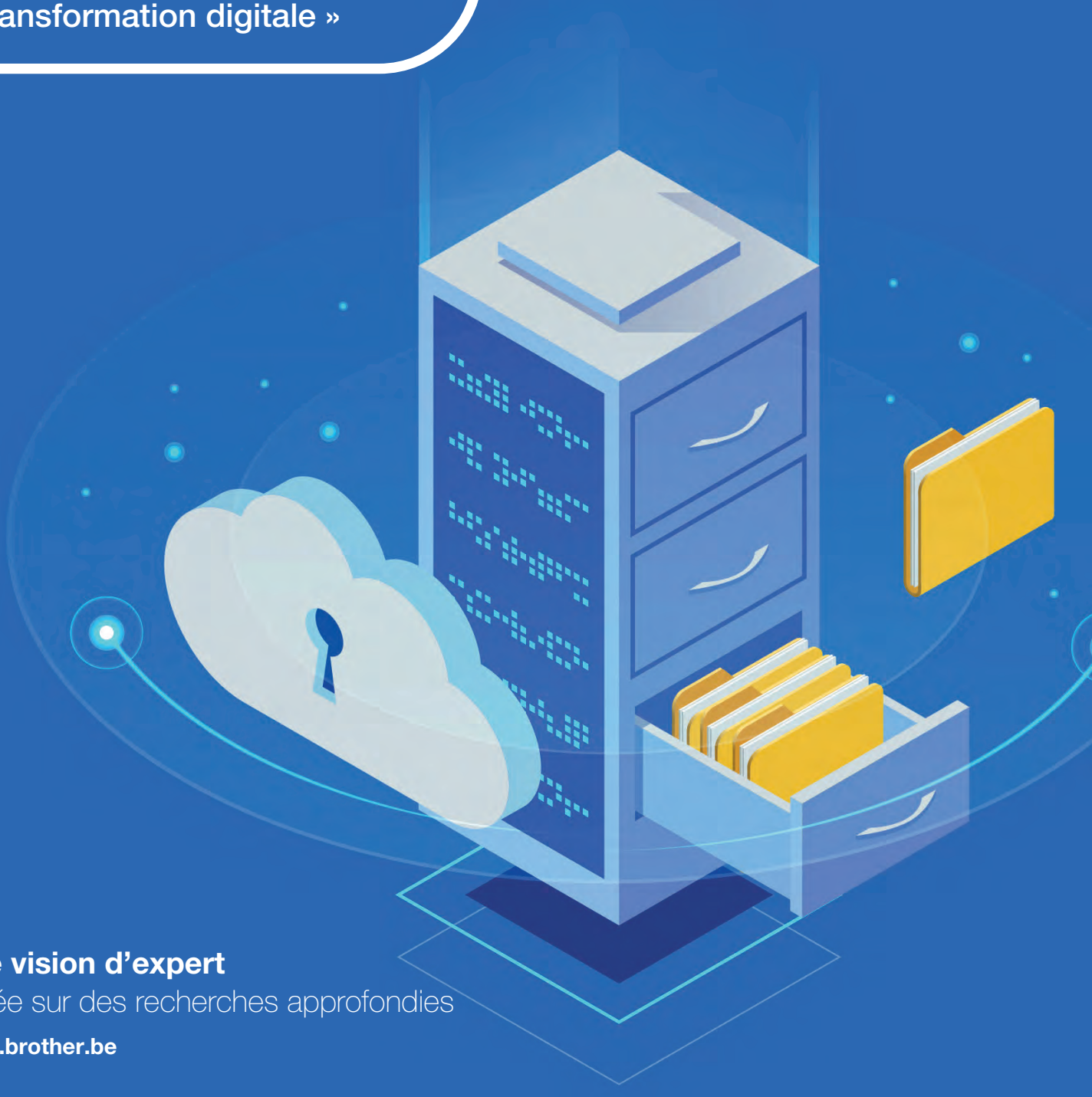
Maintenir un écosystème d'impression sécurisé

Un livre blanc issu de notre série « Brother et la transformation digitale »



Une vision d'expert
basée sur des recherches approfondies

www.brother.be

Les obstacles freinant l'investissement pour une impression sécurisée

Face aux menaces croissantes liées au piratage et aux violations de confidentialité, la plupart des PME sont bien conscientes de la nécessité de protéger leurs systèmes informatiques.

Gérer la sécurité du parc informatique est un défi qui doit être pleinement relevé. Les imprimantes, les scanners et les photocopieurs doivent bénéficier du même niveau de sécurité que les autres équipements informatiques. Si ce point est négligé, ils pourraient servir de porte d'entrée pour les pirates informatiques. Les PME sont de plus en plus conscientes de l'ampleur du problème, **72 %** des entreprises déclarant qu'il est essentiel que leurs imprimantes, scanners et photocopieurs soient sécurisés. Ce problème est encore plus présent parmi les structures qui traitent des données sensibles, dans des secteurs tels que les services professionnels **(82 %)** et la santé **(81 %)**.

Cependant, près d'un tiers des entreprises ne reconnaissent toujours pas l'importance d'un tel niveau de sécurité. En parallèle, près de la moitié d'entre elles estiment que leur organisation n'a pas suffisamment investi dans la sécurité des imprimantes.

Si les entreprises comprennent la nécessité d'investir dans la sécurité des imprimantes, pourquoi ne le font-elles pas aujourd'hui ?

Notre enquête fait ressortir deux raisons évidentes :

- Des moyens insuffisants en matière de sécurité des imprimantes
- Un manque de compréhension et de connaissances concernant les menaces et les normes en matière de sécurité

Ce livre blanc est conçu pour aider les décideurs des PME à comprendre l'importance de l'impression sécurisée et pour leur présenter les solutions dédiées. Ce document fait partie d'une série de quatre livres blancs visant à informer les décideurs sur la meilleure façon d'utiliser les technologies numériques au sein des entreprises. Ils sont basés sur des études approfondies menées auprès d'entreprises européennes, du Moyen-Orient et d'Afrique. Chacun d'entre eux abordera les thèmes suivants :

- La digitalisation des process
- Des solutions adaptées à chaque entreprise
- La sécurité du parc d'impression
- Le choix d'un équipement durable

Qui porte la responsabilité de la sécurité du parc d'impression ?

Bien souvent, la responsabilité concernant la sécurité du parc d'impression n'est pas clairement définie. Près de la moitié des PME d'Europe occidentale **(44 %)** déclarent que les personnes en charge ne sont pas précisément identifiées. Dans ce contexte, il est probable que la prise de décision et l'intégration d'une solution d'impression sécurisée en souffrent, rendant les entreprises vulnérables.

Il est possible que cette responsabilité soit minimisée car, à la différence d'équipements tels que les ordinateurs portables, la sécurité du parc d'impression n'est pas toujours considérée comme un « point faible ». Si notre enquête montre que les décideurs commencent à se rendre compte que la sécurité des impressions est vitale, cela n'est cependant pas encore une réalité au sein des effectifs des PME.

Cela rend ces dernières particulièrement vulnérables car bien souvent, seul un très petit nombre d'employés veille sur l'ensemble du matériel et des logiciels de leur organisation. Si les professionnels de l'informatique ne sont pas conscients des risques liés à la sécurité de l'impression, ce sujet n'est alors pas considéré comme une priorité.

Cependant, tous les employés sont responsables de la sécurité des informations sensibles de leur société.

Tandis que les experts en informatique sont garants de la sécurité des équipements, les employés doivent veiller à leur niveau à ce que les données demeurent hors d'atteinte. La sécurité des données représente le risque le plus élevé concernant les informations sensibles de votre activité.

La sécurité des données fait l'objet d'un large éventail de menaces, notamment :

- L'accès non autorisé aux impressions
- L'oubli de déconnexion après l'impression de documents confidentiels
- Le manque de traçabilité pour savoir qui a accédé à quels documents sur l'imprimante

Près de 9 entreprises sur 10 ont subi un incident lié à la sécurité du parc d'impression...

… et sept sur dix **(72 %)** affirment que la sécurité des données est une menace plus importante que celle des équipements. Cependant, moins d'une entreprise sur trois se déclare actuellement confiante quant aux mesures de sécurité en place au sein de leur parc d'impression. Ce chiffre est à comparer aux **53 %** d'entreprises qui estiment avoir mis en place une sécurité matérielle adaptée.

La majorité des PME **(64 %)** déclare également que la sécurisation de leurs données est une priorité absolue. C'est pour elles un défi majeur, pouvant constituer un frein réel en matière de performance.

Actuellement, près de la moitié des PME **(48 %)** indiquent avoir peu ou pas de process en place leur permettant de savoir qui imprime ou récupère les travaux d'impression. Il n'est donc pas surprenant que près de neuf entreprises sur dix **(86 %)** déclarent avoir fait l'expérience d'incidents liés à la sécurité des impressions.

Ces incidents de sécurité concernent le plus souvent des documents confidentiels laissés sans surveillance sur l'imprimante, des impressions non récupérées ou des employés collectant des documents tout aussi confidentiels, qui ne leur sont pas destinés.

En conséquence, la majorité des PME **(64 %)** commence à mettre en place des mesures pour faire face aux problèmes de sécurité liés à l'impression, en limitant l'accès à certaines imprimantes ou en instaurant l'utilisation de badges/codes PIN pour libérer les travaux d'impression aux bonnes personnes.

C'est un pas dans la bonne direction. Dans les années à venir, il sera crucial que toutes les entreprises intègrent des processus plus sécurisés. Celles qui se sont déjà engagées dans cette voie devront maintenir et augmenter leurs moyens et capacités d'audit.

Il existe trois objectifs principaux pour assurer une véritable sécurité des données, facilement mémorisables grâce à l'acronyme CIA.

Ceux-ci couvrent à la fois la sécurité des équipements et des données :

Confidentialité

Protégez les données confidentielles de votre activité pour vous assurer qu'elles soient uniquement partagées avec les bons destinataires. Les mesures d'authentification et d'autorisation sont essentielles à cet égard, car elles obligent les utilisateurs à s'authentifier et à s'assurer qu'ils ont bien l'autorisation nécessaire, avant toute impression.

Intégrité

Assurez-vous que les firmwares de vos dispositifs soient bien sécurisés et suffisamment résistants face au piratage et autres menaces externes.

Accessibilité

Soyez sûrs que vos équipements d'impression soient opérationnels et accessibles aux utilisateurs autorisés pour effectuer des tâches essentielles.

Un manque de connaissances favorise les mauvaises pratiques en matière de sécurité

Moins d'un tiers **(32 %)** des principaux responsables informatiques travaillant au sein de PME déclarent avoir des connaissances avancées en matière de sécurité et de menaces informatiques. Si les décideurs IT ont une connaissance insuffisante des éventuels dangers, les entreprises continueront à avoir des difficultés à se protéger en mettant en place des mesures appropriées. Au sein des PME, les responsables IT sont généralement en charge d'un grand nombre de technologies différentes. Il est alors compréhensible qu'ils ne soient pas des experts en matière d'impression sécurisée.

Bien souvent, le jargon informatique est pointé du doigt. Plus de la moitié **(51%)** des PME déclarent que le jargon utilisé pour la sécurité des imprimantes est trop complexe, principalement en France et en Italie.

Par ailleurs, près de **60 %** des PME déclarent avoir une bonne compréhension des normes de sécurité en vigueur.

Cependant, il semble peu probable que les décideurs aient une connaissance approfondie des fournisseurs de solutions d'impression capables de répondre à leurs besoins en matière de sécurité. Par conséquent, il n'est pas surprenant que les entreprises se tournent vers des marques qu'elles connaissent déjà pour s'équiper d'imprimantes sécurisées, sans vraiment comprendre les mesures de sécurité qu'elles embarquent ou non.

Les spécialistes de l'impression doivent s'investir davantage pour vous aider à décoder les normes de sécurité pertinentes et s'assurer que vous choisissiez la meilleure solution pour votre entreprise.

Le point de vue de Brother

Face à la complexité de la sécurité des impressions, Brother propose sept perspectives et recommandations pour aider les PME à se protéger contre les importantes répercussions financières, juridiques et de réputation que peuvent engendrer une perte de données.

Impliquez la direction

L'ampleur des dégâts causés par les cyberattaques et les violations de données, combinée aux exigences du RGPD, signifient que l'impression sécurisée doit sortir du seul périmètre du service informatique. Elle doit faire l'objet d'une réflexion stratégique au niveau du comité de direction, avec la participation du Directeur des Systèmes d'Information (DSI) et du Responsable de la Sécurité des Systèmes d'Information.

Menez un audit approfondi

Il est essentiel que les entreprises relèvent toute faille potentielle en matière d'impression sécurisée, en s'assurant que leur environnement d'impression soit soumis à des audits réguliers. C'est particulièrement important si votre entreprise dispose d'équipements récents et plus anciens. En ce qui concerne les services de gestion d'impression (Managed Print Services - MPS), la plupart des fournisseurs proposent des évaluations complètes, capables d'instaurer une surveillance continue des équipements une fois le parc d'impression optimisé et sécurisé.

Modifiez les mots de passe administrateur prédéfinis

Les mots de passe administrateur prédéfinis ou configurés par défaut représentent un point faible des équipements d'impression, qui peut être réglé facilement. Une fois l'équipement installé, il suffit de changer les mots de passe, en optant pour une suite de caractères solide et sécurisée.

Mettez à jour vos firmwares

La vulnérabilité de vos imprimantes peut être considérablement réduite en mettant régulièrement et automatiquement à jour leurs firmwares. Si vous avez des questions à ce sujet, contactez votre fournisseur d'imprimantes pour être conseillé.

Protégez vos travaux d'impression

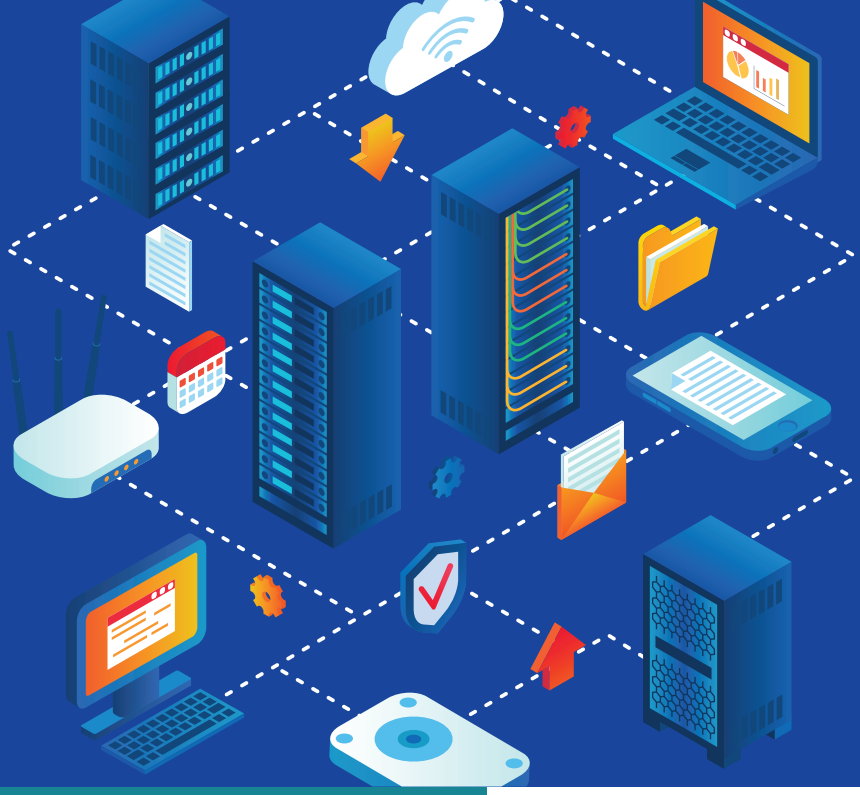
Ce ne sont pas seulement les équipements d'impression qui doivent être protégés, mais aussi le flux des documents à imprimer. Le chiffrement de bout en bout du trafic réseau assure le transfert sécurisé des travaux d'impression vers les imprimantes. Comme la plupart des imprimantes stockent temporairement les travaux d'impression, il faut s'assurer que les données soient cryptées.

Surveillez votre équipement

Connaître l'état actuel de vos imprimantes vous donne une vue d'ensemble de votre environnement d'impression. Les entreprises devraient envisager d'utiliser des outils logiciels pour surveiller leurs équipements et permettre de résoudre les problèmes dès qu'ils surviennent. Chaque appareil génère une importante quantité de données qui peuvent être utilisées pour identifier de potentiels incidents de sécurité et répondre rapidement aux attaques. Les utilisateurs de services de gestion des impressions peuvent également obtenir des rapports de conformité réguliers, incluant la surveillance et les alertes de violations de données.

Formez vos collaborateurs

Les incidents de perte de données étant souvent causés de manière involontaire, il est essentiel que les entreprises informent leurs employés sur l'importance de protéger les informations confidentielles et sur les menaces potentielles. Souvent, les fournisseurs de services en gestion des impressions peuvent vous accompagner dans la formation de vos collaborateurs.



En conclusion

Si la sécurité des systèmes d'impression a peut-être été négligée par le passé, les PME prennent de plus en plus conscience de son importance. Néanmoins, des défis majeurs doivent être relevés pour mettre en place une impression sécurisée.

Les PME devraient clairement définir les rôles des personnes en charge de la sécurité des imprimantes, afin de s'assurer que leurs équipements soient bien protégés et puissent lutter contre les menaces. Outre la sécurité des équipements, la prise en compte des failles en matière de sécurité des données est également essentielle, et la coopération des employés en interne sera nécessaire afin de minimiser les risques.

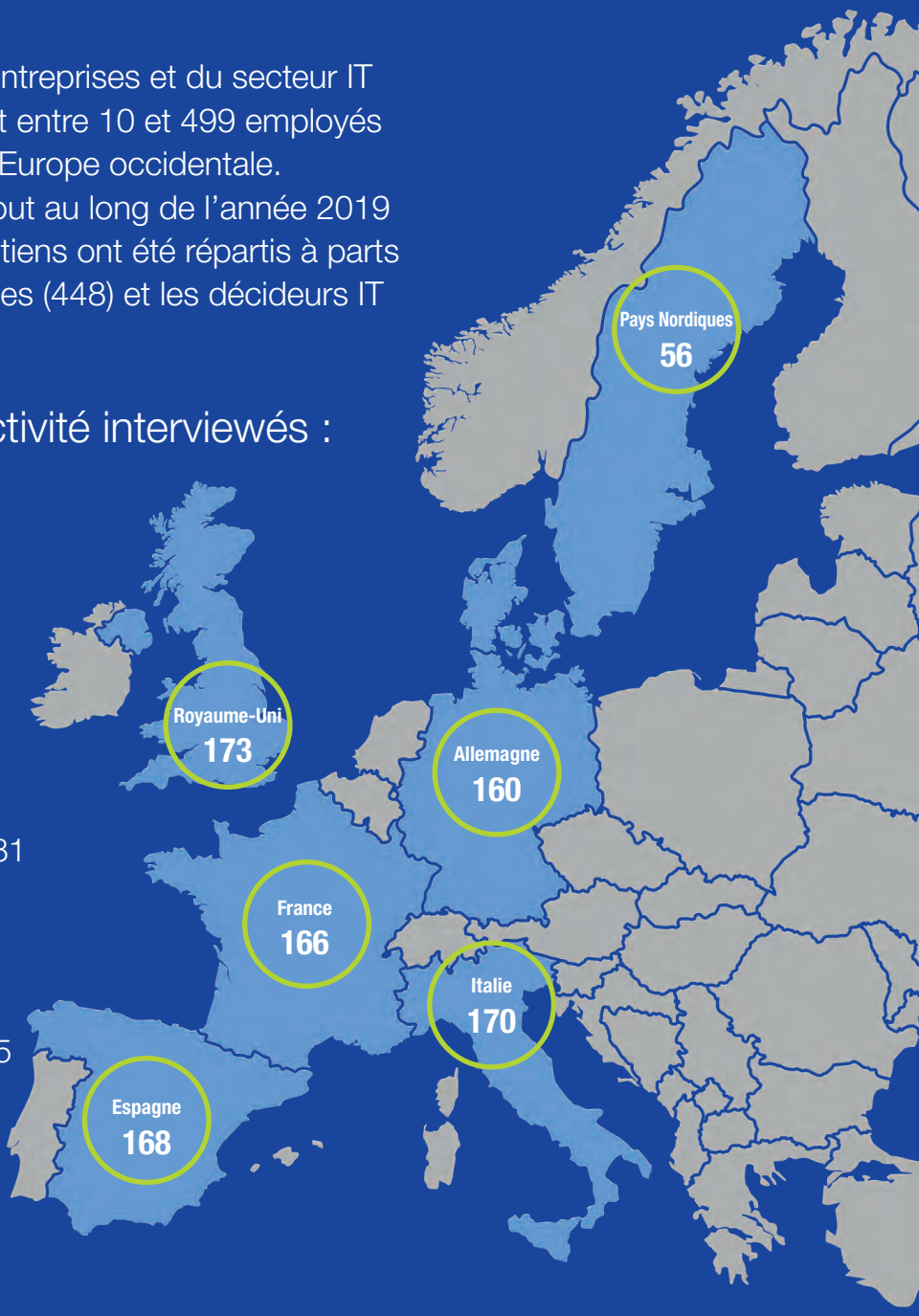
Même en cas de responsabilités clairement définies au sein des PME, disposer des connaissances suffisantes pour gérer efficacement la sécurité du parc d'impression reste un défi majeur. Les technologies d'impression et leur jargon sont de plus en plus complexes. Les entreprises doivent s'appuyer sur des fournisseurs de confiance pour prendre des décisions judicieuses.

La configuration d'un parc d'impression efficace doit être plus que simplement sécurisée.
Les autres rapports de notre série consacrée à la transformation digitale vous en diront plus sur l'importance de la digitalisation des process, l'optimisation de la productivité et la garantie d'une installation durable.

Notre méthodologie

Ce livre blanc s'appuie sur 893 sondages, menés en ligne auprès de responsables d'entreprises et du secteur IT.

Ont été sondés les responsables d'entreprises et du secteur IT travaillant au sein des PME comptant entre 10 et 499 employés et réparties sur plusieurs marchés d'Europe occidentale. Notre travail d'enquête a été mené tout au long de l'année 2019 et en début d'année 2020. Les entretiens ont été répartis à parts égales entre les décideurs stratégiques (448) et les décideurs IT des entreprises (445).



Les principaux secteurs d'activité interviewés :

- La santé - 152
- La distribution - 117
- La logistique - 113
- L'hôtellerie et la restauration - 81
- Le transport et stockage - 62
- Les services professionnels - 65
- L'industrie - 54
- La finance - 53
- L'éducation - 51
- Le BTP - 39

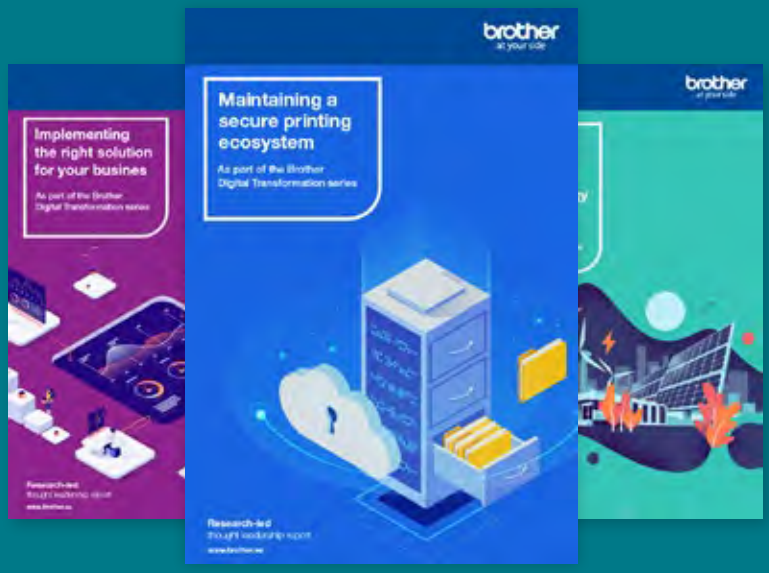
Des interviews complémentaires ont été réalisées auprès d'entreprises issues d'autres secteurs, notamment l'énergie, l'industrie pharmaceutique, l'agriculture, la défense, l'immobilier, le sport et les divertissements.

Cette enquête a été menée par l'agence Savanta, spécialiste des études de marché.

Vous souhaitez en savoir plus ?

Découvrez les autres livres blancs de notre série consacrée à la transformation digitale

brother.be/fr-be/transformation-digitale



brother
at your side

www.brother.be

Brother International (Belgium) NV

Industrialaan 32, 1702 Groot-Bijgaarden
+32 (0)2 467 42 11 - www.brother.be - info@brother.be