CYBERSÉCURITÉ - TPE ET PME BELGES

BAROMÈTRE ANNUEL

2024

SKYFORCE CYBER SECURITY

MÉTHODOLOGIE

Baromètre annuel 2024

Ce cinquième baromètre Skyforce se base sur des visites et entretiens individuels de 3.286 sociétés belges, effectués tout au long de l'année 2023.

Nos consultants ont interviewé directement les dirigeants de ces institutions, qui sont essentiellement des petites entreprises de moins de cinq collaborateurs.

Le baromètre Skyforce est l'enquête la plus large consacrée à la cybersécurité en Belgique sur cette catégorie de sociétés.

Mathieu Lardinois

Co-Founder
Marketing & Customer Care Director

"En 2023, nos experts ont réalisé un travail consciencieux en auditant plus de 3.200 entrepreneurs en Belgique. Cette démarche offre une perspective unique sur les défis et opportunités en matière de cybersécurité au sein des TPE et PME."

POINTS MARQUANTS RÉVÉLÉS PAR L'ÉDITION 2024

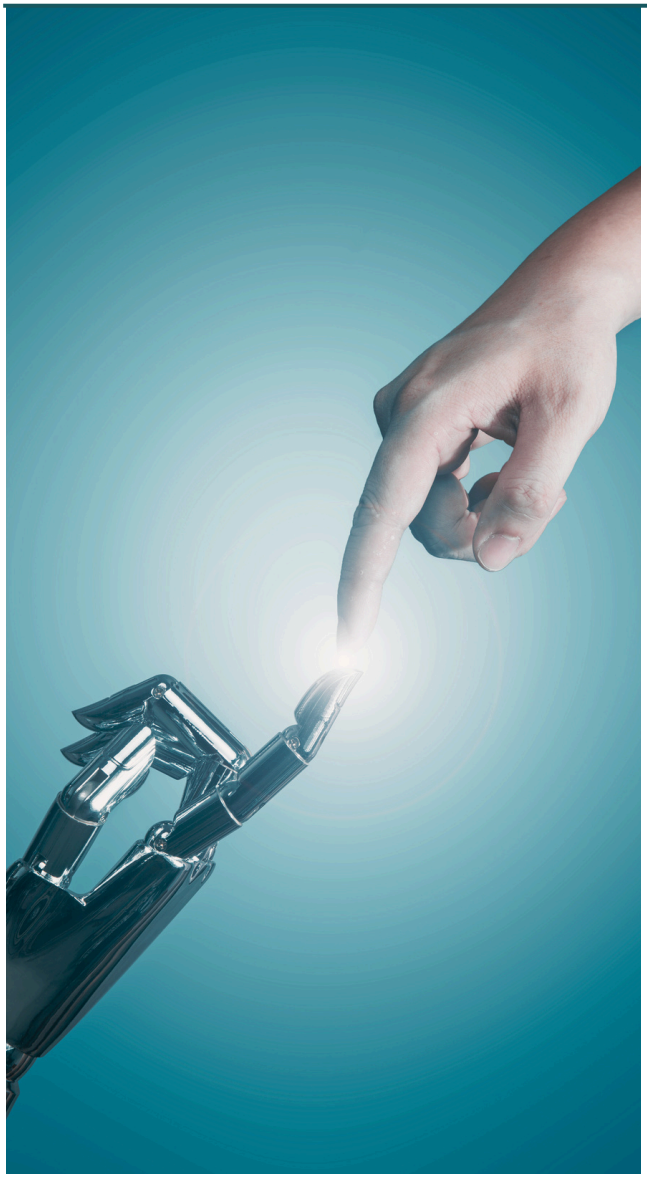
IA À DOUBLE TRANCHANT

HAUSSE DES RANSOMWARES

PROTECTION INCOMPLÈTE

GESTION PROPRE DE LA CYBERSÉCURITÉ

L'INTELLIGENCE ARTIFICIELLE : UNE ARME À DOUBLE TRANCHANT DANS LA CYBERSÉCURITÉ



Dans un monde où la technologie évolue à un rythme effréné, la cybersécurité est devenue une préoccupation majeure pour les entreprises du monde entier. Et la vôtre ! Avec l'avènement de l'intelligence artificielle (IA), cette préoccupation prend une nouvelle dimension, où les enjeux de protection des données et des systèmes deviennent de plus en plus complexes.

L'intégration croissante de l'IA dans nos vies présente des avantages indéniables, mais elle comporte également des risques significatifs. Comme l'a souligné Sam Altman, CEO de OpenAI, éditeur de ChatGPT, l'IA représente potentiellement le premier danger de cette technologie. En effet, alors que les algorithmes d'IA deviennent de plus en plus sophistiqués, ils peuvent également être utilisés de manière malveillante pour perpétrer des attaques cybernétiques de grande envergure.

Dans ce contexte, le baromètre annuel de la cybersécurité de Skyforce se veut être un outil essentiel pour comprendre les tendances, les défis et les solutions émergentes dans le domaine de la sécurité informatique. Chez Skyforce, nous prenons très au sérieux les implications de l'IA sur la cybersécurité, ainsi que les stratégies et les technologies nécessaires pour faire face à cette nouvelle réalité.

Nous vous invitons à plonger dans ce rapport, fruit d'une analyse approfondie et d'une expertise pointue, afin de mieux appréhender les enjeux cruciaux qui façonnent l'avenir de la cybersécurité.

Dominique Mangiatordi

Co-Founder & IA Expert

SKYFORCE
CYBER SECURITY

1. PROFILS-TYPE

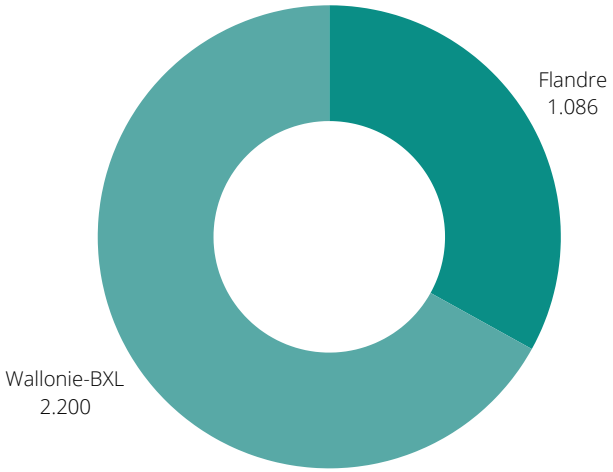
Des entreprises interrogées

Profils-type des entreprises participantes

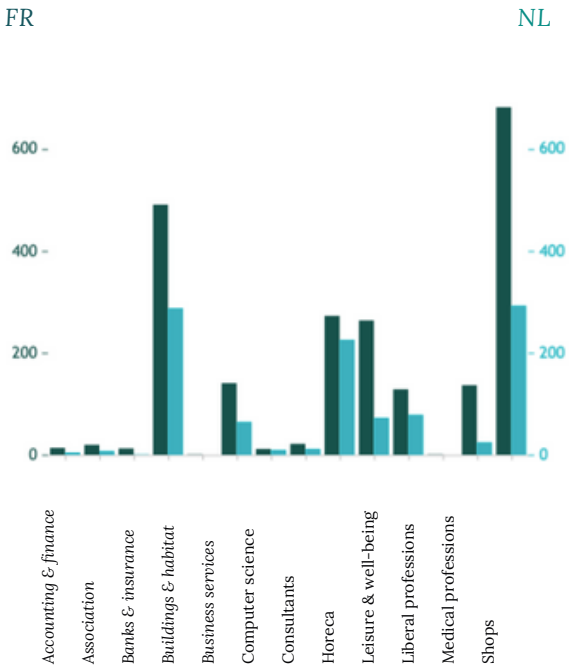
Nos consultants ont parcouru toute la Belgique, des grandes zones urbaines aux communes et villages les plus reculés. Dans la quasi-intégralité des cas, notre interlocuteur-trice est le dirigeant principal ou associé de l'entreprise.

L'échantillon est à la fois très large, mais aussi très varié sur les secteurs d'activités : commerce (au sens large), bâtiment et habitat constituent toujours les domaines d'activités les plus représentés (soit 53% des sondés). Ce sont également les secteurs qui composent principalement le tissu des petites entreprises en Belgique.

ENTREPRISES INTERVIEWÉES



DOMAINE D'ACTIVITÉ



FOCUS SUR LES TPE

Nombre de collaborateurs

1 employé	28,52%
Entre 2 et 5	60,50%
Plus de 5	10,98%

L'enquête a porté sur les TPE, comme en témoigne le fait que 89,02% des 3.286 sociétés interviewées emploient moins de 5 collaborateurs-trices. Bien que 10,98% des personnes interrogées soient issues d'entreprises de plus de 5 collaborateurs-trices, seulement 3,73% appartiennent à des entreprises de plus de 10 collaborateurs-trices.

SKYFORCE
CYBER SECURITY

2. USAGE ET PRÉSENCE

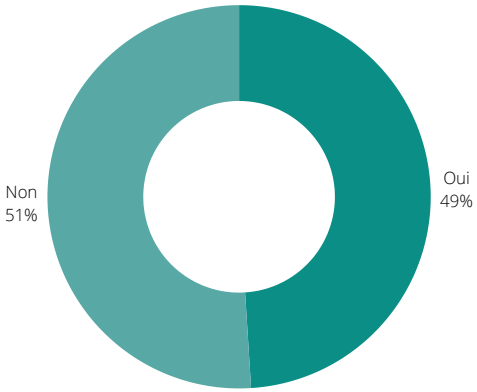
Sur Internet

Usage et présence sur le web

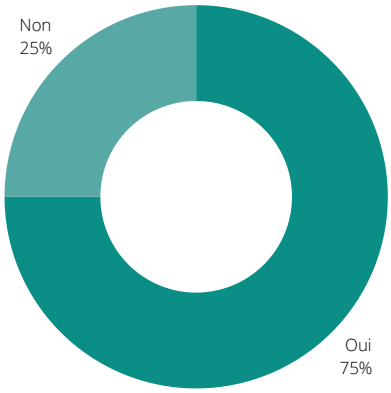
Avez-vous un site internet ?

Les entrepreneurs néerlandophones semblent toujours plus enclins que les entrepreneurs francophones à posséder un site web, avec 75% d'entre eux ayant leur propre site internet comparativement à 49% du côté wallon.
De manière globale, 58% des dirigeants disposent d'un site internet.

FR



NL

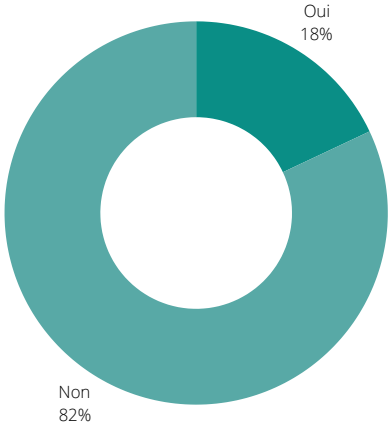


Avez-vous un site e-commerce ?

Tout comme l'année précédente, 88% des dirigeants interrogés restent sans site e-commerce et ce, malgré le succès des achats en ligne. En effet, les Belges ont dépensé près de 8 milliards d'euros en ligne au cours du premier semestre 2023.

FR

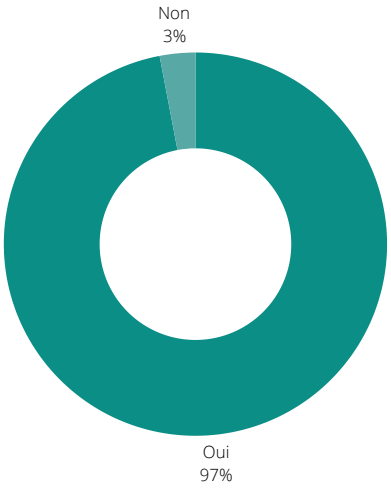
NL



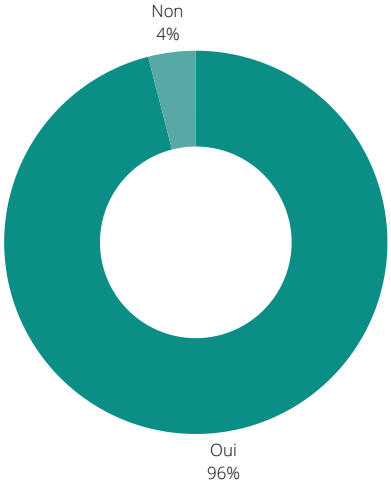
Opérations bancaires et achats en ligne

Faites-vous vos opérations bancaires et/ou vos achats sur Internet ?

FR



NL



97% des dirigeants continuent d'effectuer leurs opérations bancaires en ligne, et cette proportion reste inchangée par rapport à l'année précédente.

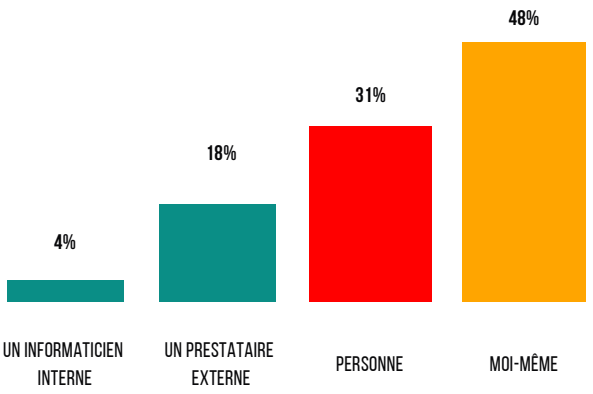
3. PROTECTION

État des lieux

Protection de nos TPE / PME

Seulement 22% des entreprises ont recours à un professionnel, tels un informaticien ou un prestataire externe, pour assurer leur sécurité informatique. Dans 78% des cas, cette tâche est assumée par le dirigeant ou n'est tout simplement pas effectuée.

Qui gère la sécurité informatique de votre entreprise ?



Cette observation est d'autant plus inquiétante, car de plus en plus d'entrepreneurs gèrent leur cybersécurité eux-mêmes.
Or, il est crucial que les chefs d'entreprises reconnaissent la nécessité d'adopter une protection informatique professionnelle. Ce passage met en lumière l'urgence pour les dirigeants d'agir face à la diminution de certaines pratiques sécuritaires et souligne l'importance vitale de la cybersécurité dans le contexte actuel.

LES PETITES ENTREPRISES, PLUS EXPOSÉES AUX CYBERATTAQUES

Conscients qu'elles disposent souvent de ressources et de capacités de défense limitées, les hackers ciblent spécifiquement les petites structures.

Cependant, les conséquences d'une cyberattaque peuvent être dévastatrices, allant de pertes financières importantes à des dommages à la réputation et à la perte de clients.

Par conséquent, il est essentiel pour ces petites entreprises de prendre des mesures proactives pour renforcer leur posture de sécurité.

Protection, état des lieux

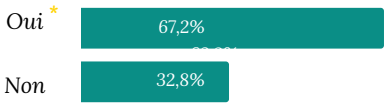
Année après année, nos audits révèlent une tendance constante : la majorité des entreprises n'instaure pas de protection complète face aux menaces en ligne.

Cette année, le cryptage des données a évolué de manière remarquable. Habituellement négligé par les chefs d'entreprise, il a augmenté de **44,44%**, soulignant ainsi une prise de conscience de son importance dans la protection des informations confidentielles et sensibles.

En revanche, l'utilisation d'un pare-feu et les sauvegardes de données ont diminué de façon significative malgré leur belle évolution les précédentes années. Le recours à un pare-feu a baissé de **16,26%**, mettant en lumière un recul dans la protection des réseaux contre les menaces extérieures.
De plus, pourtant indispensables à la pérennité d'une activité, les sauvegardes régulières des données ont diminué de **29,88%**, ce qui est particulièrement préoccupant en matière de cybersécurité. En cas de cyberattaque, telle qu'une attaque par ransomware ou une violation de données, les entreprises risquent de perdre l'intégralité ou une partie importante de leurs données si elles ne disposent pas de sauvegarde adéquate.

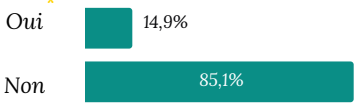
C'est pour ces raisons que nous nous engageons à poursuivre notre mission en fournissant des solutions de sécurité de pointe pour soutenir et protéger les indépendants en Belgique.

Avez-vous un antivirus ?



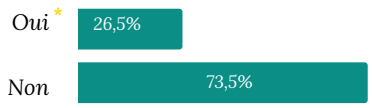
*64,5% en 2022

Disposez-vous d'un anti-spyware ?



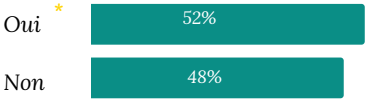
*15,9% en 2022

Disposez-vous d'un logiciel anti-spam ?



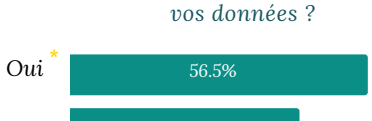
*24,9% en 2022

Avez-vous un pare-feu ?



*62,1% en 2022

Faites-vous régulièrement des sauvegardes de vos données ?



*59,5% en 2022

Les données de vos ordinateurs sont-elles cryptées ?

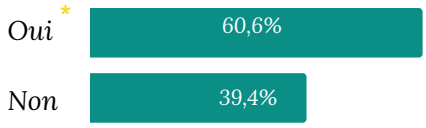
*6,3% en 2022

Confusion privé/pro

La frontière entre vie personnelle et vie professionnelle est primordiale, et les chefs d'entreprise semblent en prendre conscience. Cette année, ils sont moins nombreux (**-2,4%**) à avoir partagé le mot de passe du wifi de leur entreprise à une personne externe, et ils sont plus nombreux (**+4,3%**) à supprimer les données de leurs anciens appareils.

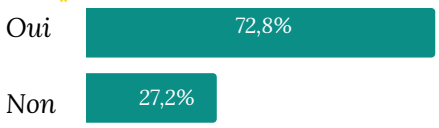
Cette évolution marque une tendance positive vers une meilleure distinction entre vie personnelle et vie professionnelle.

Avez-vous déjà partagé le mot de passe du wifi de l'entreprise à quelqu'un d'externe ?



63% en 2022

Supprimez-vous les données des anciens appareils que vous remplacez ?

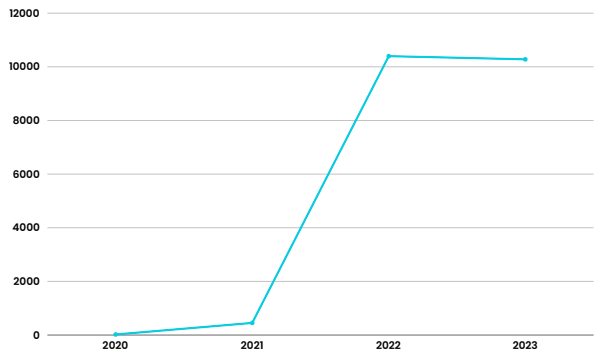


*68,5% en 2022

Quelques chiffres

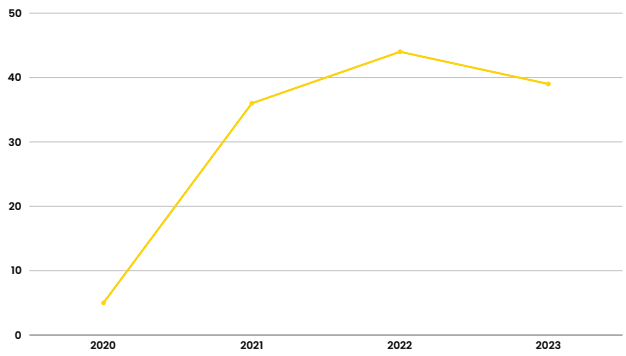
Sur les 3.7OO indépendants protégés par la Cyberbox

Phishing



Par Cyberbox / an

Ransomware



Par Cyberbox / an

Les graphiques ci-dessus indiquent le nombre de requêtes de **phishing** et de **ransomware** arrêtées par Cyberbox et par année.

L'évolution des tentatives de **phishing** et de **ransomware** démontre une augmentation significative entre 2020 et 2022, suivie d'une légère diminution en 2023. Cela suggère que les cybercriminels ont intensifié leurs efforts en raison de la transition vers un **travail à distance,** à la suite de la pandémie de **Coronavirus**, mais aussi qu'ils ciblent de plus en plus les entreprises de toutes tailles. La légère baisse observée en 2023, quant à elle, indique que les mesures de protection mises en place deviennent plus **efficaces**. Néanmoins, le nombre élevé de requêtes de phishing reste préoccupant et souligne la nécessité pour les petites structures de rester vigilantes et bien **protégées**.

Ces chiffres illustrent nettement **l'escalade des menaces** informatiques auxquelles sont confrontées les petites entreprises, mettant en évidence l'importance de la cybersécurité dans le paysage numérique actuel. La protection contre ces risques nécessite une **vigilance** continue, l'adoption de technologies de sécurité avancées telle que la Cyberbox, et une **sensibilisation** accrue aux bonnes pratiques en matière de cybersécurité.

En gardant cela à l'esprit, nous continuons à suivre de près l'évolution de ces attaques et à fournir des **ressources** et des **conseils** pour aider les petites structures à se protéger contre ces menaces grandissantes.

Hit-parade 2024

L'année 2023 n'a pas épargné nos clients, qui ont dû faire face à des **dizaines de milliers de tentatives de cyberattaques.** Afin de garantir leur sécurité, nous avons procédé à la correction de ces infections, dont nous dressons ci-dessous le classement :

1. JS/ADWARE.ADPORT.A

   Application.
   JS/ADWARE.ADPORT.A est un logiciel publicitaire (adware) indésirable, généralement installé à l'insu de l'utilisateur, souvent caché dans des logiciels gratuits téléchargés sur Internet.

2. WIN64/ROOTKIT.AGENT.AZ

   Application.
   WIN64/ROOTKIT.AGENT.AZ est un logiciel malveillant qui se cache dans votre système pour dissimuler les actions d'autres logiciels malveillants.

3. HEUR:TROJAN.SCRIPT.GENERIC

   Trojan.
   HEUR.TROJAN.SCRIPT.GENERIC identifie des scripts suspects, similaires aux Cheveaux de Troie, grâce à une analyse de leur comportement.

4. JS/ADWARE.SCULINST.S

   Application.
   JS/ADWARE.SCUNLIST.S est un adware qui s'installe sans permission, affichant des publicités intrusives et collectant des informations sur votre navigation.

5. HEUR: ADWARE.SCRIPT.PUSHER.GEN

   Application.

6. WIN32/YTDDOWNLOADER.H

   Application.
   WIN32/YTDDOWNLOADER.H est un programme indésirable, souvent installé sans accord, et qui ralentit votre ordinateur. Bien qu'il permette de télécharger des vidéos depuis des plateformes connues, il s'accompagne souvent de logiciels non souhaités.

7. HEUR: ADWARE.SCRIPT.GENERIC

   Application.

8. JS/ADWARE.SCUNLIST.J

   Application.

9. HTML/PHISHING.GEN

   Trojan.

10. JS/ADWARE.AGENT.CZ

    Application.

Constat

Pourquoi protéger son entreprise ?

Conformité réglementaire

Les entreprises sont soumises à des lois et à des réglementations, notamment le Règlement Général sur la Protection des Données. Il est donc important de se conformer aux lois et aux réglementations en matière de cybersécurité pour éviter ces conséquences.

Finances

En cas de cyberattaque, les entreprises peuvent subir d'importantes pertes financières, des interruptions de service, des coûts de récupération des données...
Et ces pertes peuvent affecter négativement la capacité de l'entreprise à fournir des services ou des produits à ses clients. En conséquence, cela entraîne également une baisse des revenus et une perte de parts de marché.

Réputation

Élément indispensable d'une société, la réputation peut être grandement impactée à la suite d'une cyberattaque. Les clients peuvent perdre confiance en l'entreprise si leurs données personnelles sont volées ou compromises, ce qui peut entraîner une baisse des ventes et une perte de clients. De plus, il est possible que les médias et d'autres entreprises diffusent des informations négatives à propos de la société en question, et endommagent sa réputation ainsi que son image de marque.

En tant que Directeur Financier de SKYFORCE Cyber Security SRL, je tiens à souligner l'importance cruciale de la cybersécurité non seulement comme un pilier de notre offre de service mais aussi comme une composante essentielle de notre propre stratégie d'entreprise. Les récentes observations sur le terrain et les études montrent clairement que les cyberattaques peuvent avoir des répercussions dévastatrices sur la réputation et les finances d'une société, soulignant notamment l'importance de protéger les données personnelles de nos clients, une responsabilité accentuée par le RGPD.

Face à ces enjeux, notre société continue d'investir de manière proactive dans des technologies de pointe, dans le renforcement des compétences de nos employés, tout en développant des partenariats stratégiques pour enrichir notre écosystème de sécurité.
Grâce à notre approche proactive et notre engagement envers l'excellence en matière de cybersécurité, nous visons à minimiser ces risques, à protéger notre réputation et à assurer une croissance durable à long terme pour notre entreprise et nos actionnaires.
En protégeant notre entreprise contre les cyberattaques, nous protégeons non seulement nos actifs financiers et notre réputation, mais nous renforçons également la confiance de nos clients et de nos partenaires dans notre capacité à fournir des services et des produits sécurisés.

Pierre-Olivier Glachant

Co-Founder & Financial Director

À PROPOS DE SKYFORCE

Fondée en 2019 et installée à Waterloo, Skyforce se positionne comme un précurseur sur le marché des services de cybersécurité intégrés à destination des très petites, petites et moyennes entreprises.

Notre expertise s'adresse à tous les secteurs d'activité. En Belgique, plus de 3.700 entreprises nous ont déjà confié leur cybersécurité, faisant de Skyforce un acteur important de la protection informatique des petites structures.

MISSION

Notre mission est de sécuriser les données des TPE et PME contre les menaces et les cyberattaques. Nous accompagnons nos clients dans la gestion sécuritaire de leur infrastructure IT, qu'elle soit monoposte ou en réseau grâce à un concept de protection innovant et inédit.

VISION

L'innovation, la veille permanente, la méthode et la rigueur sont au cœur de notre ambition pour devenir un leader international dans la sécurité du digital.