Cybersécurité des PME : comprendre les failles, combler les manques, identifier l'essentiel

Les problématiques rencontrées
par les PME en Europe et en Afrique

kaspersky

kaspersky.fr

Résumé

Les 5 points clés ..... Page 02

Méthodologie ..... Page 02

Introduction ..... Page 03

Du tableau blanc à la réalité ..... Page 04

- Faute de stratégie concrète, les PME naviguent à vue en cybersécurité ..... Page 04
- Les décideurs veulent mieux appréhender la cybersécurité ..... Page 04

Le décalage entre la direction générale, le service informatique et les partenaires externes ..... Page 06

- Surcharge, manque de personnel, manque de soutien ..... Page 06
- Partenaires externes : du fournisseur au partenaire de confiance ..... Page 07

Conclusion ..... Page 09

Kaspersky pour les PME ..... Page 09

Méthodologie
En août et en septembre, Kaspersky a chargé Arlington Research de mener un sondage en ligne à remplir de façon autonome auprès de décideurs dont les fonctions intègrent de manière significative la cybersécurité et qui travaillent pour des entreprises de moins de 500 employés en Europe et en Afrique. Arlington a conduit un total de 880 entretiens auprès de ce public, à raison de 600 en Europe et de 280 en Afrique. 60 entretiens ont été menés dans chacun des pays suivants : Allemagne, Autriche, Suisse, Royaume-Uni, France, Espagne, Italie, Grèce, Roumanie, Serbie, Maroc, Algérie, Tunisie et Cameroun. Le Sénégal et la Côte d'Ivoire ont fait l'objet de 20 entretiens chacun.

Les 5 points clés

1. **75 % des petites et moyennes entreprises (PME) en Europe et en Afrique** agissent selon des stratégies théoriques ou des objectifs flous qui ne parviennent pas à se traduire par une protection réelle, même si **29 %** d'entre elles disposent d'une stratégie de cybersécurité complète et entièrement mise en œuvre.
2. **29 % des décideurs affirment que le suivi de** toutes les cybermenaces potentielles est déjà un travail à plein temps, tandis que **18 % des PME ne disposent pas** d'une plateforme de cybersécurité digne de confiance, fiable et abordable.
3. **22 % des PME ne disposent pas ou pas suffisamment de personnel qualifié** pour gérer et exploiter des solutions de cybersécurité.
4. **34 % des décideurs déclarent avoir besoin de mieux appréhender** les moyens d'optimiser leur façon de répondre aux cyberincidents et de les résoudre, alors que cela constitue le cœur même de leur travail.
5. **21 % des décideurs déclarent recevoir tellement d'alertes système** qu'ils ne savent même plus lesquelles requièrent une attention immédiate.

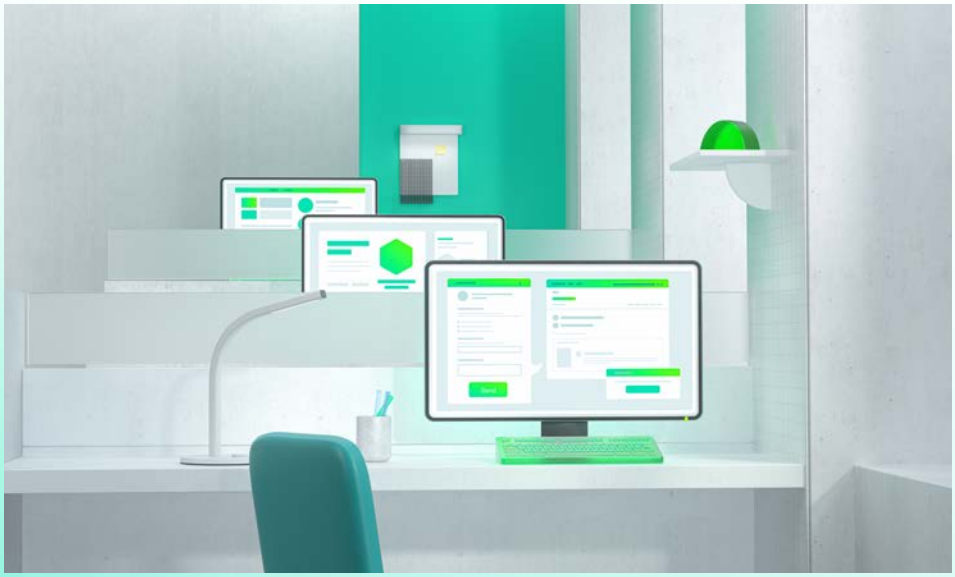
Introduction

Qu'est-ce qui pose problème, qu'est-ce qui manque et qu'est-ce qui est vraiment utile en matière de cybersécurité ? Voilà LES questions qu'aucune petite ou moyenne entreprise (PME) ne devrait ignorer, alors que la plupart le font encore. Pour un trop grand nombre d'entre elles, la cybersécurité apparaît comme un casse-tête sans intérêt et hors de prix, enveloppé dans un jargon qu'elles ne maîtrisent pas. La cybersécurité est déroutante. La cybersécurité coûte cher. Et personne ne parvient à en expliquer clairement les principes. Mais est-ce vraiment le cas ?

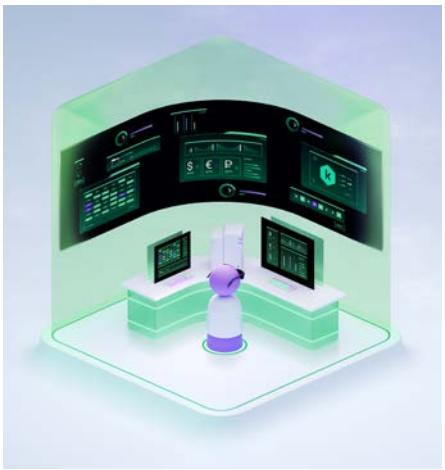
Entre-temps, les menaces évoluent rapidement. D'après le Bulletin de sécurité 2024 de Kaspersky, les systèmes de détection de l'entreprise ont signalé en moyenne 467 000 fichiers malveillants par jour à travers le monde, soit un bond de 14 % par rapport à 2023. Les détections de chevaux de Troie ont augmenté à elles seules de 33 %, tandis que les chevaux de Troie compte-gouttes ont grimpé en flèche de 150 %.

De plus, le dernier Rapport sur les menaces pour les PME de Kaspersky confirme ces chiffres, tant en Europe qu'en Afrique. En Europe, l'Autriche a enregistré le plus grand nombre d'attaques, représentant 40 % de tous les cas détectés dans lesquels des PUA (application potentiellement indésirable) et des programmes malveillants ciblant les PME imitaient des marques légitimes. Viennent ensuite l'Italie (25 %), l'Allemagne (11 %), l'Espagne (10 %) et le Portugal (6 %). En Afrique, le Maroc arrive en tête de liste avec 41 % de toutes les PUA détectées ciblant les PME, la Tunisie (24 %) et l'Algérie (16 %) étant également fortement touchées. Le Sénégal (7 %) et le Cameroun (7 %) ont enregistré des chiffres plus faibles, la Côte d'Ivoire représentant quant à elle 5 %.

Le message est clair : Les PME ne sont pas seulement dans le collimateur des cybercriminels ; elles en sont la cible principale. Mais où résident les pièges en matière de cybersécurité ?



Près de **75 %** des PME naviguent à vue, s'appuyant sur des plans vagues qui n'offrent pas de protection réelle.



Du tableau blanc à la réalité

Faute de stratégie concrète, les PME naviguent à vue en cybersécurité

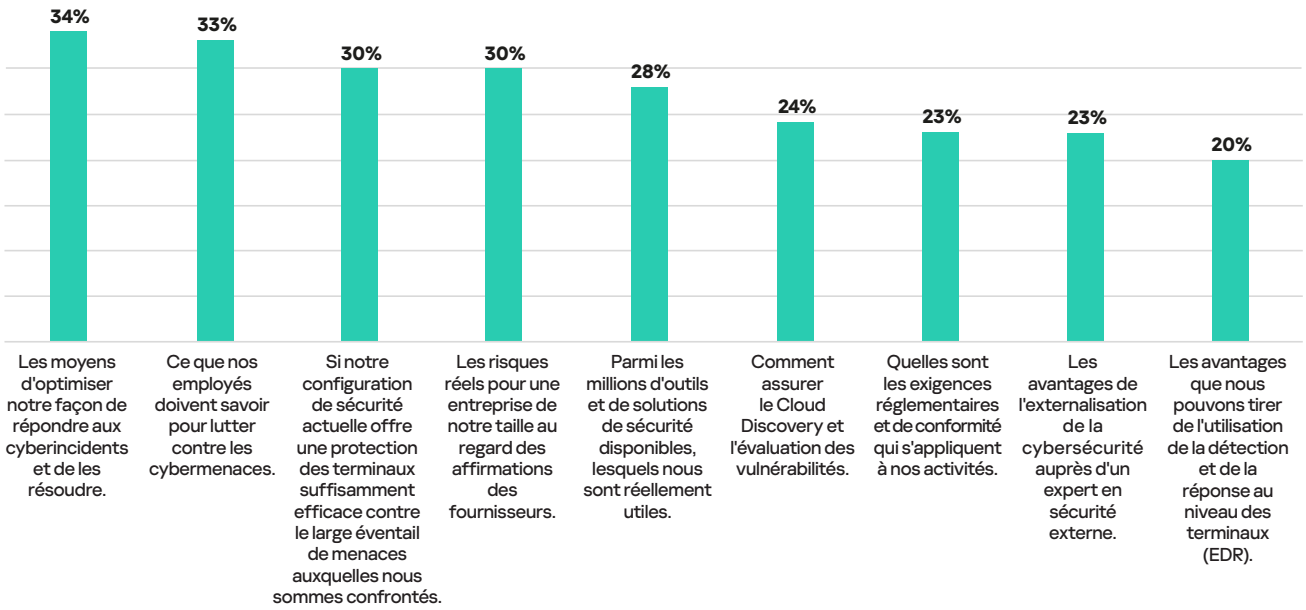
Au sein de nombreuses PME en Europe et en Afrique, la stratégie en matière de cybersécurité et la mise en œuvre de solutions efficaces sont entravées par un manque de savoir-faire et un scepticisme généralisé à l'égard des fournisseurs de services de sécurité. Malgré l'engouement pour la cybersécurité dans les salles de conseil et au cours des présentations effectuées par les fournisseurs, la réalité paraît très différente pour les petites et moyennes entreprises.

Moins d'un tiers (29 %) des PME en Europe et en Afrique déclarent disposer d'une stratégie de cybersécurité complète et pleinement mise en œuvre. Près de la moitié (46 %) d'entre elles admettent que leur stratégie existe davantage sur le papier que dans la pratique. Par ailleurs, 19 % de ces entreprises travaillent à la réalisation d'une série d'objectifs sans disposer d'une stratégie concrète, tandis que 5 % d'entre elles avouent ne pas avoir d'orientation du tout, même si elles savent qu'elles devraient probablement en avoir une. Dans l'ensemble, les trois quarts (75 %) des PME naviguent à vue, agissant selon des stratégies théoriques ou des objectifs flous qui ne parviennent pas à se traduire par une protection réelle.

Les décideurs veulent mieux appréhender la cybersécurité

Ce décalage apparaît encore plus alarmant lorsque l'on considère le peu de confiance que semblent avoir de nombreuses équipes informatiques vis-à-vis de leurs propres défenses. Un tiers (34 %) de ces équipes déclarent avoir besoin de mieux appréhender les moyens d'optimiser leur façon de répondre aux cyberincidents et de les résoudre. Elles sont presque autant (33 %) à être du même avis en ce qui concerne la façon dont les employés devraient être formés pour savoir quoi faire face aux cybermenaces. Près d'une équipe sur trois (30 %) ne sait pas vraiment si la protection de ses terminaux est suffisamment efficace contre le large éventail de menaces auxquelles elle est confrontée, tandis qu'une équipe sur cinq (20 %) admet ne pas bien comprendre les avantages de la mise en œuvre d'une solution de détection et de réponse au niveau des terminaux (EDR).

Ce que les décideurs veulent mieux appréhender...



Ce scepticisme s'étend au marché lui-même. Un peu moins d'un tiers (30 %) des PME doutent que les risques décrits par les fournisseurs reflètent réellement les dangers réels auxquels sont confrontées les entreprises de leur taille. Pendant ce temps, la confusion autour des priorités pratiques enferme ces entreprises dans un mode réactif. Moins d'un tiers (28 %) désirent mieux comprendre quels sont les outils de cybersécurité dont elles ont réellement besoin parmi une infinité d'options, tandis que 23 % peinent même à identifier les exigences réglementaires ou de conformité qui s'appliquent à elles.

Points clés à l'échelle des pays : Europe

En Europe, les PME britanniques (67 %) sont les plus susceptibles de disposer d'une stratégie (bien que celle-ci soit souvent plus théorique que pratique), suivies par les PME espagnoles (62 %) et allemandes (53 %), alors que ce chiffre est de 48 % dans l'ensemble de la région. La Suisse, quant à elle, affiche la plus forte dépendance aux objectifs plutôt qu'à la stratégie (25 % contre 18 % dans l'ensemble).

L'incertitude relative à la protection des terminaux est la plus forte en Roumanie (43 %) et en Serbie (40 %), contre 31 % dans l'ensemble. Les PME roumaines tendent également à se soucier davantage de faire la distinction entre les risques réels associés à leur taille et les affirmations des fournisseurs (38 % contre 28 % dans l'ensemble).

Le manque de connaissances en matière d'exigences réglementaires et de conformité apparaît plus important en France (35 %), en Autriche et en Serbie (32 % dans les deux cas), contre 23 % dans l'ensemble de l'Europe. Au Royaume-Uni, les PME sont plus nombreuses à vouloir mieux comprendre les avantages de l'externalisation auprès d'experts externes (33 % contre 22 % dans l'ensemble).

Points clés à l'échelle des pays : Afrique de l'Ouest et centrale

En Afrique, les professionnels de la cybersécurité camerounais sont plus enclins à tendre vers des objectifs plutôt que vers une stratégie claire (28 % contre 22 % dans l'ensemble de la région).

Les lacunes en matière de connaissances sont les plus fréquentes au Maroc (47 %) et au Cameroun (42 %), où les PME ont du mal à optimiser leur façon de répondre aux incidents et de les résoudre (contre 37 % dans l'ensemble). En Tunisie, près de la moitié (45 %) des PME ne sont pas certaines que leur configuration actuelle assure une protection suffisante de leurs terminaux, contre 29 % dans l'ensemble. Les PME algériennes ont plus souvent tendance à manquer de lucidité quant aux risques réels associés à la taille de leur entreprise au regard des affirmations des fournisseurs (38 % contre 33 % dans l'ensemble).

Le Maroc se distingue également par un plus grand nombre de PME qui ne savent pas vraiment de quels outils et solutions elles ont réellement besoin (37 % contre 31 % dans l'ensemble de la région). Le Cloud Discovery et l'évaluation des vulnérabilités constituent des défis plus importants au Cameroun (38 %), au Sénégal (35 %) et au Maroc (32 %), contre près d'un tiers (29 %) dans l'ensemble. Au Sénégal, l'incertitude en matière de conformité est particulièrement élevée (40 % contre 24 % dans l'ensemble).

Les PME camerounaises sont celles qui comprennent le moins les avantages de l'externalisation (35 % contre 26 % dans l'ensemble), tandis que le Sénégal est le pays qui a le plus de mal à identifier les avantages de la détection et de la réponse au niveau des terminaux (EDR) (35 % contre 19 % dans l'ensemble).

Le clivage entre la direction, le service informatique et les partenaires externes

Surcharge, manque de personnel, manque de soutien

Alors que la cybersécurité devrait être une priorité pour les entreprises, elle semble encore être considérée comme une simple tâche technique. Alors que les cadres dirigeants débattent des budgets et des priorités, les équipes informatiques des PME à travers l'Europe et l'Afrique sont confrontées à un défi d'une tout autre nature : 18 % d'entre elles ne disposent pas d'une plateforme de cybersécurité digne de confiance, fiable et abordable. Dès lors, il n'est pas étonnant que le simple fait de suivre les cybermenaces potentielles soit devenu un travail à plein temps pour 29 % des responsables informatiques. Un responsable informatique sur cinq (21 %) déclare recevoir tellement d'alertes système qu'il ne sait même plus lesquelles requièrent une attention immédiate. Dans le même temps, 18 % de ces responsables affirment passer plus de temps à dépanner leurs logiciels de sécurité qu'à se défendre contre les menaces réelles.

Le problème est amplifié par un manque de personnel qualifié, 22 % des PME déclarant tout simplement ne pas disposer d'effectifs suffisants pour gérer et exploiter leurs solutions de sécurité. La plupart s'appuient sur des équipes informatiques plus générales (36 %) ou sur des spécialistes en cybersécurité au sein de ces équipes (28 %). Seuls 29 % des PME disposent de leur propre équipe dédiée à la cybersécurité, tandis que 8 % d'entre elles seulement dépendent principalement de partenaires externes pour concevoir et exécuter leurs programmes de cybersécurité.

Les perceptions façonnent également la réalité. Les entreprises disposant d'équipes internes dédiées témoignent du plus haut niveau de satisfaction : 81 % d'entre elles jugent leurs performances bonnes ou très bonnes. Lorsque des spécialistes sont intégrés aux équipes informatiques, le taux de satisfaction atteint 76 %. Cependant, lorsque la cybersécurité est conçue et exécutée par des tiers, seuls 67 % des PME émettent un avis positif, ce qui fait qu'un tiers d'entre elles sont déçues des performances de leurs partenaires. Cette insatisfaction peut expliquer pourquoi si peu d'entreprises considèrent les prestataires externes comme des alliés stratégiques.

Au niveau des dirigeants, le soutien est faible. Plus d'un quart (27 %) des sondés déclarent que leurs pairs dirigeants ne saisissent pas l'importance de la cybersécurité pour leur entreprise. Par conséquent, dans de nombreuses PME, la cybersécurité reste bloquée au niveau technologique, au lieu d'être considérée comme une priorité commune au sein de l'entreprise.

Le dernier Rapport sur les menaces pour les PME de Kaspersky révèle que, dans certaines entreprises **européennes**, les **principales menaces** sont **les portes dérobées** (24 %), les **chevaux de Troie** (17 %) et **not-a-virus: Downloader** (16 %).

En Afrique, le tableau change : **not-a-virus: Downloader** domine (55 %), suivi par **DangerousObject** (14 %) et les **cheveux de Troie** (13 %).

Partenaires externes : du fournisseur au partenaire de confiance

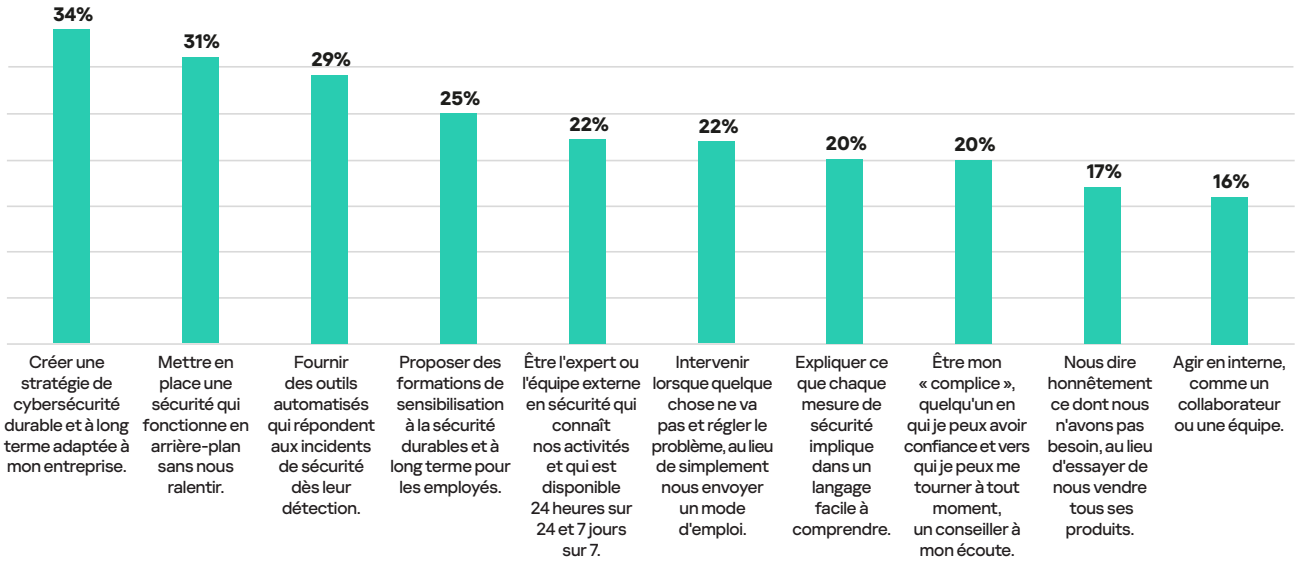
De nombreuses entreprises continuent de s'appuyer fortement sur leurs ressources internes et admettent à demi-mot qu'elles préféreraient bénéficier d'une aide, 12 % des PME déclarant qu'elles aimeraient qu'un partenaire externe se charge de leur cybersécurité, sous toutefois disposer d'un tel partenaire. Par ailleurs, même lorsque les PME font appel à une aide extérieure, les prestataires sont souvent considérés comme de simples pompiers ou techniciens, appelés pour des interventions ponctuelles plutôt que chargés de gérer la cybersécurité dans son ensemble.

Pourtant, leurs attentes sont remarquablement cohérentes et dépeignent le tableau d'un partenariat allant bien au-delà des solutions à court terme. Plus d'un tiers (34 %) des PME aspirent à trouver un partenaire capable d'élaborer des stratégies durables à long terme qui évoluent avec leur entreprise et qui ne se contente pas de répondre aux dernières violations. Un quart (25 %) d'entre elles soulignent l'importance d'une formation de sensibilisation continue pour leurs employés, car elles savent que ces derniers sont autant une cible que leurs systèmes.

Les MSP et les revendeurs peuvent agir en tant que conseillers de confiance, en comblant les lacunes en matière d'expertise et en favorisant une préparation proactive des entreprises.

D'autres mettent l'accent sur la présence et la confiance. Environ une PME sur cinq (22 %) souhaite pouvoir compter sur un expert qui comprend vraiment son environnement et qui est disponible 24 heures sur 24, et pas uniquement pendant les heures de bureau ou après l'ouverture d'un ticket. Par ailleurs, 20 % d'entre elles souhaitent avoir un interlocuteur à leur écoute, c'est-à-dire un conseiller qui fasse partie de l'équipe et qui leur fournisse des réponses honnêtes plutôt que des argumentaires de vente préétablis. Enfin, 17 % sont tout simplement lassées des ventes incitatives. Elles recherchent quelqu'un capable de leur dire « Vous n'en avez pas besoin », quelqu'un qui simplifie les choses au lieu de les compliquer.

Ce qu'un partenaire idéal peut apporter



Il ne s'agit pas là de souhaits abstraits, mais bien de la réalité des attentes des PME, qui représentent une opportunité évidente pour les fournisseurs : Les MSP et les revendeurs peuvent endosser le rôle de conseillers de confiance, en comblant les lacunes en matière d'expertise, en guidant la prise de décision et en faisant passer les entreprises d'une défense réactive à une préparation proactive.

Points clés à l'échelle des pays : Europe

En Europe, les professionnels britanniques sont les plus frustrés par les efforts nécessaires pour suivre les menaces (42 % contre 31 % dans l'ensemble de la région). Les pénuries de personnel sont plus importantes en Roumanie (32 % contre 21 % dans l'ensemble) et en Allemagne (30 % contre 21 % dans l'ensemble). Par ailleurs, les professionnels italiens reçoivent tellement d'alertes qu'ils ne parviennent même pas à savoir si elles sont sérieuses ou non (33 % contre 20 % dans l'ensemble). La Serbie, quant à elle, est confrontée à la fois à une surcharge d'alertes (28 %) et à un manque de plateformes fiables et abordables (30 % contre 16 % dans l'ensemble).

Les équipes informatiques internes dominent en Suisse (47 % contre 35 % dans l'ensemble). Les partenaires externes sont plus fréquents en Grèce (18 % contre 7 % dans l'ensemble). En Espagne, 42 % des PME recherchent un partenaire capable d'élaborer des stratégies à long terme et sur mesure, contre 33 % dans l'ensemble. Les outils automatisés qui répondent immédiatement aux incidents sont les plus appréciés en Allemagne (40 %), au Royaume-Uni (38 %) et en Roumanie (38 %), contre 31 % dans l'ensemble.

Les formations de sensibilisation à long terme pour les employés trouvent le plus d'écho au Royaume-Uni (32 % contre 25 % dans l'ensemble). En France, 28 % des PME souhaitent disposer d'une équipe d'experts externes disponible 24 heures sur 24 et 7 jours sur 7, tandis que l'Allemagne met davantage l'accent sur les partenaires qui interviennent activement en cas de crise (28 % contre 20 % dans l'ensemble).

Les explications dans un langage clair sont plus appréciées en France (28 %) et en Autriche (27 %) que dans l'ensemble de la région (21 %). L'idée d'un partenaire de confiance séduit fortement en Grèce (30 %) et au Royaume-Uni (28 %). En Suisse, 27 % des PME apprécient les partenaires qui leur disent ce dont elles n'ont pas besoin (contre 18 % dans l'ensemble), tandis qu'en Serbie, 33 % d'entre elles préfèrent les spécialistes qui agissent comme des collaborateurs internes (contre 17 % dans l'ensemble).

Points clés à l'échelle des pays : Afrique du Nord, Centrale et de l'Ouest

En Afrique, le manque de sensibilisation à la cybersécurité parmi les dirigeants est le plus marqué en Tunisie (47 % contre 28 % dans l'ensemble de la région). Le Cameroun fait état du plus grand manque de personnel qualifié (33 % contre 24 % dans l'ensemble), le Sénégal est le pays le plus confronté à un flot d'alertes de sécurité (30 % contre 23 % dans l'ensemble), et la Tunisie est le pays qui manque le plus souvent d'une plateforme fiable et abordable (32 % contre 24 % dans l'ensemble).

Les formations de sensibilisation durables et à long terme trouvent le plus d'écho au Maroc (33 % contre 26 % dans l'ensemble), où 30 % des PME souhaitent également que leur partenaire idéal agisse comme une équipe d'experts externes disponible 24 heures sur 24 et 7 jours sur 7. Au Cameroun, la responsabilité incombe la plupart du temps à l'équipe informatique générale (45 % contre 37 % dans l'ensemble), tandis que les entreprises tunisiennes sont plus susceptibles de disposer d'une équipe dédiée à la cybersécurité (42 % contre 30 % dans l'ensemble). En Côte d'Ivoire, 35 % des PME s'appuient sur des équipes internes et 20 % sur des partenaires externes, contre 9 % dans l'ensemble.

Au Cameroun, 43 % des PME considèrent que le partenaire idéal est celui qui élabore une stratégie à long terme et sur mesure (contre 36 % dans l'ensemble) et qui met en place une sécurité de fond qui ne les ralentit pas (45 % contre 32 % dans l'ensemble). Au Sénégal, les outils automatisés qui répondent instantanément aux incidents sont jugés essentiels (45 % contre 26 % dans l'ensemble), tandis que la formation est le point le moins important (15 % contre 26 % dans l'ensemble).

Le fait de faire appel à une équipe d'experts externes disponibles 24 heures sur 24 et 7 jours sur 7 séduit 40 % des PME en Côte d'Ivoire et 30 % au Maroc, contre 24 % dans l'ensemble. En Tunisie, les interventions directes lors d'incidents sont davantage valorisées (30 % contre 25 % dans l'ensemble). Les explications dans un langage clair trouvent le plus d'écho au Cameroun (27 % contre 19 % dans l'ensemble). Le Sénégal (30 %) et la Tunisie (28 %) recherchent plus souvent un conseiller ou un « partenaire » de confiance (contre 19 % dans l'ensemble), tandis que le premier affiche une préférence plus marquée pour un spécialiste externe travaillant comme une ressource interne (25 % contre 15 % dans l'ensemble).

Conclusion

Une véritable discussion autour de la cybersécurité implique d'aller au-delà des mots en vogue et de reconnaître les frustrations, lacunes et besoins réels des PME. Ce rapport met clairement en évidence ce qui pose problème, ce qui manque et ce qui est vraiment utile, à savoir des équipes surchargées, des stratégies uniquement sur le papier et un soutien insuffisant de la part des dirigeants, mais également une idée claire de ce que les entreprises attendent de leurs partenaires de confiance. La voie à suivre consiste à transformer ces angles morts en résilience, grâce à des solutions pratiques, à des conseils honnêtes et à la bonne combinaison d'expertise et de technologie, que ce soit en interne ou par l'intermédiaire d'un partenaire externe de confiance.

Kaspersky pour les PME

Le portefeuille de Kaspersky couvre un large éventail de clients, des très petites entreprises aux grandes sociétés, en combinant des solutions technologiques avancées à une expertise unique en matière de Threat Intelligence et d'autres services. Kaspersky recommande :

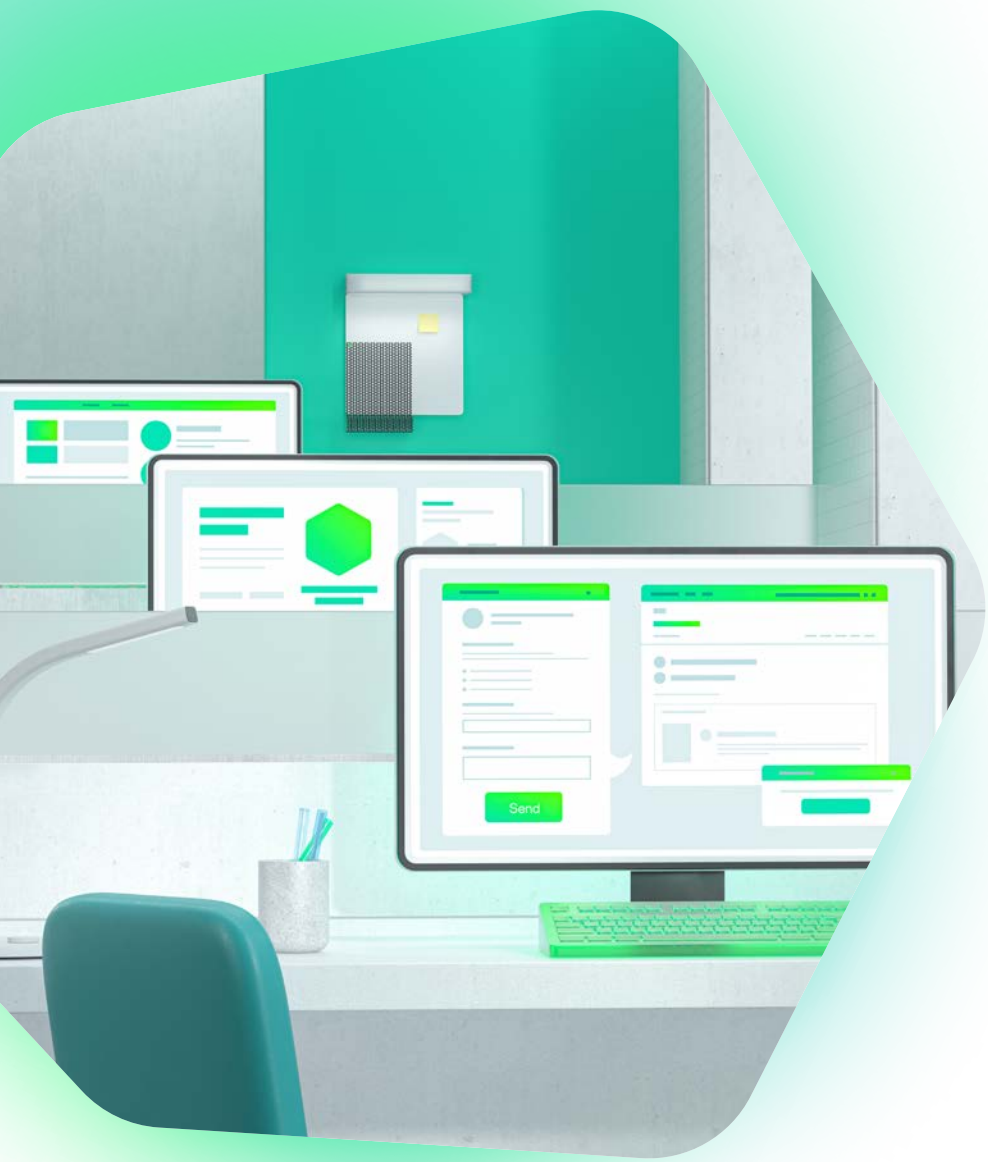
Kaspersky Small Office Security pour les très petites entreprises. Cette solution est conçue pour offrir une protection de niveau professionnel, facile à déployer et à gérer, même en l'absence d'administrateur informatique au sein du personnel. Elle protège contre les risques les plus importants : prévention des pertes financières, blocage de l'accès aux sites Internet falsifiés ou malveillants, protection des données confidentielles contre le vol et défense contre les attaques par ransomware.

Kaspersky Next pour les petites et moyennes entreprises. Cette solution associe une protection avancée des terminaux à la puissance d'enquête et de réponse de l'EDR (Endpoint Detection and Response) et de la XDR (Extended Detection and Response). Cette approche intégrée offre une protection en temps réel, une visibilité sur les menaces exploitable et la transparence dont les entreprises ont besoin pour détecter, analyser et neutraliser les attaques avant qu'elles ne causent des dommages.

Pour obtenir plus d'informations sur la manière dont les entreprises peuvent renforcer leur sécurité, consultez le dernier article du blog Kaspersky Daily dédié au renforcement de la sécurité.
Le renforcement de la sécurité désigne un ensemble de pratiques visant à protéger l'infrastructure informatique en minimisant la surface d'attaque ou, autrement dit, en maximisant la sécurité des systèmes existants sans avoir à recourir systématiquement à des outils de protection supplémentaires. Cet article examine les stratégies essentielles que toute entreprise peut adopter pour limiter son exposition aux cyberattaques, en particulier celles qui disposent de peu de ressources dédiées à la cybersécurité, voire d'aucune.

À propos de Kaspersky

Kaspersky est une entreprise mondiale de cybersécurité et de protection de la vie privée numérique fondée en 1997. Avec plus d'un milliard d'appareils protégés à ce jour contre les cybermenaces émergentes et les attaques ciblées, l'expertise approfondie de Kaspersky en matière de sécurité et de Threat Intelligence se traduit constamment par des solutions et des services innovants destinés à protéger les particuliers, les entreprises, les infrastructures critiques et les gouvernements du monde entier.
Le portefeuille complet de solutions de sécurité de l'entreprise comprend une protection numérique de pointe pour les appareils personnels, des produits et services de sécurité spécialisés pour les entreprises, ainsi que des solutions de cyberimmunité pour lutter contre les cybermenaces complexes et en constante évolution. Nous aidons des millions de particuliers et près de 200 000 entreprises clientes à protéger ce qui leur tient le plus à cœur.



Actualités sur les cybermenaces : securelist.com
Actualités sur la sécurité informatique : kaspersky.fr/blog/
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security

kaspersky

kaspersky.fr

© 2025 KASPERSKY LAB. LES MARQUES DÉPOSÉES ET LES MARQUES DE SERVICE SONT LA PROPRIÉTÉ DE LEURS DÉTENTEURS RESPECTIFS.