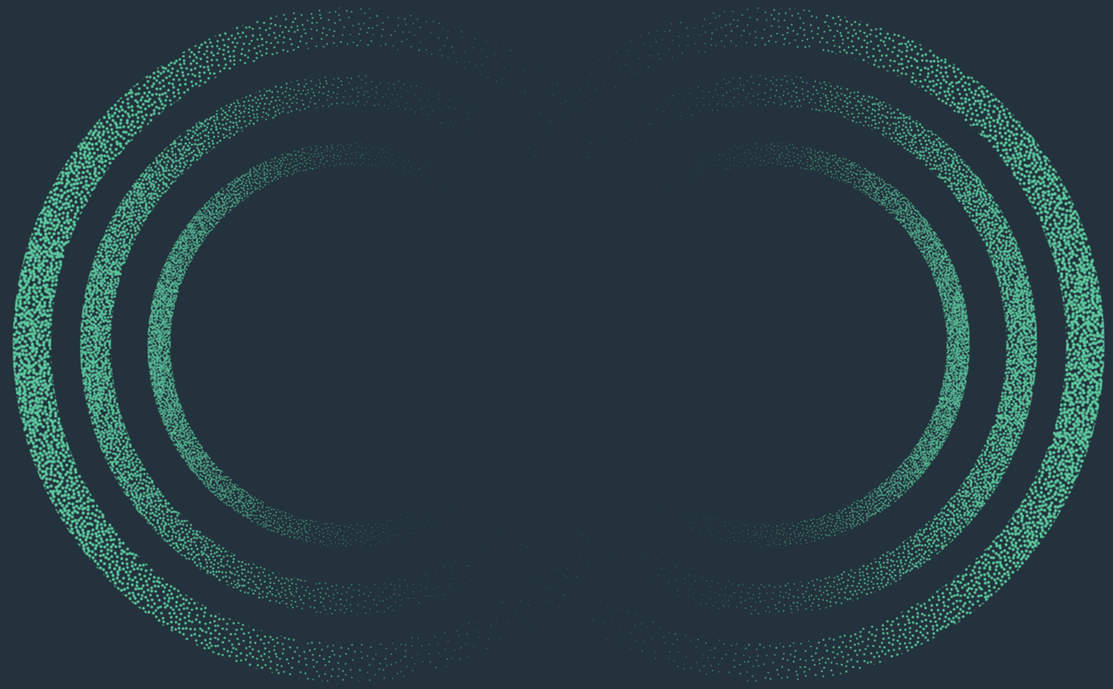
WithSecure™ Pulse 2023

IT et cybersécurité : tout savoir sur les dernières tendances

W / T H
secure

Sommaire



Résumé

Introduction

Notre étude de marché mondiale a été menée auprès de milliers de professionnels de l'informatique. Nous les avons questionnés sur leur emploi, leur entreprise et leurs priorités pour l'année à venir. Nous vous présentons ici les résultats de cette étude, pour vous aider à définir vos stratégies IT et sécurité pour l'année 2023, et au-delà.

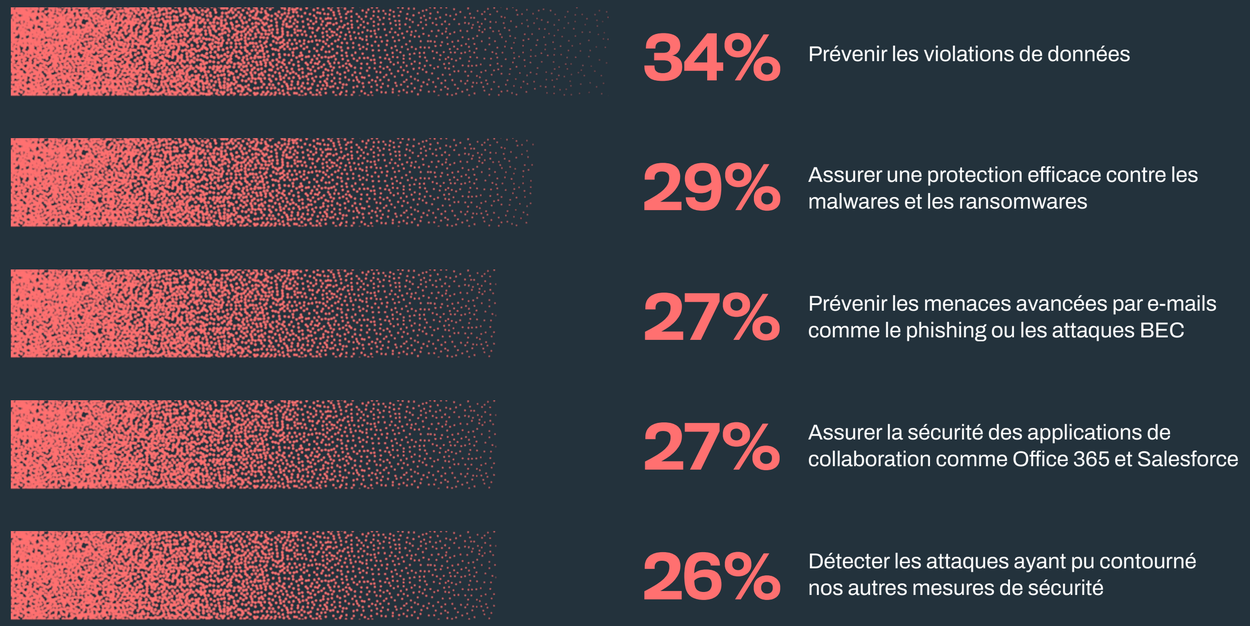
Au cours de cette étude, nommée Pulse 2023, nous avons interrogés 3 072 professionnels situés dans 12 pays : le Royaume-Uni, la France, l'Allemagne, la Belgique, les Pays-Bas, le Danemark, la Finlande, la Norvège, la Suède, les États-Unis, le Canada et le Japon. Tous les professionnels interrogés étaient des décideurs et des influenceurs IT, réseau ou cloud spécialisés en sécurité. Ils étaient responsables des achats de produits et de services de sécurité informatique pour leur entreprise.

Les priorités 2023 de la cybersécurité

Notre enquête Pulse 2023 a porté sur les priorités commerciales et techniques des responsables en sécurité, pour les 12 mois à venir. Le graphique ci-dessous illustre les 5 principales priorités évoquées.

Page 10, vous trouverez une section détaillée consacrée aux tendances observées dans notre étude Pulse 2023.

Les 5 grands défis techniques en matière de sécurité



34% Prévenir les violations de données

29% Assurer une protection efficace contre les malwares et les ransomwares

27% Prévenir les menaces avancées par e-mails comme le phishing ou les attaques BEC

27% Assurer la sécurité des applications de collaboration comme Office 365 et Salesforce

26% Détecter les attaques ayant pu contourné nos autres mesures de sécurité

« Un fait intéressant mérite d'être relevé. Les professionnels interrogés évoquent certaines priorités mais ils négligent celles qui font pourtant toute la différence en matière de cybersécurité : les compétences et l'expérience, qui font défaut à de nombreuses entreprises. »

Peter Page, WithSecure™, Head of Solution Consulting

Investir

La cybersécurité suscite de nombreux débats en entreprise, mais la question la plus fréquemment abordée est sans doute celle du budget. Les conseils d'administration s'interrogent : « Combien devons-nous dépenser pour la sécurité ? Existe-t-il un montant suffisant ? Cela dépend-il du nombre de salariés que nous employons, de notre emplacement géographique, de notre secteur ? Nos concurrents sont-ils eux aussi préoccupés par les questions de cybersécurité ? Quelle part de leur budget y consacrent-ils ? »

Nos recherches offrent quelques éclairages intéressants sur les choix d'investissement en matière de cybersécurité. Les données suggèrent que plus les entreprises font évoluer leur stratégie de sécurité, moins le coût représente un critère important.

86% des professionnels interrogés déclarent que les investissements de leur entreprise en matière de cybersécurité vont augmenter dans les 12 mois à venir.

« Je dis toujours qu'il faut commencer avec un minimum absolu de 5 %. Mais il n'y a pas de maximum : plus la sécurité est vitale pour l'entreprise, plus ce pourcentage est élevé. Et vice versa. »

Teemu Myllykangas, Director, B2B Product Management chez WithSecure™

« Les entreprises doivent décider du niveau de sécurité qu'elles souhaitent atteindre. Elles doivent déterminer quel niveau de risque elles sont prêtes à accepter, et quel degré de perturbation de l'activité elles peuvent tolérer. Une fois ces critères établis, des décisions rationnelles concernant les dépenses de sécurité peuvent être prises. »

Paul Brucciani, Head of Product Marketing chez WithSecure™

Résidence des données

Notre enquête 2023 Pulse a montré que les professionnels IT ont des opinions bien arrêtées sur le lieu où leur entreprise doit stocker et traiter les données. Ce n'est pas surprenant : les réglementations sont particulièrement nombreuses ; et les détournements de données sont un sujet particulièrement sensible.

Pour autant, les opinions peuvent diverger selon la taille de l'entreprise, son secteur, et sa localisation géographique.

Comment atteindre un consensus sur le traitement des données ? Dans quelle mesure la politique de résidence des données affecte-t-elle la relation client ?

Des désaccords peuvent apparaître au sein d'une même entreprise ; et des conflits peuvent émerger entre les décideurs IT et les influenceurs IT. Il est capital de résoudre ces désaccords. En matière de protection de la vie privée, il n'y a pas de place pour l'erreur.

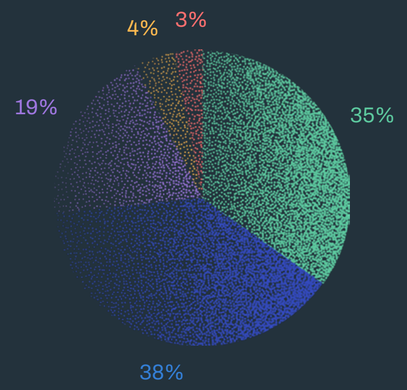
« La résidence des données est un paramètre qui doit désormais être pris en compte. Voici un exemple : un client se soucie des questions de sécurité nationale et vous, en tant que start-up, lui avez fourni votre logiciel as-a-service en mobilisant des fournisseurs de services cloud américains. Pouvez-vous poursuivre dans cette voie ? Ou devez-vous rechercher une solution alternative ? Il est important de réfléchir à ce type de questions. »

Albert Koubov Gonzalez, Consultant, WithSecure™

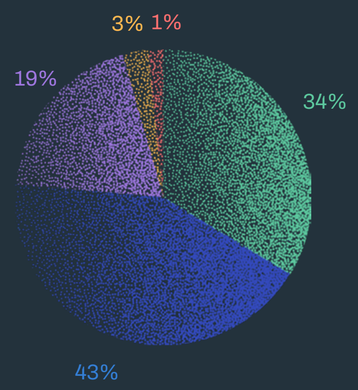
Le stockage des données

Au regard de votre poste, quelle importance revêt l'emplacement géographique pour le traitement de vos données ?

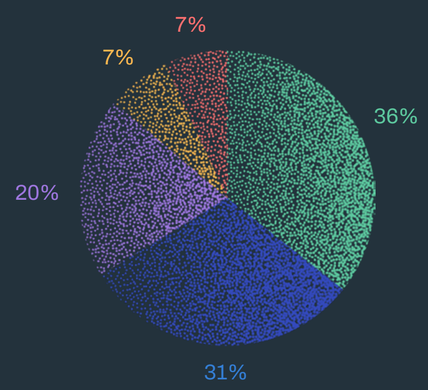
Total



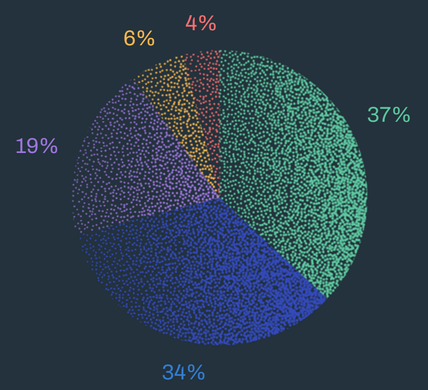
Décideurs IT



Influenceurs IT



Cadres supérieurs



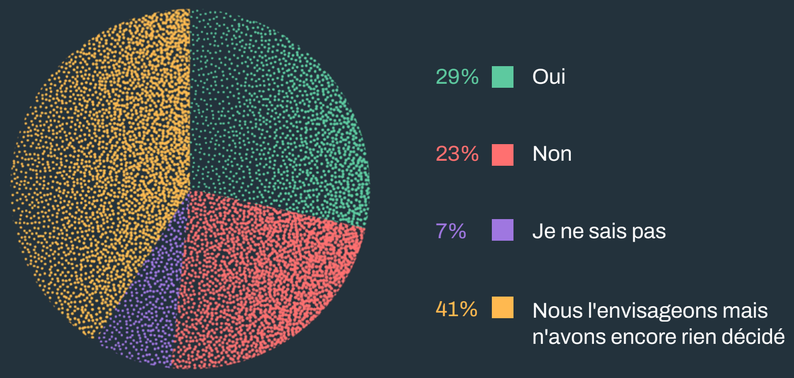
- Les données doivent être traitées dans le même pays que nos activités.
- Les données doivent être traitées dans la même région que nos opérations (par exemple, l'UE, l'Amérique du Nord, l'APAC).
- L'endroit où nous traitons les données de nos clients finaux n'a pas d'importance, tant que toutes les exigences légales et de conformité sont respectées.
- Nous ne traitons pas les données des clients finaux.
- Je ne sais pas

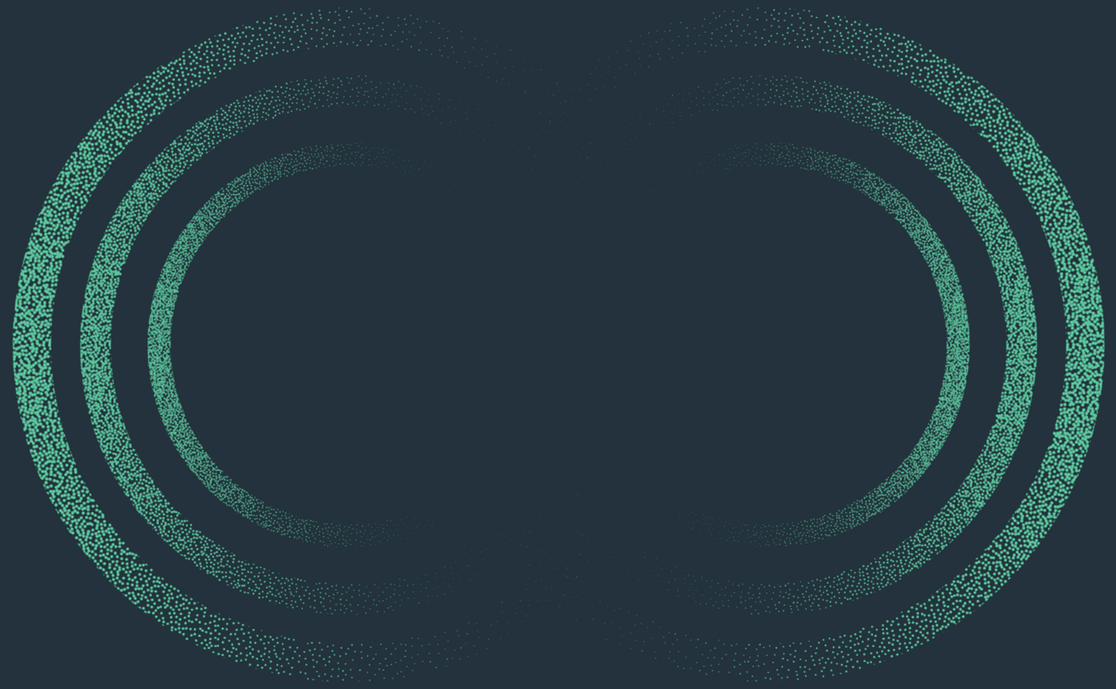
Changer de fournisseur

Changer de fournisseur de sécurité est un exercice difficile. Une telle entreprise exige du temps et des ressources. Pour autant, dans notre enquête Pulse 2023, 30 % des professionnels interrogés ont indiqué avoir changé de fournisseur au cours des six derniers mois, et 30 autres % prévoient de le faire au cours des six prochains mois.

Une vague massive de migration des fournisseurs est donc en cours. Pourquoi ? Quel est le coût d'une telle initiative ?

Votre entreprise/organisation prévoit-elle de changer de solution/fournisseur de sécurité informatique d'entreprise au cours des six prochains mois ?

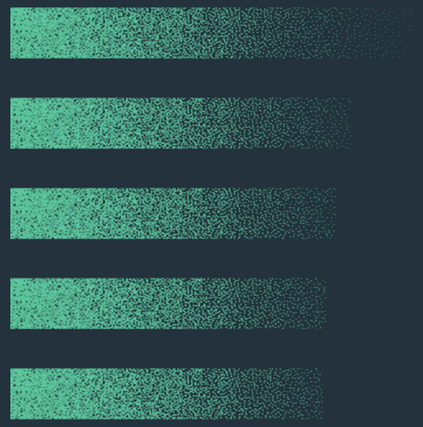




1. Les priorités 2023 de la cybersécurité

Les priorités techniques en matière de sécurité

Les principales priorités techniques



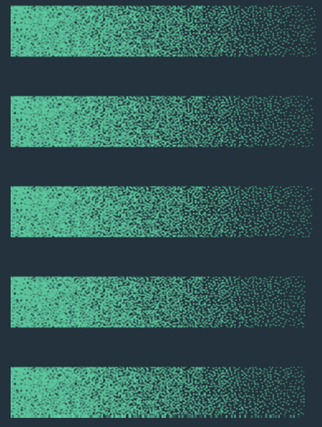
34% Prévenir les violations de données

29% Assurer une protection contre les malwares et les ransomwares

27% Prévenir les menaces avancées par e-mail comme les attaques de phishing et les attaques BEC.

27% Assurer la sécurité des applications de collaboration cloud (Office 365, Salesforce).

26% Assurer la sécurité d'un écosystème de plus en plus diversifiés (appareils, services, logiciels...)



26% Détecter les attaques ayant pu contourner nos autres mesures de sécurité

26% Assurer une protection continue contre les menaces 0-day

25% Assurer la sécurité de l'infrastructure/des plateformes de cloud public (Azure, AWS, ...)

25% Prévenir ou limiter les menaces émanant d'initiés malveillants

25% Veiller à ce que tous les correctifs et autres vulnérabilités logicielles soient traités correctement

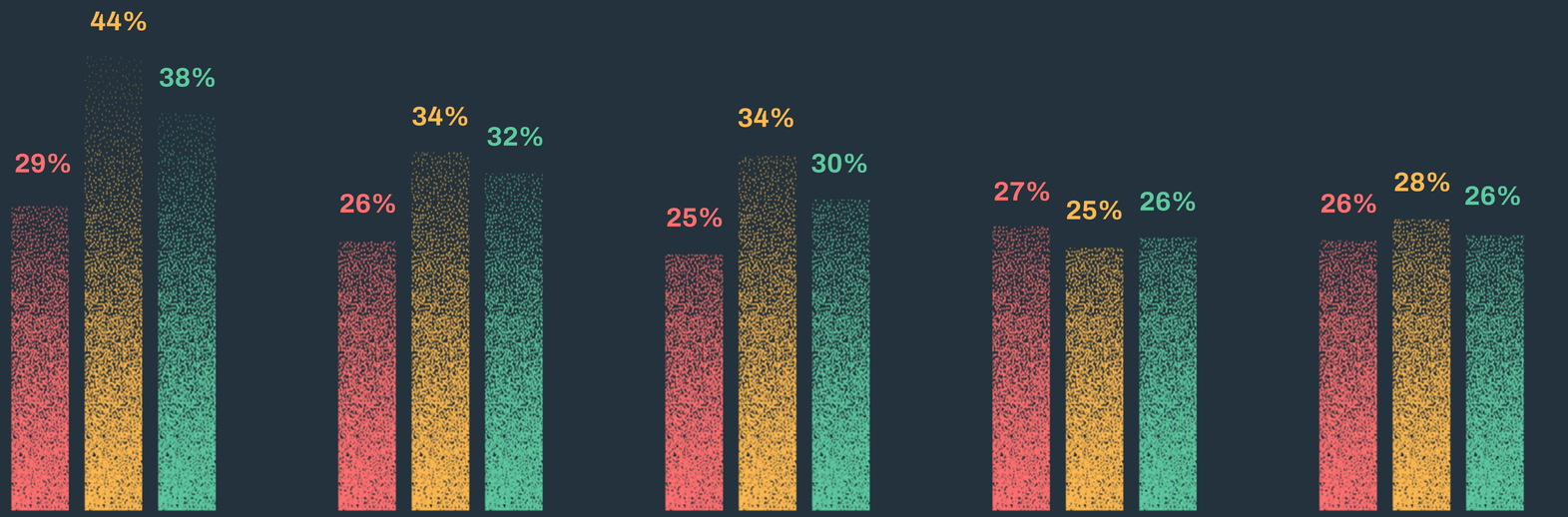
Les priorités techniques font consensus. Le plus grand défi est, sans surprise, la prévention des violations de données (33,7 %). La prévention des menaces par e-mail et la sécurité des applications de collaboration cloud figurent également en bonne place sur la liste. Les autres priorités retenues concernent généralement la détection et la réponse aux menaces.

« Parmi les priorités qu'ils mentionnent, les professionnels interrogés oublient celles qui font la différence en matière de cybersécurité : les compétences et l'expérience, qui font défaut à de nombreuses entreprises. Tout le monde cherche à prévenir les attaques via des solutions EDR ou via des services de consulting mais ces deux éléments sont cruciaux. Le système EDR doit être mis en place en plus du système EPP afin de créer une solution étanche. Les éléments « Business as Usual » peuvent avoir un impact positif durable mais ils sont négligés parce qu'ils doivent être implémenté en interne et qu'ils demandent souvent beaucoup de travail. Créer une culture de la sécurité n'est pas quelque chose que l'on peut externaliser. »

— Peter Page, Head of Solution Consulting chez WithSecure

Les 5 principaux défis techniques 2022/3, en fonction du poste occupé

- Décideurs IT
- Influenceurs IT
- Cadres supérieurs



Prévenir les violations de données

Assurer une protection contre les malwares et les ransomwares

Prévenir les menaces avancées par e-mail comme les attaques de phishing et les attaques BEC (Business Email Compromise)

Assurer la sécurité des applications de collaboration cloud (Office 365, Salesforce)

Assurer la sécurité d'un écosystème de plus en plus diversifiés (appareils, services, logiciels...)

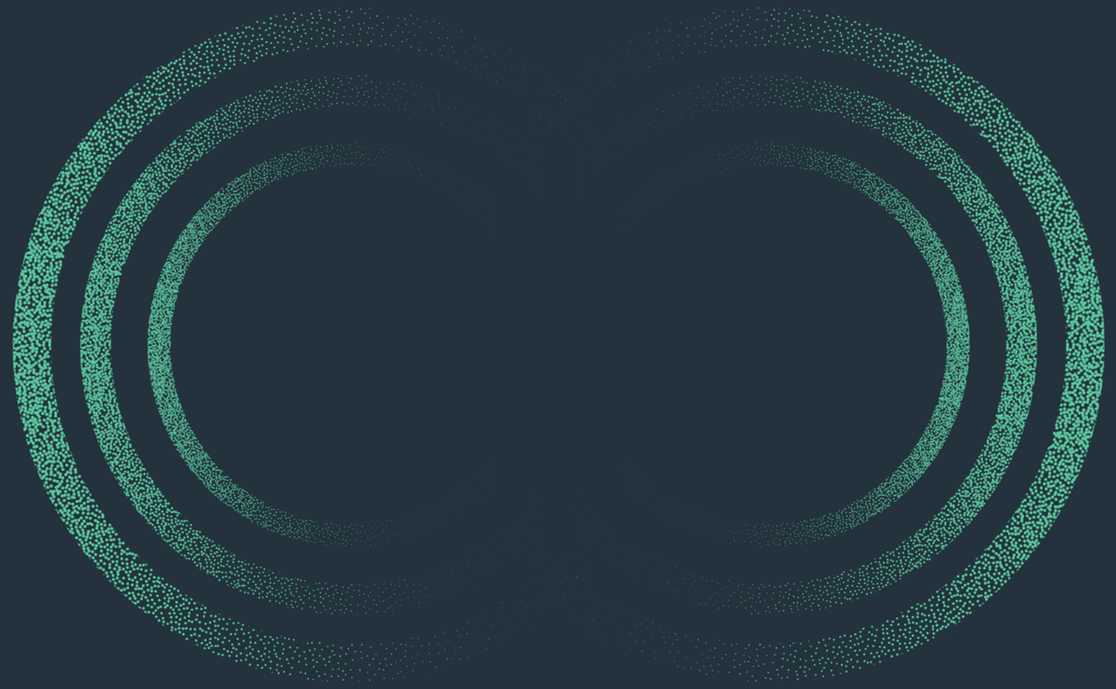
Ces données montrent dans quelle propension les cinq principales priorités sont identifiées comme telles par les décideurs informatiques, les influenceurs informatiques et les cadres supérieurs. Nous assistons à un large consensus. Certaines divergences existent toutefois, par exemple entre décideurs et influenceurs informatiques concernant la prévention des violations de données. Les entreprises doivent donc veiller à ce que tous les membres de leur équipe de sécurité soient bien sur la même longueur d'onde.

Les priorités commerciales liées à la sécurité

Principaux enjeux commerciaux

« Les inquiétudes portent notamment sur la sécurisation des télétravailleurs. Ce n'est pas une surprise. L'année 2020 a été marquée par un changement massif des modes de travail. Les entreprises ont dû s'adapter. Elles ont mené des projets d'envergure impliquant un changement d'architecture informatique (par exemple, la migration vers le cloud) tout en misant sur la formation des employés. La sécurisation du travail à distance constitue une priorité aujourd'hui, mais j'espère que lorsque cette enquête sera répétée en 2024-2025, la plupart des entreprises auront bel et bien domestiqué ces nouvelles méthodes de travail. »

— Peter Page, Head of Solution Consulting chez WithSecure



2. Investir

Quel budget consacrer à la sécurité ?

C'est une question que se posent des milliers d'entreprises partout dans le monde. Quelle part de votre budget informatique doit être consacrée à la cybersécurité ?

Le marché mondial de la sécurité de l'information devrait atteindre 174,7 milliards de dollars d'ici 2024. Ce chiffre témoigne de l'importance croissante de la cybersécurité. Face aux cybermenaces en augmentation, les entreprises réagissent en investissant davantage dans la sécurité.

Les attaques deviennent de plus en plus sophistiquées, le télétravail s'impose en entreprise et la situation géopolitique mondiale connaît de nombreux soubresauts. Dans un tel contexte, quel est le niveau de sécurité suffisant ? Et quel en est le prix ?

L'étude de WithSecure a révélé que 87,9 % des entreprises européennes prévoient d'augmenter leur budget de sécurité au cours des 12 prochains mois. À l'inverse, 8,3 % estiment être suffisamment protégées ou chercheront activement à réduire leurs dépenses de cybersécurité.

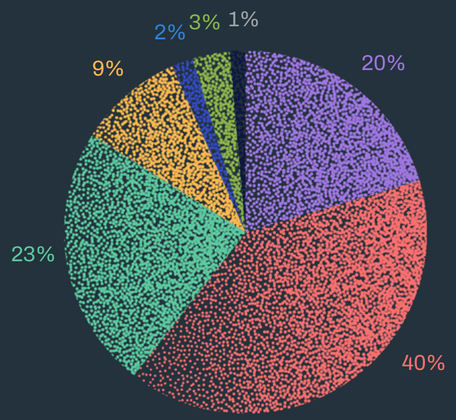
En entreprise, les opinions semblent diverger sur l'utilisation du budget. Les décideurs informatiques et les cadres supérieurs semblent globalement en phase mais les influenceurs informatiques présentent des aspirations différentes. Veillez à ce qu'une communication efficace et claire règne au sein de votre entreprise, pour éviter toute confusion ou décision de dernière minute.

Teemu Myllykangas, B2B Product Management chez WithSecure™, a pris la mesure des difficultés auxquelles sont confrontées les organisations : « *Lorsque vous demandez à une entreprise si elle dépense suffisamment, elle peine à répondre : si elle répond par l'affirmative, toute violation de données lui reviendra en pleine figure, car les clients voudront savoir comment une intrusion a pu avoir lieu malgré tout. Si elle répond non, les clients douteront de son sérieux. Il n'existe pas de réponse facile à une telle question. Les fournisseurs qui affirment le contraire vous mentent et tentent de vous vendre de faux remèdes miracles.* »

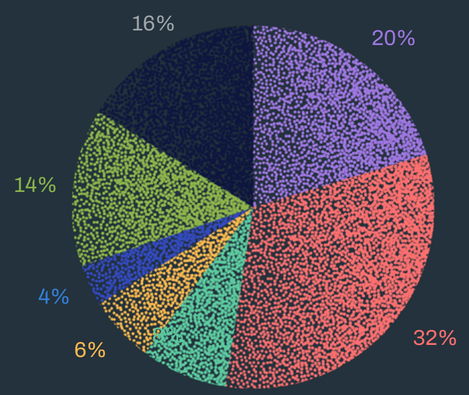
Dans le secteur, il est généralement admis que les entreprises consacrent chaque année entre 3 % et 15 % de leur budget à la sécurité. Lorsque des clients demandent à Teemu Myllykangas où ils doivent placer la barre, celui-ci se montre prudent. « *Je dis toujours qu'il faut commencer par un minimum absolu de 5 %. Et il n'y a pas de maximum : plus la sécurité est vitale pour le client, plus ce pourcentage est élevé. Et vice versa. J'ai l'habitude de décomposer le processus de budgétisation en trois étapes : 1./ mener une évaluation des risques et une modélisation des menaces pour définir le retour sur investissement ; 2/ Choisir comment utiliser le budget en se basant sur des cadres de références reconnus ; 3/ Revoir ces deux premières étapes chaque année, pour identifier les baisses de retour sur investissement et gérer le budget.* »

Intentions relatives au budget, par poste occupé

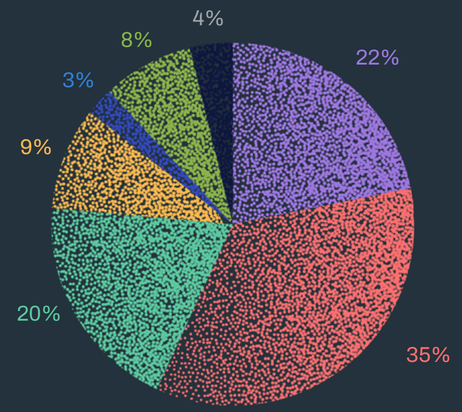
Décideurs IT



Influenceurs IT



Cadres supérieurs



- Au cours des 12 prochains mois, notre budget augmentera de 1 à 5 %
- Au cours des 12 prochains mois, notre budget augmentera de 6-10%
- Au cours des 12 prochains mois, notre budget augmentera de 11 à 15 %
- Au cours des 12 prochains mois, notre budget augmentera de plus de 15 %
- Au cours des 12 prochains mois, notre budget diminuera
- Au cours des 12 prochains mois, notre budget n'augmentera ni ne diminuera.
- Je n'en sais rien

L'évaluation des risques, un facteur crucial

« Il est difficile d'établir une règle simple permettant de déterminer si les dépenses de sécurité sont suffisantes. Les variables sont extrêmement nombreuses. Selon les circonstances, la part du budget IT alloué à la sécurité peut grandement varier. Il y a environ cinq ans, les dépenses de sécurité représentaient environ 10 % du budget informatique d'une entreprise, mais ce chiffre a augmenté depuis. Les entreprises pour lesquelles la sécurité est cruciale y consacrent environ 12 à 15 % de leur budget IT », explique Paul Brucciani, Head of Product Marketing chez WithSecure™.

La première question que vous devez vous poser est la suivante : quelles sont les menaces qui vous guettent ?

Si le pire scénario devait se produire, quelles en seraient les conséquences ? Vous devez chiffrer les pertes potentielles (ALE - Annual Loss Expectancy) et évaluer la probabilité d'une telle situation.

Les entreprises peinent généralement à répondre à ces questions et c'est là qu'intervient WithSecure™. Grâce à notre grande expérience en réponse aux incidents, nous pouvons corréler l'ALE et les facteurs de risques pour déterminer le budget à consacrer à la sécurité.

« Une fois que vous avez identifié vos risques, vous devez déterminer comment les gérer. Trois options existent : premièrement, vous pouvez transférer les risques, en souscrivant, par exemple, à une cyberassurance. Deuxièmement, vous pouvez réduire les risques en utilisant des contrôles, des technologies et des services de sécurité appropriés. Enfin, vous pouvez tout simplement accepter les risques, vivre avec et gérer les problèmes lorsqu'ils se produisent », poursuit Paul Brucciani.

« Lorsque vous choisissez de minimiser les risques, vous devez décider de la part du budget à allouer à la sécurité. Il vous faut évaluer la capacité de l'entreprise à absorber l'impact d'une attaque, et décider du niveau de risque que vous êtes prêt à accepter », conclut-il.

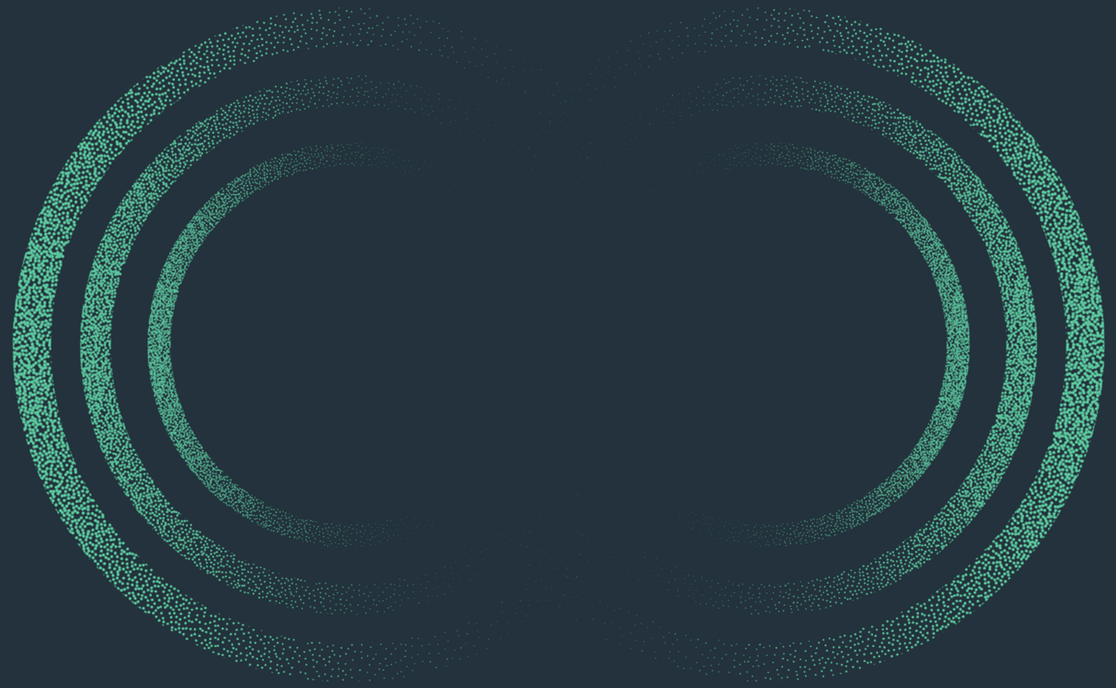
Le directeur financier de votre entreprise doit se prononcer sur ces questions. Ce n'est qu'ensuite que vous pourrez déterminer le budget et son utilisation.

Ce n'est pas juste une question de coût

La sécurité n'est pas seulement une question de budgétisation. Les résultats de notre enquête sont là pour en témoigner : seuls 13,2% des professionnels interrogés ont déclaré que le prix était leur principal critère au moment de choisir un fournisseur. En revanche, pour 21,8 %, le support 24h/24, 7j/7 constitue le facteur le plus important. Et pour 16,7 %, la confiance envers le fournisseur est le critère le plus décisif.

Il n'existe, certes, pas de formule miracle permettant de déterminer le budget à allouer à la cybersécurité, mais WithSecure™ peut vous aider en vous proposant une démarche logique, pour fournir à votre entreprise le niveau de protection optimal. Même si le prix reste un enjeu important, la sécurité va bien au-delà du résultat financier.

WithSecure™ Elements peut vous aider à réduire les risques et à optimiser votre sécurité. Cette approche combine de puissantes capacités de sécurité prédictives, préventives et réactives, toutes gérées et monitorées par un centre de sécurité unique.

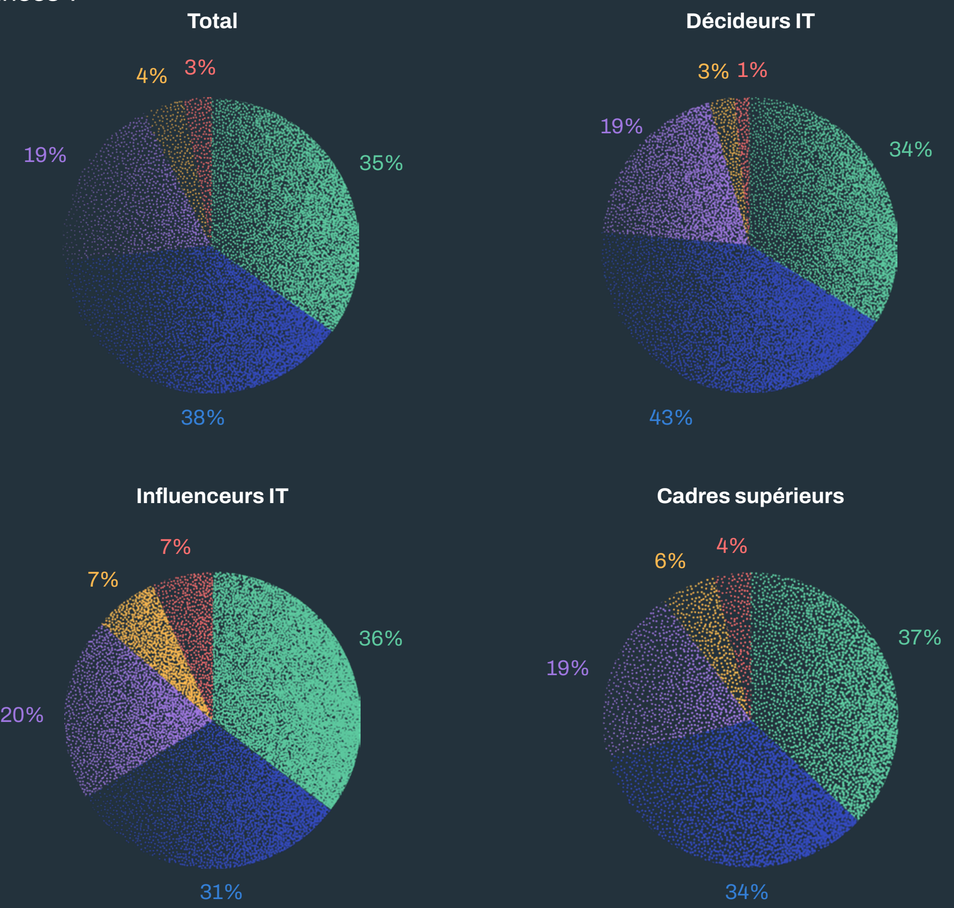


3. La résidence des données

Savez-vous où se trouvent vos données ?

Les résultats de notre enquête Pulse 2023 montrent que les professionnels accordent une grande importance à l'endroit où leurs données sont stockées et traitées. Près de 73% déclarent que les données doivent être traitées dans leur pays ou région d'activité. Moins d'un cinquième considère cette question sans importance.

Quelle importance accordez-vous à l'emplacement géographique du traitement des données ?



- Les données doivent être traitées dans le même pays que nos opérations.
- Les données doivent être traitées dans la même région que nos opérations (par exemple l'UE, l'Amérique du Nord, l'APAC).
- L'endroit où nous traitons les données de nos clients finaux n'a pas d'importance, à condition que toutes les exigences légales et de conformité applicables soient respectées.
- Nous ne traitons pas les données de nos clients finaux.
- Je ne sais pas

Où gardez-vous les données ?

Dans ces réponses, un décalage est apparu. 42,8% des décideurs informatiques exigent un traitement régional des données, contre seulement 30,9% des influenceurs informatiques. Soit la question du traitement régional/national n'est pas tranchée, soit les professionnels ont des priorités différentes selon le poste qu'ils occupent.

Plus une entreprise est grande, plus il semble que les professionnels privilégient un traitement régional des données.

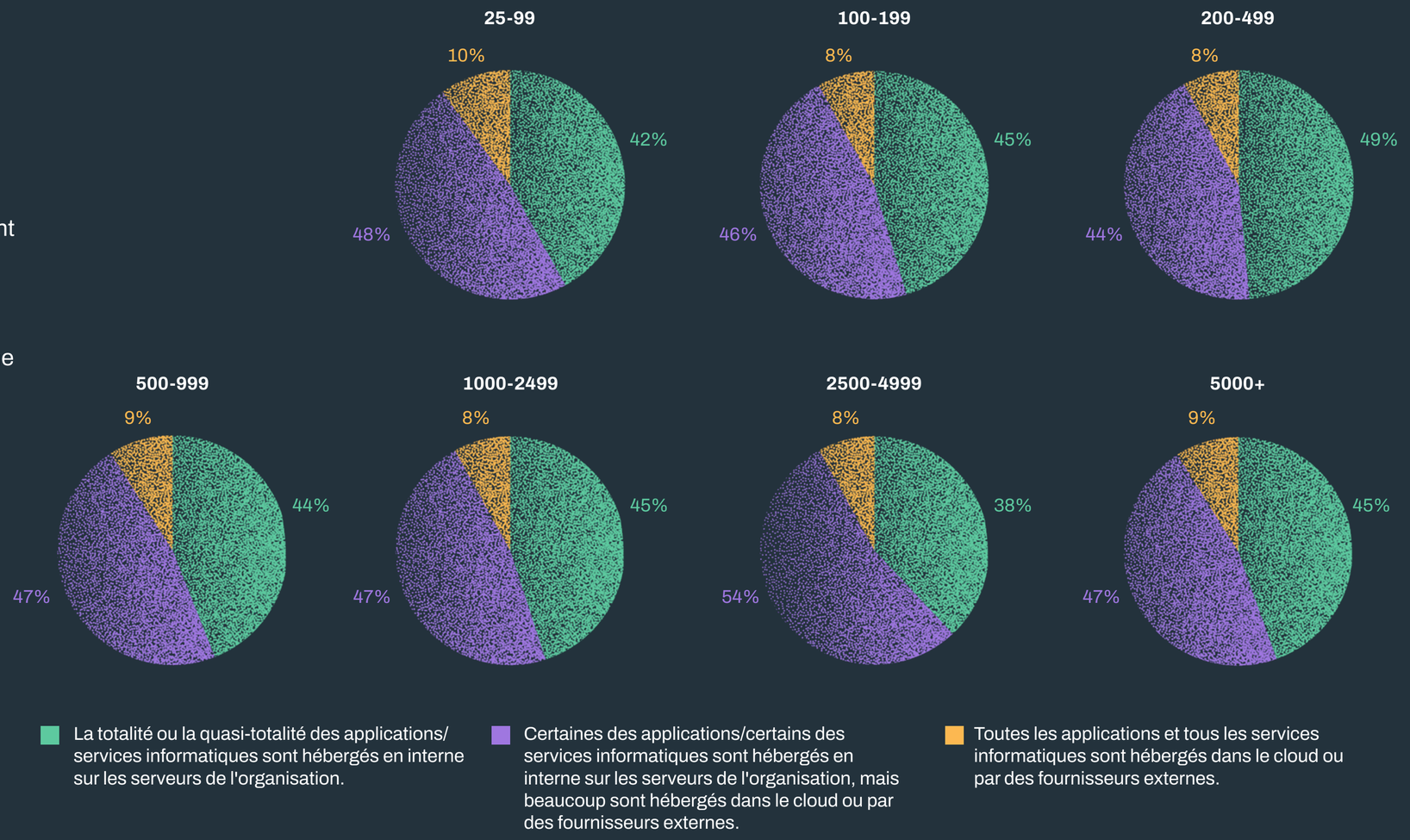
Cette tendance à privilégier une stricte résidence des données est sans doute liée aux évolutions réglementaires et aux événements récents. La souveraineté des données - c'est-à-dire les règles selon lesquelles les pays traitent les données à l'intérieur de leurs frontières - est soumises à bien des influences contradictoires : mondialisation du traitement des données, réglementations régionales, géopolitique, guerres et la réduction des risques. Dans un tel contexte, les entreprises prêtent une attention particulière à l'emplacement des données et aux endroits où elles circulent.

Traitement des données

Les données, ici, peuvent sembler contre-intuitives. Il est communément admis que le cloud a tout changé. Pourtant, il ne semble pas influencer les déclarations des professionnels interrogés.

Les chiffres restent similaires pour les approches cloud et on-premise. Les entreprises de plus de 2 500 employés sont légèrement plus susceptibles d'héberger des applications on-premise. Les entreprises américaines favorisent également cette approche, tandis que les danois, les suédois, les allemands et les britanniques préféraient souvent le cloud. Enfin, entre 6,2 et 12,1% des professionnels interrogés se montrent particulièrement avant-gardistes, avec une approche 100% cloud.

Environnement IT, selon la taille des entreprises

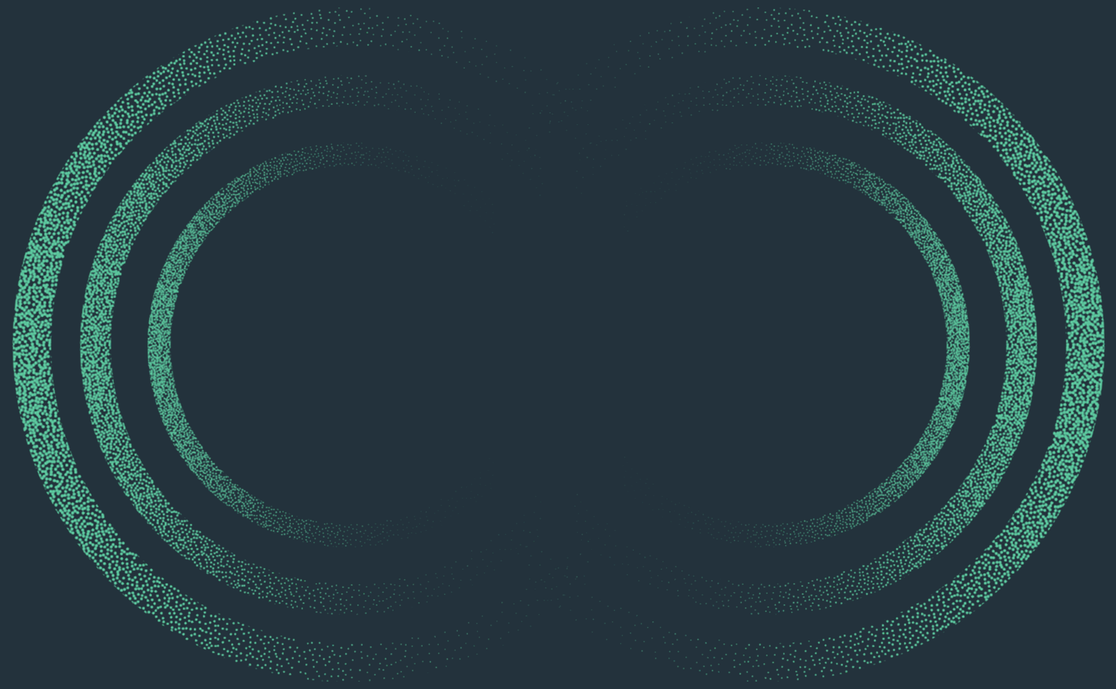


Conclusions et recommandations

Les entreprises accordent une grande importance à la résidence des données. Nos clients nous l'ont fait savoir, et pour répondre à leurs attentes, nous avons même lancé une version « Europe-only » de notre service Countercept MDR. La présente enquête Pulse 2023 confirme cette tendance : il existe bien un consensus sur le rôle majeur de la résidence des données.

Les entreprises doivent à la fois répondre aux attentes de leurs clients et satisfaire aux exigences réglementaires. C'est un travail difficile. Certaines organisations choisissent d'abandonner le cloud au profit d'un stockage et d'un traitement local des données, mais une telle initiative s'accompagne de frais importants en matière de conformité, de sécurité et de contraintes technique. Si vous vous engagez une telle démarche, nous vous conseillons dans un premier temps de veiller au respect des exigences réglementaires nationales en matière de protection des données, pour ensuite intégrer les préoccupations et exigences de vos clients.

Ne négligez pas la communication interne. Il existe une certaine déconnexion entre, d'une part, la vision des décideurs informatiques, et d'autre part, celle des influenceurs et cadres supérieurs. Les entreprises doivent chercher à déterminer si des divergences existent en leur sein, et pourquoi.



4. Changer de fournisseur de cybersécurité

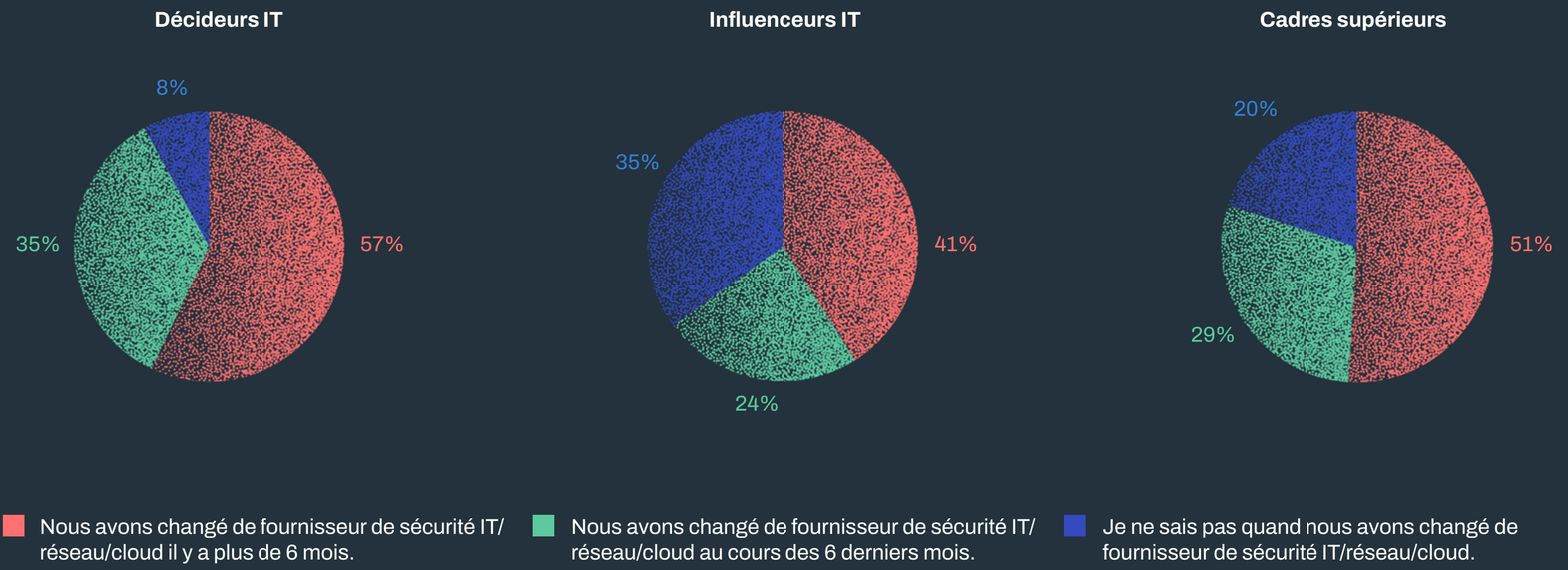
Les migrations sont fréquentes

En entreprise, la cybersécurité n'est jamais statique. Changer de fournisseur est devenu particulièrement fréquent.

D'après notre enquête, près d'un tiers (31,9 %) des professionnels interrogés ont changé de fournisseur au cours des six derniers mois, tandis que 32 % prévoient de changer de solution de sécurité ou de fournisseur au cours des six prochains mois.

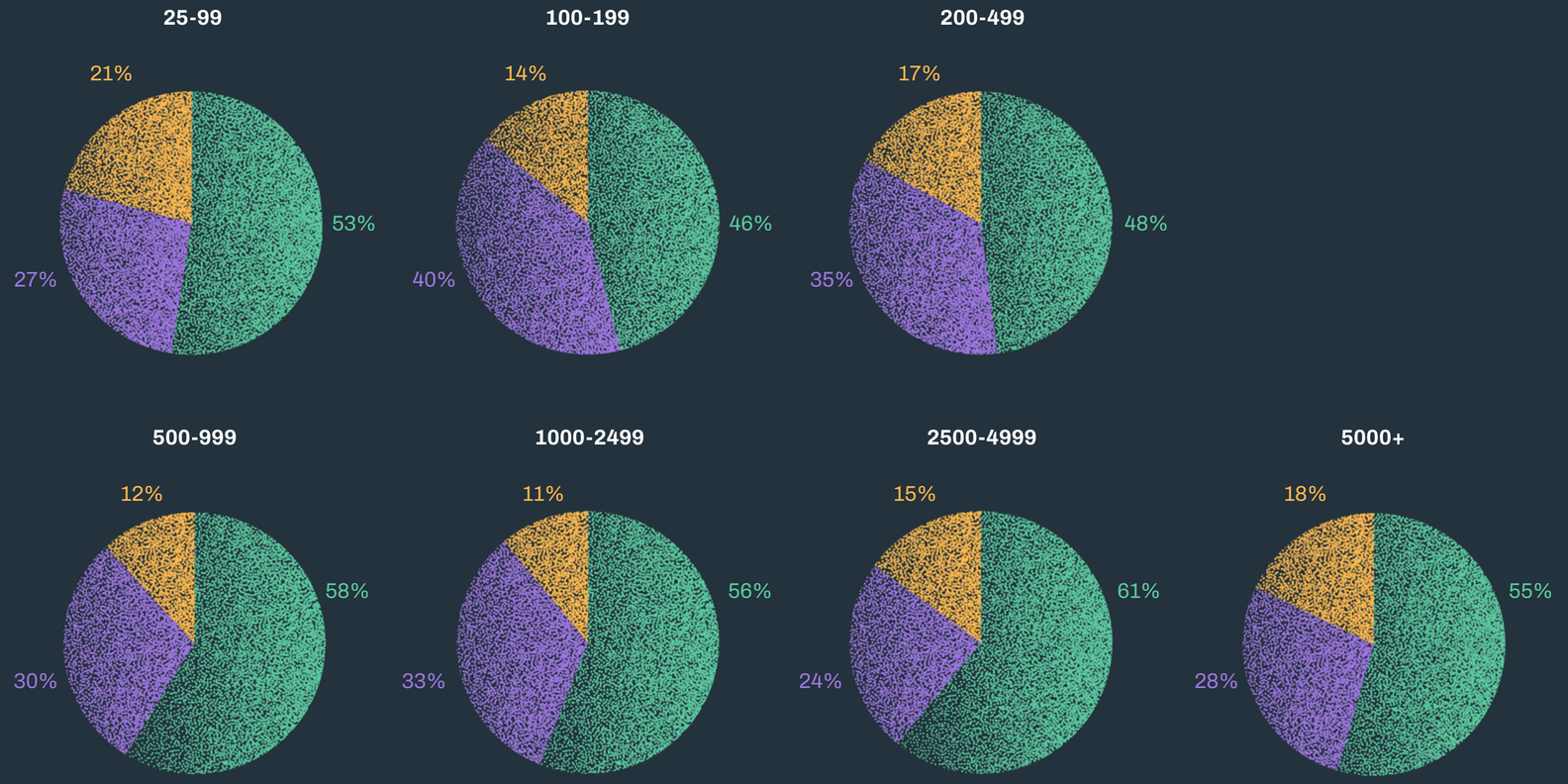
Les professionnels opérant dans la finance et les assurances ainsi que ceux travaillant dans les services IT sont les plus nombreux à avoir changé de fournisseur il y a plus de six mois (59,4 % et 58,4 % respectivement). Ils sont aussi plus nombreux à anticiper un changement dans les six prochains mois (45 % et 41,1 % respectivement).

Projet de changement de fournisseur, en fonction du poste occupé



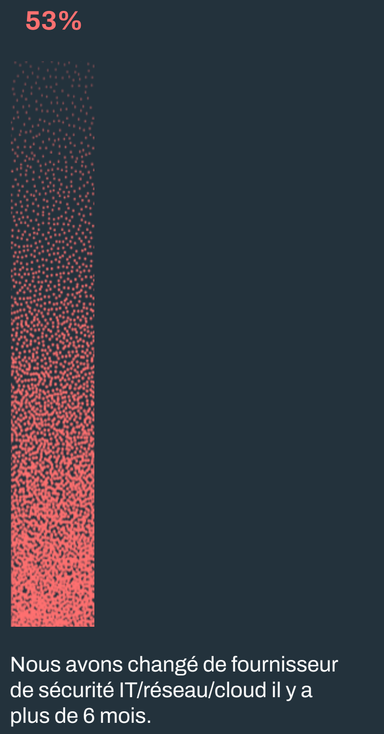
Du point de vue la taille des entreprises (n=1 800), le mouvement de migration est beaucoup plus évident pour les petites et moyennes structures que pour les grandes organisations.

Projet de changement de fournisseur, en fonction de la taille de l'entreprise

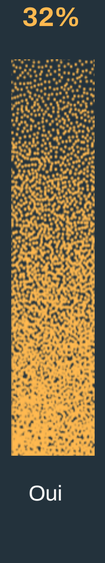


Les changements de fournisseurs sont donc particulièrement courants, mais ce processus reste compliqué et il prend du temps. Nous avons demandé à Peter Page, Head of Solution Consulting chez WithSecure, comment les entreprises pouvaient aborder au mieux ces changements de fournisseur. Nous lui avons également demandé quelle était la clé pour créer et maintenir la confiance entre les fournisseurs et leurs clients.

Changement de fournisseur de sécurité informatique/réseau/cloud



Votre entreprise prévoit-elle de changer de fournisseur de sécurité informatique au cours des 6 prochains mois ?



Quelles sont les craintes des clients au moment de changer de fournisseur ?

Les entreprises disposent souvent de ressources limitées ou restreintes. Changer de fournisseur peut alors leur demander trop d'investissement. En d'autres termes, il est parfois trop difficile de se libérer d'un fournisseur, même si ses prestations ne sont pas à la hauteur.

« Souvent, les équipes de sécurité ne sont pas celles qui implémentent les nouveaux services », explique Peter Page. *« Pour déployer des logiciels, elles doivent mobiliser les équipes de gestion de projet et les équipes IT. Elles doivent aussi faire appel aux équipes réseau car les changements affectent l'ensemble de l'entreprise. Elles doivent aussi obtenir l'adhésion de toutes les parties prenantes. »*

L'avènement des services cloud rend-il les changements de fournisseur plus faciles ?

Comme nous l'avons déjà évoqué, il est devenu plus facile de changer de fournisseur : les utilisateurs sont de plus en plus à l'aise à l'idée de passer d'un service cloud à un autre, bien plus qu'ils ne le sont avec l'idée de changer de service on-premise.

Pour Peter Page, ce phénomène est lié à une meilleure expertise du cloud. *« Il existe désormais de nombreux professionnels qui possèdent des compétences dans le développement, l'implémentation et la sécurisation du cloud. Les fournisseurs de sécurité doivent, eux aussi, disposer de ces compétences. Mais à mesure que le périmètre évolue, le service de sécurité doit évoluer lui aussi. C'est là que l'approche CSPM (Cloud Security Posture Management) entre en jeu. »*

Pourquoi la durée des contrats est-elle de plus en plus courte ?

La brièveté des contrats est sans doute liée à deux facteurs. Le premier renvoie aux produits et services proposés. Le second concerne les contrats des RSSI, généralement de courte durée : ils passent souvent moins de deux ans dans une entreprise, avant de la quitter.

Les arrivées et départs incessants de nouveaux RSSI engendrent des changements de caps, avec souvent, des changements de fournisseurs.

Il existe aussi un mouvement visant à toujours aller vers la nouveauté. Comme l'explique Peter Page, *« parfois, les ressources consacrées à l'achat de la toute dernière technologie à la mode feraient mieux d'être allouées à l'optimisation des composants de base »*

« Face à l'offre pléthorique, les entreprises peinent à choisir leur approche. Un RSSI qui s'engage dans un service pluriannuel coûteux doit être certain d'obtenir les résultats dont il a besoin, et que son conseil d'administration exige. »

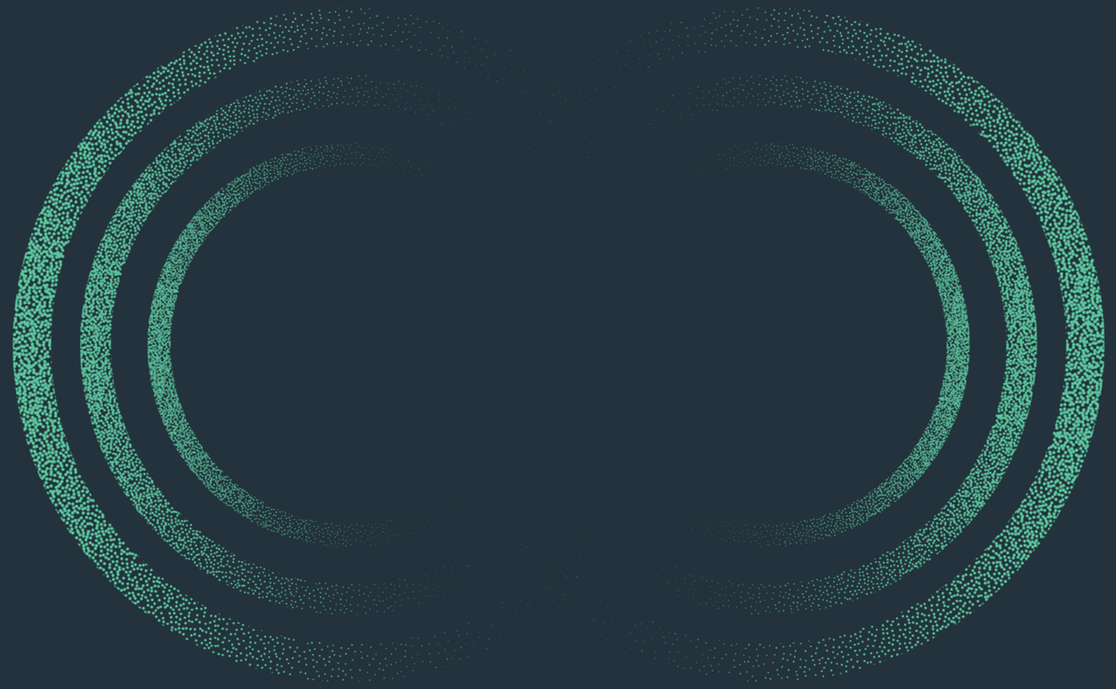
Pour les RSSI, changer de fournisseur est-il devenu plus facile, ou plus difficile ?

« Par le passé, il était difficile pour un RSSI d'obtenir l'aval du conseil d'administration pour investir dans la cybersécurité. C'est désormais plus facile : le conseil d'administration, le directeur financier et le PDG ont connaissance des intrusions informatiques et attaques ransomwares qui touchent de nombreuses entreprises. Ils sont désormais conscients de l'impact de financier d'une cyberattaque. »

« Mais, vu l'offre pléthorique, les RSSI doivent choisir entre une multitude d'options : où investir le budget ? Faut-il miser sur l'internalisation ou sur l'externalisation ? Qu'en est-il des solutions MDR, EDR, des SIEM ou du reste ? Les questions sont trop nombreuses. Les RSSI passent beaucoup de temps à faire des RDI, à discuter avec les fournisseurs... Cela devient un travail à plein temps » explique Peter Page.

L'importance du facteur temps

Pour autant, selon Peter Page, l'action est toujours préférable à l'inaction : « *Si vous ne disposez pas de la visibilité et du contrôle nécessaires sur votre écosystème, alors vous devez agir sans attendre. Si vous disposez déjà de services managés, alors la date limite est la fin du contrat. La question qui se pose alors est la suivante : à partir de quand peut-on commencer à évoquer un changement de fournisseur ? Les RSSI peuvent commencer à y réfléchir 12 mois avant la fin de leur contrat : c'est lorsqu'ils s'y prennent suffisamment en avance que nous observons les meilleurs résultats. »*



5. Conclusion

Cette enquête offre des résultats très riches sur les consensus et les divergences qui entourent la gestion des données personnelles. Certains résultats revêtent un caractère plutôt informatif, mais d'autres conclusions peuvent vous aider à gagner en efficacité.

Voici les principales idées à retenir. Certaines sont déjà claires pour les lecteurs avertis mais elles méritent d'être répétées.

1) En entreprise, ce que les professionnels perçoivent comme des priorités n'est pas toujours ce qui fait vraiment la différence. Vérifiez quelles compétences et quelles pratiques peuvent manquer à votre entreprise. Comparez-les aux priorités que vous avez définies, et recherchez les discordances.

2) Les perceptions divergent concernant les budgets de sécurité pour 2023. Ces divergences peuvent créer de la confusion, des conflits, et conduire à des décisions hâtives. Veillez à clarifier la question du budget. Chaque partie prenante doit avoir une idée de la marge de manœuvre dont elle disposera au cours de l'année prochaine pour effectuer des achats ou réaliser des changements.

3) La résidence des données est une préoccupation très présente. 70% des professionnels interrogés y voient une priorité absolue. Si vous envisagez d'abandonner une application cloud incapable de garantir la résidence des données, pensez à évaluer de près les alternatives. Une solution locale ou interne sera-t-elle aussi sûre ? Offrira-t-elle les capacités dont vous avez besoin ?

4) Si vous devez changer de fournisseur, veillez à anticiper. Les migrations réussies débutent au moins 12 mois avant l'expiration ou le renouvellement du contrat. Ne vous laissez pas paralyser par l'offre pléthorique : passez à l'action.

Nos données montrent un relatif consensus parmi les groupes interrogés, ce qui indique une bonne harmonie générale sur le plan organisationnel. Certains points suscitent toutefois des divergences significatives entre décideurs, influenceurs informatiques et cadre dirigeants. Ces domaines doivent retenir toute votre attention. Une communication claire sera votre outil le plus précieux pour cette année à venir.

Méthodologie

L'étude de marché B2B 2022 de WithSecure a été menée auprès de 3 072 professionnels (2 098 en Europe) par le biais d'une enquête en ligne réalisée au cours du mois de mai 2022 dans 12 pays dont les États-Unis, le Canada, le Japon et neuf pays européens : le Royaume-Uni, la France, l'Allemagne, la Belgique, les Pays-Bas, le Danemark, la Finlande, la Norvège et la Suède. Tous les professionnels interrogés étaient des influenceurs ou décideurs en sécurité informatique/réseau/cloud au sein de leur organisation.

Qui sommes-nous ?

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnements cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

W / T H®
secure