eBook

jumpcloud™

Les PME et l'IT

La gestion informatique face à la hausse des menaces de sécurité et aux tensions mondiales

Déterminés à proposer une expérience utilisateur sécurisée et de qualité, les responsables IT des PME doivent en parallèle endosser de nouvelles responsabilités et gérer les impacts des transformations internes et externes.

Synthèse de l’étude

Trois ans après le début de la pandémie, les entreprises doivent faire face à une somme de nouveaux défis, liés notamment aux tensions mondiales actuelles. Inflation, pénuries de talents, risque de récession, volatilité des marchés, conflits… constituent quelques-uns des impacts externes subis par les entreprises. Une pression permanente qui, associée aux préoccupations budgétaires et aux cyber-risques accrus, laisse peu de répit aux équipes IT et opérationnelles, et plonge les entreprises, PME en tête, dans un contexte d’incertitude.

Pour autant, cette situation ne semble pas entamer le moral des responsables IT pour la plupart optimistes et épanouis au travail. Un état d’esprit qui reflète la bonne santé globale des PME et surtout leur adaptation à la nouvelle réalité hybride du travail. Les équipes IT ne font pas exception. Elles ont en e□et su prouver leur capacité à protéger les ressources de l’entreprise et leur engagement à o□rir une expérience utilisateur haut de gamme.

Malgré le contexte VICA (Volatile, Incertain, Complexe, Ambigu) dans lequel elles évoluent, les clés de succès des PME reposent ainsi en grande partie sur les compétences de leur service IT. Si les équipes ont vu leur périmètre de responsabilité être considérablement élargi avec l’arrivée du travail à distance, leur capacité à administrer des environnements technologiques complexes, et à gérer des attaques de plus en plus nombreuses et sophistiquées participe pleinement à renforcer la compétitivité de l’organisation.

Au cours des trois dernières années, les équipes IT ont appris à s’adapter rapidement aux nouvelles informations, aux nouvelles technologies et aux nouveaux évènements mondiaux. Résultat, elles sont aujourd’hui plus agiles, mais aussi mieux préparées à l’inattendu et tournées vers la sécurité des employés, des appareils et des données.

C’est pourquoi, elles sont souvent le moteur qui alimente toute la PME. C’est pour mieux comprendre leur rôle et leur valeur que JumpCloud a décidé de réaliser cette étude. Objectif : obtenir une meilleure visibilité critique sur le ressenti, les responsabilités et le travail des professionnels du département IT.

Parmi les principaux points d’attention de l’enquête :

— La pression supplémentaire exercée au sein de la PME moderne et hybride par la complexité croissante des environnements internes et externes.

— Flexibilité, agilité et adaptabilité : les nouveaux maîtres mots face à l’augmenta0n51—hcFMd1toud(C □-5 (mépachbilitéernes.)]TJBDC 0.

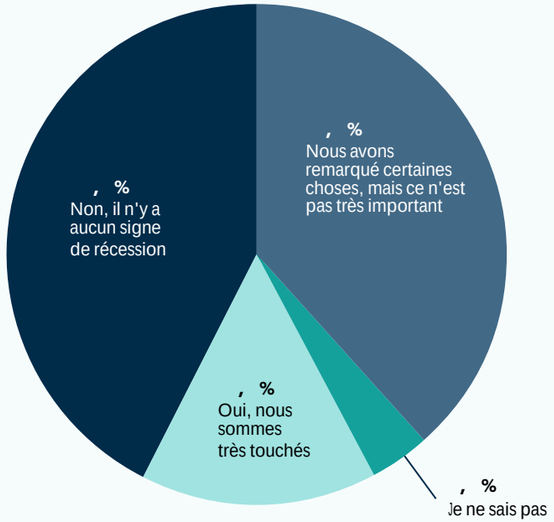
L’écosystème de la PME moderne

De l’incertitude à tous les niveaux

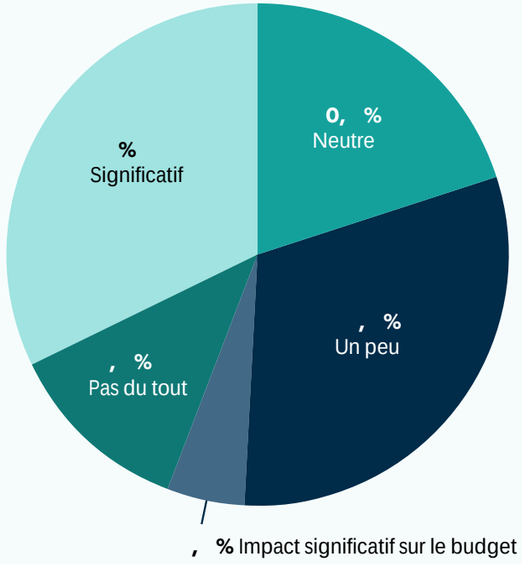
Bien que présentes depuis le début de l’année, les tensions sur les marchés mondiaux ont été ressenties de façon plus aigüe fin 2022. Par conséquent, les risques de récession n’épargnent pas les PME dont 57,3 % perçoivent un impact sur leur activité. Toutefois, celui-ci n’est jugé significatif que dans 15,4 % des cas.

Autre point d’inquiétude et non des moindres : les pénuries de compétences disponibles sur le marché. Près d’un tiers des responsables informatiques (31 %) signalent même que ce manque de talents a un impact important sur l’activité commerciale de leur entreprise. Ils sont également 31,8 % à en ressentir l’e□et limitateur sur leur activité.

Votre entreprise voit-elle des signes de récession ?



Les pénuries de talents ont-elles été un problème pour votre entreprise ?



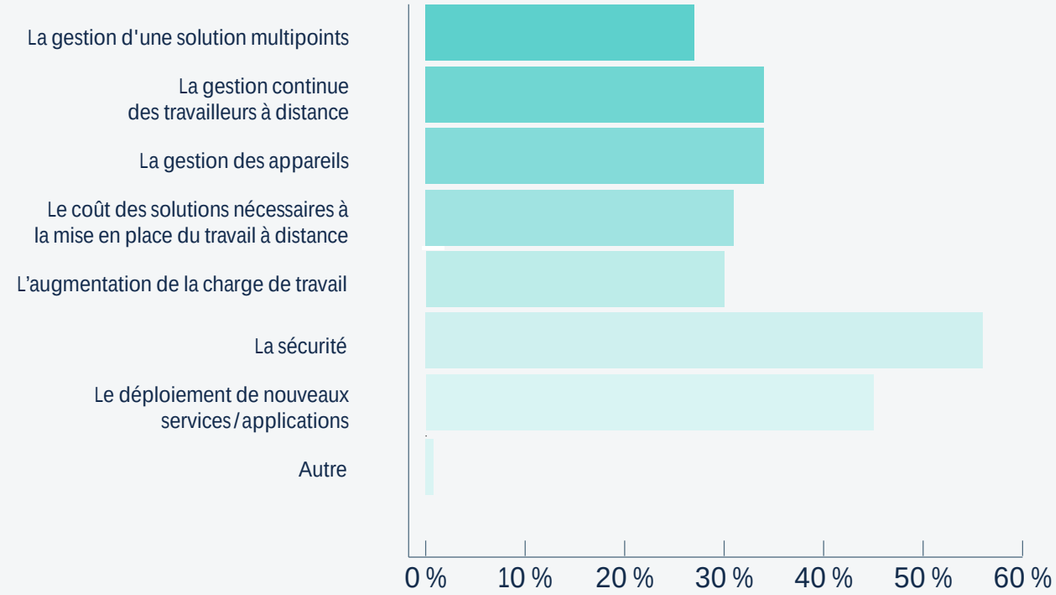
Malgré les nombreuses sources d'inquiétude et les risques de récession, les PME ont maintenu un haut niveau de dépenses. Tendance qui devrait être amenée à se poursuivre. Dans l'ensemble, 65,8 % des budgets IT devraient augmenter. Seuls 7,9 % s'attendent à le voir

Les enjeux de sécurité dans les PME

La hausse des menaces de sécurité, source de préoccupation

La sécurité continue d'être la principale préoccupation des responsables informatiques dans les PME : pour 55,8 % d'entre eux, il s'agit de leur plus grand défi en 2022.

Quel a été le plus grand défi pour votre équipe informatique en 2022 (sélectionnez les réponses qui s'appliquent) :



Les enjeux de sécurité dans les PME

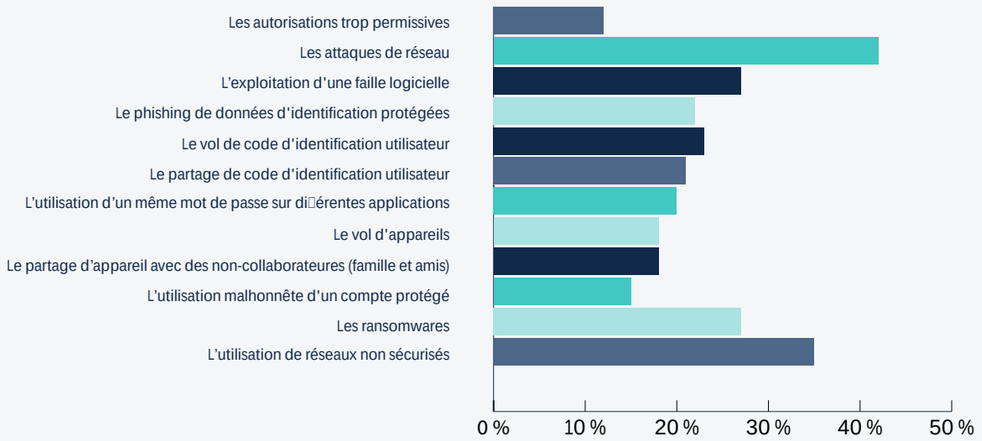
Une préoccupation constante vis-à-vis des menaces externes

Il n’est pas surprenant d’apprendre que les questions de sécurité préoccupent tant de responsables IT étant donné la multitude, la diversité et l’origine des menaces. En tête des principales sources d’inquiétude :

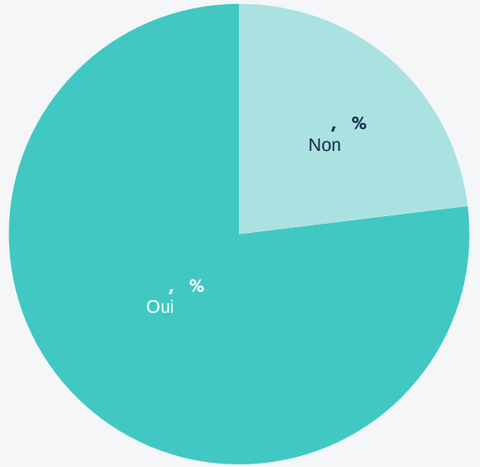
— Les attaques de réseau (44,9 %) ;
— Les ransomwares (35 %) ;
— Et l’utilisation de réseaux non sécurisés (27,9 %).

En parallèle, plus de 76 % (76,2 %) remontent également leur crainte d’attaques par fatigue MFA, un processus qui exploite la lassitude (et donc le manque de vigilance) des utilisateurs confrontés à un envoi massif de demandes d’authentification forte et à la réception de notifications push en grand nombre.

Parmi les éléments suivants, veuillez en sélectionner trois (3) qui représentent vos principaux problèmes de sécurité :



Êtes-vous préoccupé par les attaques de fatigue MFA ?



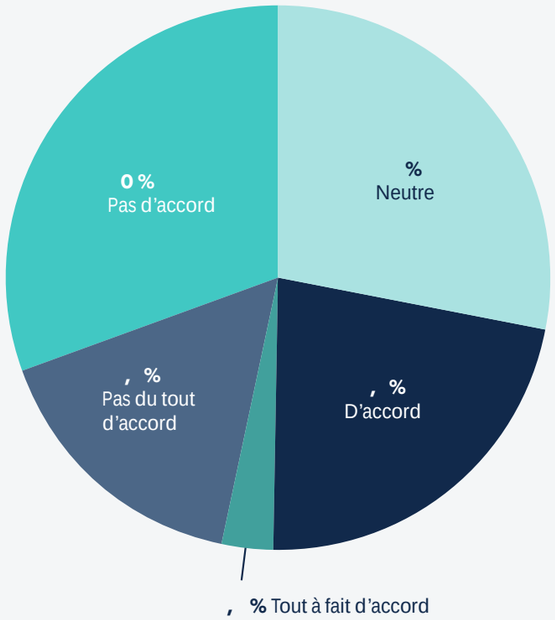
Les enjeux de sécurité dans les PME

La cybersécurité, une priorité

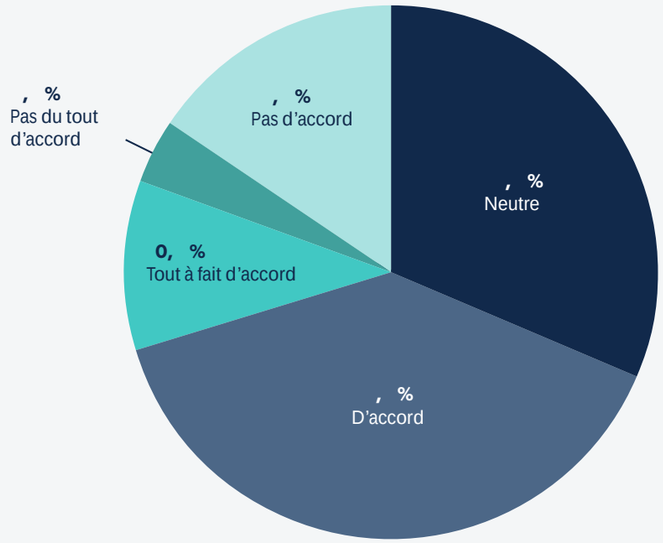
Les responsables informatiques sont plutôt confiants quant au soutien financier accordé au service IT. Une confiance qui s'exprime particulièrement dans le budget alloué à la cybersécurité : seul un responsable sur quatre (26,8 %) craint une baisse de budget dans l'année à venir. Ils sont, à l'inverse, plus d'un tiers (36 %) à ne pas envisager une diminution.

En revanche, face au rythme accéléré des attaques contre les PME et à l'évolution sophistiquée des menaces externes, près de la moitié d'entre eux (48,9 %) s'accordent à dire que réduire les dépenses en cybersécurité risquerait de rendre leur entreprise plus vulnérable. Ils sont moins de 20 % (19,9 %) à penser le contraire.

Je pense que mon organisation réduira ses dépenses en cybersécurité au cours de la prochaine année.



Je pense que toute réduction de notre budget de sécurité augmentera notre risque organisationnel.



Les enjeux de sécurité dans les PME

Une organisation hybride vectrice de points de vulnérabilité

Bien que les modèles hybrides et de travail à distance soient désormais bien en place et que les collaborateurs sont habitués à cette nouvelle organisation, les équipes informatiques restent toujours préoccupées par les menaces potentielles que les collaborateurs peuvent introduire par inadvertance. La raison : la plupart des intrusions sont en e□et la conséquence d'erreurs humaines. La moitié des responsables IT (49,8 %) reconnaît ainsi que le travail hybride rend plus di□cile le suivi et l'application des bonnes pratiques de sécurité.

En réponse à ceslité

La biométrie est de plus en plus utilisée au sein des PME, notamment afin de sécuriser les appareils personnels : 69 % des responsables IT y ont recours. Parmi les techniques privilégiées : l'empreinte digitale est la plus couramment utilisée

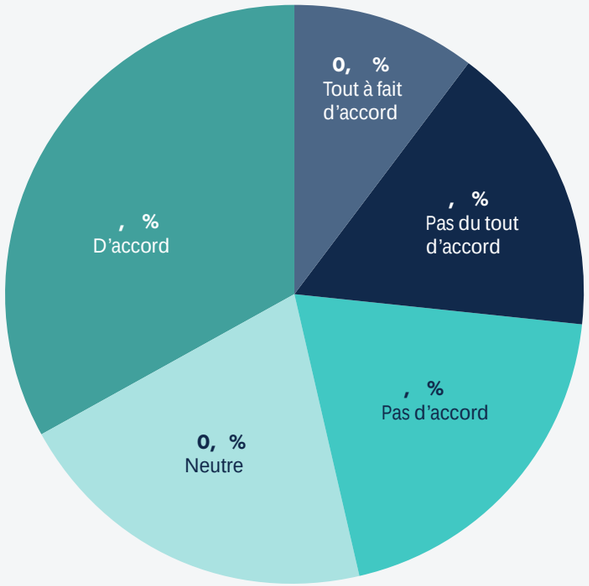
Les enjeux de sécurité dans les PME

Vers le mode « sans mot de passe »

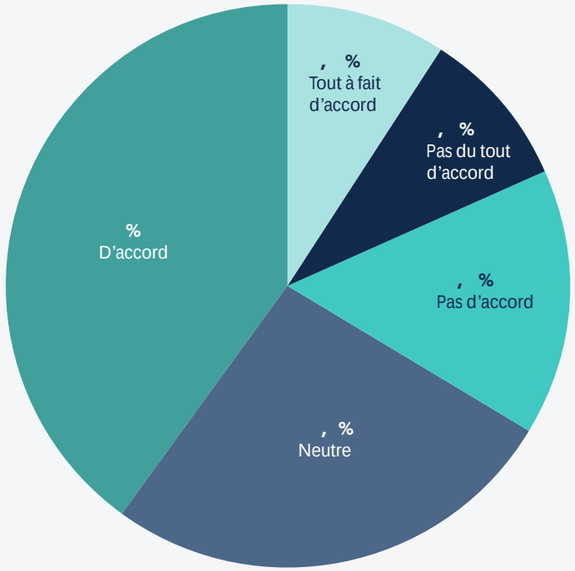
L’adoption de plus en plus fréquente de la biométrie dans l’authentification peut être une solution afin de mieux équilibrer expérience et sécurité des collaborateurs. Et ce, d’autant plus que la tendance en faveur de l’authentification sans mot de passe est elle aussi de plus en plus a□rmée au sein des PME : 43,7 % en font ainsi d’ores et déjà une priorité.

Une approche qui compte autant d’adeptes que de sceptiques. En e□et, dans 48,9 % des cas, l’authentification sans mot de passe s’apparente davantage à un mot à la mode qu’à une véritable priorité IT.

L’authentification sans mot de passe est une priorité pour notre entreprise.



L’authentification sans mot de passe est plus un mot à la mode dans l’industrie qu’une priorité informatique.



L’écosystème IT

Prolifération des outils et gestion centralisée

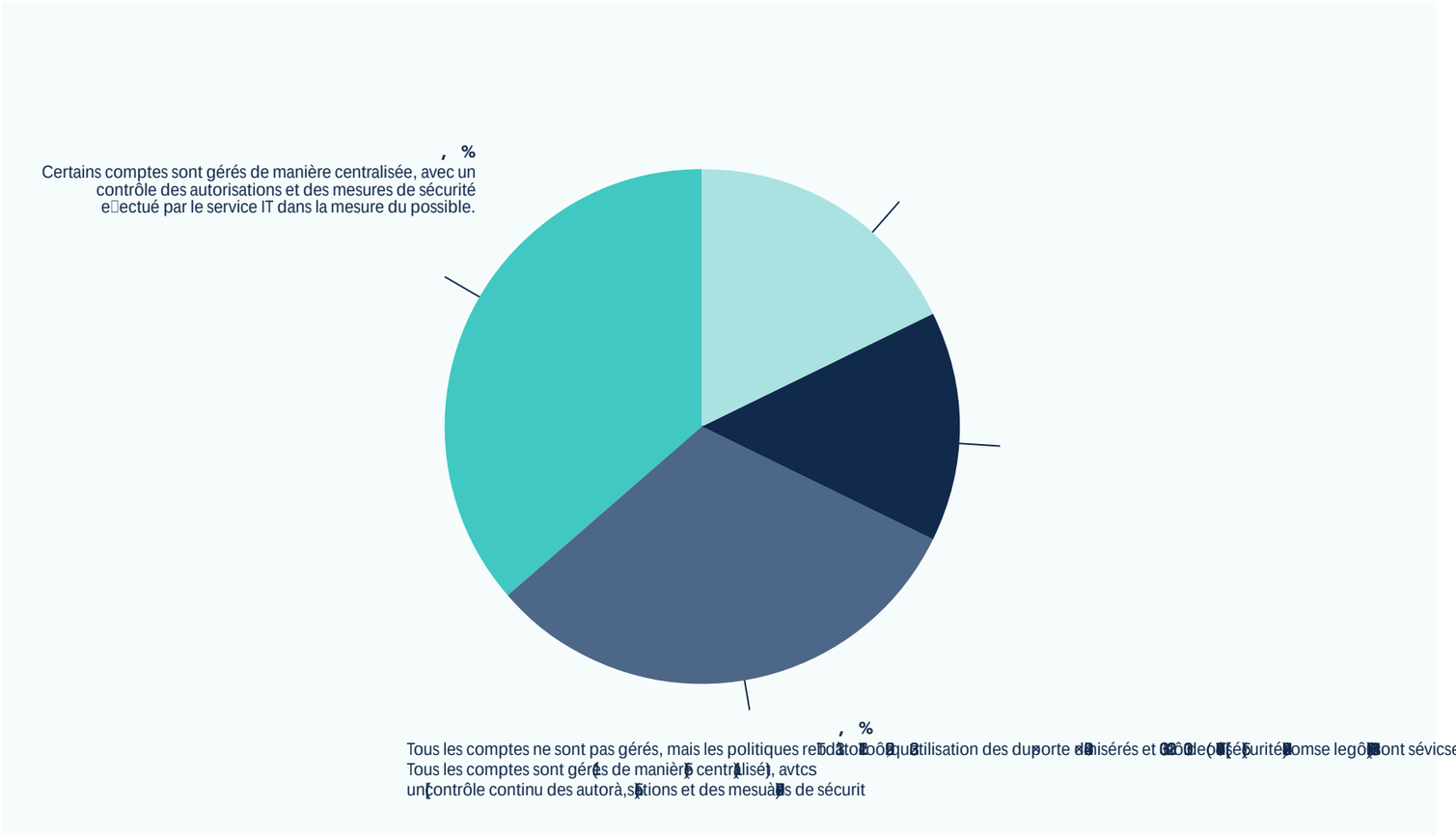
Le rôle des responsables informatiques est de faire en sorte que les collaborateurs aient la capacité à travailler correctement. Sur ce point, force est de constater qu’il existe une grande diversité dans la gestion des utilisateurs. Ainsi, concernant la facilité d’accès des collaborateurs aux outils dont ils ont besoin, il apparaît que l’environnement IT en place di□ère fortement d’une PME à l’autre :

— Dans 36,2 % des cas, seuls certains comptes sont gérés de manière centralisée, avec un contrôle des autorisations et des mesures de sécurité e□ectué par le service IT dans la mesure du possible ;

— Dans 31,5 % des organisations, tous les comptes ne sont pas gérés, mais les politiques relatives à l’utilisation des supports administrés et à l’analyse des niveaux de sécurité (comme le MFA) sont strictement appliquées ;

— Ce n’est que dans 17,9 % des PME que la totalité des comptes sont gérés de manière centralisée, avec un contrôle continu des autorisations et des mesures de sécurité ;

— Enfin, pour 14,4 % d’entre elles, si tous les comptes ne sont pas gérés, des mesures de sécurité comme les exigences en termes de MFA sont néanmoins encouragées mais non mandatées.



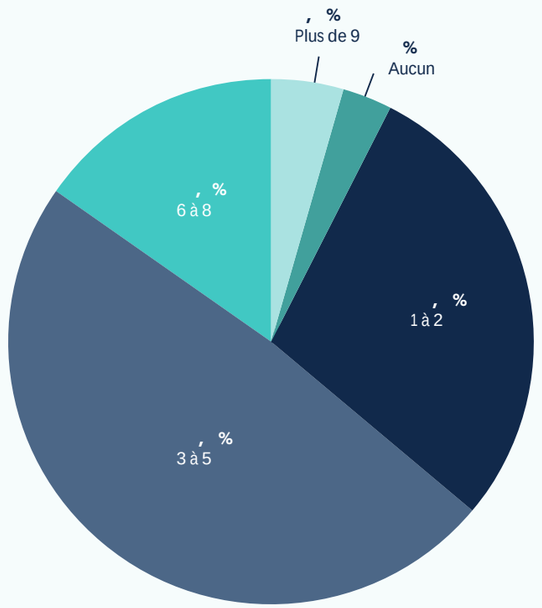
L’écosystème IT

Prolifération des outils et gestion centralisée

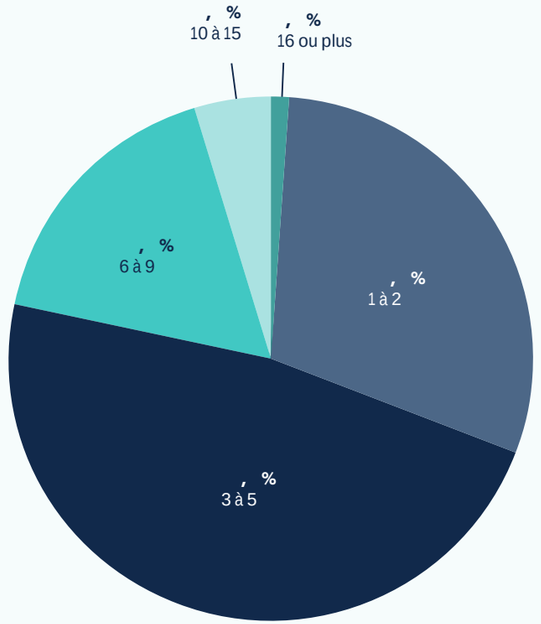
En parallèle, la prolifération des outils continue d’être problématique. Près d’un administrateur IT sur six (15,1 %) déclare avoir besoin de six à huit outils ou plus pour gérer le parcours des collaborateurs, avec une forte majorité entre trois et cinq applications. Même constat du côté des collaborateurs : 16,9 % des responsables IT estiment que les collaborateurs de leur PME doivent utiliser entre six et neuf mots de passe pour travailler. Dans près de la moitié des cas, le nombre moyen cité est lui aussi compris entre trois et cinq.

Les réponses sont donc très disparates selon l’environnement IT de la PME car près d’un administrateur sur trois établit à un ou deux le nombre de mots de passe di□érents nécessaires. Il apparaît alors clairement que les PME a□chent des niveaux de maturité technologiques très di□érents.

Combien d’outils ou d’applications votre organisation utilise-t-elle pour gérer le parcours des employés et les outils dont ils ont besoin pour faire leur travail (par exemple : intégration, gestion des appareils, outils de sécurité, services d’annuaire, délocalisation, service d’assistance, etc.) ?



En moyenne, combien de mots de passe différents vos collaborateurs ont-ils pour se connecter à leurs ressources ?



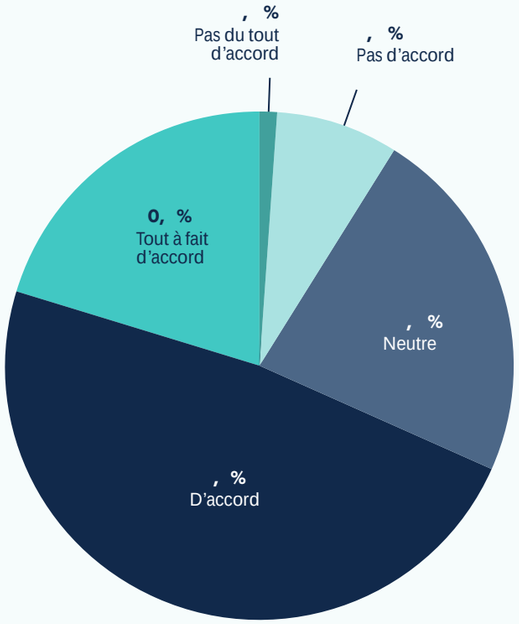
L’écosystème IT

Prolifération des outils et gestion centralisée

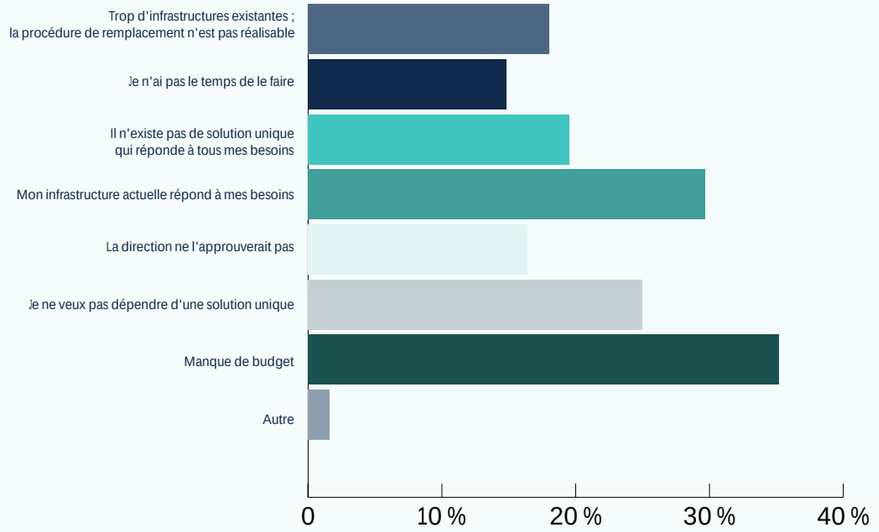
L’impact de la prolifération des outils ne se limite pas qu’aux seuls utilisateurs finaux. Les responsables IT doivent eux aussi jongler avec un certain nombre de solutions et d’outils malgré un intérêt réel porté à leur consolidation. Ils sont ainsi 68,2 % à préférer utiliser une seule solution pour e□ectuer leur travail.

Une consolidation encore trop peu déployée, principalement faute de budget (dans 35,2 % des cas), mais aussi par refus de dépendre d’une seule technologie (25 %) ou parce que l’infrastructure existante répond à leurs besoins existants (29,7 %).

Je préférerais utiliser une seule solution/un seul outil pour faire mon travail plutôt que de gérer plusieurs solutions différentes.



Quelles raisons vous empêchent de consolider les produits informatiques ? (Sélectionnez tout ce qui s’y rapporte):



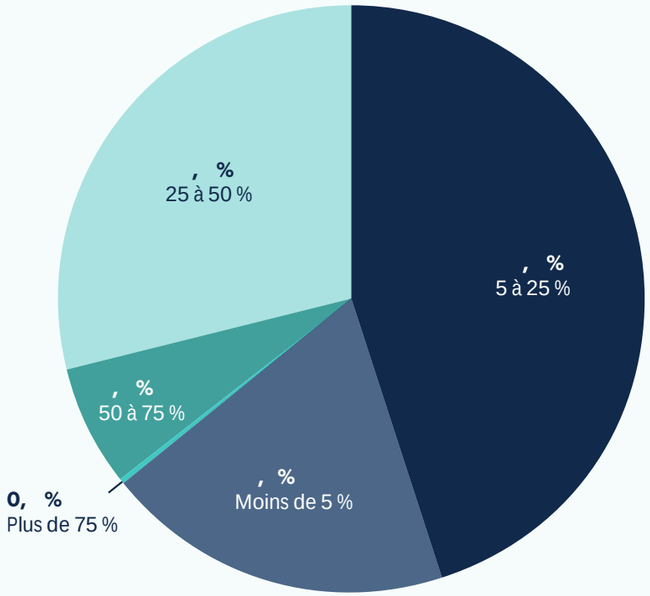
L’écosystème IT

Prolifération des outils et gestion centralisée

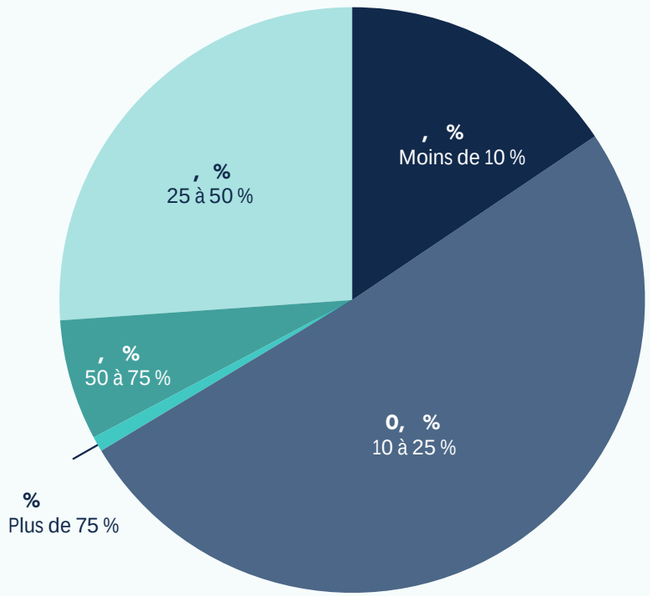
La prolifération des outils et l’évolution des technologies ont poussé les équipes informatiques à consacrer une grande partie de leur temps à la relation fournisseur. 35,7 % passent ainsi plus d’un quart de leur temps à communiquer avec leurs fournisseurs.

Une tendance qui fait écho à la part du budget alloué aux licences logicielles. En e□et, on retrouve quasiment la même proportion de responsables IT (33,6 %) à consacrer plus de 25 % de leur budget à ces coûts de licence. Dans une grande majorité (50,9 %), ils prévoient d’accorder 10 à 25 % de leur budget.

Quel pourcentage environ de vos heures de travail consacrez-vous à la communication avec les fournisseurs ?



Quel pourcentage environ de votre budget informatique annuel est consacré aux licences logicielles ?



Panorama des supports IT utilisés

La nouvelle norme de l’hétérogénéité

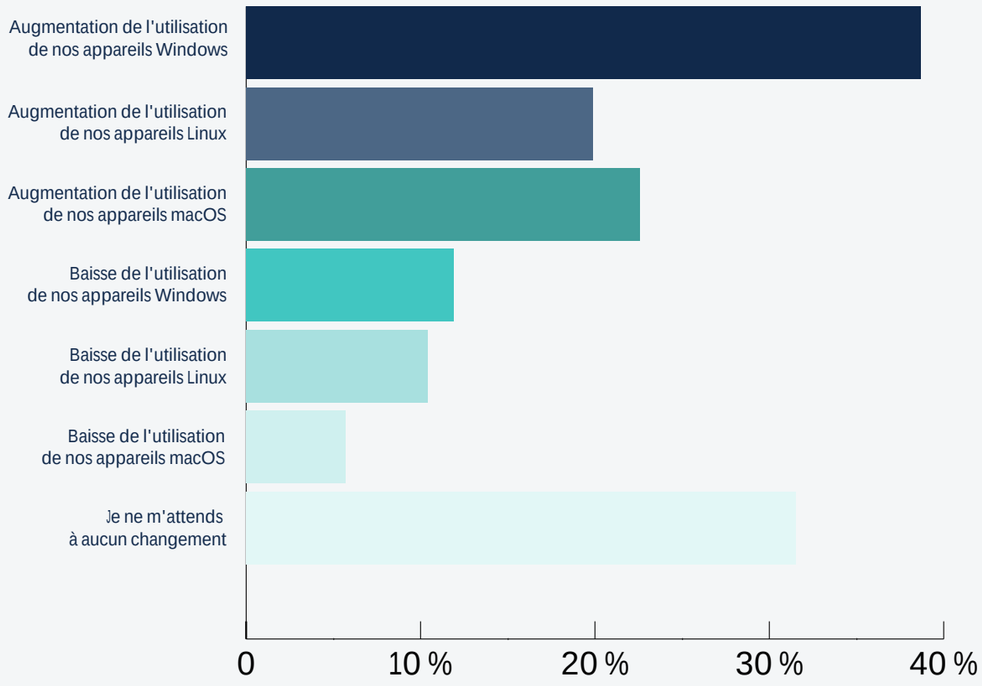
Côté système d’exploitation, un seul mot d’ordre : la flexibilité !
Si Windows occupe de loin la première place au sein de l’environnement de travail standard (avec 73,1 % des appareils), macOS se hisse en 2e position avec 17,3 % des supports. Le podium est complété par Linux avec 15,3 % des équipements.

Les administrateurs IT s’attendent à voir cette hétérogénéité continuer à croître l’année prochaine avec une tendance à la hausse pour les trois systèmes d’exploitation : + 38,7 % attendus vis-à-vis de l’utilisation des appareils sous Windows, +22,6 % sous Mac et +19,9 % pour Linux.

Quelle est la répartition des types d’appareils Windows/Linux/macOS sur votre lieu de travail (veuillez saisir X % Windows / X % Linux / X % macOS) ?

OS	Moy.	Min	Max	StdDev	Sum	Total des réponses
Windows	73,1	0,0	100	27,3	29,234	400
Linux	15,3	0,0	100	17,7	5,235	342
macOS	17,3	0,0	100	19,4	5,831	338

Au cours de la prochaine année, je prévois (sélectionnez tout ce qui s’applique) :



La tendance en faveur du Bring Your Own Device (BYOD) est évidente dans les PME. Seuls 12,4 % des responsables estiment qu'aucun collaborateur n'utilise d'appareil personnel pour le travail. À titre de comparaison, plus d'un sur trois (35 %) est convaincu de leur usage, même limité.

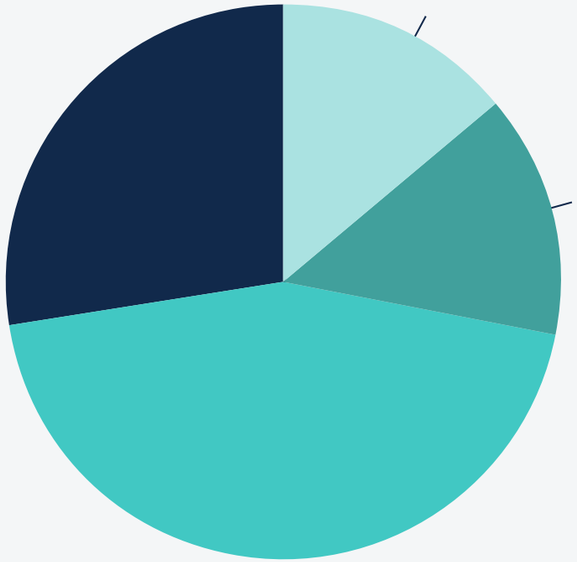
Pour lutter contre les risques potentiels générés par cette pratique, les équipes informatiques ont adopté des politiques, des procédures et des

L’heure est au travail hybride ! Près de

Les PME et les fournisseurs de services managés (MSP)

Les MSP, un relais fort pour les PME

Les MSP restent un partenaire majeur des PME. Aujourd'hui, 85,5 % déclarent envisager ou déjà travailler avec des MSP. Parmi elles : 58,8 % confirment qu'un MSP accompagne leur équipe informatique interne ou gère même entièrement leur programme informatique, incluant la technologie, les processus et le support.



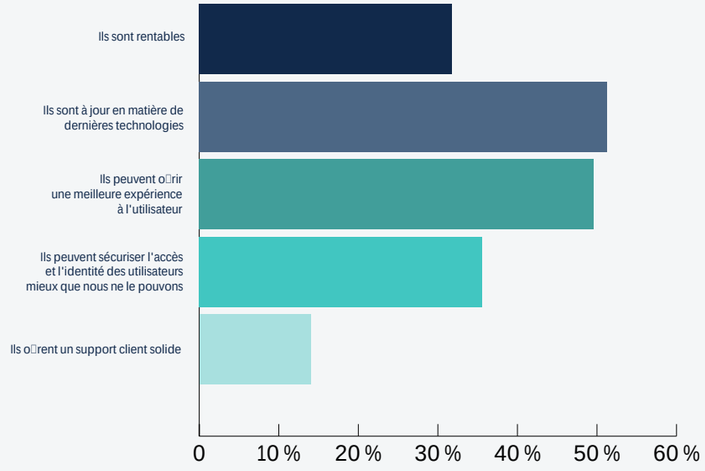
Les PME et les fournisseurs de services managés (MSP)

Objectifs et résultats

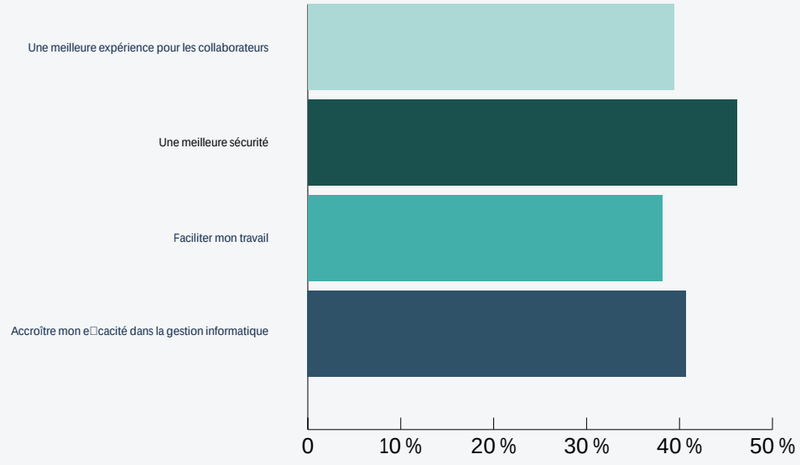
Les MSP sont considérés comme une valeur ajoutée dans de multiples domaines, à commencer par le fait qu'ils sont les plus à même d'être à jour sur les dernières technologies (51,3 %) et à fournir une meilleure expérience utilisateur (49,6 %). Autres atouts : leur capacité à assurer une meilleure gestion sécurisée des identités et des accès (35,6 %) et à être rentables (31,8 %). Enfin, 14 % des responsables IT mentionnent la qualité de leur support client.

Parmi tous ces avantages, l'impact le plus bénéfique de ces MSP repose sur l'amélioration de la sécurité IT au quotidien (46,2 %), juste devant l'amélioration de l'e□cacité dans la gestion IT (40,7 %). L'expérience collaborateur (39,4 %) et la facilitation du travail des responsables IT (38,1 %) complètent la liste des avantages perçus.

Nous utilisons des MSP parce que (sélectionnez tout ce qui s'applique) :



L'utilisation d'un MSP a entraîné (sélectionnez tout ce qui s'applique)



Les PME et les fournisseurs de services managés (MSP)

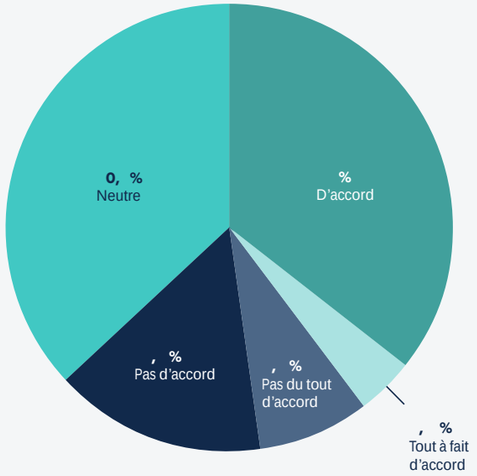
Les freins à l'adoption

Consultez **The MSP's 2023 Planning Kit** et bénéficiez d'outils pour lancer votre planning commercial, et définir vos stratégies de vente, techniques et de support pour l'année.

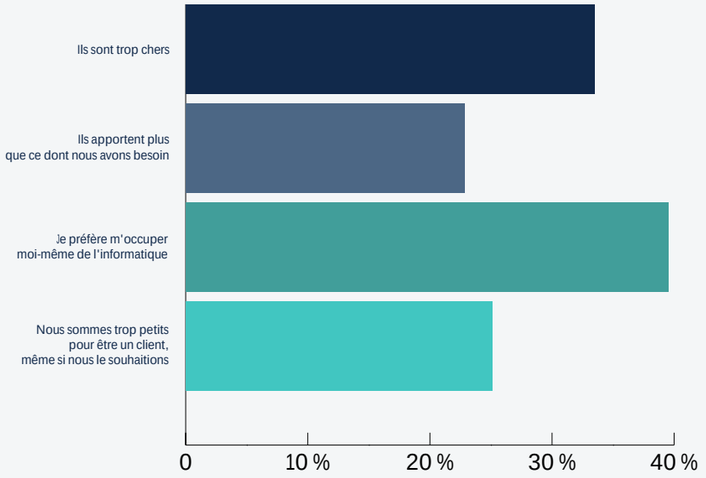
Cependant, les inquiétudes concernant le maintien d'une sécurité robuste par les MSP demeurent élevées. Aujourd'hui, près de quatre responsables IT sur dix (39,5 %) reconnaissent être préoccupés quant à la manière dont les MSP gèrent la sécurité. Seuls 24,1 % n'éprouvent aucune inquiétude.

Parmi les principaux freins à l'adoption des MSP, la volonté de conserver la maîtrise de son IT en interne (pour 39,5 % des administrateurs IT) et le coût lié à l'externalisation (33,5 %) arrivent en tête. Les autres raisons invoquées reposent principalement sur la trop petite taille de l'entreprise pour avoir recours à un MSP (25,1 %) et l'inadéquation de l'o□re : les MSP proposant plus que ce dont la PME a besoin (22,8 % des réponses).

J'ai des inquiétudes sur la façon dont les MSP gèrent la sécurité :



Nous n'utilisons pas de MSP parce que (sélectionnez tout ce qui s'applique) :



Que retenir ?

En 2022, les équipes IT ont dû composer avec de multiples incertitudes. Dans un contexte de tensions mondiales, les experts IT se sont alors fortement impliqués dans leur travail et ont activement recherché des solutions innovantes pour résoudre les diverses problématiques générées par la nouvelle organisation hybride du travail.

Malgré la capacité à assurer une stabilité opérationnelle certaine, les perspectives pour les 12 prochains mois suggèrent que la prise en compte de l'inconnu et de l'imprévisible tend à devenir la nouvelle réalité du secteur industriel (et du monde).

Alors que la sécurité continue d'être le principal défi et la priorité des PME, il existe un certain nombre d'alternatives pour leur permettre de mieux gérer leur IT au regard des réponses obtenues dans cette enquête.

Parmi lesquelles :

La consolidation, plébiscitée par près de 70 % des décideurs IT. Si le coût associé demeure encore un frein trop important, les nombreux avantages qui en résultent, tels que l'expérience utilisateur et la sécurité renforcée, devraient à terme convaincre les différentes parties prenantes.

La complémentarité entre authentification multi-facteur et biométrie : si la première se détache par sa simplicité d'utilisation, la deuxième fait la différence par le très haut niveau de sécurité qu'elle génère. Résultat, la biométrie devrait dans les années à venir se généraliser dans les PME, toutes tailles confondues. En attendant, elle s'avère le complément idéal de la politique MFA.

La mise en place d'une solution de Mobile Device Management (MDM) : les PME sont confrontées à la fois à une vraie mixité en matière de systèmes d'exploitation, Windows en tête, et au recours massif au BYOD. Un usage des appareils personnels qui transfère alors une grande partie de la responsabilité de la sécurité aux utilisateurs pas toujours au fait des meilleures pratiques de sécurité. En conséquence, le déploiement de solutions MDM est un moyen efficace pour les organisations de centraliser la gestion IT, d'alléger la charge des administrateurs et de garantir l'application des procédures et des politiques de sécurité.

L'optimisation des coûts : les responsables IT ont une très bonne connaissance de leur stack technologique et du ROI associé, et une parfaite maîtrise de leur budget. Les dirigeants de PME seraient ainsi avisés de les consulter et de les écouter pour évaluer leurs priorités d'investissement à venir.

En 2023, les PME doivent saisir l'opportunité d'être accompagnées par des experts capables de maintenir leur organisation opérationnelle et d'en assurer la sécurité. L'engagement de JumpCloud de rendre le travail possible, ''Make Work Happen®'', prend ici tout son sens. Conçue et construite pour les PME, la plate-forme JumpCloud favorise une gestion très professionnelle des sujets IT, facilement et à moindre coût. La plate-forme dans son intégralité a en effet été développée selon un modèle de croissance axé sur le produit (PLG). À la clé : la garantie pour les équipes IT et les partenaires MSP de disposer d'une forte valeur ajoutée. Comment ? En anticipant leurs besoins et en proposant une solution basée sur leur retour d'expérience.

Pour vous lancer sans plus attendre et gratuitement avec JumpCloud, visitez notre site : **https://jumpcloud.com/fr/**

Méthodologie :

JumpCloud a interrogé 403 décideurs informatiques de PME basés en France, notamment des managers, des cadres-dirigeants et des directeurs issus d'entreprises de moins de 2 500 employés et de secteurs d'activité très variés. L'enquête en ligne a été menée par Propeller Insights, du 21 au 23 février 2023.

pcloud