SOPHOS

Remédier à la pénurie de compétences en cybersécurité dans les PME

Étude des répercussions directes de la pénurie de compétences en cybersécurité sur les petites et moyennes entreprises et des moyens de surmonter ces difficultés en tenant compte des contraintes budgétaires et des ressources disponibles.

Un livre blanc Sophos. Octobre 2024

Introduction

La pénurie mondiale de compétences en cybersécurité est désormais connue et bien documentée. Cette tendance ne devrait pas s'inverser de sitôt, aussi est-il essentiel que les petites et moyennes entreprises se mobilisent pour en atténuer les effets.

Comprendre ce défi est la première étape pour pouvoir y répondre. Ce rapport présente les résultats d'une enquête indépendante menée auprès de praticiens de la sécurité de premier plan dans le monde entier, et révèle les répercussions de la pénurie de compétences sur les petites et moyennes entreprises au quotidien. Sur la base de ces observations, il fournit des conseils pratiques pour relever ces défis en tenant compte des contraintes de ressources et de budget existantes. Il présente également les solutions Sophos qui permettent aux petites entreprises d'obtenir de meilleurs résultats en matière de cybersécurité.

À propos de l'enquête

Sophos a commandé une enquête indépendante auprès de 5 000 professionnels de l'IT et de la cybersécurité à travers 14 pays. Parmi les personnes interrogées, 1 402 travaillent dans des organisations comptant entre 100 et 500 employés, le segment considéré comme les petites et moyennes entreprises (PME) dans ce rapport. Cette enquête a été menée au cours du premier trimestre 2024.

Les petites entreprises sont touchées de manière disproportionnée par la pénurie de compétences

La pénurie de compétences pèse lourdement — et démesurément — sur les PME. L'enquête révèle que les **entreprises de moins de 500 salariés considèrent la pénurie de compétences et d'expertise internes en cybersécurité comme leur deuxième risque le plus important en matière de cybersécurité**, juste après les menaces de type « zero-day ». Par contraste, pour les entreprises de plus de 500 salariés, elle se classe au septième rang.

Classement relatif de la « pénurie de compétences et d'expertise internes en cybersécurité » en tant que risque de cybersécurité pour l'entreprise

PME (n=1 402)	GRANDES ENTREPRISES (n=3 598)	
100 À 500 EMPLOYÉS	501 À 1000 EMPLOYÉS	1 001 À 5 000 EMPLOYÉS
N° 2	N° 7	N° 7

Quels sont, selon vous, les trois principaux risques de cybersécurité pour votre entreprise ? Positionnement relatif de la « pénurie de compétences et d'expertise internes en cybersécurité » parmi les réponses classées en premier (chiffres de base dans le graphique)

Si les entreprises de toutes tailles sont touchées par la pénurie de compétences, il en ressort clairement que ce sont les PME qui en ressentent le plus fortement les effets. Les risques principaux pour les grandes organisations, tels que la pénurie d'outils de cybersécurité (risque classé n° 2 pour les entreprises comptant entre 501 et 1 000 employés) et le vol de données d'accès et d'identifiants (risque classé n° 2 pour les entreprises comptant entre 1 001 et 5 000 employés), sont des préoccupations secondaires pour les petites entreprises qui doivent relever le défi plus fondamental consistant à trouver des personnes pour exploiter leurs investissements existants.

Pénurie de compétences : un défi à deux têtes

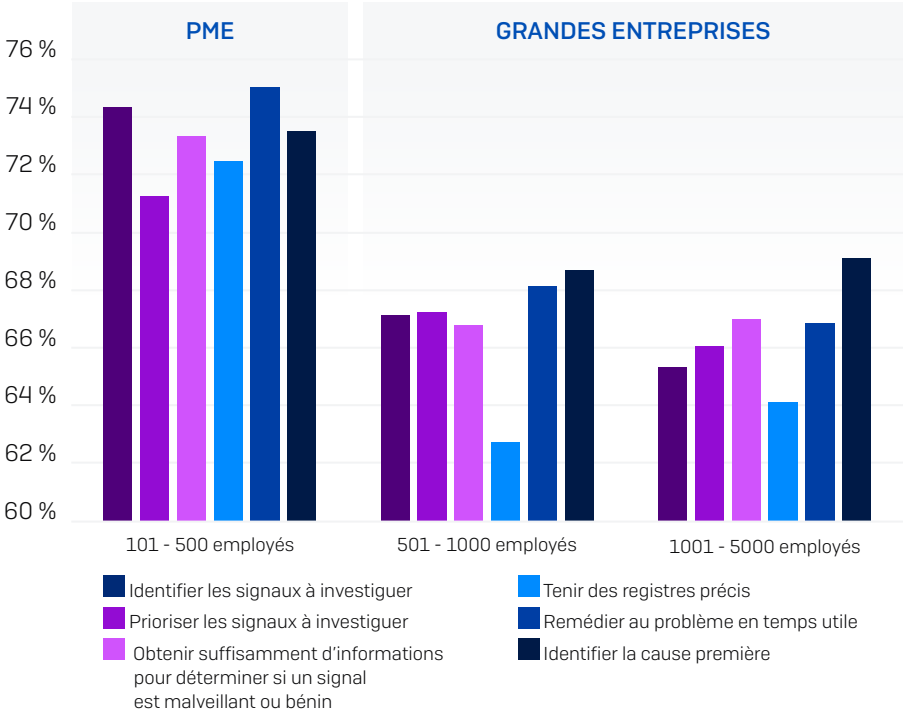
La pénurie de compétences est sous-tendue par un fait simple : il n'y a pas assez de professionnels qualifiés dans le domaine de la cybersécurité. Ce manque impacte les PME de deux manières.

Le manque d'expertise

Les cybermenaces et les technologies de sécurité sont complexes. Bien faire en matière de cybersécurité est une compétence avancée qui requiert un haut degré d'expertise — et, pour couronner le tout, la barre ne cesse de s'élever. Les cyberattaques devenant de plus en plus complexes, un niveau d'expertise plus élevé est nécessaire pour les bloquer.

L'enquête révèle que **96 % des répondants travaillant dans ces petites entreprises considèrent qu'au moins un aspect de l'investigation des alertes suspectes est source de difficultés**. Si les grandes entreprises sont souvent confrontées à des problèmes de sécurité, c'est dans les PME que le défi est le plus lourd.

Pourcentage des entreprises qui considèrent que les tâches liées aux opérations de sécurité sont difficiles à mener



Si votre entreprise investigue les alertes de sécurité en interne, dans quelle mesure les étapes suivantes sont-elles difficiles pour votre entreprise lorsqu'elle enquête sur des cas d'alertes suspectes ? « Très difficile » et « Assez difficile » (chiffres de base dans le tableau)

L'aspect pratique du développement d'une expertise en matière de cybersécurité représente un défi tout particulier pour ceux qui travaillent dans des PME. Lorsque l'équipe informatique/sécurité ne compte qu'une petite poignée de personnes, il est bien difficile de consacrer régulièrement du temps à la formation continue. Sans compter qu'avec moins de collègues, les membres de l'équipe ont moins d'occasions d'apprendre de leurs pairs.

Manque de capacité

Les adversaires n'ont pas des horaires de bureau, c'est pourquoi la cybersécurité est une exigence permanente. En réalité, 91 % des attaques de ransomware commencent en dehors des heures de travail normales, car elles ont ainsi plus de chances de passer sous les radars[1].

Selon les opérateurs de première ligne, pour garantir une couverture de cybersécurité 24 h/24 et 7 j/7, il faut compter au moins quatre ou cinq employés à temps plein, de façon à couvrir les jours de congés, les arrêts maladie et les week-ends. Pour la plupart des PME, cet objectif est tout bonnement irréalisable, compte tendu de la taille des effectifs internes.

À titre d'illustration, l'enquête révèle qu'**un tiers (33 %) des PME ne disposent d'aucune personne chargée de surveiller, d'investiguer et de répondre activement aux alertes**. Or, faute d'un intervenant actif, les petites organisations sont très vulnérables aux attaques.

33 %
des PME ne confient à aucun employé la surveillance et l'investigation des alertes de sécurité

Au cours de l'année écoulée (y compris les nuits, les week-ends et les périodes de vacances), quel pourcentage de temps votre entreprise a-t-elle consacré à la surveillance et à l'examen des alertes de sécurité par un intervenant actif ? n=1 402 entreprises de 100 à 500 employés.

1 Comment stopper les adversaires actifs : les leçons tirées de la ligne de front de la cybersécurité, Sophos

L'impact de la pénurie de compétences en cybersécurité sur les petites entreprises

La pénurie de compétences a de nombreuses répercussions sur les PME. Il s'agit du segment le plus susceptible de voir ses données chiffrées lors d'une attaque de ransomware, avec 74 % des incidents entraînant un chiffrement des données. Cela reflète probablement leur moindre capacité à repérer et à neutraliser les adversaires avant que le ransomware ne soit exécuté.

Pourcentage des attaques de ransomware ayant abouti à un chiffrement des données

PME (n=1 402)	GRANDES ENTREPRISES (n=3 598)	
100 À 500 EMPLOYÉS	501 À 1000 EMPLOYÉS	1 001 À 5 000 EMPLOYÉS
74 %	72 %	66 %

Source : L'état des ransomwares 2024, Sophos Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Oui. Chiffres de base dans le graphique.

De plus, avec moins de personnes pour partager la charge de travail en matière de cybersécurité, le risque de burnout de la plupart des talents est élevé. Dans une autre enquête commandée par Sophos dans la région Asie-Pacifique et au Japon, **85 % des entreprises ont déclaré que leurs professionnels de la cybersécurité et de l'informatique étaient confrontés à la fatigue et à l'épuisement**, près d'un sur quatre (23 %) en faisant l'expérience « fréquemment », et 62 % « occasionnellement ». Il est inquiétant de constater que 90 % des entreprises déclarent que les cas d'épuisement et de grande fatigue professionnelle ont augmenté au cours des 12 derniers mois, 30 % d'entre elles affirmant que ces augmentations ont été « significatives ».

85 %
des entreprises indiquent que leurs professionnels de la cybersécurité/IT font face à de la fatigue et de l'épuisement

Comment combler le déficit de compétences dont sont victimes les petites entreprises ?

Le recrutement de personnel n'est pas une solution envisageable pour la plupart des PME. Embaucher davantage de collaborateurs spécialisés dans la cybersécurité requiert un budget considérable, qui aurait des répercussions disproportionnées sur les budgets alloués aux effectifs dans les petites organisations par rapport aux plus grandes. Dans le même temps, les entreprises sont en concurrence pour attirer les meilleurs talents, lesquels sont en nombre limité. Les personnes possédant des compétences recherchées peuvent être sélectives et préfèrent souvent travailler dans des entreprises de plus grande taille qui offrent davantage d'opportunités de développement entre pairs. La solution pour remédier aux insuffisances en matière d'expertise et de capacité est de se tourner vers des spécialistes de la sécurité tiers et d'employer des solutions de cybersécurité conçues pour les PME.

Travailler avec des spécialistes de la sécurité tiers

Faire appel à des spécialistes tiers en cybersécurité est souvent le moyen le plus simple et le plus rentable de renforcer l'expertise et les capacités. Les deux méthodes les plus courantes consistent à recourir à des services MDR (Managed Detection and Response) ou MSP (Managed Service Providers).

Les services **MDR** fournissent généralement des services de chasse, de détection et de réponse aux menaces pilotés par des experts 24 h/24 et 7 j/7 pour l'ensemble de votre environnement. Les analystes surveillent votre entreprise, identifiant et répondant aux activités suspectes et neutralisant les attaques avant qu'elles n'impactent votre organisation.

Orientez-vous vers un fournisseur qui s'adapte à vos besoins et à votre façon de travailler, que vous souhaitiez externaliser entièrement la détection et la réponse aux menaces ou collaborer avec les analystes de votre fournisseur. De plus, compte tenu des budgets invariablement serrés, il est important de choisir un service capable de tirer parti de vos technologies de sécurité en place, afin d'éviter les coûts et les perturbations liés au remplacement des solutions existantes.

Pour financer les services MDR, vous pouvez chercher à réaliser des économies auprès de votre compagnie d'assurance cyber. Les utilisateurs de services MDR sont largement considérés comme des « clients de premier niveau » par les compagnies d'assurance, du fait qu'ils sont moins susceptibles de soumettre une demande d'indemnisation. En conséquence, les assureurs appliquent généralement des tarifs avantageux aux entreprises qui utilisent des services MDR. L'argent ainsi économisé peut être réaffecté au financement du service lui-même.

Étude de cas Sophos : organisation à but non lucratif regroupant 350 collaborateurs

Une organisation à but non lucratif de Caroline du Nord (États-Unis) employant 350 personnes a été en mesure de réduire sa prime de cyberassurance de 8 000 $ en utilisant le service MDR de Sophos. Étant donné que leur abonnement annuel à Sophos MDR s'élevait à 8 467 $, les économies réalisées sur l'assurance leur ont permis de bénéficier de services de détection et de réponse aux menaces 24 h/24 et 7 j/7 assurés par des experts, pour un coût supplémentaire de seulement 467 $.

Depuis de nombreuses années, les **MSP** (fournisseurs de services managés) fournissent une assistance en matière d'informatique et de cybersécurité aux plus petites entreprises, agissant comme leur équipe interne. À mesure que les cybermenaces gagnent en complexité, les entreprises de taille moyenne décident de plus en plus de collaborer avec des MSP en complément de leurs ressources internes.

Les services MDR et les MSP ne sont pas exclusifs l'un de l'autre : une autre enquête de Sophos révèle que la plupart des MSP (81 %) proposent des services MDR,[2] ce qui permet de bénéficier des deux niveaux de support par l'intermédiaire d'un seul fournisseur. Certains MSP choisissent de fournir des services MDR uniquement en interne, tandis que d'autres préfèrent faire appel à des fournisseurs tiers spécialisés.

Choisissez des solutions spécialement conçues pour les PME

La plupart des solutions de cybersécurité sont conçues et élaborées pour les entreprises de grande taille disposant d'équipes importantes chargées de les déployer et de les gérer. Si l'utilisation de solutions d'entreprise peut sembler attrayante, les entreprises de plus petite taille ont souvent du mal à en tirer des avantages en termes de sécurité et de retour sur investissement (ROI), car elles ne sont pas en mesure de les utiliser de manière efficace.

2 MSP (Managed Service Providers) Perspectives 2024 - Sophos

Il convient plutôt de rechercher des outils de sécurité techniquement avancés, mais conçus pour être simples d'utilisation pour les équipes IT très souvent surchargées. Cette réorientation de la stratégie d'achat ne devrait pas entraîner une augmentation des dépenses — et pourrait même offrir la possibilité de réduire les dépenses liées aux technologies et à la gestion. Lors de l'évaluation des solutions de sécurité, tenez compte à la fois des fonctionnalités de la plateforme et du produit.

Plateforme

- Une plateforme de cybersécurité est un outil centralisé qui permet de déployer, de surveiller et de gérer plusieurs solutions de cybersécurité en un seul et même endroit, par exemple la sécurité réseau et Endpoint, la sécurité des messageries électroniques et les pare-feux.
- La consolidation de vos solutions de cybersécurité au sein d'une plateforme unique réduit considérablement les frais d'administration courants : plus besoin de passer d'une console à l'autre pour comprendre ce qui se passe. La réduction du nombre de prestataires avec lesquels vous travaillez permet de réduire les frais généraux liés à la gestion des fournisseurs.
- Une plateforme efficace doit également permettre à vos solutions de sécurité de travailler ensemble, en partageant des données télémétriques, des informations, des politiques basées sur l'utilisateur, etc., afin de renforcer vos cyberdéfenses.

Fonctionnalités du produit

- Les fournisseurs présentent de longues listes de fonctions et de possibilités sur leurs sites web. Avant d'évaluer ces solutions, prenez le temps de définir exactement ce dont vous avez besoin et ce dont vous n'avez pas besoin, cela vous évitera de payer pour des technologies inutiles.
- Pour tirer le meilleur parti de vos investissements en matière de cybersécurité, vous devez pouvoir les déployer et les utiliser efficacement. Choisissez des solutions qui appliquent automatiquement les paramètres recommandés dès le premier jour, afin d'éviter toute configuration manuelle fastidieuse et risquée. Recherchez également des contrôles intuitifs conçus pour des environnements réels, qui soient simples d'utilisation.
- Les erreurs de configuration des outils de sécurité constituent un risque majeur pour les PME. Il est essentiel de maintenir une bonne posture pour préserver votre sécurité. Pour cela vous devez privilégier les solutions qui fournissent une visibilité simple à comprendre sur les déploiements sous-optimaux et un support technique rapide.

- Compte tenu de la taille réduite de votre entreprise, il est peu probable que votre équipe soit en mesure de se consacrer uniquement aux tâches liées à la cybersécurité. Il est donc particulièrement important de mettre en place des solutions qui répondent automatiquement aux attaques et qui prennent des mesures jusqu'à ce que vous puissiez intervenir.

Comment Sophos peut vous aider ?

Sophos possède une vaste expérience dans la protection des PME contre les cybermenaces avancées et nous avons spécialement conçu bon nombre de nos produits et services pour répondre justement spécifiquement à leurs besoins.

Spécialistes de la sécurité tiers

MDR

Sophos propose le service MDR le plus fiable du marché, sécurisant plus d'organisations que tout autre éditeur. Nous disposons d'informations approfondies sur les attaques contre les petites entreprises et exploitons la télémétrie de l'ensemble de notre clientèle pour améliorer la protection de tous les utilisateurs.

Le service MDR de Sophos est très apprécié par les clients et les analystes. Parmi les récompenses récentes, citons :

- Gartner® Peer Insights™ Customers' Choice depuis deux ans, avec une note de 4,8/5 obtenue sur 647 avis au 17 septembre 2024.
- Leader de G2 pour les services MDR, avec la solution MDR la mieux notée par les clients du marché intermédiaire.
- IDC MarketScape a nommé Sophos comme Leader pour les services MDR (Managed Detection and Response) au niveau mondial dans son étude Vendor Assessment 2024.

MSP

Sophos dispose d'un vaste écosystème de partenaires MSP qui fournissent les produits et services Sophos — y compris Sophos MDR — aux PME du monde entier.

Des solutions spécialement conçues pour les PME

Plateforme

Sophos Central est la plateforme Cloud-Native basée sur l'IA, la plus complète et la plus évolutive du secteur. Elle est utilisée pour gérer toutes les solutions de cybersécurité de next-gen de Sophos, notamment Sophos Endpoint, Sophos Firewall, Sophos XDR, Sophos MDR, Sophos Email et Sophos ZTNA. Les intégrations avec un large éventail de technologies non Sophos, notamment Microsoft et Google, garantissent que les clients puissent tirer pleinement parti de leurs investissements existants en matière de sécurité.

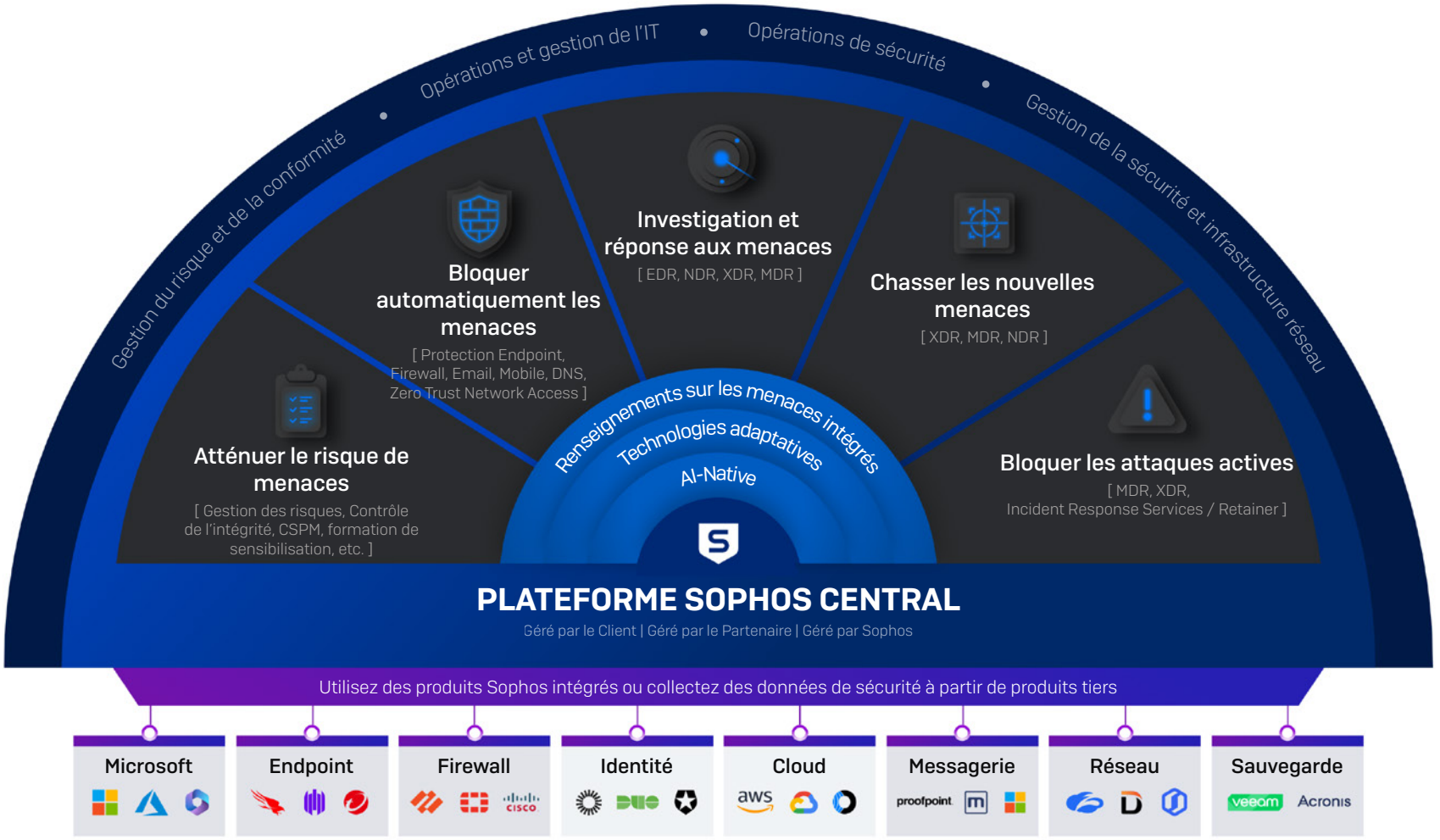
Fonctionnalités du produit

Les solutions Sophos sont hautement sophistiquées et s'appuient sur des décennies d'expérience en matière de lutte contre les cybermenaces. Elles sont également conçues pour être simples d'utilisation, ce qui permet à toutes les entreprises, quels que soient leur taille et leur effectif, de bénéficier de capacités de défense de premier plan.

Par exemple :

- **Sophos Endpoint** se déploie automatiquement en appliquant les paramètres recommandés, y compris notre protection anti-ransomwares et nos capacités anti-exploit, leaders sur le marché : aucun réglage manuel n'est nécessaire.
- Le système de gestion et de reporting centralisé de **Sophos Firewall** permet de gérer plusieurs pare-feux en un seul endroit, ce qui est particulièrement utile pour les entreprises avec des sites distants.
- **Sophos Endpoint** inclut des défenses adaptatives qui détectent la présence d'adversaires dans votre environnement et y répondent automatiquement, ce qui permet d'élever vos défenses et de vous donner le temps de répondre.
- La fonction « Intégrité du compte » intégrée à **Sophos Endpoint** offre une visibilité claire et en temps réel de l'état de la sécurité, avec un bouton « Corriger automatiquement » qui permet de revenir aux paramètres recommandés en un seul clic.
- L'intégration de **Sophos Firewall** à la plateforme Sophos permet de bloquer automatiquement les menaces actives et de coordonner une réponse avec les solutions Endpoint et ZTNA, ainsi que les Switchs et les points d'accès sans fil, empêchant ainsi tout mouvement latéral.

La plateforme de cybersécurité Sophos



Conclusion

L'enquête révèle que la pénurie de compétences en cybersécurité pèse tout particulièrement sur les petites et moyennes entreprises. Les lacunes qui en résultent en termes de compétences et de capacités se répercutent matériellement sur la capacité des entreprises à se défendre contre les attaques. Dans la mesure où le manque de ressources qualifiées n'est pas près de réduire, les petites organisations auraient tout intérêt à prendre des mesures pour en atténuer l'impact en travaillant avec des spécialistes tiers et en choisissant des solutions spécifiquement conçues pour leurs activités.

Pour en savoir plus sur les solutions Sophos pour les PME, contactez votre interlocuteur ou partenaire Sophos, ou bien visitez www.sophos.fr

2024-12-05 FR-WP [PC]

SOPHOS