THALES

Ponemon INSTITUTE

ÉTUDE SUR LES TENDANCES MONDIALES EN MATIÈRE DE CHIFFREMENT

France | Septembre 2017

TABLE OF CONTENTS

Sponsorisée par Thales e-Security

MENÉE EN TOUTE INDÉPENDANCE PAR PONEMON INSTITUTE LLC

PARTIE 1. DOCUMENT DE SYNTHÈSE

L'Institut Ponemon a le plaisir de vous présenter les résultats de *l'Étude sur les tendances mondiales en matière de chiffrement en 2017 : France*, qui est sponsorisée par Thales e-Security. Nous avons effectué un sondage auprès de 345 professionnels de la sécurité en France pour étudier l'utilisation du chiffrement et l'impact de cette technologie sur l'approche de la sécurité dans les entreprises de ce pays.

La première étude sur les tendances en matière de chiffrement avait été réalisée en 2005 sur un échantillon de répondants aux États-Unis. Depuis, nous avons élargi la portée de l'étude pour inclure les répondants de 11 pays : États-Unis, Royaume-Uni, Allemagne, France, Australie, Japon, Brésil, Fédération de Russie, Mexique, Inde et Moyen-Orient (combinaison de répondants résidant en Arabie saoudite et dans les Émirats arabes unis).[1]

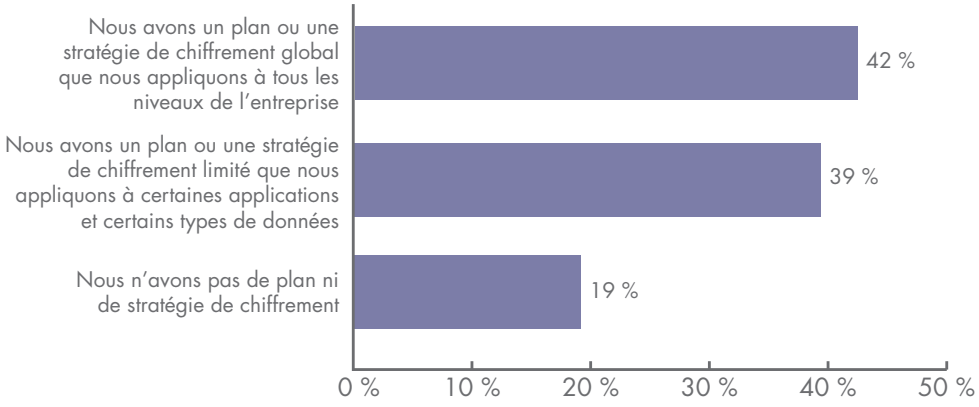
Face aux atteintes massives à la protection des données et aux cyberattaques, les entreprises s'empressent d'améliorer leur approche de la sécurité des données. En fait, 81 % des entreprises représentées dans cette étude ont adopté une stratégie de chiffrement plus ou moins élaborée, comme l'indique la Figure 1. Cette constatation et d'autres résultats démontrent l'importance du chiffrement et de la gestion des clés pour bénéficier d'une approche solide de la sécurité informatique.

Une synthèse des résultats principaux est donnée ci-après. La section suivante du présent rapport fournit plus de détails sur chacun des résultats principaux répertoriés ci-dessous.

Les secteurs d'activité au sein de l'entreprise forment le facteur le plus influant sur l'orientation des stratégies de chiffrement. Même s'il existe une dispersion de la responsabilité de la stratégie de chiffrement au sein de l'entreprise, les secteurs d'activité (41 %) exercent la plus grande influence. Quatorze pour cent des répondants déclarent qu'aucune fonction n'est responsable isolément de la stratégie de chiffrement.

Quels sont les types de données les plus fréquemment chiffrés ? Les données relatives aux paiements sont les plus susceptibles d'être chiffrées, tandis que les données relatives à la santé sont les moins susceptibles d'être chiffrées.

Figure 1. Quelle affirmation décrit le mieux la stratégie de chiffrement de votre entreprise ?



[1] En plus du présent rapport consacré à la France, d'autres rapports nationaux sont disponibles pour l'Australie (AU), le Brésil (BZ), l'Inde (IN), le Japon (JP), le Moyen-Orient (ME) et le Mexique (MX).

Un dysfonctionnement du système ou des processus est la menace la plus significative pour les données sensibles. Les dysfonctionnements de système ou de processus constituent les risques les plus importants d'exposition des données sensibles ou confidentielles, selon 42 % des répondants. Pour 30 % des répondants, les pirates informatiques constituent une menace grave. En revanche, les fournisseurs de services tiers et les demandes légales de données sont considérés comme les moins menaçants (20 % et 7 %, respectivement).

La conformité aux règlementations externes et aux obligations de confidentialité ou de sécurité des données constitue le facteur principal d'utilisation du chiffrement. Soixante-six pour cent des répondants indiquent que la conformité aux règlementations externes et aux obligations de confidentialité ou de sécurité des données est la raison principale de l'utilisation de technologies de chiffrement. D'autres raisons sont la protection des informations contre des menaces spécifiques et identifiées ainsi que la protection de la propriété intellectuelle de l'entreprise (55 % et 49 % des répondants, respectivement).

La difficulté majeure consiste à connaître l'emplacement des données sensibles au sein de l'entreprise. Soixante-dix pour cent des répondants indiquent que la difficulté première consiste à connaître l'emplacement des données sensibles au sein de l'entreprise, tandis que 49 % estiment que le déploiement initial de la technologie de chiffrement est difficile.

Il n'existe pas de technologie dominante parce que les entreprises présentent une très grande diversité de besoins. Le déploiement extensif le plus probable concerne le chiffrement des communications via Internet (p. ex. SSL), des sauvegardes, des archives et des bases de données. En revanche, les services de cloud public et les conteneurs docker sont les moins susceptibles de faire l'objet d'un chiffrement extensif ou partiel.

Certaines caractéristiques de chiffrement sont considérées comme étant plus importantes que d'autres. Selon les résultats, les caractéristiques les plus importantes sont la performance et la latence du système, le mécanisme d'inviolabilité par un matériel dédié (p. ex. HSM) et la gestion des clés. Les moins importantes sont l'assistance pour la séparation régionale (p. ex. souveraineté des données) et la séparation des fonctions et contrôles basés sur les rôles.

Quel est le degré de pénibilité de la gestion des clés ? 57% des répondants disent que la gestion des clés est très compliquée. Pour quelles raisons la gestion des clés est-elle pénible ? Les raisons majeures sont l'inadéquation des outils de gestion des clés et la possession mal définie. Les systèmes de gestion des clés les plus couramment employés sont les suivants : processus manuel (p. ex. tableur, document papier), politique formelle de gestion des clés (KMP) et système/serveur central de gestion des clés.

Quelles sont les clés les plus difficiles à gérer ? Les clés considérées comme étant les plus difficiles à gérer sont les clés de signature (p. ex., signature de code, signatures numériques), les clés associées à SSL/TLS et les clés SSH.

L'importance des modules de sécurité matérielle (HSM) dans le cadre d'une stratégie de chiffrement ou de gestion des clés va croître au cours des 12 prochains mois. Pour 33 % des répondants, les HSM sont importants et pour 41 % ils gagneront en importance au cours des 12 prochains mois. Les trois grands domaines d'utilisation des modules de sécurité matérielle sont le chiffrement au niveau des applications, le traitement des transactions de paiement et SSL/TLS. Au cours des 12 prochains mois, les entreprises sont plus susceptibles de déployer le traitement des transactions de paiement et SSL/TLS.

Comment les entreprises utilisent-elles les HSM ? Cinquante-cinq pour cent des répondants disent que leurs entreprises ont une équipe centralisée fournissant un service de chiffrement et 45 % des répondants disent que chaque titulaire d'une application/équipe est responsable de ses services de chiffrement.

La plupart des entreprises transfèrent des données sensibles ou confidentielles vers le cloud. Trente-sept pour cent des répondants indiquent que leurs entreprises transfèrent actuellement des données sensibles ou confidentielles vers le cloud (qu'elles soient chiffrées ou non ou rendues illisibles par un autre mécanisme) et 33 % des répondants déclarent que le transfert est prévu pour les 12 à 24 prochains mois.

Comment les données au repos dans le cloud sont-elles protégées ? Selon 41 % des répondants, le chiffrement est effectué sur place avant l'envoi des données au cloud à l'aide des clés générées et gérées par l'entreprise. Selon 37 % des répondants, le chiffrement est effectué dans le cloud à l'aide des clés générées/gérées par le fournisseur de cloud.

PARTIE 2. RÉSULTATS PRINCIPAUX

Cette section présente l'analyse des résultats principaux. L'audit complet des résultats est présenté dans l'annexe du présent rapport. Nous avons articulé le rapport autour des thèmes suivants :

- Stratégie, menaces et facteurs principaux
- Choix de déploiement
- Attitudes à propos de la gestion des clés Importance des modules de sécurité matérielle (HSM)
- Chiffrement du cloud

Stratégie, menaces et facteurs principaux

Les secteurs d'activité au sein de l'entreprise forment le facteur le plus influant sur l'orientation des stratégies de chiffrement. Comme le montre la Figure 2, les secteurs d'activité ou la Direction générale (41 % des répondants) sont les plus influents. Pour 26 % des répondants, les opérations informatiques sont responsables de la stratégie de chiffrement.

Quels sont les types de données les plus fréquemment chiffrés ? La Figure 3 répertorie sept types de données couramment chiffrés par les entreprises des répondants. Comme indiqué, la fréquence de chiffrement est la plus grande pour les données relatives aux paiements. Les données relatives à la santé sont les moins susceptibles d'être chiffrées.

Figure 2. Influence des opérations informatiques, des secteurs d'activité et des services de la sécurité

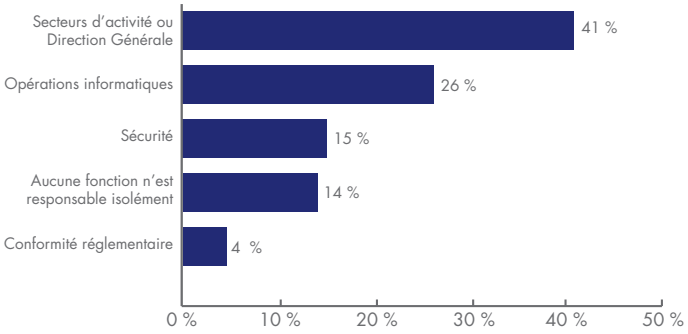
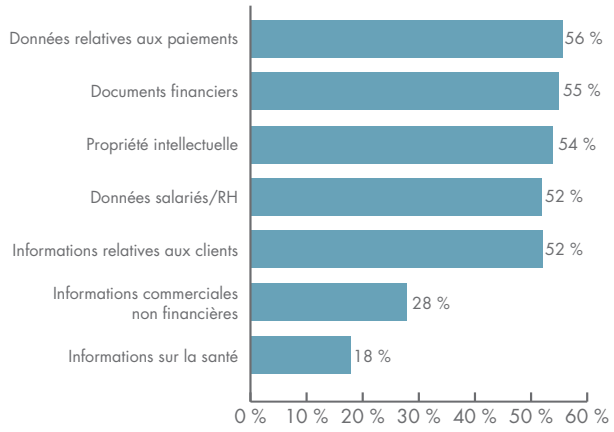
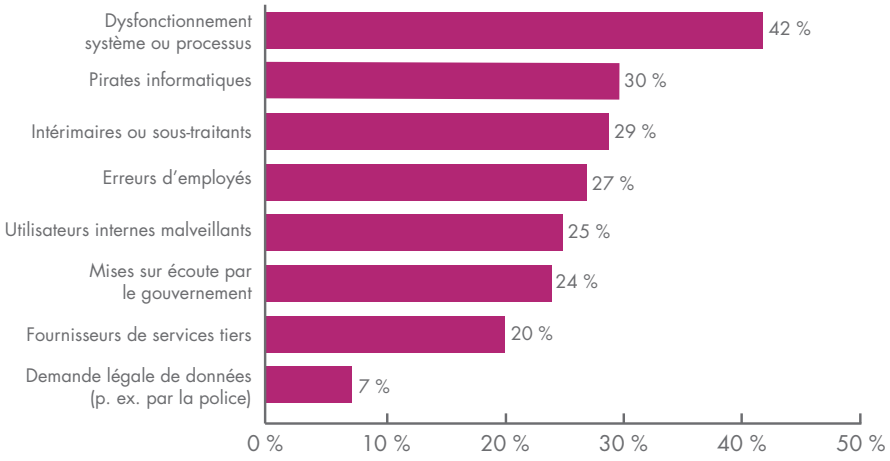


Figure 3. Types de données couramment chiffrés
Plusieurs réponses possibles



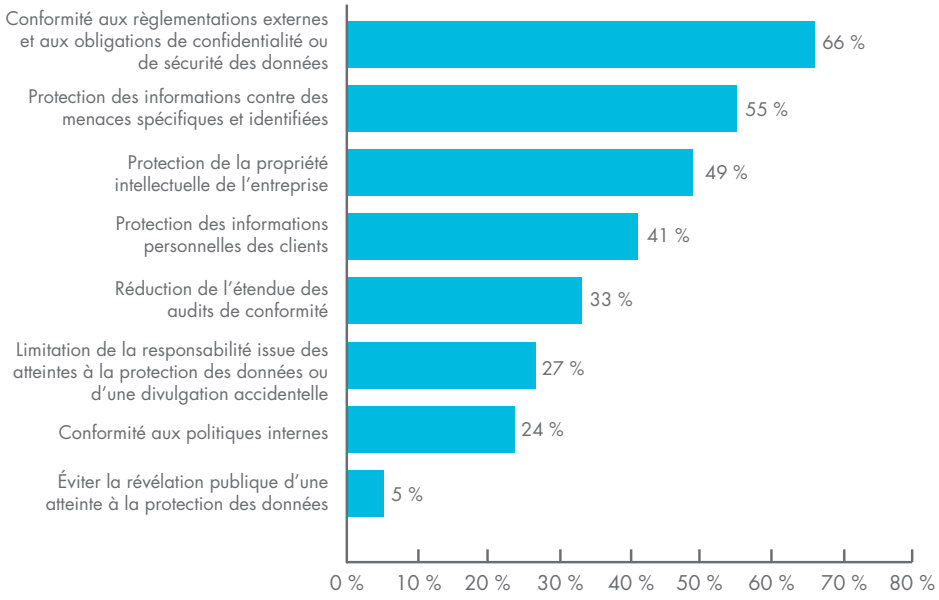
Les dysfonctionnements de système ou de processus constituent la menace la plus grande pour les données sensibles. La Figure 4 montre que les dysfonctionnements de système ou de processus constituent le plus grand risque d'exposition des données sensibles ou confidentielles, selon 42 % des répondants. Pour 30 % des répondants, les pirates informatiques sont une menace tandis que 29 % des répondants citent les intérimaires ou les sous-traitants. En revanche, les fournisseurs de services tiers et une demande légale de données (par la police, par exemple) sont considérés comme les moins menaçants (20 % et 7 %, respectivement).

Figure 4. Risques principaux d'exposition des données sensibles ou confidentielles
Deux réponses possibles



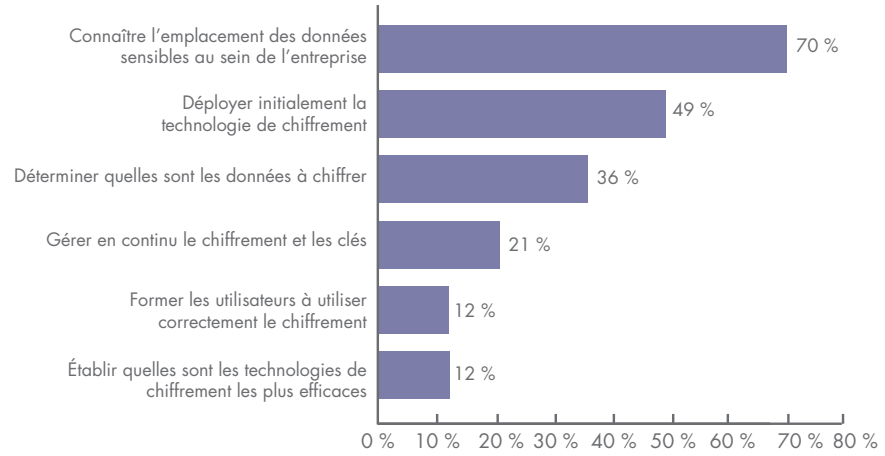
La conformité aux règlementations externes et aux obligations de confidentialité ou de sécurité des données constitue le facteur principal d'utilisation des technologies de chiffrement. La Figure 5 présente huit facteurs de déploiement du chiffrement. Soixante-six pour cent des répondants indiquent que la conformité aux règlementations externes et aux obligations de confidentialité ou de sécurité des données est le facteur principal d'incitation au chiffrement. Les autres raisons sont notamment la protection des informations contre des menaces spécifiques et identifiées ainsi que la protection de la propriété intellectuelle de l'entreprise (55 % et 49 % des répondants, respectivement).

Figure 5. Facteurs principaux incitant à utiliser des solutions technologiques de chiffrement
Trois réponses possibles



La difficulté majeure consiste à connaître l'emplacement des données sensibles au sein de l'entreprise. La Figure 6 établit par ordre décroissant d'importance les 6 difficultés rencontrées par une entreprise pour exécuter efficacement sa stratégie de chiffrement des données. Soixante-dix pour cent des répondants indiquent que la difficulté majeure consiste à connaître l'emplacement des données sensibles au sein de l'entreprise tandis que 49 % estiment que le déploiement initial de la technologie de chiffrement est l'un des principaux défis.

Figure 6. Difficultés majeures concernant la planification et l'exécution d'une stratégie de chiffrement des données
Deux réponses possibles

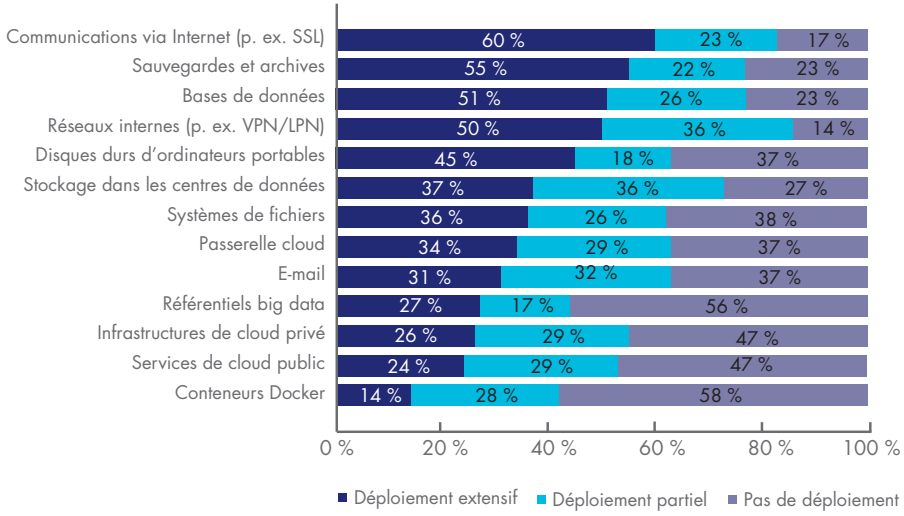


Choix de déploiement

Il n'existe pas de technologie de chiffrement dominante au sein des entreprises. Nous avons demandé aux répondants si des technologies de chiffrement précises étaient déployées largement ou seulement partiellement au sein de leurs entreprises. « Déploiement extensif » signifie que la technologie de chiffrement est appliquée dans l'ensemble de l'entreprise « Déploiement partiel » signifie que l'application de la technologie de chiffrement est confinée ou limitée à un objet précis (solution ponctuelle).

Comme le montre la Figure 7, il n'existe pas de technologie dominante parce que les entreprises ont une très grande diversité de besoins. Le déploiement extensif le plus probable concerne le chiffrement des communications via Internet (p. ex. SSL), des sauvegardes, des archives et des bases de données. En revanche, les services de cloud public et les conteneurs docker sont les moins susceptibles de faire l'objet d'un chiffrement extensif ou partiel.

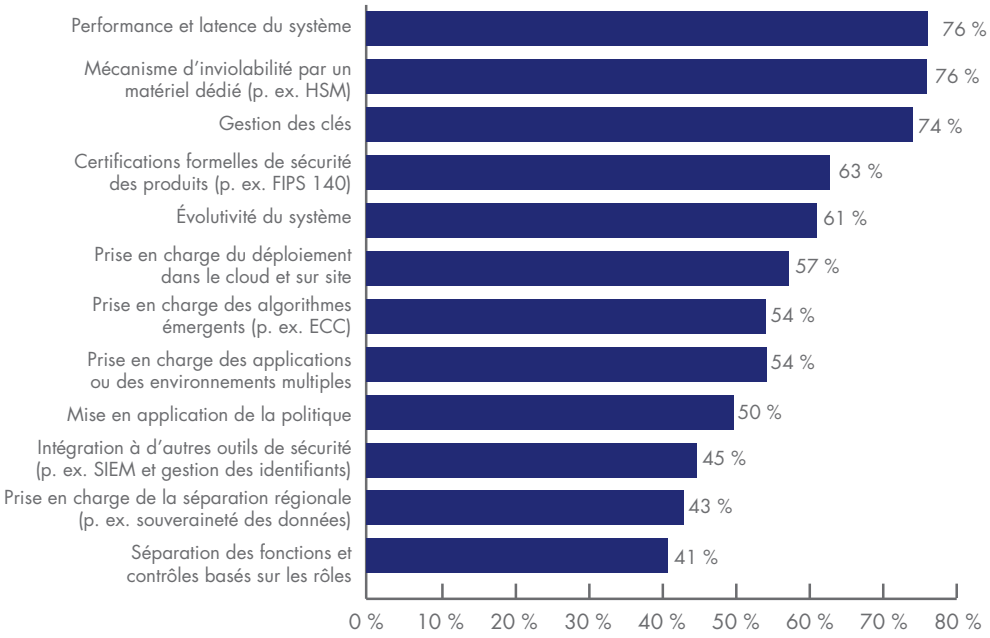
Figure 7. Le recours aux technologies de chiffrement



Certaines caractéristiques de chiffrement sont considérées comme étant plus importantes que d'autres. La Figure 8 répertorie 12 caractéristiques de la technologie de chiffrement. Chaque pourcentage représente la réponse « très importante » (sur une échelle de 4 points). Il a été demandé aux répondants d'évaluer quelles étaient les caractéristiques de la technologie de chiffrement qu'ils jugeaient les plus importantes pour la situation de sécurité de leur entreprise.

Selon les résultats, les caractéristiques les plus importantes sont la performance et la latence du système, le mécanisme d'inviolabilité par un matériel dédié (p. ex. HSM) et la gestion des clés. Les moins importantes sont l'assistance pour la séparation régionale (p. ex. souveraineté des données) et la séparation des fonctions et contrôles basés sur les rôles.

Figure 8. Caractéristiques les plus importantes des solutions technologiques de chiffrement
Combinaison des réponses Très importante et Importante



Attitudes à propos de la gestion des clés

Quel est le degré de pénibilité de la gestion des clés ? Les répondants ont été invités à utiliser une échelle de points pour évaluer la « pénibilité » globale associée à la gestion des clés au sein de leur entreprise, l'échelle allant de 1 = impact minime à 10 = impact sévère. La Figure 9 montre que 57 % (23 + 34) des répondants ont donné une note égale ou supérieure à 7, suggérant ainsi un degré de pénibilité plutôt élevé.

Figure 9. Quel est le degré de pénibilité de la gestion des clés ?
1 = impact minime ; 10 = impact sévère

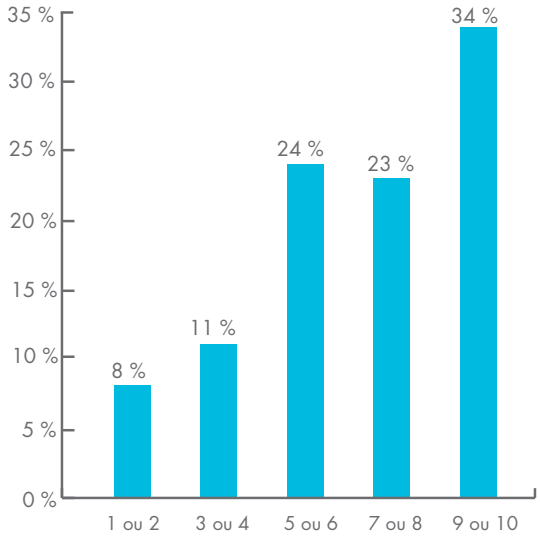
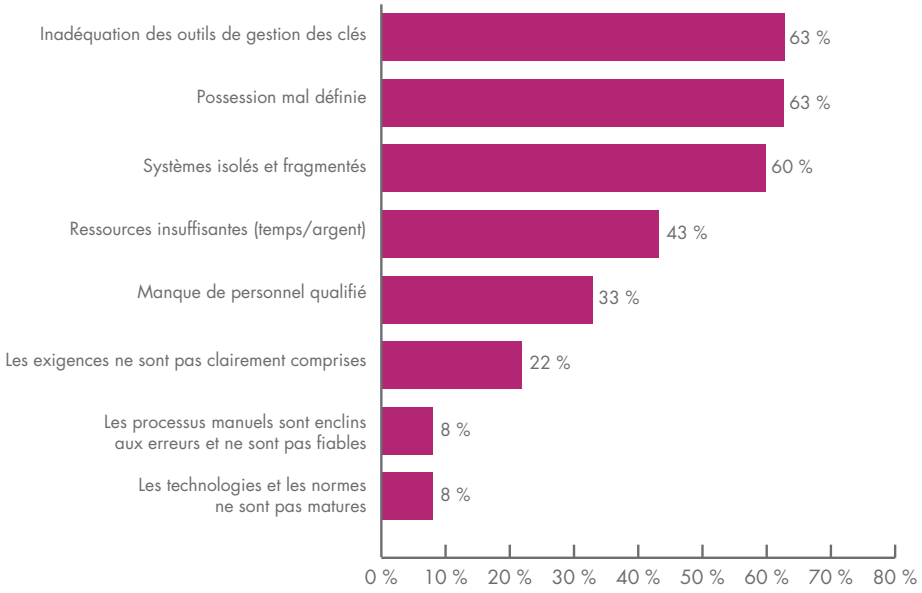


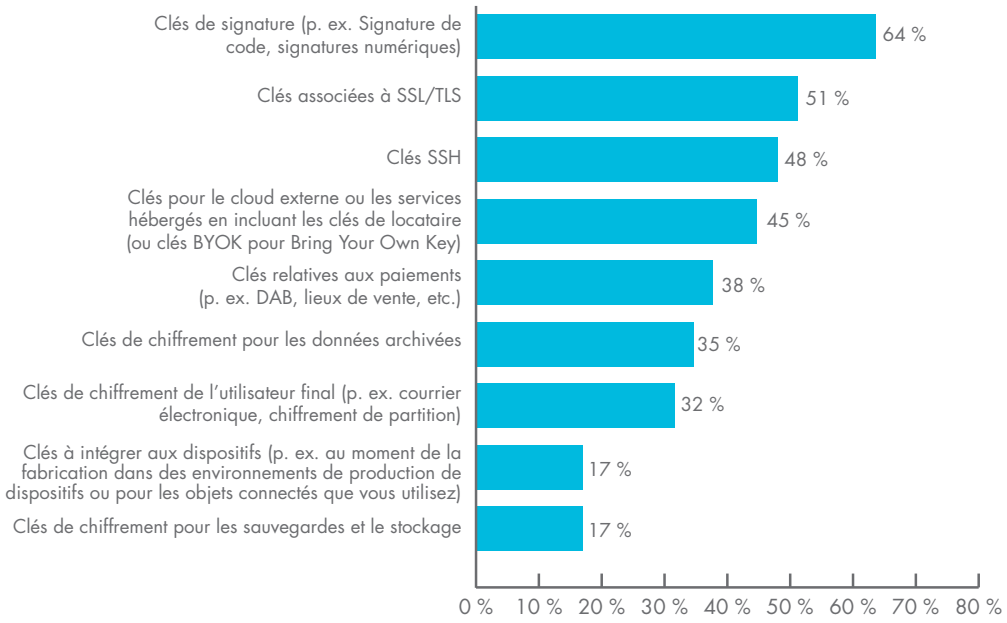
Figure 10. Qu'est-ce qui rend la gestion des clés si pénible ?
Trois réponses possibles



Pour quelles raisons la gestion des clés est-elle pénible ? La Figure 10 montre les raisons de la difficulté de la gestion des clés. Les raisons majeures sont l'inadéquation des outils de gestion des clés, la possession mal définie ainsi que l'isolation et la fragmentation des systèmes.

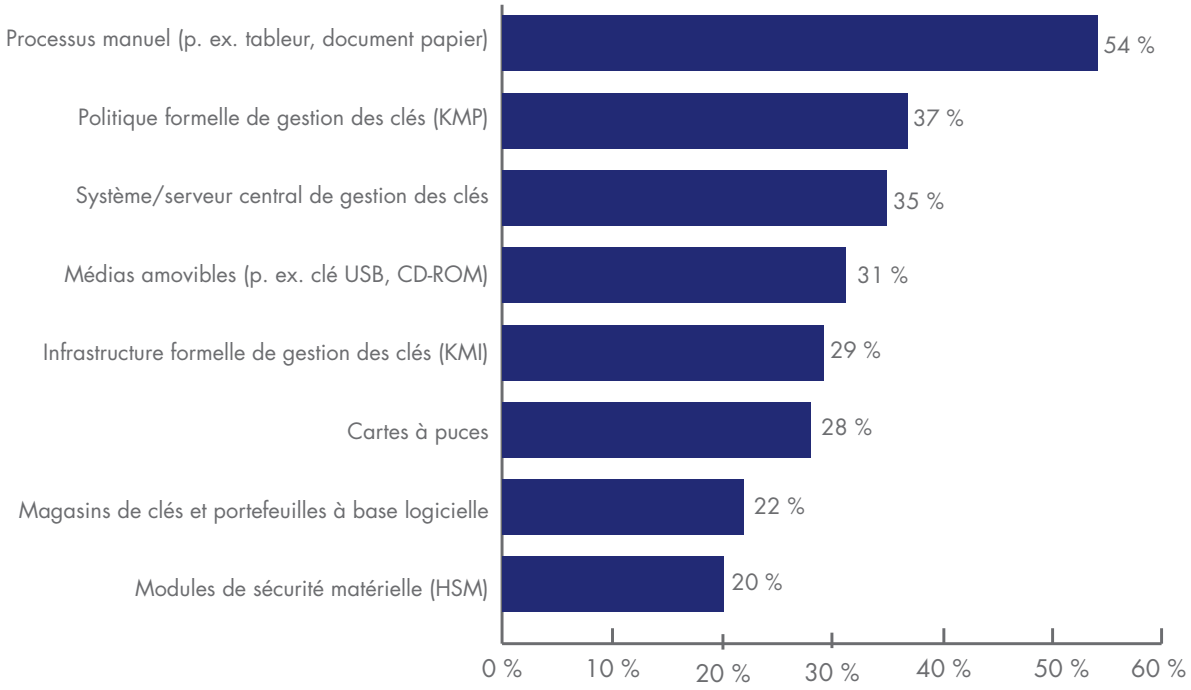
Quelles sont les clés les plus difficiles à gérer ? Selon la Figure 11, les clés considérées comme étant les plus difficiles à gérer sont les clés de signature (p. ex., signature de code, signatures numériques), les clés associées à SSL/TLS et les clés SSH.

Figure 11. Types des clés les plus difficiles à gérer
Combinaison des réponses Très pénible et Pénible



Comme le montre la Figure 12, les entreprises des répondants continuent d'utiliser un grand nombre de systèmes de gestion de clés. Les systèmes les plus couramment employés sont les suivants : processus manuel (p. ex. tableur, document papier), politique formelle de gestion des clés (KMP) et système/serveur central de gestion des clés.

Figure 12. Quels sont les systèmes de gestion des clés actuellement utilisés par votre entreprise ?
Plusieurs réponses possibles



LES CLÉS CONSIDÉRÉES COMME ÉTANT LES PLUS DIFFICILES À GÉRER SONT LES CLÉS DE SIGNATURE (P. EX., SIGNATURE DE CODE, SIGNATURES NUMÉRIQUES), LES CLÉS ASSOCIÉES À SSL/TLS ET LES CLÉS SSH.

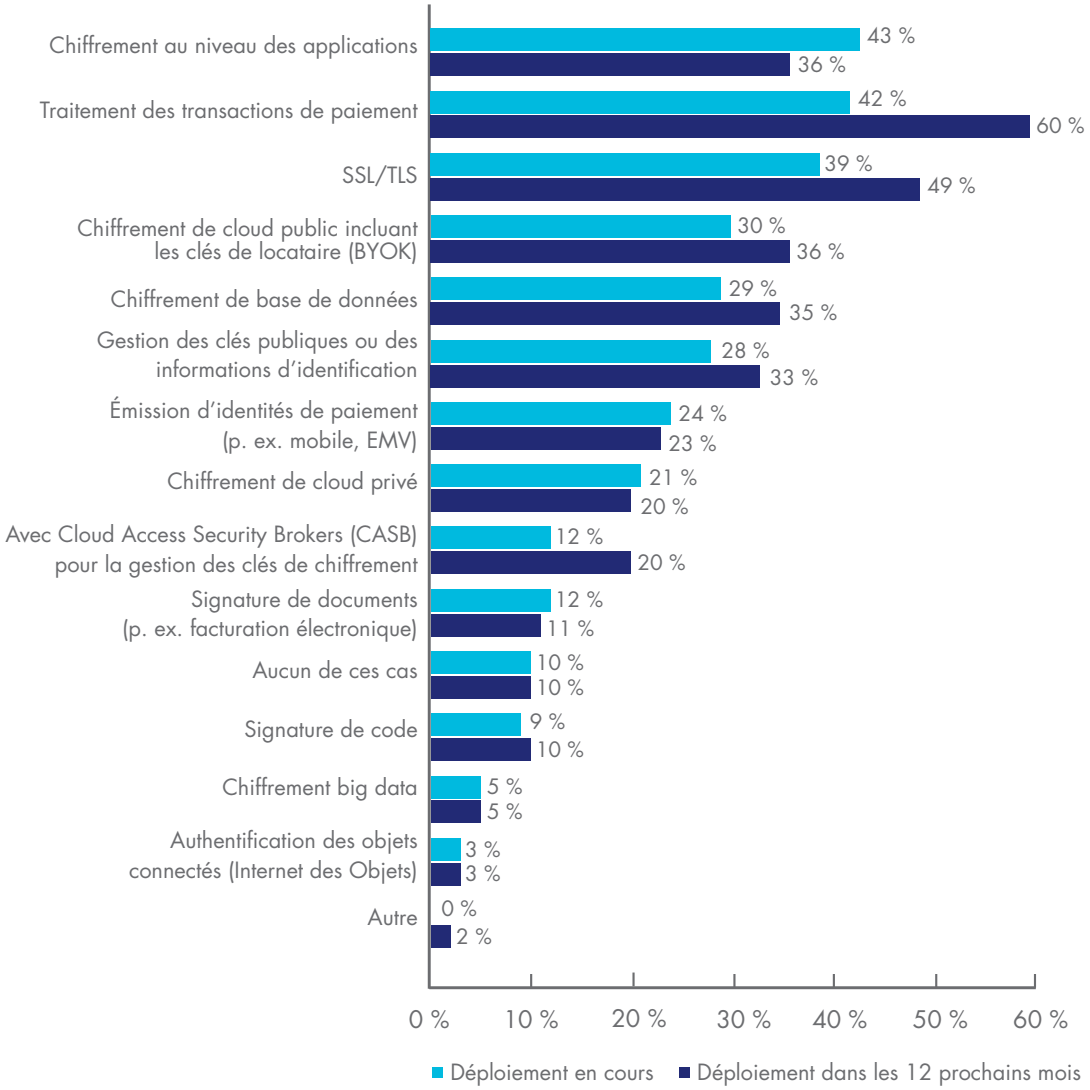
Importance des modules de sécurité matérielle (HSM)

Les modules de sécurité matérielle vont devenir plus importants pour la stratégie de chiffrement ou de gestion des clés au cours des 12 prochains mois. Nous avons demandé aux répondants dont l'entreprise déploie actuellement des modules de sécurité matérielle quelle était l'importance de ces modules dans la stratégie de chiffrement ou de gestion des clés. 51 % des répondants ont déclaré qu'ils étaient importants et 56 % ont dit qu'ils gagneront en importance au cours des 12 prochains mois.

La Figure 13 récapitule les objectifs ou cas d'utilisation principaux d'un déploiement de modules de sécurité matérielle. Comme le montre la figure, les trois raisons principales sont le chiffrement au niveau des applications, le traitement des transactions de paiement, SSL/TLS et le chiffrement du cloud public incluant les clés de locataire (BYOK). Au cours des 12 prochains mois, le traitement des transactions de paiement et SSL/TLS présenteront la plus grande croissance.

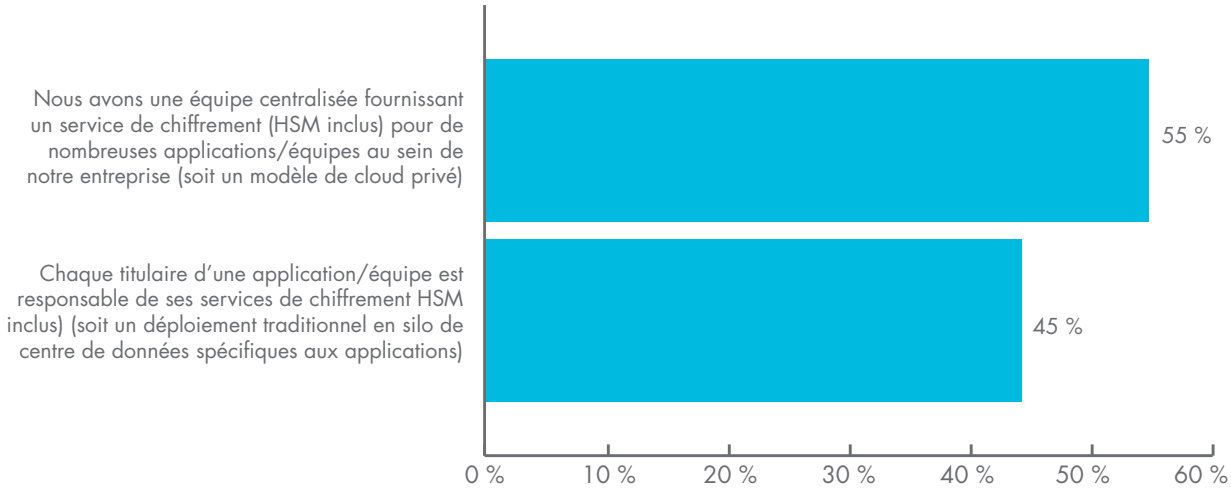
Figure 13. Comment les HSM sont-ils actuellement déployés ou seront déployés dans les 12 prochains mois

Plusieurs réponses possibles



Comment les entreprises utilisent-elles les HSM ? Selon la Figure 14, 55 % des répondants disent qu'ils ont une équipe centralisée fournissant un service de chiffrement et 45 % répondent que chaque titulaire d'une application/équipe est responsable de ses services de chiffrement.

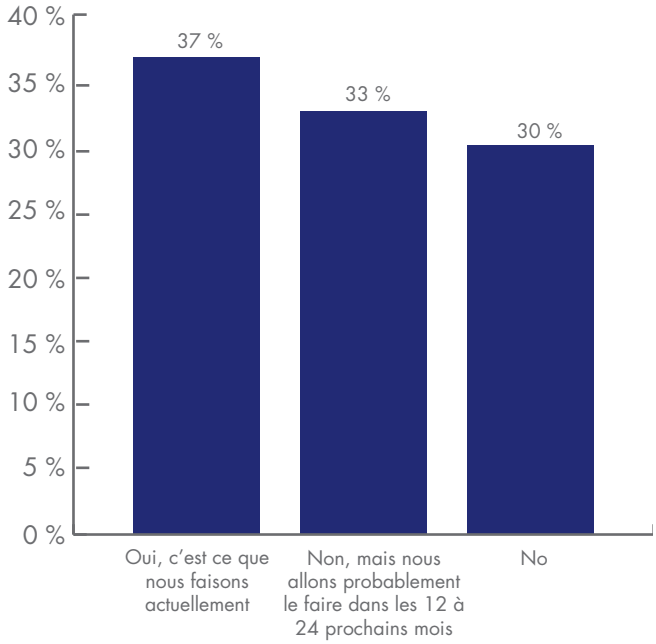
Figure 14. Quelle affirmation décrit le mieux l'utilisation des HSM au sein de votre entreprise ?



Chiffrement du cloud

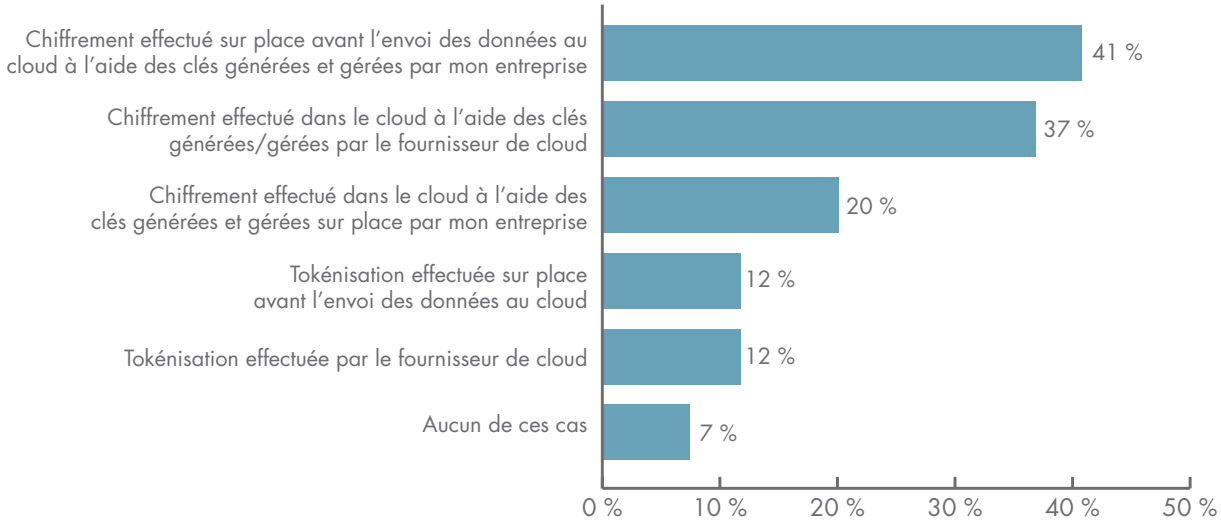
La plupart des entreprises transfèrent des données sensibles ou confidentielles vers le cloud. Comme le montre la Figure 15, 37 % des répondants indiquent que leurs entreprises transfèrent actuellement des données sensibles ou confidentielles vers le cloud (qu'elles soient chiffrées ou non ou rendues illisibles par un autre mécanisme) et 33 % des répondants déclarent que le transfert est prévu pour les 12 à 24 prochains mois.

Figure 15. Transférez-vous actuellement des données sensibles ou confidentielles vers le cloud ?



Comment les données au repos dans le cloud sont-elles protégées ? Comme le montre la Figure 16, 41 % des répondants disent que le chiffrement est effectué sur place avant l'envoi des données au cloud à l'aide de clés générées et gérées par l'entreprise. Selon 37 % des répondants, le chiffrement est effectué dans le cloud à l'aide des clés générées/gérées par le fournisseur de cloud.

Figure 16. Comment votre entreprise protège-t-elle les données au repos dans le cloud ?



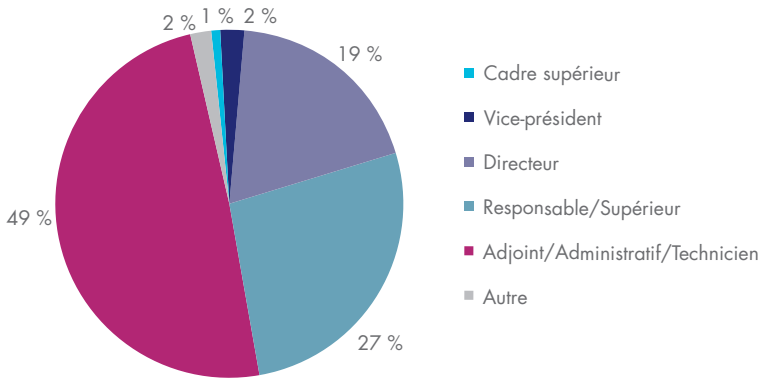
ANNEXE 1. MÉTHODES ET LIMITATIONS

Le Tableau 2 rapporte les éléments du taux de retour pour la France. Le taux de réponse pour cette étude a été établi après une période de sondage de 49 jours qui s'est terminée en février 2017. Notre base de sondage consolidée de professionnels en France englobait 12 756 personnes dont les compétences en matière d'informatique ou de sécurité étaient bien établies. Nous avons obtenu 413 retours de cette base de sondage, parmi lesquels 68 ont été rejetés pour des raisons de fiabilité. Notre échantillon final de 2017 pour la France comprenait 345 personnes, soit un taux de réponse global de 2,7 %.

Tableau 2. Taux de réponse au sondage	Fréq	%
Base de sondage totale	12 756	100 %
Total des retours	413	3,2 %
Sondages rejetés ou filtrés	68	0,5 %
Échantillon final	345	2,7 %

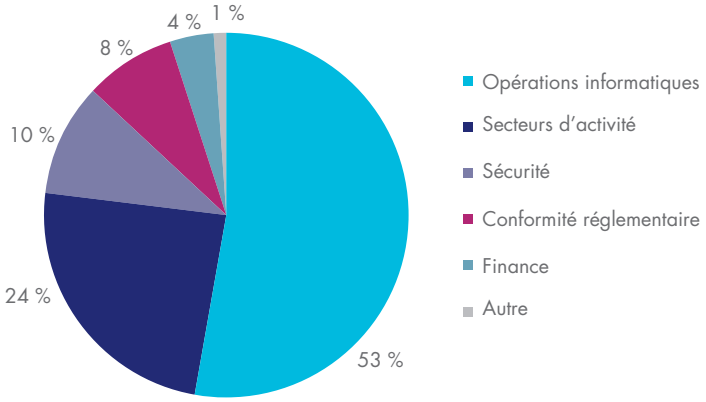
La Figure 17 synthétise les niveaux hiérarchiques approximatifs des répondants ayant participé à notre étude. Comme vous pouvez le voir, presque la moitié des répondants (49 %) occupe au moins un poste de supervision.

Figure 17. Distribution des répondants selon le niveau hiérarchique



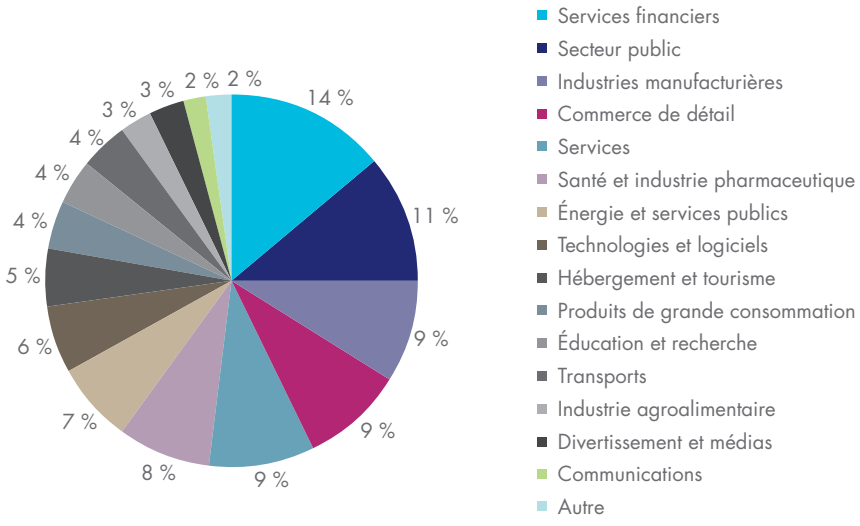
La Figure 18 indique les segments d'activité auxquels appartiennent les répondants. Comme le montre la figure, 14 % des répondants travaillent dans les services financiers (services bancaires, gestion des investissements, courtage, paiements et cartes de crédit). On compte 11 % travaillant dans le secteur public et 9 % actifs dans les industries manufacturières.

Figure 18. Distribution des répondants selon le domaine fonctionnel



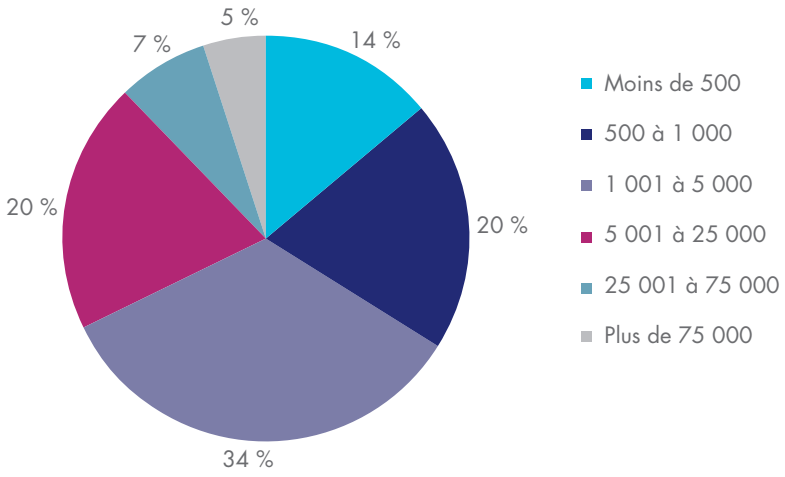
Selon la Figure 19, plus de la moitié des répondants (66 %) travaillent dans des entreprises de grande taille dont l'effectif à l'échelle mondiale est supérieur à 1 000 employés.

Figure 19. Distribution des répondants selon leur segment d'activité primaire



Selon la Figure 20, plus de la moitié des répondants (66 %) travaillent dans des entreprises de grande taille dont l'effectif à l'échelle mondiale est supérieur à 1 000 employés.

Figure 20. Distribution des répondants selon l'effectif total de l'entreprise



Limitations

Les limitations inhérentes à une étude par sondage doivent être soigneusement prises en compte avant de tirer des conclusions sur la base des résultats présentés ici. Les éléments suivants sont des limitations spécifiques que l'on retrouve dans la plupart des études de marché basées sur des sondages.

Biais de non-réponse : Les résultats actuels sont basés sur un échantillon de réponses à un sondage. Nous avons envoyé le sondage à un échantillon représentatif de professionnels de l'informatique et de la sécurité informatique en France, ce qui a nous a permis d'obtenir un grand nombre de retours exploitables. Malgré les tests de non-réponse, il est toujours possible que les personnes n'ayant pas participé présentaient des caractéristiques nettement différentes en termes d'opinions par rapport à ceux qui ont répondu au sondage.

Biais de la base de sondage : L'exactitude des résultats du sondage dépend du degré de représentativité des personnes constituant nos bases de sondage en France qui sont composées de professionnels de l'informatique ou de la sécurité informatique.

Résultats issus d'une auto-évaluation : La qualité d'une étude par sondage repose sur l'intégrité des réponses confidentielles fournies par les répondants. Même si certains poids et contrepoids ont été intégrés à notre processus d'évaluation du sondage, notamment des contrôles de bien-fondé, il reste toujours possible que certains répondants n'aient pas été honnêtes dans leurs réponses.

ANNEXE 2. TABLEAUX DES DONNÉES DU SONDAGE

Les tableaux suivants fournissent les résultats de l'échantillon concernant la France.

Réponse au sondage	FR
Base de sondage	12 756
Total des retours	413
Sondages rejetés ou filtrés	68
Échantillon final	345
Taux de réponse	2,7 %
Pondération de l'échantillon	7 %

Partie 1. Approche du chiffrement

Q1. Veuillez sélectionner l'affirmation qui décrit le mieux l'approche de votre entreprise en matière de mise en œuvre du chiffrement au sein de l'entreprise.	FR
Nous avons un plan ou une stratégie de chiffrement global que nous appliquons à tous les niveaux de l'entreprise	42 %
Nous avons un plan ou une stratégie de chiffrement limité que nous appliquons à certaines applications et certains types de données	39 %
Nous n'avons pas de plan ni de stratégie de chiffrement	19 %
Total	100 %

Q2. Ci-dessous sont répertoriés les domaines où il est possible de déployer des technologies de chiffrement. Veuillez indiquer quels domaines font l'objet d'un déploiement extensif, d'un déploiement partiel ou d'une absence actuelle de déploiement au sein de votre entreprise.

Q2a-1. Sauvegardes et archives	FR
Déploiement extensif	55 %
Déploiement partiel	22 %
Pas de déploiement	23 %
Total	100 %

Q2b-1. Référentiels big data	FR
Déploiement extensif	27 %
Déploiement partiel	17 %
Pas de déploiement	56 %
Total	100 %

Q2c-1. Passerelle cloud	FR
Déploiement extensif	34 %
Déploiement partiel	29 %
Pas de déploiement	37 %
Total	100 %

Q2d-1. Stockage dans les centres de données	FR
Déploiement extensif	37 %
Déploiement partiel	36 %
Pas de déploiement	27 %
Total	100 %

Q2e-1. Bases de données	FR
Déploiement extensif	51 %
Déploiement partiel	26 %
Pas de déploiement	23 %
Total	100 %

Q2f-1. Conteneurs Docker	FR
Déploiement extensif	14 %
Déploiement partiel	28 %
Pas de déploiement	58 %
Total	100 %

Q2g-1. Email	FR
Déploiement extensif	31 %
Déploiement partiel	32 %
Pas de déploiement	37 %
Total	100 %

Q2h-1. Services de cloud public	FR
Déploiement extensif	24 %
Déploiement partiel	29 %
Pas de déploiement	47 %
Total	100 %

Q2i-1. Systèmes de fichiers	FR
Déploiement extensif	36 %
Déploiement partiel	26 %
Pas de déploiement	38 %
Total	100 %

Q2j-1. Communications via Internet (p. ex. SSL)	FR
Déploiement extensif	60 %
Déploiement partiel	23 %
Pas de déploiement	17 %
Total	100 %

Q2k-1. Réseaux internes (p. ex. VPN/LPN)	FR
Déploiement extensif	50 %
Déploiement partiel	36 %
Pas de déploiement	14 %
Total	100 %

Q2l-1. Disques durs d'ordinateurs portables	FR
Déploiement extensif	45 %
Déploiement partiel	18 %
Pas de déploiement	37 %
Total	100 %

Q2m-1. Infrastructures de cloud privé	FR
Déploiement extensif	26 %
Déploiement partiel	29 %
Pas de déploiement	45 %
Total	100 %

Q3. Qui influe le plus sur l'orientation de la stratégie de chiffrement de votre entreprise ? Veuillez sélectionner la réponse la plus évidente.	FR
Opérations informatiques	26 %
Sécurité	15 %
Conformité réglementaire	4 %
Secteurs d'activité ou Direction Générale	41 %
Aucune fonction n'est responsable isolément	14 %
Total	100 %

Q4. Pour quelles raisons votre entreprise chiffre-t-elle les données sensibles et confidentielles ? Veuillez sélectionner les trois raisons principales.	FR
Protection de la propriété intellectuelle de l'entreprise	49 %
Protection des informations personnelles des clients	41 %
Limitation de la responsabilité issue des atteintes à la protection des données ou d'une divulgation accidentelle	27 %
Éviter la révélation publique d'une atteinte à la protection des données	5 %
Protection des informations contre des menaces spécifiques et identifiées	55 %
Conformité aux politiques internes	24 %
Conformité aux règlementations externes et aux obligations de confidentialité ou de sécurité des données	66 %
Réduction de l'étendue des audits de conformité	33 %
Total	300 %

Q5. Quelles sont les plus grandes difficultés rencontrées dans la planification et l'exécution d'une stratégie de chiffrement des données ? Veuillez sélectionner les deux raisons principales.	FR
Connaître l'emplacement des données sensibles au sein de l'entreprise	70 %
Déterminer quelles sont les données à chiffrer	36 %
Établir quelles sont les technologies de chiffrement les plus efficaces	12 %
Déployer initialement la technologie de chiffrement	49 %
Gérer en continu le chiffrement et les clés	21 %
Former les utilisateurs à utiliser correctement le chiffrement	12 %
Total	200 %

Q6. Quelle est l'importance de ces caractéristiques, associées aux solutions de chiffrement, et susceptibles d'être utilisées par votre entreprise ? Combinaison des réponses Très importante et Importante.	FR
Mise en application de la politique	50 %
Gestion des clés	74 %
Prise en charge des applications ou des environnements multiples	54 %
Séparation des fonctions et contrôles basés sur les rôles	41 %
Évolutivité du système	61 %
Mécanisme d'inviolabilité par un matériel dédié (p. ex. HSM)	76 %
Intégration à d'autres outils de sécurité (p. ex. SIEM et gestion des identifiants)	45 %
Prise en charge de la séparation régionale (p. ex. souveraineté des données)	43 %
Performance et latence du système	76 %
Prise en charge des algorithmes émergents (p. ex. ECC)	54 %
Prise en charge du déploiement dans le cloud et sur site	57 %
Certifications formelles de sécurité des produits (p. ex. FIPS 140)	63 %

Q7. Quels sont les types de données que chiffre votre entreprise ? Veuillez sélectionner toutes les réponses applicables.	FR
Informations relatives aux clients	52 %
Informations commerciales non financières	28 %
Propriété intellectuelle	54 %
Documents financiers	55 %
Données salariés/RH	52 %
Données relatives aux paiements	56 %
Informations sur la santé	18 %

Q8. Quelles sont les menaces principales qui pourraient entraîner l'exposition de données sensibles ou confidentielles ? Veuillez sélectionner les deux choix principaux.	FR
Pirates informatiques	30 %
Utilisateurs internes malveillants	25 %
Dysfonctionnement système ou processus	42 %
Erreurs d'employés	27 %
Intérimaires ou sous-traitants	29 %
Fournisseurs de services tiers	20 %
Demande légale de données (p. ex. par la police)	7 %
Mises sur écoute par le gouvernement	24 %
Total	204 %

Partie 2. Gestion des clés

Q9. Veuillez évaluer la « pénibilité » globale associée à la gestion des clés ou des certificats au sein de votre entreprise, sur une échelle allant de 1 = impact minime à 10 = impact sévère	FR
1 ou 2	8 %
3 ou 4	11 %
5 ou 6	24 %
7 ou 8	23 %
9 ou 10	34 %
Total	100 %

Q10. Qu'est-ce qui rend la gestion des clés si pénible ? Veuillez sélectionner les trois raisons principales.	FR
Possession mal définie	63 %
Ressources insuffisantes (temps/argent)	43 %
Manque de personnel qualifié	33 %
Les exigences ne sont pas clairement comprises	22 %
Inadéquation des outils de gestion des clés	63 %
Systèmes isolés et fragmentés	60 %
Les technologies et les normes ne sont pas matures	8 %
Les processus manuels sont enclins aux erreurs et ne sont pas fiables	8 %
Total	300 %

Q11. Vous trouverez ci-après une grande variété de clés pouvant être gérées par votre entreprise. Veuillez évaluer la « pénibilité » globale associée à la gestion de chaque type de clé. Combinaison des réponses Très pénible et Pénible.	FR
Clés de chiffrement pour les sauvegardes et le stockage	17 %
Clés de chiffrement pour les données archivées	35 %
Clés associées à SSL/TLS	51 %
Clés SSH	48 %
Clés de chiffrement de l'utilisateur final (p. ex. courrier électronique, chiffrement de partition)	32 %
Clés de signature (p. ex. signature de code, signatures numériques)	64 %
Clés relatives aux paiements (p. ex. DAB, lieux de vente, etc.)	38 %
Clés à intégrer aux dispositifs (p. ex. au moment de la fabrication dans des environnements de production de dispositifs ou pour les objets connectés que vous utilisez)	17 %
Clés pour le cloud externe ou les services hébergés en incluant les clés de locataire (ou clés BYOK pour Bring Your Own Key)	45 %

Q12a. Quels sont les systèmes de gestion des clés actuellement utilisés par votre entreprise ?	FR
Politique formelle de gestion des clés (KMP)	37 %
Infrastructure formelle de gestion des clés (KMI)	29 %
Processus manuel (p. ex. tableur, document papier)	54 %
Système/serveur central de gestion des clés	35 %
Modules de sécurité matérielle (HSM)	20 %
Médias amovibles (p. ex. clé USB, CD-ROM)	31 %
Magasins de clés et portefeuilles à base logicielle	22 %
Cartes à puces	28 %
Total	256 %

Q12b. Quels sont les systèmes de gestion de clés que votre entreprise n'utilise pas ou ne connaît pas ?	FR
Politique formelle de gestion des clés (KMP)	62 %
Infrastructure formelle de gestion des clés (KMI)	71 %
Processus manuel (p. ex. tableur, document papier)	45 %
Système/serveur central de gestion des clés	61 %
Modules de sécurité matérielle (HSM)	80 %
Médias amovibles (p. ex. clé USB, CD-ROM)	68 %
Magasins de clés et portefeuilles à base logicielle	77 %
Cartes à puces	73 %
Total	537 %

Partie 3. Modules de sécurité matérielle (HSM)

Q13. Quelle réponse décrit le mieux votre degré de connaissance des modules de sécurité matérielle ?	FR
Très bonne connaissance	23 %
Bonne connaissance	31 %
Assez bonne connaissance	12 %
Aucune connaissance (passer à Q17a)	34 %
Total	100 %

Q14a. Est-ce que votre entreprise utilise des modules de sécurité matérielle (HSM) ?	FR
Oui	30 %
No (passer à Q17a)	70 %
Total	100 %

Q14b. Pour quelles raisons votre entreprise déploie-t-elle actuellement des modules de sécurité matérielle ou prévoit-elle d'en utiliser ? Veuillez sélectionner toutes les réponses applicables.

Q14b-1. Modules HSM utilisés aujourd'hui	FR
Chiffrement au niveau des applications	43 %
Chiffrement de base de données	29 %
Chiffrement big data	5 %
Chiffrement de cloud public incluant les clés de locataire (BYOK)	30 %
Chiffrement de cloud privé	21 %
SSL/TLS	39 %
Gestion des clés publiques ou des informations d'identification	28 %
Authentification des objets connectés (Internet des Objets)	3 %
Signature de documents (p. ex. facturation électronique)	12 %
Signature de code	9 %
Traitement des transactions de paiement	42 %
Émission d'identités de paiement (p. ex. mobile, EMV)	24 %
Avec Cloud Access Security Brokers (CASB) pour la gestion des clés de chiffrement	12 %
Aucun de ces cas	10 %
Autre	0 %
Total	307 %

Q14b-2. Déploiement de HSM prévu pour les 12 prochains mois	FR
Chiffrement au niveau des applications	36 %
Chiffrement de base de données	35 %
Chiffrement big data	5 %
Chiffrement de cloud public incluant les clés de locataire (BYOK)	36 %
Chiffrement de cloud privé	20 %
SSL/TLS	49 %
Gestion des clés publiques ou des informations d'identification	33 %
Authentification des objets connectés (Internet des Objets)	3 %
Signature de documents (p. ex. facturation électronique)	11 %
Signature de code	10 %
Traitement des transactions de paiement	60 %
Émission d'identités de paiement (p. ex. mobile, EMV)	23 %
Avec Cloud Access Security Brokers (CASB) pour la gestion des clés de chiffrement	20 %
Aucun de ces cas	10 %
Autre	2 %
Total	353 %

Q14c-1. Si vous utilisez des HSM conjointement avec des applications basées sur le cloud public, quels modèles utilisez-vous actuellement ? Veuillez sélectionner toutes les réponses applicables.	FR
Location/utilisation de HSM provenant du fournisseur de cloud public, hébergés dans le cloud	32 %
Possession et exploitation de HSM sur place au sein de votre entreprise, avec accès en temps réel par des applications hébergées sur le cloud Possession et exploitation de HSM dans le but de générer et de gérer des clés	56 %
BYOK (Bring Your Own Key) à envoyer au cloud pour utilisation par le fournisseur de cloud	18 %
Possession et exploitation de HSM qui intègrent un CASB (Cloud Access Security Broker) pour gérer les clés et les opérations de chiffrement (p. ex., chiffrement de données en voie de transfert vers le cloud, gestion de clés pour les applications du cloud)	11 %
Aucun de ces cas	3 %
Total	120 %

Q14c-2. Si vous utilisez des HSM conjointement avec des applications basées sur le cloud public, quels sont les modèles que vous prévoyez d'utiliser au cours des 12 prochains mois ? Veuillez sélectionner toutes les réponses applicables.	FR
Location/utilisation de HSM provenant du fournisseur de cloud public, hébergés dans le cloud	36 %
Possession et exploitation de HSM sur place au sein de votre entreprise, avec accès en temps réel par des applications hébergées sur le cloud	66 %
Possession et exploitation de HSM dans le but de générer et de gérer des clés BYOK (Bring Your Own Key) à envoyer au cloud pour utilisation par le fournisseur de cloud	19 %
Possession et exploitation de HSM qui intègrent un CASB (Cloud Access Security Broker) pour gérer les clés et les opérations de chiffrement (p. ex., chiffrement de données en voie de transfert vers le cloud, gestion de clés pour les applications du cloud)	24 %
Aucun de ces cas	2 %
Total	147 %

Q15. Selon vous, quelle est l'importance des HSM dans votre stratégie de chiffrement ou de gestion des clés ? Combinaison des réponses Très importante et Importante	FR
Q15a. Importance aujourd'hui	51 %
Q15b. Importance au cours des 12 prochains mois	56 %

Q16. Quelle affirmation décrit le mieux l'utilisation des HSM au sein de votre entreprise ?	FR
Nous avons une équipe centralisée fournissant un service de chiffrement (HSM inclus) pour de nombreuses applications/équipes au sein de notre entreprise (soit un modèle de cloud privé).	55 %
Chaque titulaire d'une application/équipe est responsable de ses services de chiffrement (HSM inclus) (soit un déploiement traditionnel en silo de centre de données spécifiques aux applications).	45 %
Total	100 %

Partie 4. Questions sur le budget

Q17a. Êtes-vous responsable de la gestion de la totalité/d'une partie du budget informatique de votre entreprise cette année ?	FR
Oui	49 %
Non (passer à Q18)	51 %
Total	100 %

	FR
Q17b. Quel est le pourcentage approximatif du budget informatique de 2017 qui sera dévolu aux activités de sécurité informatique ?	8,9 %

	FR
Q17c. Quel est le pourcentage approximatif du budget de sécurité informatique de 2017 qui sera dévolu aux activités de chiffrement ?	12,4 %

Partie 6 : Chiffrement du cloud : Pour chaque réponse aux questions suivantes, partez du principe qu'elles concernent uniquement les services de cloud public.

Q35a. Est-ce que votre entreprise utilise actuellement les services d'informatique dématérialisée (cloud) pour un type quelconque de données ou d'applications – à la fois sensibles et non sensibles ?	**FR**
Oui, c'est ce que nous faisons actuellement	59 %
Non, mais nous allons probablement le faire dans les 12 à 24 prochains mois	23 %
Non (passer à la Partie 7 si vous n'utilisez pas de services de cloud pour aucun type de données ou d'application)	18 %
Total	100 %

Q35b. Transférez-vous actuellement des données sensibles ou confidentielles vers le cloud (qu'elles soient chiffrées ou non ou rendues illisibles par un autre mécanisme) ?	**FR**
Oui, c'est ce que nous faisons actuellement	37 %
Non, mais nous allons probablement le faire dans les 12 à 24 prochains mois	33 %
Non (passer à la Partie 7 si vous n'utilisez pas ou ne prévoyez pas d'utiliser des services de cloud pour les données sensibles ou confidentielles)	30 %
Total	100 %

Q35c. Selon vous, qui est le responsable principal de la protection des données sensibles ou confidentielles qui sont transférées vers le cloud ?	**FR**
Le fournisseur du cloud	49 %
L'utilisateur du cloud	21 %
Responsabilité partagée	30 %
Total	100 %

Q35d. Comment votre entreprise protège-t-elle les données au repos dans le cloud ?	FR
Chiffrement effectué dans le cloud à l'aide des clés générées/gérées par le fournisseur de cloud	37 %
Chiffrement effectué dans le cloud à l'aide des clés générées et gérées sur place par mon entreprise	20 %
Chiffrement effectué sur place avant l'envoi des données au cloud à l'aide des clés générées et gérées par mon entreprise	41 %
Tokénisation effectuée par le fournisseur de cloud	12 %
Tokénisation effectuée sur place avant l'envoi des données au cloud	12 %
Aucun de ces cas	7 %
Total	129 %

Q35e. Pour le chiffrement des données au repos dans le cloud, la stratégie de mon entreprise consiste à . . .	FR
Utiliser uniquement les clés contrôlées par mon entreprise	52 %
Utiliser uniquement les clés contrôlées par le fournisseur du cloud	26 %
Utiliser une combinaison de clés contrôlées par mon entreprise et le fournisseur du cloud, en ayant une préférence pour les clés contrôlées par mon entreprise	12 %
Utiliser une combinaison de clés contrôlées par mon entreprise et le fournisseur du cloud, en ayant une préférence pour les clés contrôlées par le fournisseur du cloud	10 %
Total	100 %

Q35f. Utilisez-vous actuellement ou prévoyez-vous d'utiliser les applications SaaS suivantes pour le chiffrement (sélectionnez toutes les réponses applicables) ?	FR
Microsoft Office 365	56 %
Salesforce.com	33 %
Box	30 %
Concur	6 %
Workday	3 %
Google Apps	37 %
ServiceNow	12 %
DocuSign	13 %
ZenDesk	12 %
Autre	6 %
Total	208 %

Partie 7 : Fonctions et caractéristiques organisationnelles

D1. Quel niveau organisationnel décrit le mieux le poste que vous occupez actuellement ?	FR
Cadre supérieur	1 %
Vice-président	2 %
Directeur	19 %
Responsable/Superviseur	27 %
Adjoint/Administratif/Technicien	49 %
Autre	2 %
Total	100 %

D2. Sélectionnez le domaine fonctionnel décrivant le mieux votre emplacement organisationnel.	FR
Opérations informatiques	53 %
Sécurité	10 %
Conformité réglementaire	8 %
Finance	4 %
Secteurs d'activité	24 %
Autre	1 %
Total	100 %

D3. Quelle industrie décrit le mieux le cœur de métier de votre entreprise ?	FR
Industrie agroalimentaire	3 %
Communications	2 %
Produits de grande consommation	4 %
Défense et aéronautique	1 %
Éducation et recherche	4 %
Énergie et services publics	7 %
Divertissement et médias	3 %
Services financiers	14 %
Santé et industrie pharmaceutique	8 %
Hébergement et tourisme	5 %
Industries manufacturières	9 %
Secteur public	11 %
Commerce de détail	9 %
Services	9 %
Technologies et logiciels	6 %
Transports	4 %
Autre	1 %
Total	100 %

D4. Quel est le nombre de personnes employées par votre entreprise à l'échelle mondiale ?	FR
Moins de 500	14 %
500 à 1 000	20 %
1 001 à 5 000	34 %
5 001 à 25 000	20 %
25 001 à 75 000	7 %
Plus de 75 000	5 %
Total	100 %

À propos de Ponemon Institute

Le Ponemon Institute© a pour mission de faire progresser les pratiques de traitement responsable des informations et de gestion de leur confidentialité au sein des entreprises et des administrations publiques. Pour atteindre cet objectif, l'Institut mène des études indépendantes, forme les dirigeants des secteurs public et privé et vérifie les pratiques de confidentialité et de protection des données des entreprises dans divers secteurs d'activité.

À propos de Thales e-Security

Thales e-Security est l'un des principaux fournisseurs mondiaux de solutions de gestion de confiance numérique et de protection des données sécurisant les données et les applications les plus sensibles. Les produits Thales répondent aux enjeux liés à l'identité et à la protection de la vie privée à l'aide de technologies logicielles et matérielles de cryptage, de signature numérique et de gestion. Dans un monde de plus en plus connecté, nos solutions permettent de contrecarrer les attaques ciblées et de réduire le risque d'exposition des données sensibles introduit par le cloud computing et la virtualisation, l'utilisation des outils de communication du commerce sur le lieu de travail, la mobilité accrue ou encore les big data. www.thales-esecurity.com

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 61 000 collaborateurs dans 56 pays, Thales a réalisé en 2014 un chiffre d'affaires de 13 milliards d'euros. Avec plus de 20 000 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 du Groupe 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.

THALES

www.thalesesecurity.com

©2017 Thales