THALES

Ponemon INSTITUTE

ÉTUDE SUR LES TENDANCES EN MATIÈRE DE CHIFFREMENT EN FRANCE

Septembre 2018

SOMMAIRE

Sponsorisé par Thales eSecurity

MENÉ DE MANIÈRE INDÉPENDANTE PAR PONEMON INSTITUTE LLC

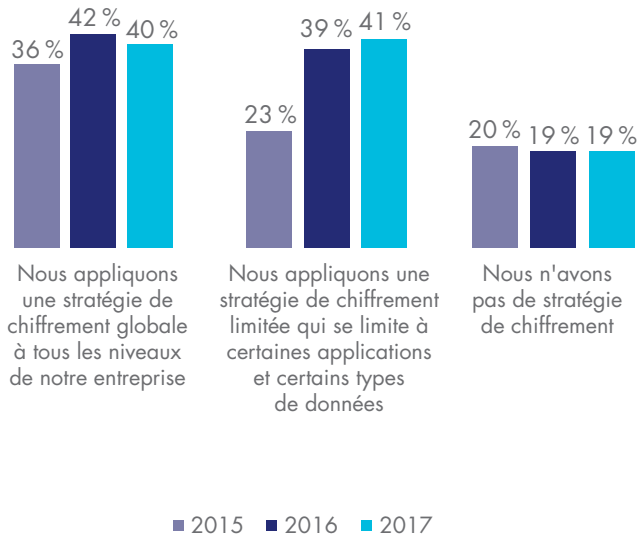
PREMIÈRE PARTIE. SYNTHÈSE

Ponemon Institute a l'honneur de présenter les résultats de l'*Étude sur les tendances en matière de chiffrement pour la France pour 2018*, sponsorisée par Thales eSecurity. Nous avons interrogé 370 professionnels de la sécurité informatique en France pour étudier l'utilisation du chiffrement et l'impact de cette technologie sur la posture de sécurité des enterprises de cette région.

La première étude sur les tendances en matière de chiffrement a été menée en 2005 sur un échantillon de professionnels de la sécurité informatique américains. Depuis, nous avons étendu la portée de la recherche pour inclure des professionnels de 12 pays dont la France. L'Australie, le Brésil, la France, l'Allemagne, l'Inde, le Japon, le Mexique, le Moyen-Orient, la Fédération de Russie, la Corée du Sud, le Royaume-Uni et les États-Unis figurent parmi les pays concernés.[1]

Comme indiqué figure 1, de plus en plus d'enterprises représentées dans cette étude reconnaissent l'importance d'avoir une stratégie de chiffrement, qu'elle soit globale au niveau de l'entreprise (40 % des sondés) ou limitée, dans le but de cibler certains types d'application et de données (41 % des sondés).

Figure 1. Quelle description s'applique le mieux à la stratégie de chiffrement de votre enterprise ?



Vous trouverez ci-dessous un récapitulatif des résultats clés. Plus d'informations sont disponibles dans la section suivante de ce rapport pour chaque résultat clé indiqué ci-dessous.

Les processus informatiques gagnent en influence dans la mise en application des stratégies de chiffrement. La responsabilité de la stratégie de chiffrement est répartie dans l'ensemble de l'enterprise, mais l'influence des opérations informatiques a augmenté de 26 % chez les individus sondés l'année dernière à 38 % pour les sondés de l'étude de cette année. À l'inverse, l'influence des secteurs d'activité a baissé de 41 % à 25 %.

Quels types de données sont les plus susceptibles d'être chiffrés ? La plupart des entreprises chiffrent en priorité les données relatives au paiement, à la propriété intellectuelle, aux registres financiers, aux RH/sur les employés, aux clients et à la santé. Peu d'entreprises chiffrent les informations commerciales non financières.

Un dysfonctionnement du système ou d'un processus représente la menace principale de divulgation de données sensibles ou confidentielles. D'après 42 % des sondés, les dysfonctionnements du système ou d'un processus représentent le risque principal de divulgation de données sensibles ou confidentielles. Pour 30 % des sondés, les hackers représentent la menace la plus importante, tandis que 29 % des sondés estiment que la menace porte plus sur les travailleurs temporaires ou contractuels.

La conformité aux règles relatives à la sécurité des données et à la confidentialité est le facteur principal d'utilisation des technologies de chiffrement. D'après 59 % des sondés, l'importance de la conformité aux exigences et aux règles relatives à la sécurité des données et à la confidentialité externes reste le facteur principal. 51 % et 46 % des sondés affirment que la protection des informations contre des menaces spécifiques et la protection de la propriété intellectuelle de l'entreprise sont des facteurs importants.

[1] Le Moyen-Orient inclut les Émirats Arabes Unis et l'Arabie Saoudite.

Localiser les données sensibles dans l'enterprise reste l'un des défis les plus importants. Pour 70 % des sondés, localiser les données sensibles dans l'enterprise est le défi le plus important à relever pour la planification et l'exécution d'une stratégie de chiffrement des données. Le deuxième défi le plus important (indiqué par 50 % des sondés) est le déploiement initial de la technologie de chiffrement.

Aucune technologie de chiffrement spécifique ne domine, car les enterprises ont des besoins très variés. Le chiffrement des disques durs des portables, des communications numériques et des sauvegardes et archives sont les fonctionnalités le plus souvent déployées de manière globale. À l'inverse, le chiffrement des plateformes et appareils liés à l'Internet des objets (IoT) reste minoritaire mais en croissance, tandis que les conteneurs Docker sont moins souvent chiffrés.

Certains aspects de la sécurité sont considérés comme plus importants que d'autres. Au cours des trois dernières années, les fonctionnalités suivantes ont énormément gagné en importance : la résistance au sabotage grâce à du matériel dédié, les certificats de sécurité, les performances du système et la latence, le support du déploiement sur site et dans le cloud, la possibilité d'évolution du système et le support d'applications et d'environnements multiples. Une fonctionnalité dont l'importance a baissé mais qui reste néanmoins importante pour 50 % des sondés est la mise en application de la politique de sécurité de l'entreprise.

À quel point la gestion de clé est-elle difficile ? 60 % des sondés affirment que la gestion de clé est difficile. Les raisons principales de ces difficultés sont les suivantes : il n'y a pas de responsabilité claire, les systèmes sont isolés et fragmentés et les outils de gestion de clé sont inadéquats. Les entreprises des sondés continuent à utiliser divers systèmes de gestion de clé. Les systèmes déployés sont le plus souvent des processus manuels (par ex. feuille de calcul, système papier) et des politiques formelles de gestion de clés (KMP).

Quelles clés sont les plus difficiles à gérer ? Le niveau de difficulté de la gestion des clés SSH a drastiquement augmenté depuis l'année dernière. La difficulté de gestion des clés suivantes a légèrement diminué : clés de signature (par ex. signature du code, signatures numériques), clés de cloud externe ou de services hébergés, dont Bring Your Own Key (BYOK) et les clés de chiffrement de l'utilisateur final.

L'importance des modules de sécurité matériel (HSM) pour la stratégie du chiffrement ou de gestion de clé va croître au cours des 12 prochains mois. Nous avons demandé aux sondés dont les enterprises déploient actuellement des HSM de nous indiquer leur importance pour la stratégie de chiffrement ou de gestion de clé. 53 % des sondés indiquent qu'ils sont importants aujourd'hui, et 63 % estiment qu'ils seront importants au cours des 12 prochains mois. Le traitement des transactions, le chiffrement de la base de données et les Cloud Access Security Brokers (CASB) sont des cas d'utilisation qui devraient devenir plus fréquents au cours des 12 prochains mois. Le chiffrement au niveau de l'application et la fourniture des données de paiement sont des cas dont la fréquence devrait diminuer.

Comment les enterprises utilisent les HSMs. 63 % des sondés en France indiquent qu'ils ont une équipe centralisée de cryptographie. La moyenne mondiale est de 61 %. 31 % des sondés affirment que chaque équipe/propriétaire d'application individuelle est responsable de ses propres services cryptographiques.

La plupart des enterprises transfèrent les données sensibles ou confidentielles dans le cloud. 58 % des sondés affirment que leurs enterprises transfèrent actuellement les données sensibles ou confidentielles dans le cloud (qu'elles soient chiffrées ou rendues illisibles d'une manière ou d'une autre) et 20 % des sondés se préparent à le faire au cours des 12 à 24 mois prochains. 50 % des sondés affirment que le fournisseur du cloud est le principal responsable de la protection des données confidentielles ou sensibles transférées sur le cloud.

Comment les données stockées dans le cloud sont-elles protégées ? 44 % des sondés affirment que le chiffrement est effectué sur site avant d'envoyer les données dans le cloud à l'aide de clés générées et gérées par l'enterprise et 40 % des sondés affirment que le chiffrement est effectué dans le cloud à l'aide de clés générées et gérées par le fournisseur du cloud.

40 %

des entreprises disposent désormais d'une **stratégie de chiffrement** cohérente à l'échelle de l'entreprise

DEUXIÈME PARTIE. RÉSULTATS CLÉS

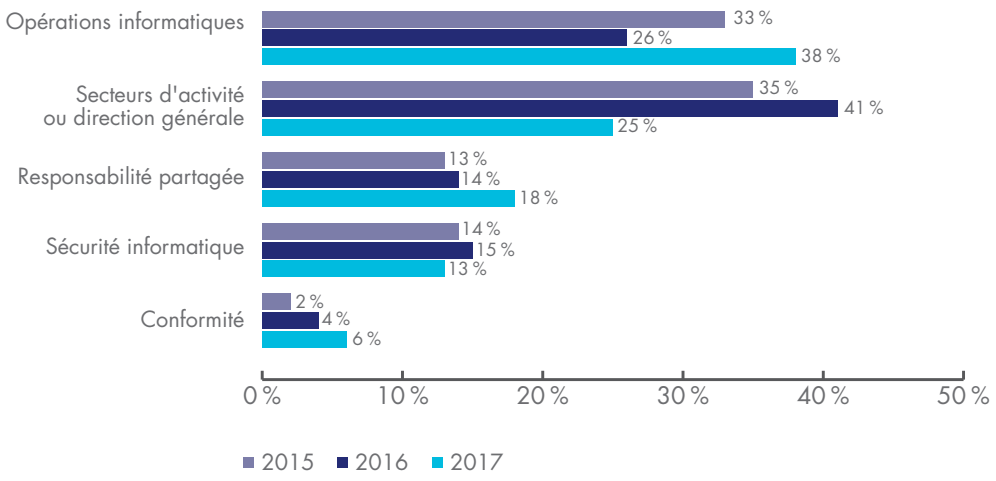
Dans cette section, nous présentons une analyse des résultats clés. Les résultats complets vérifiés sont présentés dans l'annexe de ce rapport. Nous avons organisé le rapport selon les thèmes suivants :

- Stratégie et adoption du chiffrement
- Menaces, priorités et facteurs principaux
- Choix de déploiement
- Fonctionnalités du chiffrement considérées comme les plus importantes
- Attitudes relatives à la gestion de clé
- Importance des modules de sécurité matériel (HSM)[2]
- Chiffrement du cloud

Stratégie et adoption du chiffrement

Les opérations informatiques gagnent en influence dans la mise en application des stratégies de chiffrement. Comme indiqué à la figure 2, si la responsabilité de la stratégie de chiffrement est répartie dans l'ensemble de l'enterprise, l'influence des opérations informatiques a augmenté de 26 % (sondage de l'année dernière) à 38 % dans l'étude de cette année. À l'inverse, l'influence des secteurs d'activité a baissé de 41 % à 25 %.

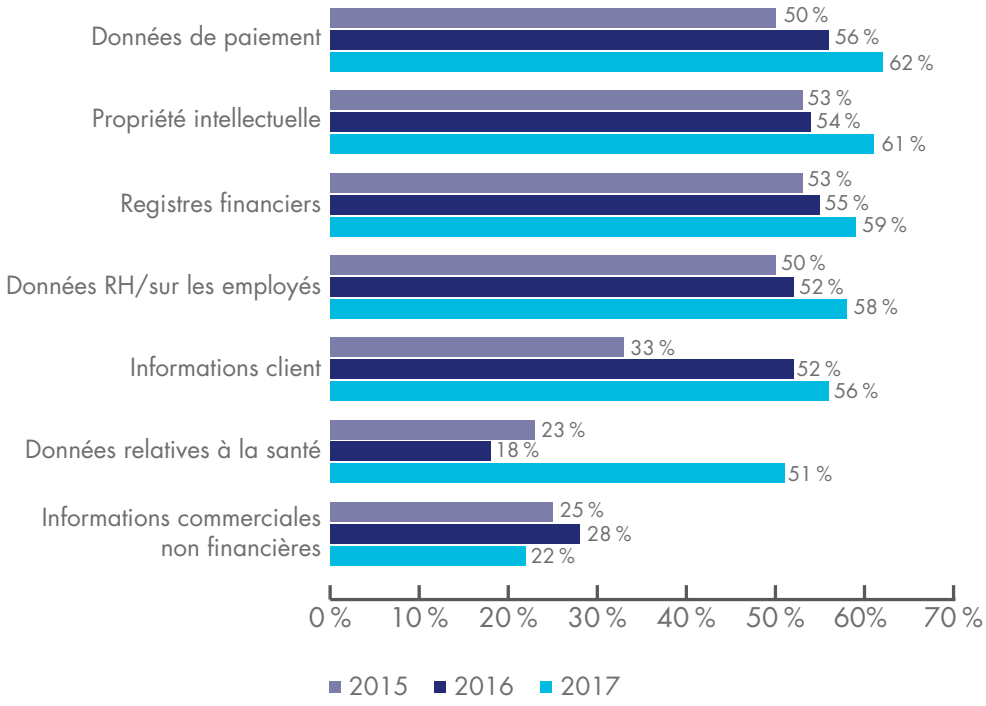
Figure 2. Influence des opérations informatiques, des secteurs d'activité et de la sécurité



[2] Les HSMs sont des dispositifs conçus spécifiquement pour créer un environnement résistant aux infractions permettant d'effectuer des processus cryptographiques (par ex. chiffrement ou signature numérique) et de gérer les clés associées à ces processus. Ces dispositifs sont utilisés pour protéger les activités de chiffrement des données critiques et peuvent servir à appliquer strictement des politiques de sécurité et le contrôle des accès. Les HSMs sont généralement validés par des normes de sécurité informatique formelles telles que FIPS 140-2.

Quels types de données sont les plus susceptibles d'être chiffrés ? La figure 3 fournit une liste de sept types de données couramment chiffrés par les enterprises des sondés. Comme indiqué, cette année, les entreprises chiffrent en priorité chiffrent les données relatives au paiement, à la propriété intellectuelle, aux antécédents financiers, aux données sur les employés, aux clients et à la santé. Le chiffrement des données commerciales et financière est nettement moins important.

Figure 3. Types de données couramment chiffrés
Plusieurs réponses autorisées

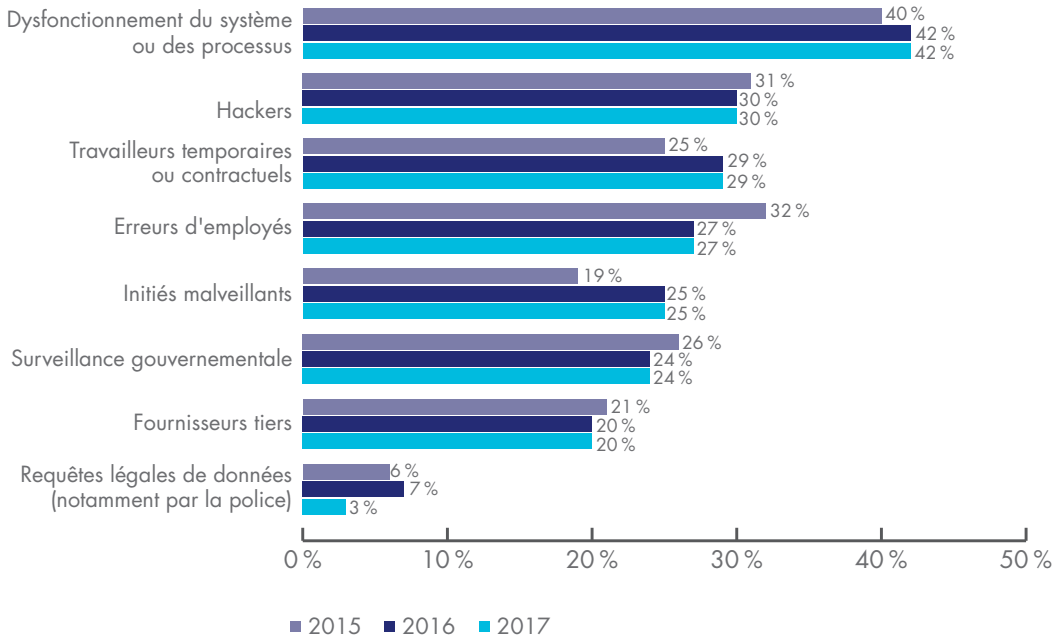


« CETTE ANNÉE, DAVANTAGE D'ENTREPRISES CHIFFRENT LES DONNÉES RELATIVES AU PAIEMENT, À LA PROPRIÉTÉ INTELLECTUELLE, AUX REGISTRES FINANCIERS, AUX DONNÉES SUR LES EMPLOYÉS, AUX CLIENTS ET À LA SANTÉ. »

Menaces, priorités et principaux facteurs

Un dysfonctionnement du système ou des processus est la menace principale de divulgation de données sensibles ou confidentielles. La figure 4 indique que pour 42 % des sondés, les menaces les plus importantes de divulgation de données sensibles ou confidentielles sont les dysfonctionnements du système ou des processus. Pour 30 % des sondés, les hackers représentent la menace la plus importante, tandis que 29 % des sondés estiment que la menace porte davantage sur des travailleurs temporaires ou contractuels.

Figure 4. Principales menaces susceptibles d'entraîner la divulgation des données sensibles ou confidentielles
Deux réponses autorisées

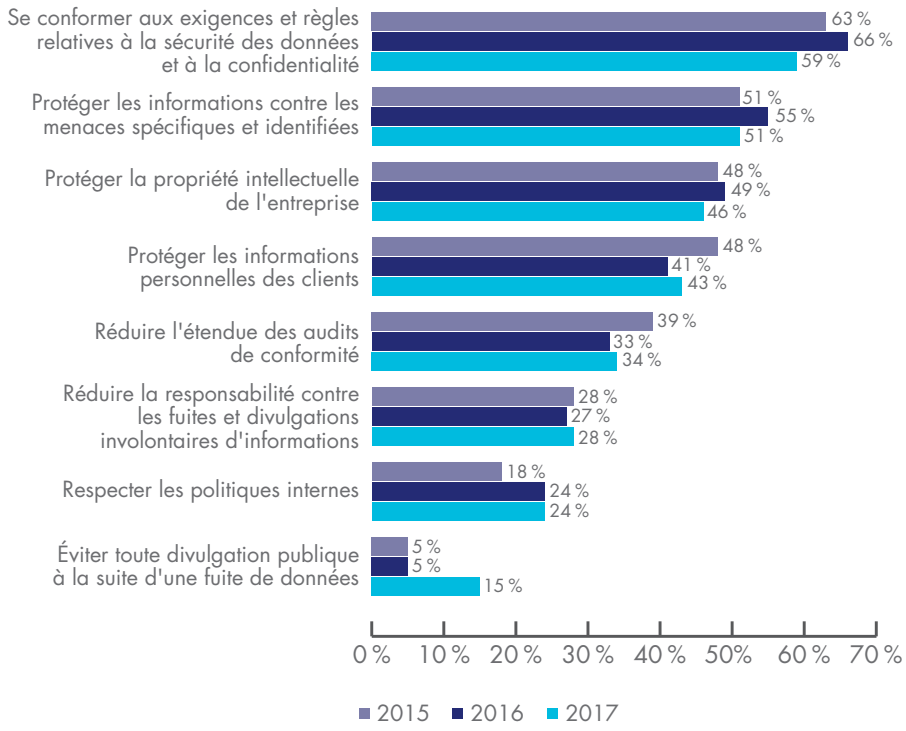


« POUR 42 % DES SONDÉS, LES MENACES LES PLUS IMPORTANTES DE DIVULGATION DE DONNÉES SENSIBLES OU CONFIDENTIELLES SONT LES DYSFONCTIONNEMENTS DU SYSTÈME OU DES PROCESSUS. »

La conformité aux règles relatives à la sécurité informatique et à la confidentialité est le facteur principal d'utilisation des technologies de chiffrement. Huit facteurs de déploiement du chiffrement sont présentés figure 5. Selon 59 % des sondés, la conformité aux exigences et aux règles relatives à la sécurité des données et à la confidentialité externes reste le facteur principal.

51 % et 46 % des sondés affirment que la protection des informations contre des menaces spécifiques et la protection de la propriété intellectuelle de l'entreprise sont des facteurs importants.

Figure 5. Facteurs principaux d'utilisation des technologies de chiffrement
Trois réponses autorisées

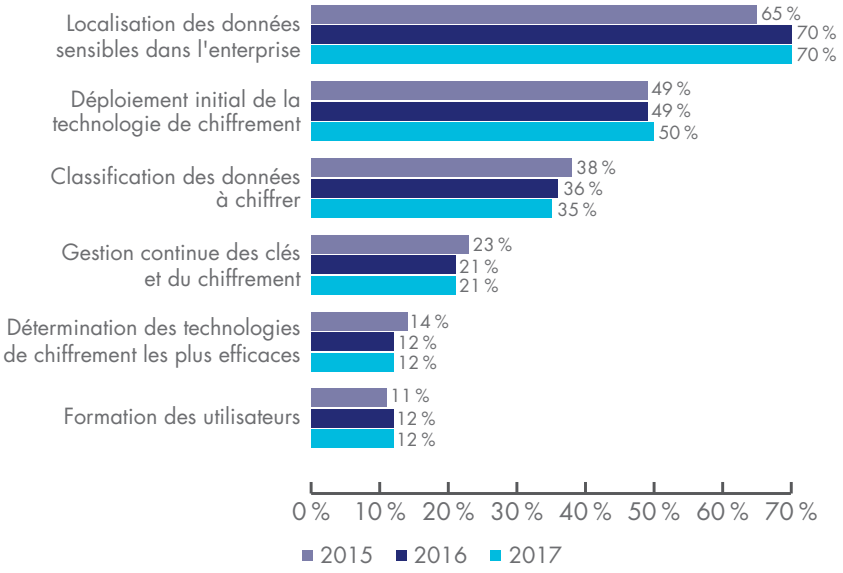


« D'APRÈS 59 % DES SONDÉS, LA CONFORMITÉ AUX EXIGENCES ET RÈGLES RELATIVES À LA SÉCURITÉ DES DONNÉES ET À LA CONFIDENTIALITÉ RESTE LE FACTEUR PRINCIPAL. »

Localiser les données sensibles dans l'enterprise reste l'un des défis les plus importants. Le schéma 6 présente six difficultés relatives à l'application efficace de la stratégie de chiffrement des données dans l'entreprise, par ordre décroissant d'importance.

Pour 70 % des sondés, localiser les données sensibles dans l'enterprise est le défi le plus important à relever pour la planification et l'exécution d'une stratégie de chiffrement des données. Le deuxième défi le plus important est le déploiement initial de la technologie de chiffrement (pour 50 % des sondés).

Figure 6. Difficultés principales liées à la planification et l'exécution d'une stratégie de chiffrement des données
Deux réponses autorisées



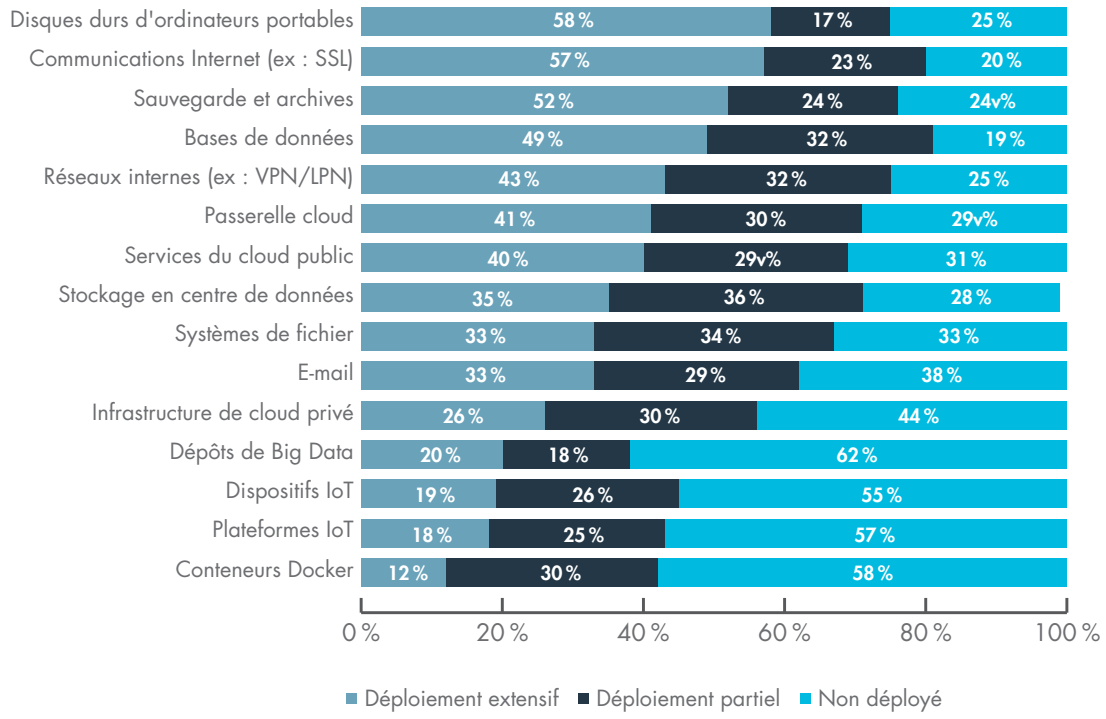
« POUR 70 % DES SONDÉS, LOCALISER LES DONNÉES SENSIBLES DANS L'ENTERPRISE EST LE DÉFI LE PLUS IMPORTANT À RELEVER POUR LA PLANIFICATION ET L'EXÉCUTION D'UNE STRATÉGIE DE CHIFFREMENT DES DONNÉES. »

Choix de déploiement

Il n'y a pas de technologie de chiffrement dominante dans les enterprises. Nous avons demandé aux sondés d'indiquer si des technologies de chiffrement spécifiques étaient déployées de manière de manière globale ou partielle dans leur enterprise.

Comme indiqué schéma 7, aucune technologie ne domine car les enterprises ont des besoins très divers. Le chiffrement des disques durs des ordinateurs portables, des communications numériques et des sauvegardes et archives sont les fonctionnalités le plus souvent déployées de manière globale. À l'inverse, les plateformes et appareils liés à l'Internet des objets (IoT) sont un cas encore minoritaire mais en croissance, tandis que les conteneurs Docker sont moins souvent chiffrés.

Figure 7. Utilisation des technologies de chiffrement

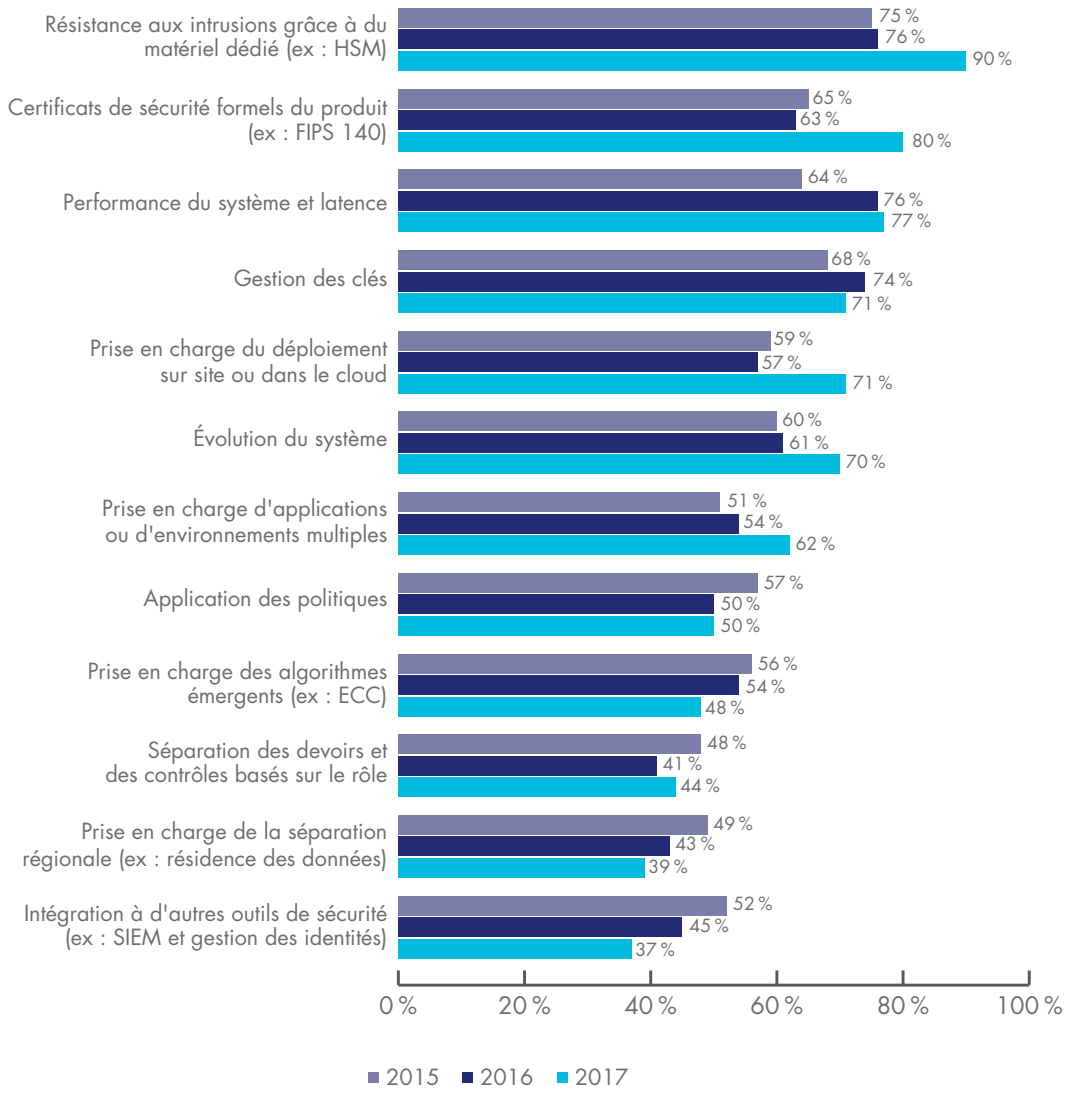


Les contraintes considérées comme les plus importantes liées à la mise en place de technologies de chiffrement

Certaines contraintes sont en effet considérées comme plus importantes que d'autres. Le schéma 8 liste 12 caractéristiques liés au déploiement de technologies de chiffrement. Chaque pourcentage correspond au nombre de sondés estimant la contrainte importante ou très importante (sur une échelle de 1 à 4). Les sondés devaient noter les fonctionnalités de la technologie de chiffrement qu'ils considéraient comme les plus importantes pour la posture de sécurité de leur enterprise.

Au cours des trois dernières années, les éléments suivants ont énormément gagné en importance : la résistance au sabotage grâce à du matériel dédié, les certificats de sécurité, les performances du système et la latence, le support du déploiement sur site et dans le cloud, la possibilité d'évolution du système et le support d'applications et d'environnements multiples. Un aspect dont l'importance a baissé mais qui reste néanmoins présent de manière significative pour 50 % des sondés est l'application des politique de sécurité du groupe.

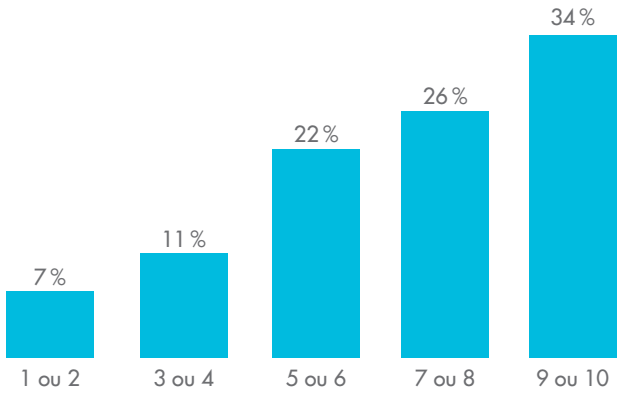
Figure 8. Contraintes majeures liées à l'utilisation de technologies de chiffrement
Réponses « Importante » et « Très importante » combinées



Attitudes relatives à la gestion de clé

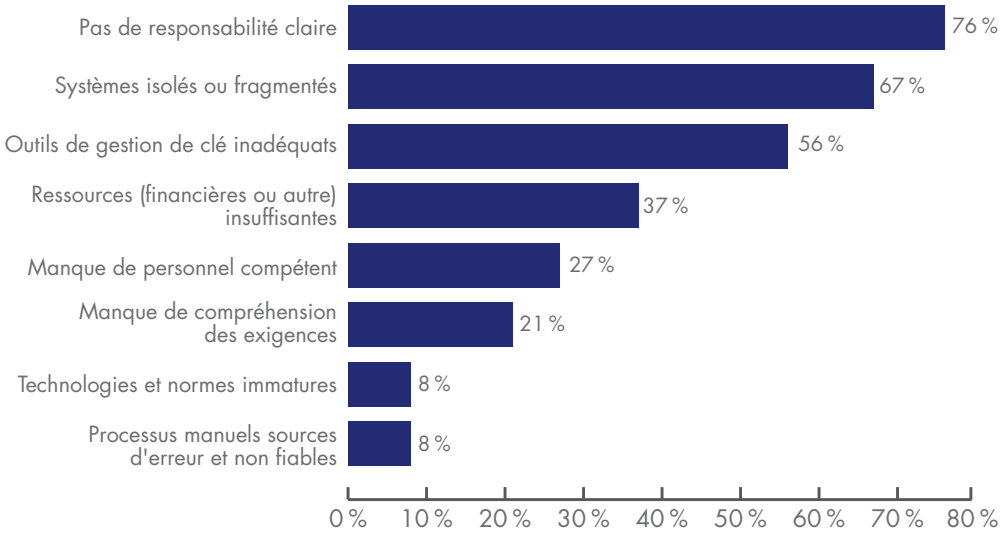
À quel point la gestion de clé est-elle difficile ? Sur une échelle de 1 à 10, les sondés ont dû noter la difficulté associée à la gestion des clés dans leur enterprise, où 1 correspond à un impact minimal et 10 à un impact sévère. Le schéma 9 montre que 60 % (26 + 34) des sondés ont choisi une note de 7 ou plus, ce qui indique une difficulté assez élevée.

Figure 9. À quel point la gestion de clé est-elle difficile ?
1 = impact minimal, 10 = impact sévère



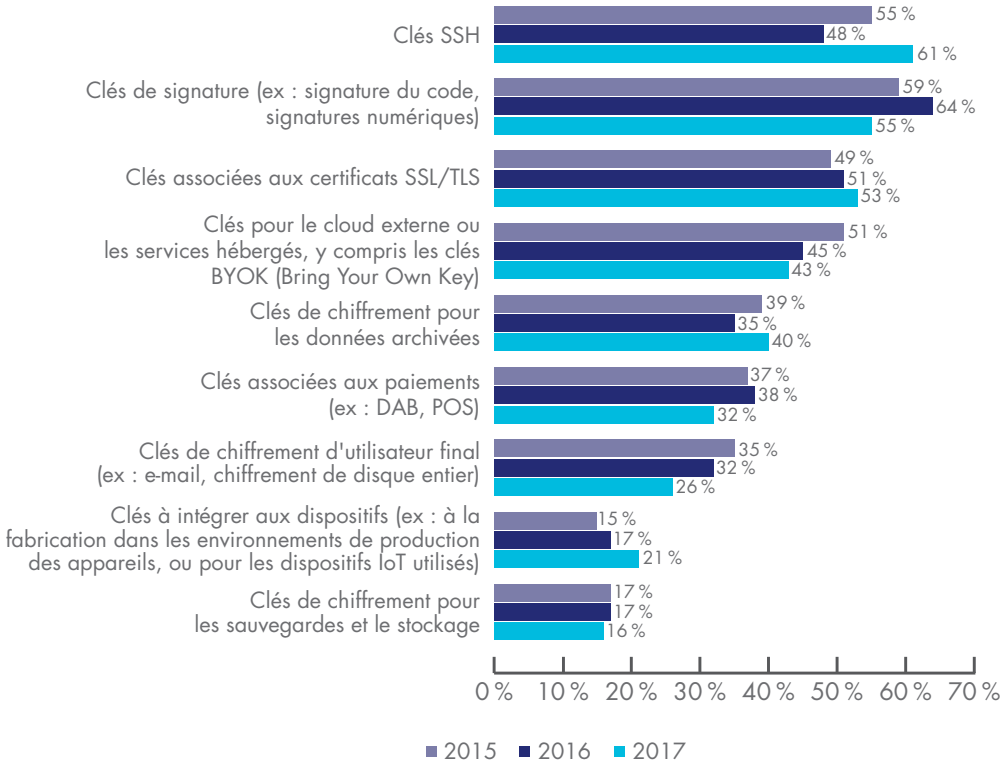
Pourquoi la gestion de clé est-elle difficile ? La figure 10 montre pourquoi la gestion des clés est si difficile. Les raisons principales de ces difficultés sont les suivantes : pas de responsabilité claire, les systèmes sont isolés et fragmentés et les outils de gestion de clé sont inadéquats.

Figure 10. Pourquoi la gestion de clé est-elle si difficile ?
Trois réponses autorisées



Quelles clés sont les plus difficiles à gérer ? D'après la figure 11, la difficulté de gestion des clés SSH a drastiquement augmenté depuis l'année dernière. La difficulté de gestion des clés suivantes a légèrement diminué : clés de signature (par ex. signature du code, signatures numériques), clés de cloud externe ou de services hébergés, dont les clés Bring Your Own Key (BYOK) et les clés de chiffrement de l'utilisateur final.

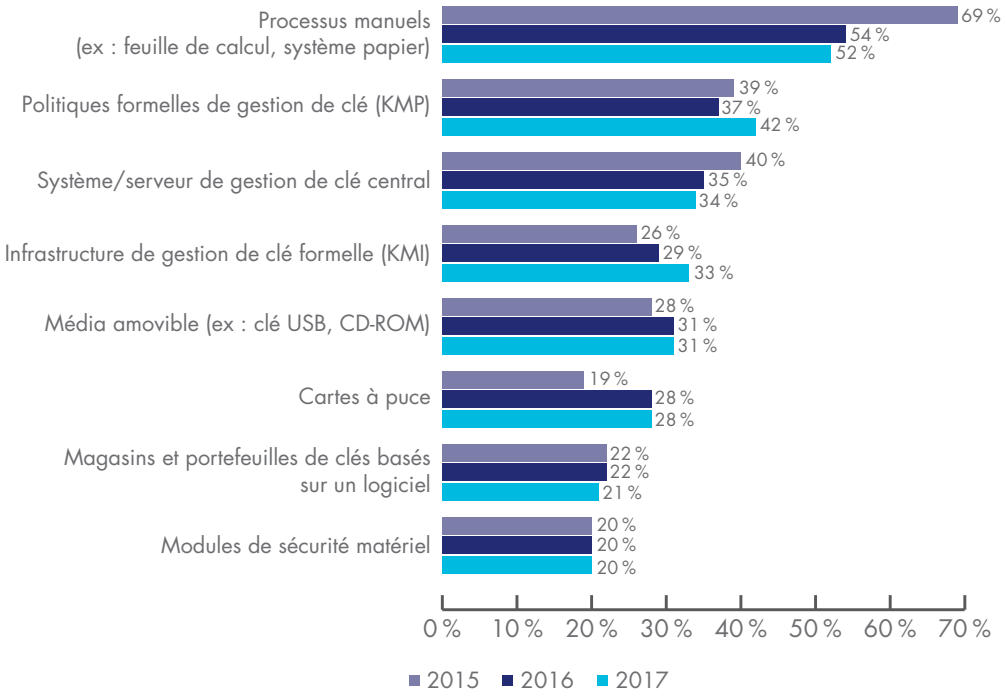
Figure 11. Types de clés les plus difficiles à gérer
Réponses « Difficile » et « Extrêmement difficile » combinées



« LA DIFFICULTÉ DE GESTION DES CLÉS SSH A DRASTIQUEMENT AUGMENTÉ DEPUIS L'ANNÉE DERNIÈRE. » « LA DIFFICULTÉ DE GESTION DES CLÉS SUIVANTES A LÉGÈREMENT DIMINUÉ : CLÉS DE SIGNATURE (PAR EX. SIGNATURE DU CODE, SIGNATURES NUMÉRIQUES), CLÉS DE CLOUD EXTERNE OU DE SERVICES HÉBERGÉS, DONT LES CLÉS BRING YOUR OWN KEY (BYOK) ET LES CLÉS DE CHIFFREMENT DE L'UTILISATEUR FINAL. »

Comme indiqué schéma 12, les entreprises des sondés continuent à utiliser divers systèmes de gestion de clé. Les systèmes déployés sont le plus souvent des processus manuels (par ex. feuille de calcul, système papier) et des politiques formelles de gestion de clés (KMP).

Figure 12. Quels systèmes de gestion de clé sont utilisés par votre enterprise ?
Plusieurs réponses autorisées

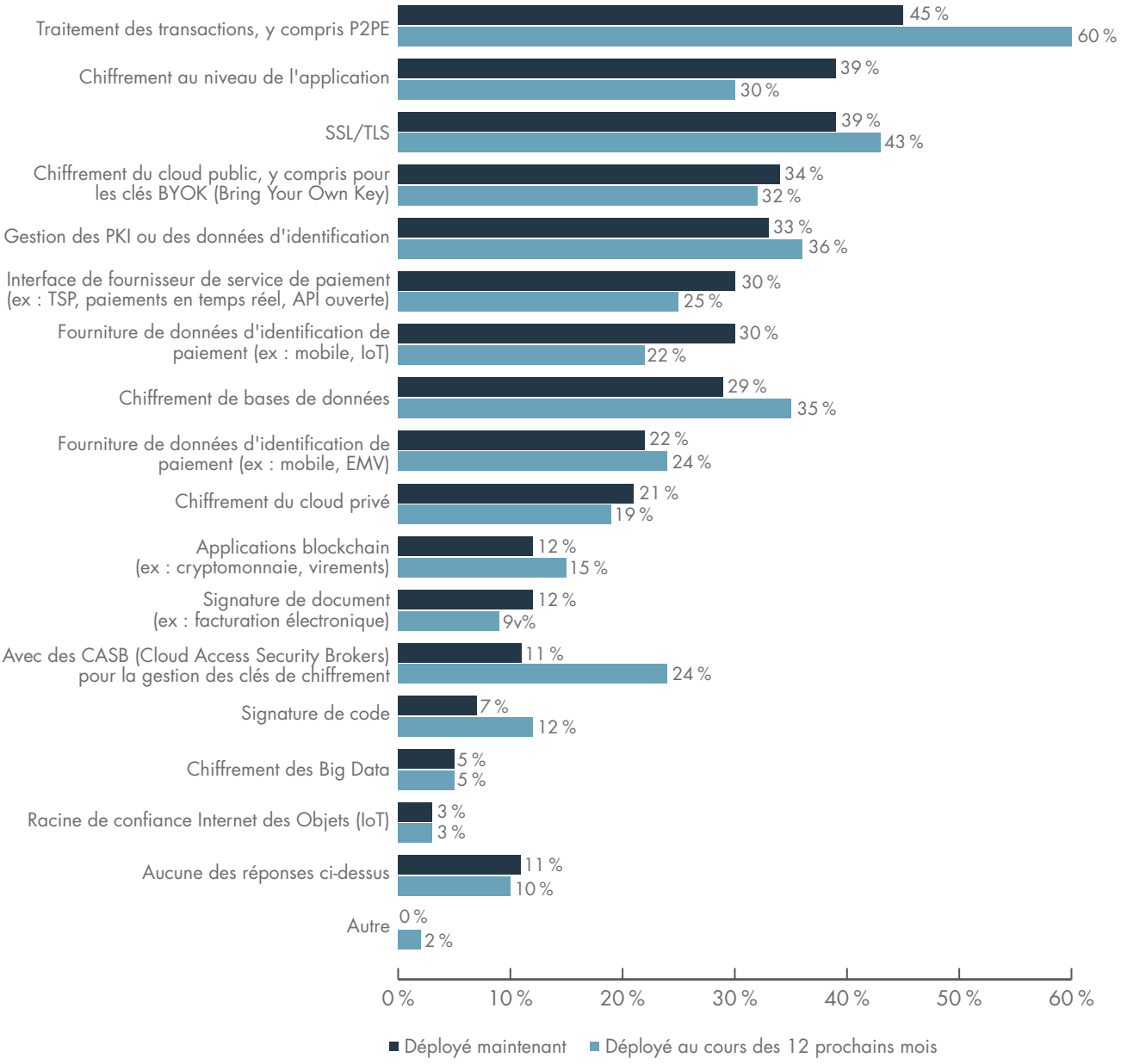


« LES ENTREPRISES CONTINUENT À UTILISER DIVERS SYSTÈMES DE GESTION DE CLÉ. LES SYSTÈMES DÉPLOYÉS SONT LE PLUS SOUVENT DES PROCESSUS MANUELS (PAR EX. FEUILLE DE CALCUL, SYSTÈME PAPIER) ET DES POLITIQUES FORMELLES DE GESTION DE CLÉ (KMP). »

Importance des modules de sécurité matériel (HSM)

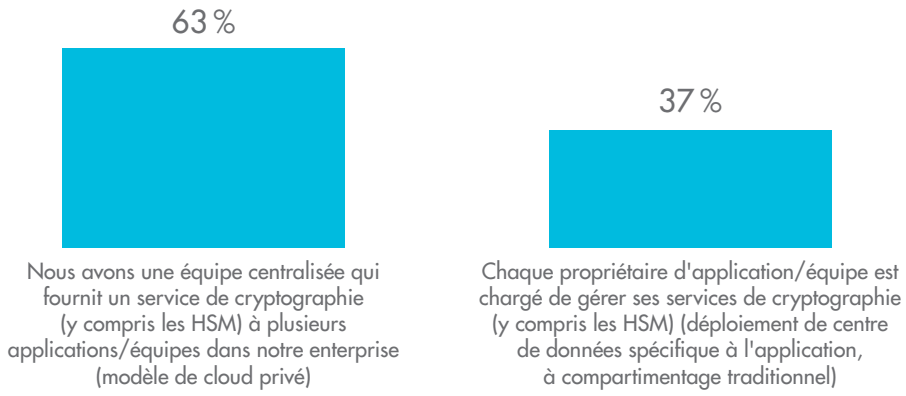
L'importance des HSMs pour la stratégie du chiffrement ou de la gestion de clé va croître au cours des 12 prochains mois. Nous avons demandé aux sondés dont les enterprises déploient actuellement des HSMs de nous indiquer leur importance pour la stratégie de chiffrement ou de gestion de clé. 53 % des sondés indiquent qu'ils sont importants aujourd'hui, et 63 % estiment qu'ils seront importants au cours des 12 prochains mois. Le schéma 13 résume les objectifs primaires ou les cas d'utilisation de déploiement des HSMs. Le traitement des transactions, le chiffrement de la base de données et les Cloud Access Security Brokers (CASB) sont des cas d'utilisation qui devraient devenir plus fréquents au cours des 12 prochains mois. Le chiffrement au niveau de l'application et la fourniture des données de paiement sont des cas dont la fréquence devrait diminuer.

Figure 13. Comment les HSM sont déployés ou vont l'être au cours des 12 prochains mois
Plusieurs réponses autorisées



Comment les enterprises utilisent les HSM. D'après la figure 14, 63 % des sondés indiquent qu'ils ont une équipe centralisée de cryptographie. La moyenne mondiale est de 61 % des sondés. 37 % des sondés affirment que chaque équipe/propriétaire d'application individuelle est responsable de ses propres services cryptographiques.

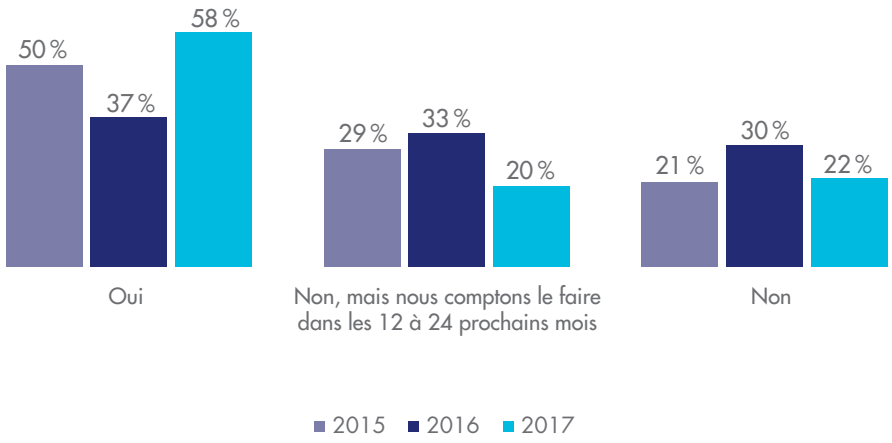
Figure 14. Quelle description correspond le mieux à l'utilisation des HSM par votre enterprise ?



Chiffrement du cloud

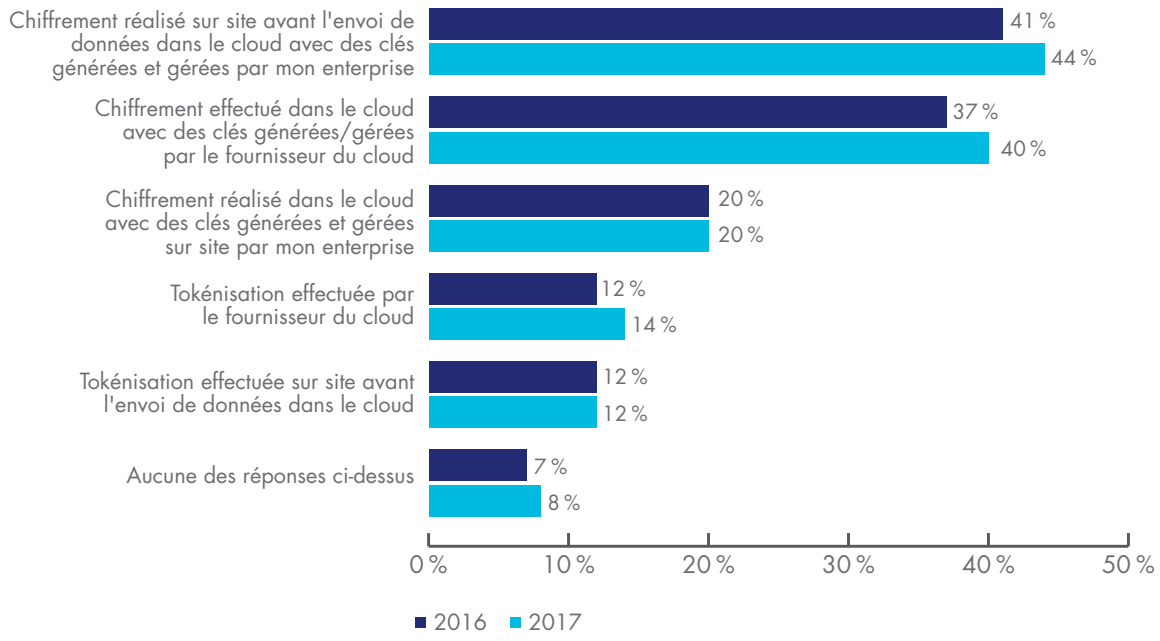
La plupart des enterprises transfèrent les données sensibles ou confidentielles dans le cloud. Comme indiqué schéma 15, 58 % des sondés affirment que leurs enterprises transfèrent actuellement les données sensibles ou confidentielles dans le cloud (qu'elles soient chiffrées ou rendues illisibles d'une manière ou d'une autre) et 20 % des sondés se préparent à le faire au cours des 12 à 24 mois prochains. 50 % des sondés affirment que le fournisseur du cloud est le principal responsable de la protection des données confidentielles ou sensibles transférées sur le cloud.

Figure 15. Transférez-vous actuellement vos données sensibles dans le cloud ?



Comment les données stockées dans le cloud sont-elles protégées ? Comme indiqué figure 16, 44 % des sondés affirment que le chiffrement est effectué sur site avant d'envoyer les données dans le cloud à l'aide de clés générées et gérées par l'enterprise et 40 % des sondés affirment que le chiffrement est effectué dans le cloud à l'aide de clés générées et gérées par le fournisseur du cloud.

Figure 16. Comment votre enterprise protège-t-elle les données inactives dans le cloud ?



« 44 % DES SONDÉS AFFIRMENT QUE LE CHIFFREMENT EST EFFECTUÉ SUR SITE AVANT D'ENVOYER LES DONNÉES DANS LE CLOUD À L'AIDE DE CLÉS GÉNÉRÉES ET GÉRÉES PAR L'ENTERPRISE ET 40 % DES SONDÉS AFFIRMENT QUE LE CHIFFREMENT EST EFFECTUÉ DANS LE CLOUD À L'AIDE DE CLÉS GÉNÉRÉES ET GÉRÉES PAR LE FOURNISSEUR DU CLOUD. »

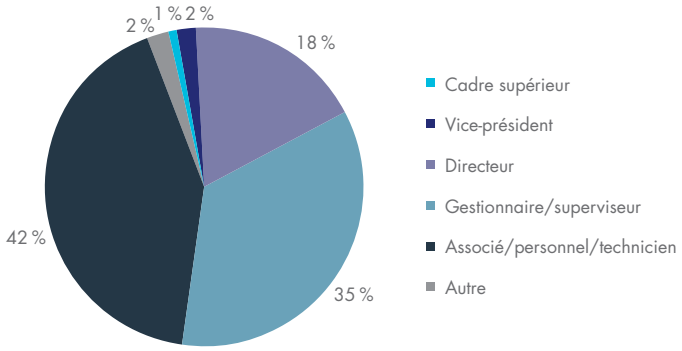
ANNEXE 1. MÉTHODES ET LIMITES

Le tableau 2 montre les réponses des sondés pour la France. Les réponses de l'échantillon de cette étude ont été collectées au cours d'une période de 49 jours ayant pris fin en janvier 2018. Pour la France, notre cadre d'échantillonnage est composé de 12 650 professionnels de l'informatique ou de la sécurité informatique reconnus. De ce cadre, nous avons reçu 440 retours, dont 70 ont été rejetés pour des questions de fiabilité. Notre échantillonnage final pour la France était de 370, ce qui représente un taux de réponse de 2,9 %.

Tableau 1. Échantillon de réponses	Fréquence	Pourcentage
Cadre d'échantillonnage total	12 650	100 %
Total des retours	440	3,5 %
Enquêtes rejetées ou écartées	70	0,6 %
Échantillon final	370	2,9 %

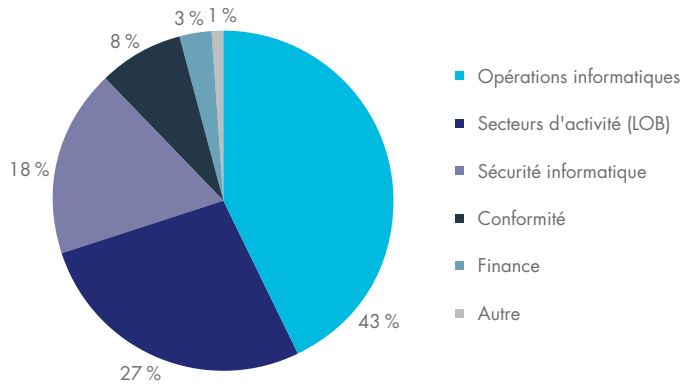
Le schéma 17 résume les niveaux hiérarchiques des sondés. Comme indiqué, plus de la moitié des sondés (56 %) occupent au minimum des postes de cadre.

Figure 17. Répartition des sondés en fonction de leur niveau hiérarchique



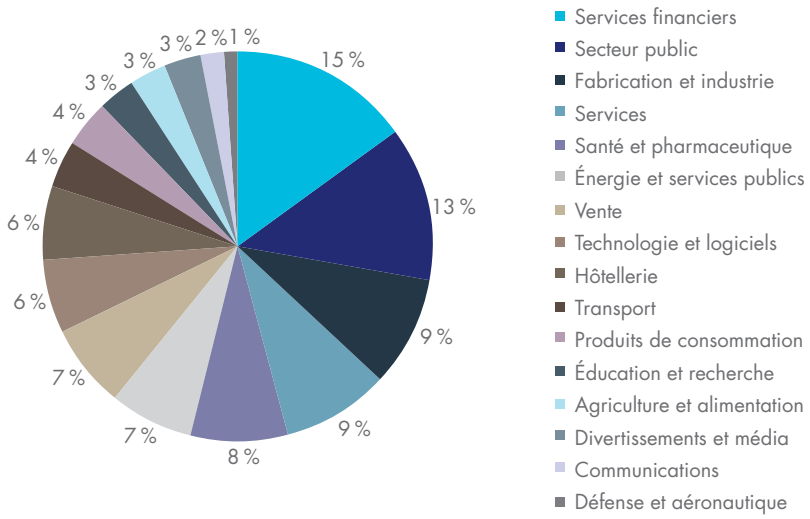
Le schéma 18 indique le secteur de travail des sondés. Comme indiqué, 43 % des sondés travaillent dans les opérations informatiques, 27 % travaillent dans divers secteurs d'activité, 18 % travaillent dans la sécurité informatique et 8 % travaillent dans la conformité.

Figure 18. Répartition des sondés en fonction de leur secteur de travail



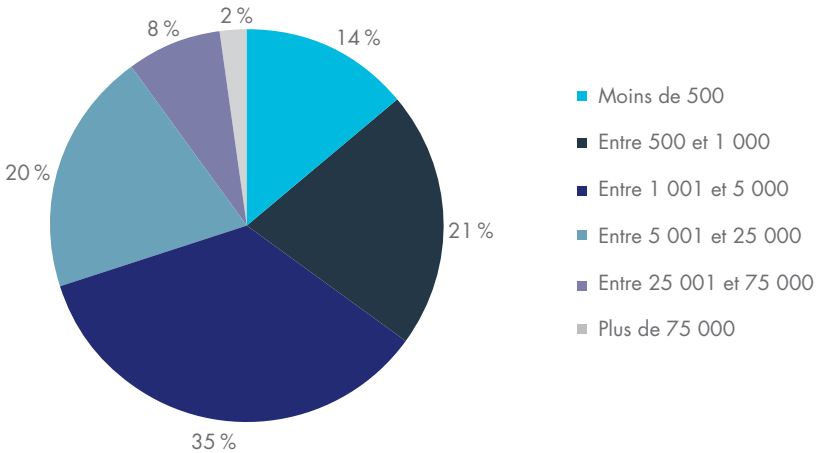
La figure 19 indique les secteurs industriels primaires des enterprises des sondés. Comme indiqué, 15 % des sondés travaillent dans les services financiers, dont la banque, la gestion des investissements, l'assurance, le courtage, les paiements et les cartes bancaires. 13 % des sondés travaillent dans le secteur public, 9 % dans la fabrication et l'industrie, 9 % dans l'industrie des services, et 8 % travaillent dans les secteurs de la santé et pharmaceutique.

Figure 19. Répartition des sondés en fonction de leur secteur industriel principal



D'après le schéma 20, plus de la moitié (65 %) des sondés travaillent dans de grandes enterprises dont l'effectif est supérieur à 1 000 employés.

Figure 20. Répartition des sondés en fonction de l'effectif de l'enterprise



Limites

Ce type d'enquête a des limites inhérentes qui doivent être bien prises en compte avant de tirer des conclusions des résultats présentés. Les éléments suivants sont des limites spécifiques communes à la plupart des enquêtes de ce type.

- **Biais de non-réponse :** les résultats actuels sont fondés sur un échantillon de réponses à l'enquête. Nous avons envoyé l'enquête à un échantillon représentatif de praticiens de la sécurité informatique en France, ce qui nous a permis d'obtenir de nombreuses réponses utilisables. Malgré des tests de non-réponse, il est toujours possible que les individus qui n'ont pas participé aient des opinions sous-jacentes très différentes de ceux qui ont répondu à l'enquête.

- **Biais de cadre d'échantillonnage :** la précision des résultats de l'étude dépend de la représentativité de notre cadre d'échantillonnage vis à vis des professionnels de l'informatique et des praticiens de la sécurité informatique en France.

- **Résultats auto-rapportés :** la qualité de l'étude dépend de l'intégrité des réponses confidentielles reçues de la part des sondés. Un système de contrôle a été mis en place dans notre processus d'évaluation de l'étude, dont des tests d'intégrité, mais il est toujours possible que certains sondés n'aient pas répondu sincèrement.

ANNEXE 2. TABLEAUX DE DONNÉES DE L'ÉTUDE

Le tableau suivant fournit les résultats pour l'échantillon japonais.

Réponse à l'enquête	FR
Cadre d'échantillonnage	12 650
Total des retours	440
Enquêtes rejetées ou écartées	70
Échantillon final	370
Taux de réponse	2,9 %

1re partie. Posture de chiffrement

Q1. Veuillez sélectionner la réponse correspondant le mieux à l'approche de votre enterprise vis-à-vis de l'exécution du chiffrement sur toute l'entreprise.	FR
Nous n'avons pas de stratégie de chiffrement	40 %
Nous appliquons une stratégie de chiffrement globale à tous les niveaux de notre entreprise	41 %
Nous appliquons une stratégie de chiffrement limitée qui s'applique à certaines applications et certains types de données	19 %
Total	100 %

Q2. Parmi les domaines suivants, dans lesquels les technologies de chiffrement peuvent-elles être déployées ? Veuillez indiquer les domaines pour lesquels le chiffrement est déployé de manière globale, partiellement, ou n'est pas déployé par votre enterprise.

Q2a-1 Sauvegarde et archives	FR
Déploiement extensif	52 %
Déploiement partiel	24 %
Non déployé	24 %
Total	100 %

Q2b-1. Dépôts de Big Data	FR
Déploiement extensif	20 %
Déploiement partiel	18 %
Non déployé	62 %
Total	100 %

Q2c-1 Passerelle cloud	FR
Déploiement extensif	41 %
Déploiement partiel	30 %
Non déployé	29 %
Total	100 %

Q2d-1. Stockage en centre de données	FR
Déploiement extensif	35 %
Déploiement partiel	36 %
Non déployé	28 %
Total	100 %

Q2e-1. Bases de données	FR
Déploiement extensif	49 %
Déploiement partiel	32 %
Non déployé	19 %
Total	100 %

Q2f-1. Conteneurs Docker	FR
Déploiement extensif	12 %
Déploiement partiel	30 %
Non déployé	58 %
Total	100 %

Q2g-1. E-mail	FR
Déploiement extensif	33 %
Déploiement partiel	29 %
Non déployé	38 %
Total	100 %

Q2h-1. Services du cloud public	FR
Déploiement extensif	40 %
Déploiement partiel	29 %
Non déployé	31 %
Total	100 %

Q2i-1. Systèmes de fichier	FR
Déploiement extensif	33 %
Déploiement partiel	34 %
Non déployé	33 %
Total	100 %

Q2j-1. Communications Internet (ex : SSL)	FR
Déploiement extensif	57 %
Déploiement partiel	23 %
Non déployé	20 %
Total	100 %

Q2k-1. Réseaux internes (ex : VPN/LPN)	FR
Déploiement extensif	43 %
Déploiement partiel	32 %
Non déployé	25 %
Total	100 %

Q2l-1. Disques durs d'ordinateurs portables	FR
Déploiement extensif	58 %
Déploiement partiel	17 %
Non déployé	25 %
Total	100 %

Q2m-1 Infrastructure de cloud privé	FR
Déploiement extensif	26 %
Déploiement partiel	30 %
Non déployé	44 %
Total	100 %

Q2n-1 Dispositifs Internet des Objets (IoT)	FR
Déploiement extensif	19 %
Déploiement partiel	26 %
Non déployé	55 %
Total	100 %

Q2o-1 Plateformes Internet des Objets (IoT)	FR
Déploiement extensif	18 %
Déploiement partiel	25 %
Non déployé	57 %
Total	100 %

Q3. Quel rôle a le plus d'influence dans l'orientation de la stratégie de chiffrement ? Veuillez sélectionner la meilleure option.	FR
Opérations informatiques	38 %
Sécurité	13 %
Conformité	6 %
Secteurs d'activité ou direction générale	25 %
Responsabilité partagée	18 %
Total	100 %

Q4. Pourquoi votre enterprise chiffre-t-elle les données confidentielles et sensibles ? Veuillez sélectionner les trois meilleures réponses.	FR
Protéger la propriété intellectuelle de l'entreprise	46 %
Protéger les informations personnelles des clients	43 %
Réduire la responsabilité contre les fuites et divulgations involontaires d'informations	28 %
Éviter toute divulgation publique à la suite d'une fuite de données	15 %
Protéger les informations contre les menaces spécifiques et identifiées	51 %
Respecter les politiques internes	24 %
Se conformer aux exigences et règles relatives à la sécurité des données et à la confidentialité externes	59 %
Réduire l'étendue des audits de conformité	34 %
Total	300 %

Q5. Quelles sont les difficultés principales liées à la planification et l'exécution d'une stratégie de chiffrement des données ? Veuillez sélectionner les deux meilleures réponses.	FR
Localisation des données sensibles dans l'enterprise	70 %
Classification des données à chiffrer	35 %
Détermination des technologies de chiffrement les plus efficaces	12 %
Déploiement initial de la technologie de chiffrement	50 %
Gestion continue des clés et du chiffrement	21 %
Formation des utilisateurs du chiffrement	12 %
Total	200 %

Q6. Quelle est l'importance des fonctionnalités suivantes associées aux solutions de chiffrement susceptibles d'être utilisées par votre enterprise ? Réponses « Importante » et « Très importante » combinées.	**FR**
Application des politiques	50 %
Gestion des clés	71 %
Prise en charge d'applications ou d'environnements multiples	62 %
Séparation des devoirs et des contrôles basés sur le rôle	44 %
Évolution du système	70 %
Résistance aux intrusions grâce à du matériel dédié (ex : HSM)	90 %
Intégration à d'autres outils de sécurité (ex : SIEM et gestion des identités)	37 %
Prise en charge de la séparation régionale (ex : résidence des données)	39 %
Performance du système et latence	77 %
Prise en charge des algorithmes émergents (ex : ECC)	48 %
Prise en charge du déploiement sur site ou dans le cloud	71 %
Certificats de sécurité formels du produit (ex : FIPS 140)	80 %

Q7. Quels types de données votre enterprise chiffre-t-elle ? Veuillez sélectionner toutes les réponses qui s'appliquent.	**FR**
Informations client	56 %
Informations commerciales non financières	22 %
Propriété intellectuelle	61 %
Registres financiers	59 %
Données RH/sur les employés	58 %
Données de paiement	62 %
Données relatives à la santé	51 %

Q8. Quelles sont les principales menaces susceptibles d'entraîner la divulgation des données sensibles ou confidentielles ? Veuillez sélectionner les deux meilleures réponses.	**FR**
Pirates	30 %
Initiés malveillants	25 %
Dysfonctionnement du système ou des processus	42 %
Erreurs d'employés	27 %
Travailleurs temporaires ou contractuels	29 %
Fournisseurs tiers	20 %
Requêtes légales de données (notamment par la police)	3 %
Surveillance gouvernementale	24 %
Total	200 %

2e partie. Gestion de clé

Q9. Notez la difficulté associée à la gestion des clés ou des certificats dans votre enterprise : 1 = impact minimal et 10 = impact sévère.	**FR**
1 ou 2	7 %
3 ou 4	11 %
5 ou 6	22 %
7 ou 8	26 %
9 ou 10	34 %
Total	100 %

Q10. Pourquoi la gestion de clé est-elle si difficile ? Veuillez sélectionner les trois meilleures réponses.	**FR**
Pas de responsabilité claire	76 %
Ressources (financières ou autres) insuffisantes	37 %
Manque de personnel compétent	27 %
Manque de compréhension des exigences	21 %
Outils de gestion de clé inadéquats	56 %
Systèmes isolés ou fragmentés	67 %
Technologies et normes immatures	8 %
Processus manuels sources d'erreur et non fiables	8 %
Total	300 %

Q11. Voici un grand nombre de clés susceptibles d'être gérées par votre enterprise. Notez la difficulté associée à la gestion de chaque type. Réponses « Difficile » et « Extrêmement difficile » combinées.	**FR**
Clés de chiffrement pour les sauvegardes et le stockage	16 %
Clés de chiffrement pour les données archivées	40 %
Clés associées aux certificats SSL/TLS	53 %
Clés SSH	61 %
Clés de chiffrement d'utilisateur final (ex : e-mail, chiffrement de disque entier)	26 %
Clés de signature (ex : signature du code, signatures numériques)	55 %
Clés associées aux paiements (ex : DAB, POS)	32 %
Clés à intégrer aux dispositifs (ex : à la fabrication dans les environnements de production des appareils, ou pour les dispositifs IoT utilisés)	21 %
Clés pour le cloud externe ou les services hébergés, y compris les clés BYOK (Bring Your Own Key)	43 %

Q12a. Quels systèmes de gestion de clé sont utilisés par votre enterprise ?	FR
Politiques formelles de gestion de clé (KMP)	42 %
Infrastructure de gestion de clé formelle (KMI)	33 %
Processus manuels (ex : feuille de calcul, système papier)	52 %
Système/serveur de gestion de clé central	34 %
Modules de sécurité matériel	20 %
Média amovible (ex : clé USB, CD-ROM)	31 %
Magasins et portefeuilles de clés basés sur un logiciel	21 %
Cartes à puce	28 %
Total	260 %

Q12b. Quels systèmes de gestion de clé votre enterprise n'utilise-t-elle pas ou ne connaît-elle pas ?	FR
Politiques formelles de gestion de clé (KMP)	38 %
Infrastructure de gestion de clé formelle (KMI)	45 %
Processus manuels (ex : feuille de calcul, système papier)	35 %
Système/serveur de gestion de clé central	46 %
Modules de sécurité matériel	52 %
Média amovible (ex : clé USB, CD-ROM)	48 %
Magasins et portefeuilles de clés basés sur un logiciel	68 %
Cartes à puce	63 %
Total	395 %

3e partie. Modules de sécurité matériel

Q13. Quelle description correspond le plus à votre niveau de connaissance des HSM ?	FR
Connaissances élevées	19 %
Connaissances moyennes	30 %
Peu de connaissances	11 %
Aucune connaissance (passer à Q17a)	40 %
Total	100 %

Q14a. Votre enterprise utilise-t-elle des HSM ?	FR
Oui	43 %
Non (passer à Q17a)	57 %
Total	100 %

Q14b. Dans quel but votre enterprise déploie-t-elle ou prévoit-elle d'utiliser des HSM ? Veuillez sélectionner toutes les réponses qui s'appliquent.

Q14b-1. HSM utilisés aujourd'hui	FR
Chiffrement au niveau de l'application	39 %
Chiffrement de bases de données	29 %
Chiffrement des Big Data	5 %
Chiffrement du cloud public, y compris pour les clés BYOK (Bring Your Own Key)	34 %
Chiffrement privé du cloud	21 %
SSL/TLS	39 %
Gestion des PKI ou des données d'identification	33 %
Racine de confiance Internet des Objets (IoT)	3 %
Signature de document (ex : facturation électronique)	12 %
Signature de code	7 %
Traitement des transactions, y compris P2PE	45 %
Fourniture de données d'identification de paiement (ex : mobile, EMV)	22 %
Fourniture de données d'identification de paiement (ex : mobile, IoT)	30 %
Interface de fournisseur de service de paiement (ex : TSP, paiements en temps réel, API ouverte)	30 %
Avec des CASB (Cloud Access Security Brokers) pour la gestion des clés de chiffrement	11 %
Applications blockchain (ex : cryptomonnaie, virements)	12 %
Aucune des réponses ci-dessus	11 %
Autre	0 %
Total	384 %

Q14b-2. HSM en prévision de déploiement les 12 prochains mois	FR
Chiffrement au niveau de l'application	30 %
Chiffrement de bases de données	35 %
Chiffrement des Big Data	5 %
Chiffrement du cloud public, y compris pour les clés BYOK (Bring Your Own Key)	32 %
Chiffrement privé du cloud	19 %
SSL/TLS	43 %
Gestion des PKI ou des données d'identification	36 %
Racine de confiance Internet des Objets (IoT)	3 %
Signature de document (ex : facturation électronique)	9 %
Signature de code	12 %
Traitement des transactions	60 %
Fourniture de données d'identification de paiement (ex : mobile, EMV)	24 %
Fourniture de données d'identification de paiement (ex : mobile, IoT)	22 %
Interface de fournisseur de service de paiement (ex : TSP, paiements en temps réel, API ouverte)	25 %
Avec des CASB (Cloud Access Security Brokers) pour la gestion des clés de chiffrement	24 %
Applications blockchain (ex : cryptomonnaie, virements)	15 %
Aucune des réponses ci-dessus	10 %
Autre	2 %
Total	405 %

Q14c-1. Si vous utilisez des HSM avec des applications basées sur le cloud public, quels modèles utilisez-vous ? Veuillez sélectionner toutes les réponses qui s'appliquent.	FR
Location/utilisation de HSM du fournisseur du cloud public, hébergés dans le cloud	26 %
Détention et application de HSM sur site, avec un accès en temps réel par des applications hébergées sur le cloud	57 %
Détention et application de HSM pour générer et gérer des clés BYOK (Bring Your Own Key) à envoyer sur le cloud par le fournisseur du cloud	18 %
Détention et application de HSM qui s'intègrent au CASB pour gérer les clés et les opérations de cryptographie (ex : chiffrement de données allant sur le cloud, gestion de clés pour les applications du cloud)	10 %
Aucune des réponses ci-dessus	3 %
Total	114 %

Q14c-2. Si vous utilisez des HSM avec des applications basées sur le cloud public, quels modèles prévoyez-vous d'utiliser dans les 12 prochains mois ? Veuillez sélectionner toutes les réponses qui s'appliquent.	**FR**
Location/utilisation de HSM du fournisseur du cloud public, hébergés dans le cloud	30 %
Détention et application de HSM sur site, avec un accès en temps réel par des applications hébergées sur le cloud	67 %
Détention et application de HSM pour générer et gérer des clés BYOK (Bring Your Own Key) à envoyer sur le cloud par le fournisseur du cloud	18 %
Détention et application de HSM qui s'intègrent au CASB pour gérer les clés et les opérations de cryptographie (ex : chiffrement de données allant sur le cloud, gestion de clés pour les applications du cloud)	27 %
Aucune des réponses ci-dessus	2 %
Total	144 %

Q15. Selon vous, quelle est l'importance de l'utilisation des HSM dans votre stratégie de chiffrement ou de gestion de clé ? Réponses « Importante » et « Très importante » combinées.	**FR**
Q15a. Importance aujourd'hui	53 %
Q15b. Importance dans les 12 prochains mois	63 %

Q16. Quelle description correspond le mieux à l'utilisation des HSM par votre enterprise ?	**FR**
Nous avons une équipe centralisée qui fournit un service de cryptographie (y compris les HSM) à plusieurs applications/équipes dans votre enterprise (modèle de cloud privé)	63 %
Chaque propriétaire d'application/équipe est chargé de gérer ses services de cryptographie (y compris les HSM) (déploiement de centre de données spécifique à l'application, à compartimentage traditionnel)	37 %
Total	100 %

4e partie. Questions de budget

Q17a. Êtes-vous responsable de la gestion d'une partie ou de tout le budget informatique de l'enterprise cette année ?	FR
Oui	49 %
Non (passer à Q18)	51 %
Total	100 %

Q17b. Quel pourcentage approximatif du budget informatique de 2018 sera alloué aux activités de sécurité informatique ?	FR
	9,1 %

Q17c. Quel pourcentage approximatif du budget de sécurité informatique de 2018 sera alloué aux activités de chiffrement ?	FR
	13,2 %

6e partie. Chiffrement du cloud : Les réponses aux questions suivantes ne prennent en compte que les services du cloud public.

Q35a. Votre enterprise utilise-t-elle des services de cloud computing pour des classes de données ou d'applications, sensibles ou non ?	FR
Oui	56 %
Non, mais nous comptons le faire dans les 12 à 24 prochains mois	24 %
Non (passer à la partie 7 si vous n'utilisez pas de services du cloud pour des classes de données ou d'applications)	20 %
Total	100 %

Q35b. Transférez-vous des données sensibles ou confidentielles dans le cloud (qu'elles soient ou non chiffrées ou rendues illisibles d'une manière ou d'une autre) ?	FR
Oui	58 %
Non, mais nous comptons le faire dans les 12 à 24 prochains mois	20 %
Non (passer à la partie 7 si vous n'utilisez pas et ne prévoyez pas d'utiliser des services du cloud pour les données sensibles ou confidentielles)	22 %
Total	100 %

Q35c. Selon vous, quel est le principal responsable de la protection des données confidentielles ou sensibles transférées sur le cloud.	FR
Le fournisseur du cloud	50 %
L'utilisateur du cloud	24 %
Responsabilité partagée	26 %
Total	100 %

Q35d. Comment votre enterprise protège-t-elle les données inactives dans le cloud ?	FR
Chiffrement effectué dans le cloud avec des clés générées/gérées par le fournisseur du cloud	40 %
Chiffrement réalisé dans le cloud avec des clés générées et gérées sur site par mon enterprise	20 %
Chiffrement réalisé sur site avant l'envoi de données dans le cloud avec des clés générées et gérées par mon enterprise	44 %
Tokénisation effectuée par le fournisseur du cloud	14 %
Tokénisation effectuée sur site avant l'envoi de données dans le cloud	12 %
Aucune des réponses ci-dessus	8 %
Total	137 %

Q35e. Pour le chiffrement des données inactives dans le cloud, la stratégie de mon enterprise est de...	FR
N'utiliser que des clés contrôlées par mon enterprise	50 %
N'utiliser que des clés contrôlées par le fournisseur du cloud	25 %
Utiliser une combinaison de clés contrôlées par mon enterprise et par le fournisseur du cloud, avec une préférence pour les clés contrôlées par mon enterprise	13 %
Utiliser une combinaison de clés contrôlées par mon enterprise et par le fournisseur du cloud, avec une préférence pour les clés contrôlées par le fournisseur du cloud	12 %
Total	100 %

Q35f. Quelle est l'importance des fonctionnalités suivantes associées au chiffrement du cloud pour votre enterprise ? Réponses « Importante » et « Très importante » combinées.	**FR**
Prise en charge de la gestion de BYOK (Bring Your Own Key)	56 %
Contrôle d'accès d'utilisateur privilégié	56 %
Contrôles d'accès granulaires	78 %
Journaux d'audit identifiant l'utilisation des clés	70 %
Journaux d'audit identifiant les tentatives d'accès aux données	29 %
Intégration SIEM, visualisation et analyse des journaux	62 %
Prise en charge de la gestion de clé conforme FIPS 140-2	29 %
Prise en charge du standard KMIP pour la gestion de clé	44 %
Capacité de chiffrer et de changer les clés des données en utilisation sans indisponibilité	45 %
Moyenne	52 %

Q35g-1. Combien de fournisseurs de cloud public votre enterprise utilise-t-elle ?	**FR**
1	29 %
2	25 %
3	17 %
4 ou plus	29 %
Total	100 %

Q35g-2. Combien de fournisseurs de cloud public votre enterprise prévoit-elle d'utiliser dans les 12 à 24 prochains mois ?	**FR**
1	23 %
2	23 %
3	16 %
4 ou plus	38 %
Total	100 %

7e partie. Caractéristiques enterprisenelles

D1. Quel niveau organisationnel correspond le mieux à votre position actuelle ?	FR
Cadre supérieur	1 %
Vice-président	2 %
Directeur	18 %
Gestionnaire/superviseur	35 %
Associé/personnel/technicien	42 %
Autre	2 %
Total	100 %

D2. Sélectionnez le secteur de travail qui correspond le mieux à votre enterprise ?	FR
Opérations informatiques	43 %
Sécurité	18 %
Conformité	8 %
Finance	3 %
Secteurs d'activité (LOB)	27 %
Autre	1 %
Total	100 %

D3. Quel secteur décrit le mieux le secteur principal de votre enterprise ?	FR
Agriculture et alimentation	3 %
Communications	2 %
Produits de consommation	4 %
Défense et aéronautique	1 %
Éducation et recherche	3 %
Énergie et services publics	7 %
Divertissements et média	3 %
Services financiers	15 %
Santé et pharmaceutique	8 %
Hôtellerie	6 %
Fabrication et industrie	9 %
Secteur public	13 %
Vente	7 %
Services	9 %
Technologie et logiciels	6 %
Transport	4 %
Autre	0 %
Total	100 %

D4. Quel est l'effectif total de votre enterprise ?	FR
Moins de 500	14 %
Entre 500 et 1 000	21 %
Entre 1 001 et 5 000	35 %
Entre 5 001 et 25 000	19 %
Entre 25 001 et 75 000	8 %
Plus de 75 000	2 %
Total	100 %

À propos de Ponemon Institute

La mission de Ponemon Institute© est d'améliorer et de rendre plus responsable les pratiques de gestion de la confidentialité et des informations dans les entreprises et les gouvernements. Pour atteindre cet objectif, l'institut mène des études indépendantes, éduque les dirigeants des secteurs privé et public et vérifie les pratiques de confidentialité et de protection des données dans diverses industries.

À propos de Thales eSecurity

Thales eSecurity est un leader dans le domaine des services et solutions de sécurité des données avancés qui génèrent de la confiance quel que soit l'endroit où l'information est créée, partagée ou stockée. Nous garantissons la sécurité et la fiabilité des données des entreprises privées et des administrations publiques où qu'elles se trouvent, aussi bien dans les locaux physiques, le cloud, les centres de données ou les environnements big data, sans pour autant altérer la souplesse opérationnelle. La sécurité ne sert pas uniquement à limiter les risques, elle est le tremplin d'initiatives numériques qui font désormais partie de notre vie quotidienne, comme l'argent et les identités électroniques, les soins et les véhicules connectés et, avec l'avènement de l'Internet des Objets, même les appareils électroménagers. 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 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. Thales eSecurity appartient au groupe Thales.

À propos de Thales

Les personnes auxquelles nous faisons confiance pour diriger le monde font confiance à Thales. Nos clients sont très ambitieux : ils veulent nous faciliter la vie et nous protéger. À l'aide d'une combinaison d'expertise, de talents et de cultures, nos architectes créent d'extraordinaires solutions de haute technologie. Des solutions qui rendent le futur possible aujourd'hui. Des profondeurs des océans à l'infinité de l'espace et du cyber-espace, nous aidons nos clients à penser plus malin et à agir plus rapidement, afin de maîtriser un environnement toujours plus complexe à chaque moment décisif. Avec 65 000 employés dans 56 pays, Thales a enregistré des ventes de 15,8 milliards d'euros en 2017.

Platinum partner– Geobridge

Établie en 1997, la société GEOBRIDGE s'est établie comme l'un des premiers fournisseurs de solutions de sécurité des informations à prendre en charge la cryptographie et les applications de paiement pour les processeurs de paiement, les institutions financières et les enterprises de vente. Aujourd'hui, GEOBRIDGE est un leader dans le domaine des solutions de sécurité et de la conformité qui fournit des solutions et des services de cryptographie et de gestion des clés, de sécurité des paiements, de conformité et de virtualisation des HSMs à nos clients. Notre liste de clients inclut des entreprises de la liste Fortune 500, des institutions financières, des enterprises dans le secteur de la santé et des gouvernements du monde entier, dont l'Amérique du Nord. GEOBRIDGE s'appuie sur l'expertise de notre équipe dans la confidentialité des données, le développement de programmes, l'application et la gouvernance pour aider à créer des solutions afin de limiter les risques de nos clients.

Platinum partner – Venafi

Venafi est le leader sur le marché de la cyber-sécurité dans la protection de l'identité automatisée, et la sécurisation des connexions et des communications machine-machine. Venafi protège les types d'identité des machines en gérant des clés cryptographiques et des certificats numériques pour SSL/TLS, l'IoT, les mobiles et SSH. Venafi permet la visibilité mondiale de l'identité de machines et identifie les risques associés pour l'entreprise dans son ensemble (sur site, mobile, virtuel, cloud et IoT) à des vitesses et une échelle uniquement possibles grâce à l'automatisation. Venafi utilise ces informations pour mettre en place des contre-mesures automatisées qui réduisent les risques de sécurité informatique et de disponibilité liés aux identités de machine faibles ou compromises tout en protégeant le flux d'informations vers les machines de confiance et en empêchant la communication avec les machines qui ne sont pas sûres.

Avec un portefeuille de 31 brevets, Venafi fournit des solutions novatrices pour les 2 000 enterprises les plus exigeantes en matière de sécurité au monde. Venafi est soutenue par des investisseurs de haut niveau, dont Foundation Capital, Intel Capital, Origin Partners, Pelion Venture Partners, QuestMark Partners, Mercato Partners et NextEquity. Pour plus d'informations, consultez www.venafi.com.

THALES

www.thalesesecurity.com