètre d'intervention des entreprises tout en ouvrant la voie à de nouveaux modèles économiques, sources de croissance et de rentabilité. Pour saisir cette opportunité, les entreprises exploitent tout ce qu'offre la technologie numérique, mais peuvent alors, dans la précipitation du déploiement, compromettre la sécurité de leurs données sensibles.

L'adoption générale, au sein des entreprises, du cloud, du big data, des objets connectés, des conteneurs, des paiements mobiles et des technologies blockchain a atteint des niveaux record. Certaines technologies (comme le big data) affichent jusqu'à 99 % d'adoption, 94 % des entreprises prévoyant même d'utiliser des données sensibles au sein de ces environnements. Face à l'ampleur des nouveaux usages, ce problème devient hypercritique, d'autant que les organisations recourent désormais à de nombreux types d'environnements ou multiples fournisseurs.



## Les attaques fragilisent les défenses des entreprises à des niveaux records.

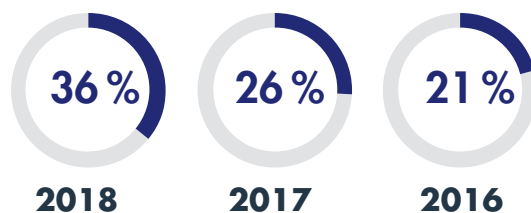
L'étendue et l'impact croissants des menaces se reflètent très clairement à travers le nombre d'attaques et les niveaux de vulnérabilité. Le piratage de données atteint des sommets – 67 % des organisations dans le monde déclarent avoir déjà fait l'objet d'attaques (71 % aux États-Unis). Ce phénomène a été plus élevé que jamais l'an dernier – 36 % des entreprises dans le monde ont été piratées (presque la moitié – 46 % – aux États-Unis) en 2017. Les entreprises apparaissent donc d'autant plus vulnérables, 44 % d'entre elles dans le monde (53 % aux États-Unis) se sentant très, voire extrêmement vulnérables face au piratage.

### Entreprises piratées



des entreprises ont déjà été piratées par le passé.

### Entreprises piratées au cours des trois dernières années



Chaque année, de plus en plus d'entreprises sont confrontées au piratage de données.

## DÉPLOIEMENT DANS LE CLOUD – SÉCURISATION INDISPENSABLE DES DONNÉES

Sécuriser les données où qu'elles soient déployées devient un problème critique.

L'usage du cloud est devenu universel, et les cas d'utilisation continuent de se multiplier – les taux d'adoption dans les entreprises explosent. Désormais, le cloud computing (39 %) est étroitement lié à la nécessité d'éviter toute pénalité due au piratage de données (39 %), suivie de près par la conformité (37 %) comme principale motivation des dépenses de sécurité informatique.

La plupart des entreprises mènent des stratégies multi-cloud, l'utilisation du SaaS (Software as a Service) étant particulièrement forte – 42 % utilisent 50 applications SaaS ou plus, et la majorité des entreprises utilisent au moins 2 fournisseurs IaaS (Infrastructure as a service) et PaaS (Platform as a service). L'explosion du cloud met à mal le concept traditionnel de « périmètre » d'une entreprise, puisque l'infrastructure et les logiciels associés ne sont plus sous le contrôle des entreprises. En conséquence, la sécurité des données devient une technologie de premier plan, et les solutions de chiffrement dans le cloud, la grande priorité en matière de sécurité (à 44 %). La multiplication des fournisseurs crée un autre problème : celui de la gestion, du suivi et du stockage des clés de chiffrement pour tous ces environnements, afin de conserver le contrôle des données. Face à la gestion des applications BYOK (Bring your own key) à travers des clouds multiples et à un ensemble grandissant d'exigences de conformité, les entreprises ont besoin de solutions qui leur permettent de gérer les clés de chiffrement et d'accéder aux données en toute sécurité, sans frais généraux inacceptables.

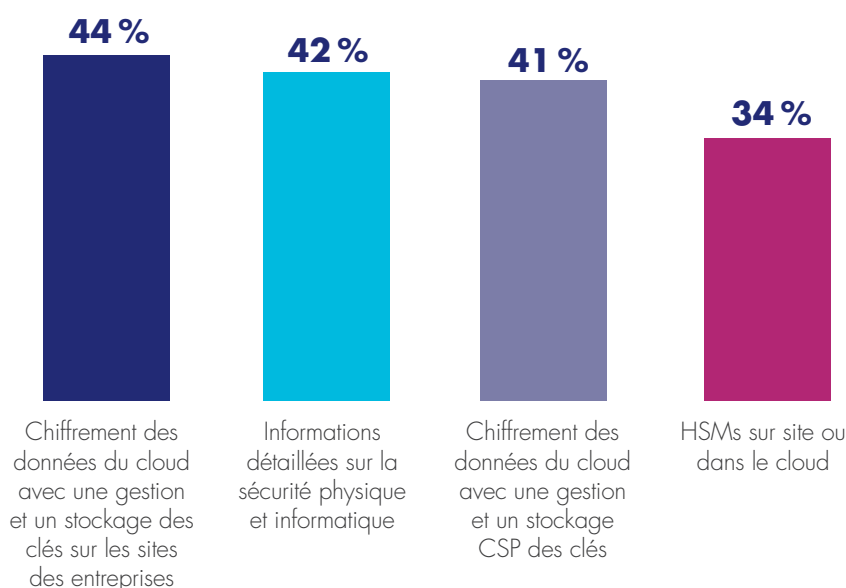


### Principales préoccupations concernant la sécurité du cloud

(Pourcentages des entreprises très/extrêmement préoccupées)



### En chiffrement, certaines solutions de contrôle de sécurité sont nécessaires pour renforcer le déploiement du cloud



## LE BIG DATA EST UNIVERSEL : LA PROTECTION DES DONNÉES SENSIBLES EST IMPÉRATIVE

Le big data métamorphose tout, et ce, à l'échelle mondiale. Aujourd'hui 99 % des entreprises y recourent (45 % l'utilisent déjà avec des informations sensibles), raison pour laquelle ces environnements sont toujours plus à risque, en termes de conformité, de réglementation au regard de la confidentialité, et de piratage des données. La nature complexe et la mutation rapide de ces environnements facilitent la localisation des données sensibles, où qu'elles soient, ce qui complique le problème et suscite des risques d'accès inapproprié. À cela s'ajoute une autre complexité, puisque le big data est souvent mis en œuvre dans des environnements de cloud. Ainsi, les entreprises perçoivent un risque associé à l'infrastructure et à l'emplacement des données qui ne sont plus sous leur contrôle.



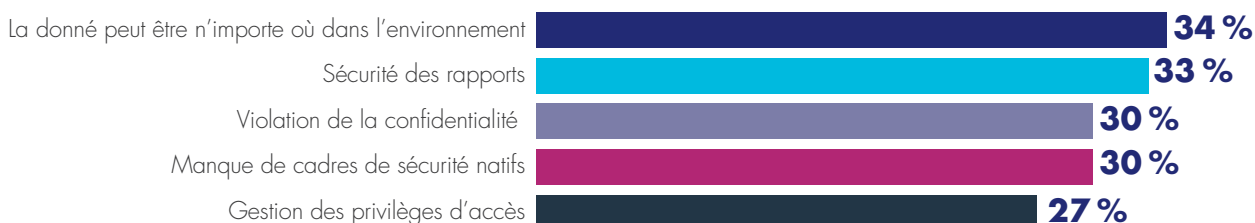
**99%** des entreprises recourent au big data



**45%** utilisent des données sensibles dans leurs environnements big data



### Principales préoccupations sur l'utilisation de données sensibles dans des environnements big data



### Comment accélérer l'adoption du big data ?



**38 %**  
Renforcement de l'authentification utilisateurs

**36 %**  
Meilleure gestion et suivi

**35 %**  
Contrôles des accès et chiffrement au niveau du système

**32 %**  
Chiffrement des données permettant des analyses

**31 %**  
Certifications de conformité

## LES MODES DE PAIEMENTS MOBILES EN HAUSSE – LE CHIFFREMENT EST LA CLE

Les applications de paiement mobile se répandent de plus en plus. En effet, 91 % des entreprises interrogées cette année comptent une application de paiement mobile en développement ou déjà déployée. Simultanément, beaucoup se préoccupent des vulnérabilités de l'écosystème des paiements mobiles. Ce mode de paiement requiert par définition une sécurité des données à chaque étape, puisqu'il fait courir le risque d'une perte d'informations financières et personnelles. C'est pourquoi le chiffrement devient une technologie clé, indispensable pour sécuriser l'environnement des paiements mobiles de bout en bout et pour se conformer rapidement à des règlements et à des normes industrielles qui évoluent très vite.

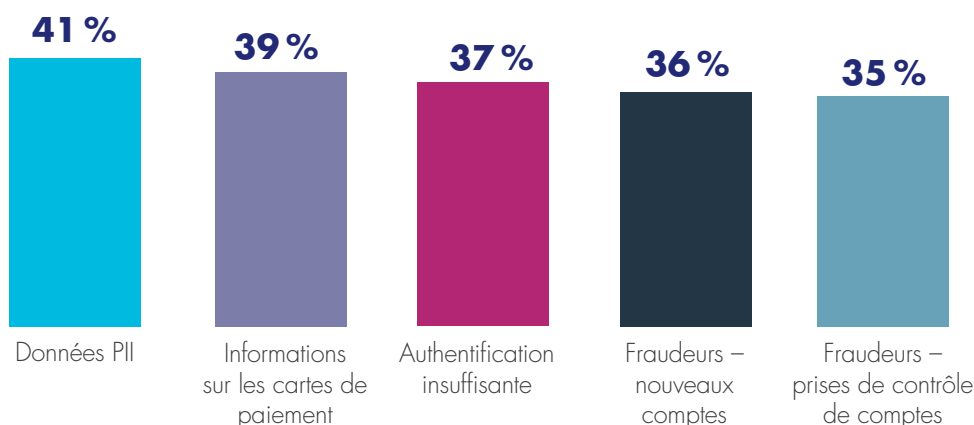


**91 %** utilisent ou comptent utiliser un mode de paiements mobiles



**37 %** utilisent aujourd'hui des données sensibles sur des applications mobiles

### Principales préoccupations concernant les paiements mobiles



### Le chiffrement, un outil clé pour sécuriser les modes de paiements mobiles



Le chiffrement permet d'identifier l'identité grâce aux certificats de naissance numériques des appareils.



Le chiffrement protège les données en cours de transfert.



Le chiffrement protège les données stockées sur les appareils.



Le chiffrement et les contrôles des accès aident les entreprises à respecter les exigences de conformité pour les entrepôts de données d'arrière-plan.

« Les attaques réussies ont atteint des records chez les entreprises aussi bien moyennes que grandes, plus de deux tiers (67 %) des organisations dans le monde et presque trois quarts (71 %) aux États-Unis ayant déjà été piratées. De plus, près de la moitié (46 %) des entreprises interrogées aux États-Unis avaient fait l'objet d'une attaque en 2017, soit presque le double (24 %) par rapport à l'année précédente. Ce chiffre s'élève à plus d'un tiers (36 %) à l'échelle mondiale pour 26% en 2016. »

« Clairement, faire ce que nous avons fait pendant des décennies ne fonctionne plus. D'où la question plus directe que se posent les responsables informatiques et les chefs d'entreprise : "Comment mettre fin au piratage" ?»

—Garrett Bekker, analyste en chef chez 451 Research, Sécurité des informations  
**Auteur du Rapport 2018 de Thales sur les menaces informatiques**

## LE CHIFFREMENT EST LA SOLUTION

Les technologies de chiffrement sont capitales pour protéger les données stockées, transférées et utilisées. Par ailleurs, le chiffrement sécurise les données de façon à respecter les exigences de conformité, les bonnes pratiques et les règlements relatifs à la protection des données. C'est le seul outil qui assure la sécurité et le contrôle des données non seulement dans les centres de données traditionnels, mais aussi avec les technologies utilisées pour réaliser la transformation numérique de l'entreprise.

## À PROPOS DE THALES

Thales est un leader mondial des hautes technologies pour les marchés de l'Aérospatial, du Transport, de la Défense et de la Sécurité. Fort de 64 000 collaborateurs dans 56 pays, Thales a réalisé en 2016 un chiffre d'affaires de 14,9 milliards d'euros. Avec plus de 25 000 ingénieurs et chercheurs, Thales offre une capacité unique pour créer et déployer des équipements, des systèmes et des services pour répondre aux besoins de sécurité les plus complexes. Son implantation internationale exceptionnelle lui permet d'agir au plus près de ses clients partout dans le monde. Thales est l'un des leaders européens de la sécurité et se positionne comme intégrateur de systèmes à forte valeur ajoutée, équipementier et fournisseur de services. Les équipes sécurité de Thales aident les États, les autorités locales et les opérateurs civils à protéger les citoyens, les données sensibles et les infrastructures critiques grâce à des solutions intégrées et résilientes.

En matière de protection des données, Thales propose tout ce dont a besoin une entreprise pour protéger et gérer ses données, ses identités et ses propriétés intellectuelles tout en respectant les obligations de conformité réglementaire : chiffrement des données, gestion avancée des clés, tokénisation, autorisations d'accès pour les utilisateurs privilégiés et application des normes les plus strictes en matière de certification pour offrir des solutions d'une fiabilité optimale. Les professionnels de la sécurité du monde entier font appel à Thales pour accélérer en toute confiance leurs processus de transformation numérique.

[CLIQUEZ ICI POUR LIRE LE RAPPORT COMPLET](#)

## NOS SPONSORS





**THALES**

[www.thalessecurity.com](http://www.thalessecurity.com)

©2018 Thales