CYBERSÉCURITÉ - TPE ET PME BELGES

BAROMÈTRE ANNUEL

2023

SKYFORCE CYBER SECURITY

MÉTHODOLOGIE

Baromètre annuel 2023

Ce quatrième baromètre Skyforce se base sur des visites et entretiens individuels de 3.840 sociétés belges, effectués tout au long de l'année 2022.
Nos consultants ont interviewé directement les dirigeants de ces institutions, qui sont essentiellement des microentreprises 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.

« Nous mettons un point d'honneur à former nos représentants de manière continue afin de garantir des audits de qualités, cohérents et rigoureux. De cette façon, nous pouvons également améliorer la qualité de nos services. »

Mathieu Lardinois

Co-Founder & Sales Manager

3840 ENTREPRISES SONDÉES

POINTS MARQUANTS RÉVÉLÉS PAR L'ÉDITION 2023

CYBERSÉCURITÉ NON GÉRÉE PAR UN PROFESSIONNEL

DONNÉES TOUJOURS NON CRYPTÉES

PROTECTION INCOMPLÈTE

PHISHING DE PLUS EN PLUS SOPHISTIQUÉS

SKYFORCE
CYBER SECURITY

PHISHING : MENACE MAJEURE

En 2023, le phishing continue d'être une attaque courante et efficace

Méthode utilisée par les cybercriminels pour dérober des données confidentielles telles que des mots de passe, des numéros de carte de crédit et bien plus encore, le phishing reste une attaque courante qui fonctionne !

Les tendances 2023 :

- IA

Les pirates informatiques utilisent désormais des outils d'intelligence artificielle afin de réaliser des phishing sophistiqués. Ces outils leur permettent de générer automatiquement des e-mails frauduleux, de faux sites web, et même des messages vocaux personnalisés pour tromper leur cible.

- Business email compromise (BEC) & email account compromise (EAC)

Ce genre de techniques vise à faire en sorte que la victime pense recevoir un e-mail de la part d'un cadre supérieur afin de l'amener à transférer de l'argent ou à communiquer des informations confidentielles.

- Whaling phishing

Attaques ciblant spécifiquement les hauts dirigeants d'une entreprise en se faisant passer pour un partenaire commercial par exemple, afin d'obtenir des informations sensibles ou des accès privilégiés.

Philippe Verwerft

Co-Founder & ICT Director

"Chaque jour, nous sommes confrontés à la persistance et à la crédibilité des attaques par phishing. Nous recevons fréquemment des sollicitations de personnes confrontées à ce type d'attaques. Nous intervenons immédiatement pour résoudre ces situations."

1. PROFILS-TYPE

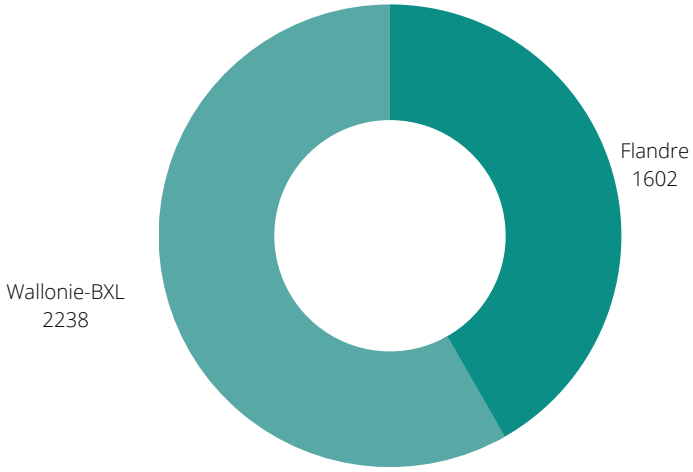
Des entreprises interrogées

Profils-type des entreprises participantes

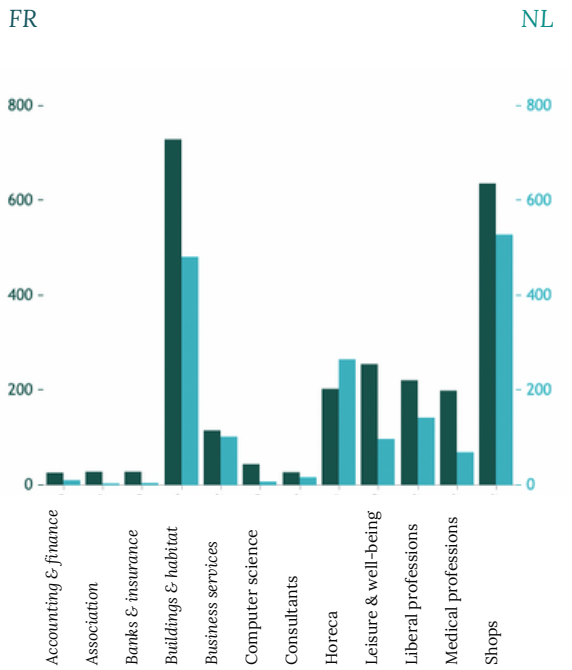
Nos consultants ont parcouru toute la Belgique, des grandes zones urbaines aux communes et villages les plus reculés. Dans la quasi-intégralité des cas, notre interlocuteur/interlocutrice est le dirigeant principal ou associé de l'entreprise.

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 62% 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	30,42%
Entre 2 et 5	58,07%
Plus de 5	11,51%

L'enquête a porté sur les TPE, comme en témoigne le fait que 88,49% des 3.840 sociétés interviewées emploient moins de 5 collaborateurs. Bien que 11,51% des personnes interrogées soient issues d'entreprises de plus de 5 collaborateurs-trices, seulement 3,86% appartiennent à des entreprises de plus de 10 collaborateurs-trices.

SKYFORCE CYBER SECURITY

2. USAGE ET PRÉSENCE

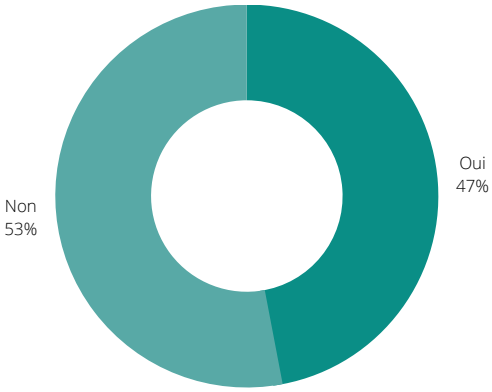
Sur Internet

Usage et présence sur le web

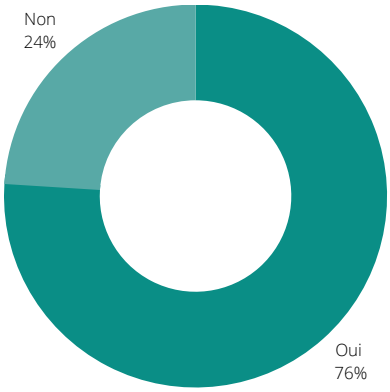
Avez-vous un site internet ?

La situation reste constante par rapport aux précédentes années. Les dirigeants interviewés ont toujours des usages très différents d'Internet. On note une claire distinction régionale, mais, de manière globale, 62% des interrogés disposent d'un site web.

FR



NL

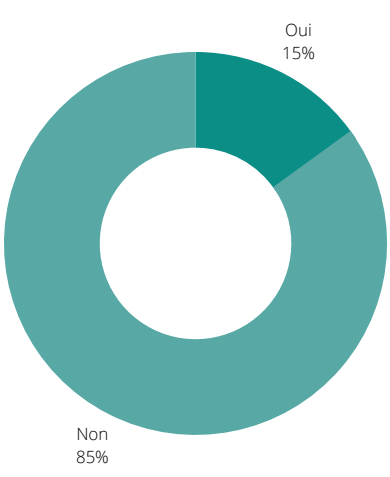


Avez-vous un site e-commerce ?

La situation demeure stable : en tout, 88% des personnes interrogées n'ont pas de site e-commerce, ce qui est comparable aux années précédentes. Bien que la vente en ligne ait augmenté avec la digitalisation et la crise sanitaire, les sondés sont encore peu nombreux à bénéficier d'un site e-commerce, malgré les difficultés à toucher leur public en ligne.

FR

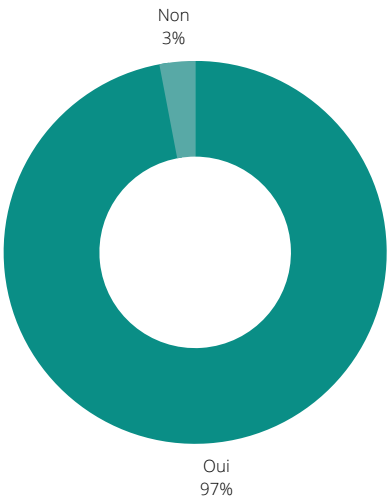
NL



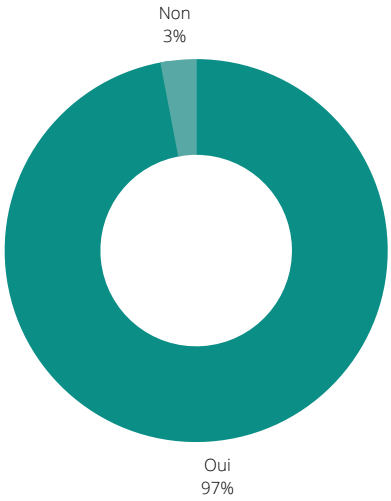
Opérations bancaires et achats en ligne

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

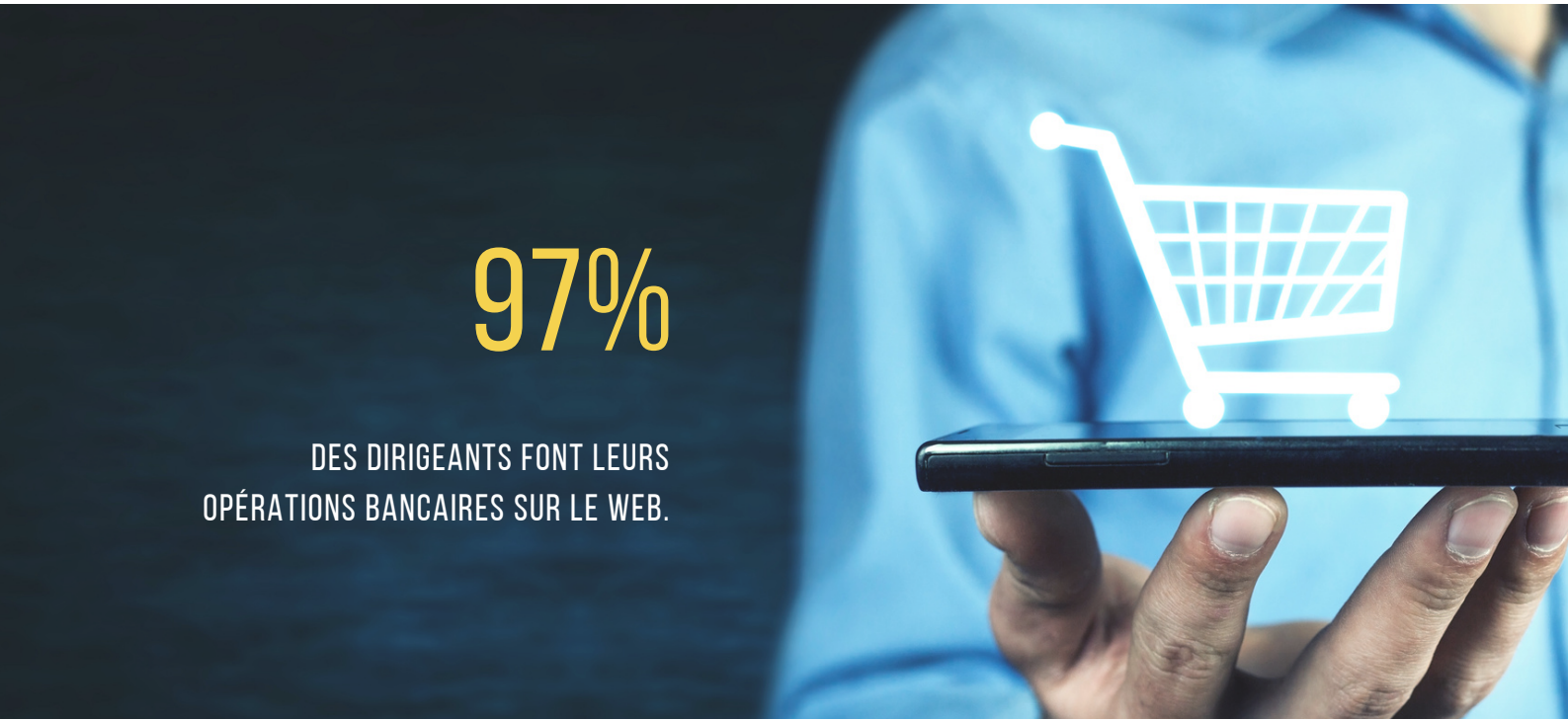
FR



NL



97% des dirigeants continuent d'effectuer leurs opérations bancaires en ligne, et cette proportion reste stable par rapport à l'année précédente, avec une augmentation d'à peine 1%.



3. PROTECTION

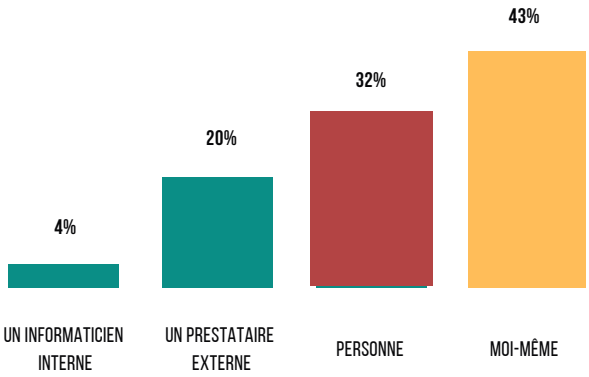
État des lieux

Protection de nos TPE / PME

Seulement 24% des entreprises ont recours à un professionnel, tels un informaticien ou un prestataire externe, pour assurer leur sécurité informatique. Dans 76% des cas, cette tâche est assumée par le dirigeant ou n'est tout simplement pas effectuée.

Malgré une légère augmentation de 4% des dirigeants qui décident d'opter pour une protection informatique professionnelle, la situation demeure préoccupante.
Or, la quasi-totalité des piratages informatiques pourrait facilement être évitée.

Qui gère la sécurité informatique de votre entreprise ?



LES PETITES ENTREPRISES, EN PREMIÈRE LIGNE DES CYBERATTAQUES

Les pirates informatiques sont toujours à la recherche de cibles faciles, et malheureusement, les petites entreprises sont en haut de leur liste. Ces derniers savent qu'elles ont souvent moins de ressources et moins de temps pour se prémunir contre les cyberattaques, et sont donc plus vulnérables.

C'est pourquoi il est essentiel pour les petites structures de prendre des mesures de sécurité en ligne pour se protéger contre ces hackers.

Protection, état des lieux

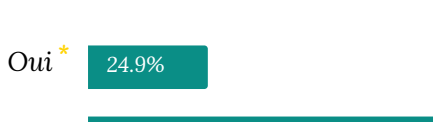
La première observation reste que la majorité des sociétés interrogées disposent, dans les meilleurs cas, d'une protection incomplète en dépit de leur exposition digitale toujours plus grande et des pirates informatiques de plus en plus compétents.

On constate toutefois une augmentation de l'utilisation d'un pare-feu (+19,65 %), d'un logiciel anti-spam (+22,06 %), ainsi que de l'utilisation de back-up qui continue de progresser (+5,7 %). La conscientisation semble donc continuer de faire son chemin du côté des dirigeants d'entreprise qui ne se demandent plus s'ils seront un jour la cible d'une attaque, mais plutôt quand et comment cela se produira.
Néanmoins, bien que des progrès aient été réalisés en matière de sécurité informatique, près de la moitié des entreprises interrogées courent encore le risque de perdre leurs données en cas de cyberattaque.

Par ailleurs, le cryptage des données et des appareils demeure négligé au sein des petites structures (-23 %). Ce constat est d'autant plus inquiétant, car, en cas d'intrusion, le cybercriminel peut accéder aisément aux informations privées, confidentielles et sensibles, mais aussi aux mots de passe.

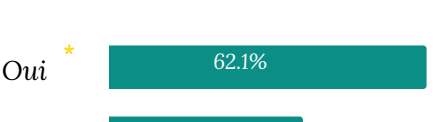
Enfin, le facteur temps reste un obstacle pour ces dirigeants qui sont sur tous les fronts afin d'assurer la gestion de leur société.
C'est pourquoi nous sommes déterminés à fournir une solution complète et un service de proximité pour aider les petites entreprises à protéger leur activité contre ces menaces.

Avez-vous un antivirus ?



*63.2% en 2021

Disposez-vous d'un anti-spyware ?



*17.2% en 2021

Disposez-vous d'un logiciel anti-spam ?

*20.4% en 2021

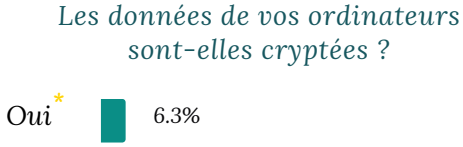
Avez-vous un pare-feu ?

*51.9% en 2021

Faites-vous régulièrement des sauvegardes de vos données ?

*56.3% en 2021

Les données de vos ordinateurs sont-elles cryptées ?

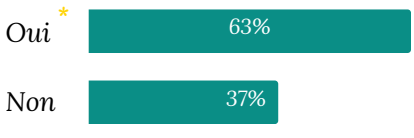


*8.2% en 2021

Confusion privé/pro

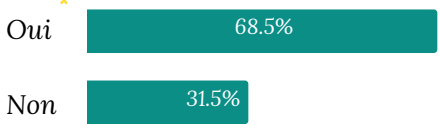
La frontière entre vie personnelle et vie professionnelle suscite encore de nombreuses préoccupations, comme le montrent les statistiques : **63%** des individus interrogés ont déjà **partagé le mot de passe Wi-Fi** de leur entreprise avec une personne extérieure. Cela constitue 4% supplémentaire en comparaison à 2021. Or, il est crucial de définir des **limites** claires entre ces deux sphères, car leur mélange représente une porte ouverte aux pirates informatiques et au vol de données sensibles.

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



*59.1% en 2021

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

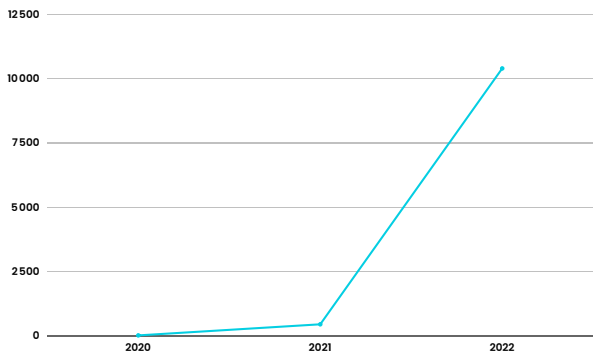


*67.7% en 2021

Quelques chiffres

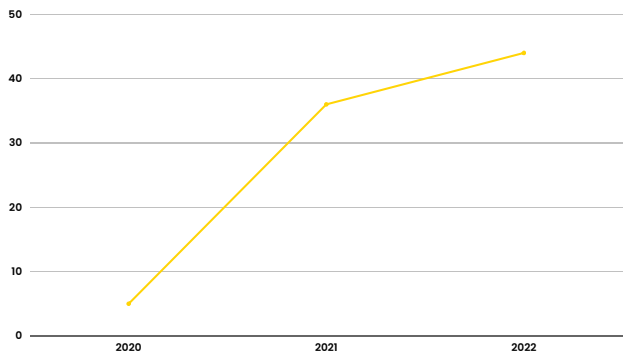
Sur les 3.OOO indépendants protégés par la Cyberbox

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.
Les chiffres montrent une claire **tendance à la hausse** concernant ces attaques.

Nous pouvons observer que le nombre moyen de requêtes de ransomware bloquées par Cyberbox a augmenté progressivement, passant de 5 en 2020 à 36 en 2021, puis à 44 en 2022, soit environ 8 fois plus.
Pour les requêtes de phishing en revanche, la croissance est nettement plus importante, passant de 21 en 2020 à 452 en 2021, puis à 10.397 en 2022, soit près de **500 fois plus élevées** en 3 ans !

Le nombre de cyberattaques continue de croître chaque année, avec des **conséquences** de plus en plus graves pour les petites entreprises.
En gardant à l'esprit l'importance de la cybersécurité, 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 2022

L'année 2022 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. HEUR:TROJAN.SCRIPT.GENERIC

   Trojan

2. JS/ADWARE.ADPORT.A

   Application

3. HTML/PHISHING.GEN

   Trojan

4. JS/ADWARE.SCULINST.J

   Application

5. MSIL/AGENT.CQF

   Trojan

6. JS/ADWARE.SCULINST.S

   Application

7. JS/ADWARE.TERRACLICKS.A

   Application

8. JS/ADWARE.AGENT.AY

   Application

9. WIN32/YTDDOWNLOADER.H

   Application

10. JS/PACKED.AGENT.K

    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.

Christophe Henri

Co-Founder & Technical Operations Manager

"Au fil des ans, la technologie a transformé la façon dont nous travaillons et interagissons les uns avec les autres. Alors que nous profitons des avantages de cette transformation, nous devons également être conscients des menaces qui l'accompagnent. Les cyberattaques sont de plus en plus fréquentes et sophistiquées, et aucune entreprise n'est à l'abri. C'est pourquoi il est primordial que les petites structures prennent des mesures pour protéger leurs données et leurs infrastructures informatiques.
En fin de compte, la cybersécurité est un élément essentiel de toute entreprise moderne, quelle que soit sa taille. En protégeant vos données et en assurant la sécurité de votre infrastructure informatique, vous pouvez protéger votre entreprise contre les pertes financières, une mauvaise réputation et toutes autres conséquences désastreuses d'une cyberattaque."

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 3.000 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.