UNE APPROCHE RÉSILIENTE POUR LES PROFESSIONNELS DE L'INFORMATIQUE ET DE LA CYBERSÉCURITÉ

Décembre 2024

Derek E. Brink, CISSP
Vice-président et chercheur, Cybersécurité et IT GRC

ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

En collaboration avec : zscaler™

Résumé

Les professionnels de l'informatique et de la cybersécurité d'aujourd'hui s'attachent à maintenir la flexibilité, l'adaptabilité, la réactivité et la résilience de leur organisation. Mais il ne faut pas négliger la résilience personnelle des professionnels de la technologie, c'est-à-dire compléter leurs « compétences techniques » en investissant également dans les « compétences non techniques » des personnes et des processus qui permettent d'atteindre ces objectifs. Notre objectif est la résilience organisationnelle, mais le soutien et le renforcement des professionnels de la technologie dans ces domaines sont essentiels pour y parvenir.

Des progrès considérables en matière de résilience organisationnelle

Favoriser la résilience organisationnelle est un énorme défi, compte tenu des tendances technologiques actuelles, notamment :

- Une **base d'utilisateurs diversifiée** (employés, partenaires, fournisseurs et clients) qui, pour la plupart des organisations, comprend une combinaison d'utilisateurs **distants et hybrides**.
- Un **accès rapide, sécurisé et conforme aux applications et données cloud**, depuis **n'importe quel endroit** et **sur n'importe quel appareil**.
- Les attentes en matière d'**expériences numériques de qualité**, la **continuité des activités** étant une priorité absolue.

Au cours des douze dernières années, les professionnels de l'informatique et de la cybersécurité se sont attachés à détecter les incidents de sécurité et à y répondre plus rapidement, ce qui leur a permis de réaliser d'importantes améliorations. Le graphique de la Figure 1 est basé sur des données empiriques concernant le temps de séjour des attaquants (le temps pendant lequel les attaquants ne sont pas détectés sur les systèmes compromis) publiées chaque année par la société d'investigation en cybersécurité Mandiant (qui fait maintenant partie de Google Cloud).

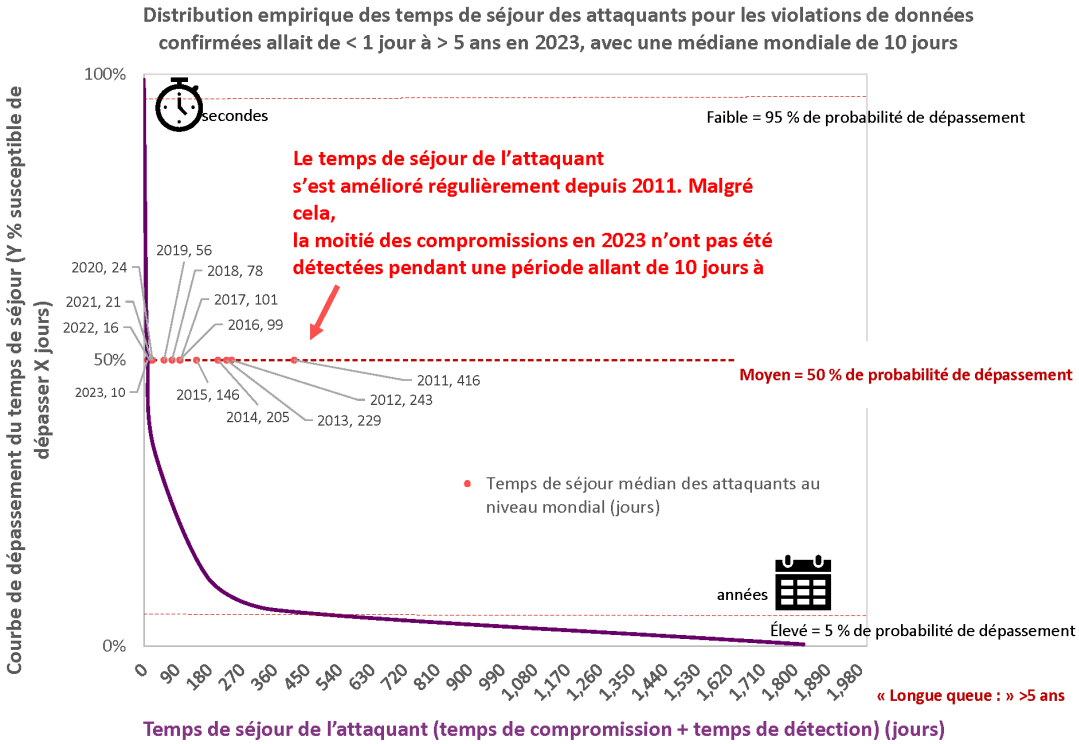
Notons en particulier ce qui suit :

- La distribution empirique des temps de séjour des attaquants pour les violations de données confirmées allait *de moins d'un jour à plus de 5 ans* en 2023, avec une *médiane mondiale de 10 jours*.

  La durée médiane de séjour de l'attaquant s'est améliorée régulièrement depuis 2011 (416 jours). Malgré cela, la moitié de toutes les compromissions en 2023 n'ont pas été détectées pendant une période allant *de 10 jours à 5 ans*

Voir *Favorisez-vous un lieu de travail résilient ? Entretien avec Aberdeen Strategy & Research*

Figure 1 : Les professionnels de l'informatique et de la cybersécurité ont considérablement amélioré la résilience des organisations



Source : Données empiriques adaptées de Mandiant M-Trends 2011-2023 ; Aberdeen, décembre 2024

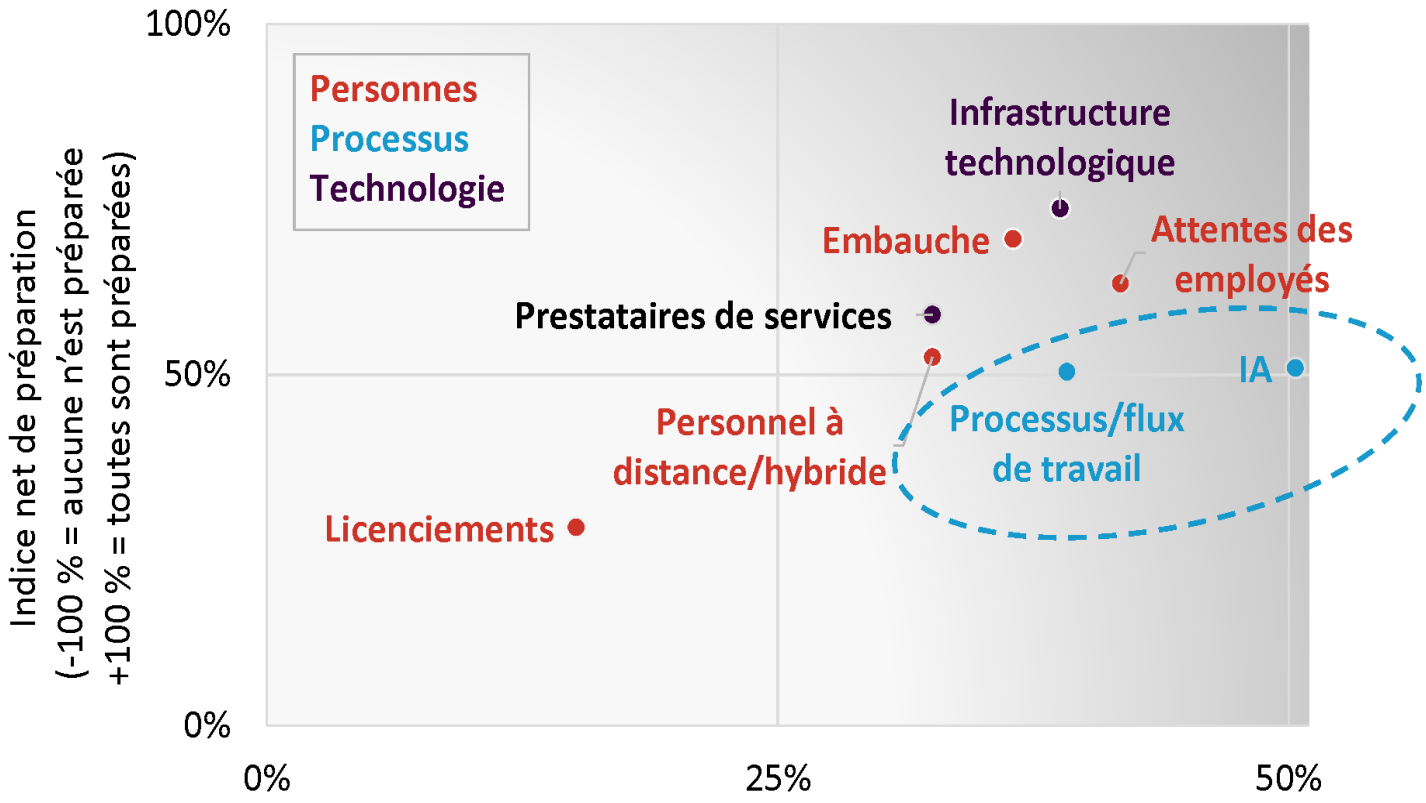
Source : Données empiriques adaptées de Mandiant M-Trends 2011-2023 ; Aberdeen, décembre 2024

Qu'en est-il de la résilience personnelle ?

L'étude 2024 *Future of Workplace* d'Aberdeen a interrogé les répondants sur l'**impact prévu à court terme** de plusieurs changements environnementaux, ainsi que sur leur **degré de préparation** et celui de leur organisation à gérer ces impacts. Sur la base des résultats de cette étude, la Figure 2 montre que la résilience personnelle s'applique aux trois domaines traditionnels que sont les *personnes*, les *processus* et la *technologie*, et que les organisations sont **généralement confiantes** dans leur capacité à gérer l'impact de pratiquement tous les changements environnementaux qu'elles prévoient dans les 12 à 18 prochains mois.

Relativement, elles se sentent le moins bien préparées pour les initiatives à fort impact concernant les processus opérationnels et les flux de travail, ce qui souligne la nécessité d'accroître la résilience personnelle dans les initiatives de l'organisation impliquant l'**automatisation** et l'**IA**.

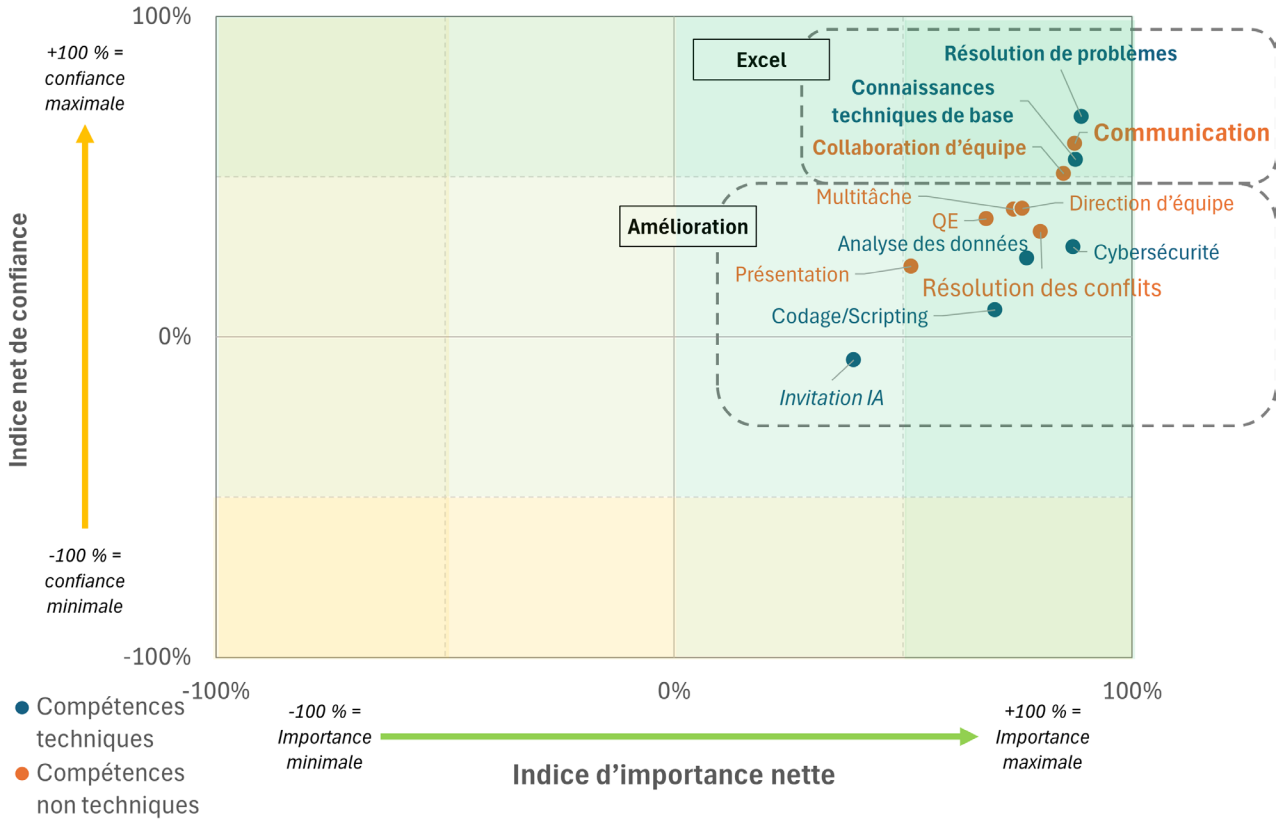
Figure 2 : Les professionnels de la technologie soulignent la nécessité d'accroître leur résilience personnelle dans les initiatives à fort impact impliquant l'automatisation et l'IA



Source : Aberdeen, décembre 2024

Pour aller un peu plus loin, le rapport Spiceworks Ziff Davis *State of IT 2025* a interrogé des professionnels techniques sur un ensemble représentatif de compétences techniques et de « compétences non techniques », selon deux dimensions : l'*importance* des compétences et la *confiance* qu'ils ont dans chacun de ces domaines. Voir la Figure 3.

Figure 3 : Confiance des professionnels de la technologie dans leurs compétences – Quatre compétences dans lesquelles ils excellent et neuf opportunités dans lesquelles ils pourraient se mettre à niveau



Source : Adapté du rapport Spiceworks Ziff Davis *State of IT* 2025 ; Aberdeen, décembre 2024

Sur la base de ces résultats, voici quatre domaines dans lesquels les professionnels de la technologie excellent actuellement :

- **Compétences techniques** : *connaissances techniques de base, résolution de problèmes*
- **Compétences non techniques** : *communication, collaboration d'équipe*

De la même manière, voici neuf opportunités que les professionnels de la technologie pourraient saisir pour se mettre à niveau :

- **Compétences techniques** : *cybersécurité, analyse de données, codage/scripting, IA*
- **Compétences non techniques** : *multitâche, direction d'équipe, présentation (communication verbale), résolution de conflits, intelligence émotionnelle (QE)*

En général, les caractéristiques des professionnels de la technologie qui ont développé leur résilience personnelle sont les suivantes :

- la capacité à gérer les incidents avec agilité et sang-froid ; la parfaite gestion de la pression ;
- La capacité à rester calme et à prendre de bonnes décisions lorsque tout s'emballe ;
- la « mémoire musculaire » mentale et opérationnelle nécessaire pour réagir et se rétablir efficacement en cas d'incident ;
- de solides compétences en matière de communication, de présentation, de collaboration et de résolution de problèmes ;
- un état d'esprit d'apprentissage permanent.

La résilience personnelle, telle qu'elle ressort d'une sélection d'exemples concrets

Le Tableau 1 présente quelques exemples concrets d'incidents de cybersécurité qui illustrent les principales dimensions de la résilience personnelle.

Tableau 1 : La résilience personnelle, illustrée par des incidents réels

Incidents nécessitant de la résilience personnelle (à titre d'exemple)	Traits de résilience personnelle
Cyberattaque contre le service national de santé britannique (NHS). L'attaque *WannaCry* de 2017 contre le NHS a entraîné d'importantes perturbations opérationnelles, ce qui s'est traduit par des conditions de stress élevé pour le personnel informatique et les employés afin de maintenir les services de santé et de réduire les dommages au minimum.	• Gestion de crise • Résolution de problèmes • Collaboration
Attaque NotPetya contre Maersk. Lorsque le géant du transport maritime Maersk a été frappé par le ransomware *NotPetya* en 2017, ses opérations mondiales ont été interrompues. Les équipes informatiques de Maersk ont réagi en reconstruisant l'ensemble de leur infrastructure informatique en seulement 10 jours.	• Gestion de crise • Adaptabilité • Innovation
Attaque de ransomware contre l'hôpital universitaire de Düsseldorf. Cet incident survenu en 2020 a entraîné la mort tragique d'un patient en raison d'une défaillance du système, mettant en évidence les conséquences potentiellement immédiates des atteintes à la cybersécurité sur les services publics. Les professionnels de l'informatique et de la santé ont réagi rapidement et sous une pression extrême pour rétablir les systèmes, gérer les communications et adapter les protocoles.	• Communication de crise • Résolution de problèmes • Apprentissage permanent
Évolution des technologies et des réponses réglementaires L'accent mis par la réglementation sur la gouvernance et les normes éthiques en matière d'intelligence artificielle (IA) dans les pays de l'UE met en évidence la nature dynamique de la technologie, de la réglementation et de leur impact sur la cybersécurité.	• Apprentissage permanent • Communication et collaboration interculturelles

Cybermenaces contre les infrastructures critiques. Plusieurs incidents récents visant des infrastructures critiques dans plusieurs pays de l'UE mettent en évidence la complexité potentielle des aspects réglementaires et culturels de la résilience personnelle.	• Apprentissage permanent • Communication et collaboration interculturelles • Adaptabilité au contexte

Source : Aberdeen, décembre 2024

Tout est lié : Comment la résilience personnelle des professionnels de la technologie contribue à l'obtention de résultats stratégiques pour l'entreprise

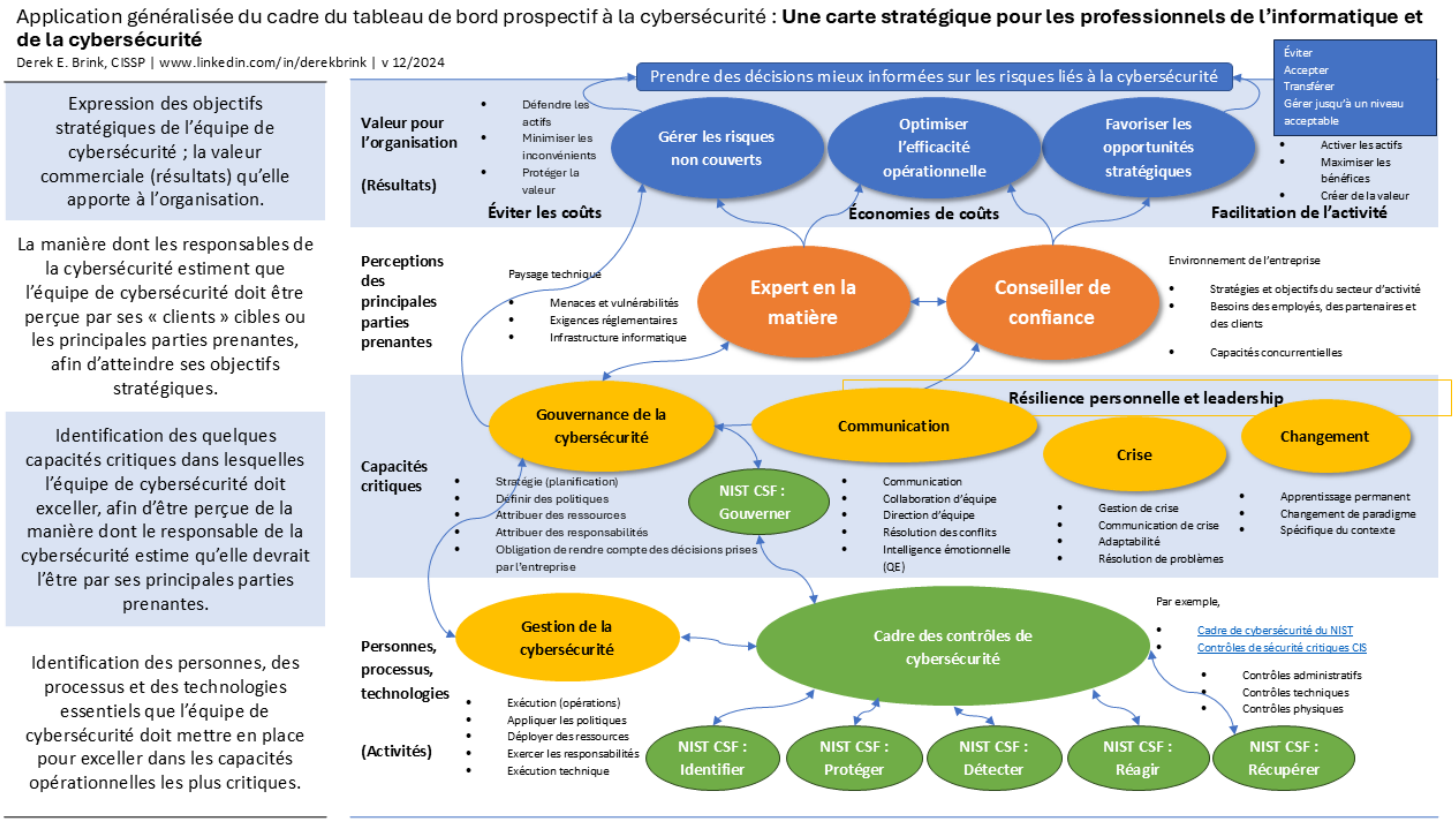
Depuis de nombreuses années, Aberdeen écrit sur l'importance de **relier les activités techniques et les capacités clés aux résultats de l'entreprise**. L'une des visualisations les plus utiles à cet égard est « *Une carte stratégique pour les professionnels de l'informatique et de la cybersécurité* » (voir Figure 4), qui est l'application généralisée par Aberdeen du célèbre cadre du tableau de bord prospectif au thème de la cybersécurité.

Depuis 1992, le *cadre du tableau de bord prospectif* aide les organisations à décrire, communiquer et mettre en œuvre leurs stratégies en se concentrant sur les liens de cause à effet entre les activités techniques (personnes, processus et technologies) et les résultats stratégiques de l'entreprise.

Le tableau de bord prospectif est généralement défini du haut vers le bas (c'est-à-dire en commençant par les résultats stratégiques de l'entreprise), mais il est toujours exécuté du bas vers le haut. La Figure 4 ci-dessous illustre le point de vue d'Aberdeen sur les liens entre les quatre niveaux du tableau de bord prospectif (c'est-à-dire les *activités*, les *capacités critiques*, les *perceptions des principales parties prenantes* et les *résultats stratégiques*) appliqués à la cybersécurité.

- Les caractéristiques de la « résilience personnelle » évoquées précédemment apparaissent en jaune dans les capacités critiques (ligne 3).
- Il s'agit des « compétences non techniques » qui aident les professionnels techniques d'aujourd'hui à compléter leurs « compétences techniques » traditionnelles en matière de technologies (ligne 4).
- À leur tour, ces caractéristiques de résilience personnelle aident les professionnels de la technologie à être perçus par les principales parties prenantes comme des experts en la matière et des conseillers de confiance (ligne 2).
- En fin de compte, ce sont ces liens de cause à effet qui permettent d'obtenir les résultats stratégiques liés à la résilience organisationnelle (ligne 1).

Figure 4 : Comment la résilience personnelle est essentielle pour atteindre les résultats stratégiques de l'entreprise



Source : Aberdeen, décembre 2024

Résumé et principaux enseignements

- Les professionnels de l'informatique et de la cybersécurité ont fait de grands progrès en matière de **résilience organisationnelle** au cours des dernières années.
- Pour les professionnels de la technologie d'aujourd'hui, l'étude d'Aberdeen met en évidence la nécessité d'accroître également leur **résilience personnelle**.
- Les caractéristiques clés de la résilience personnelle peuvent facilement être observées dans des **exemples concrets** d'incidents de cybersécurité.
- Investir dans les « compétences non techniques » de la résilience personnelle aidera les professionnels techniques d'aujourd'hui à compléter leurs « compétences techniques » traditionnels en matière de technologies. Ensemble, ils contribueront à produire les **résultats commerciaux stratégiques** liés à la résilience organisationnelle.

Recherches connexes

- *Favorisez-vous un lieu de travail résilient ? Entretien avec Aberdeen Strategy & Research*, novembre 2024
- *Professionnels de l'informatique et de la cybersécurité : Qu'en est-il de votre résilience personnelle ? Entretien avec Aberdeen Strategy & Research*, décembre 2024

À propos d'Aberdeen Strategy & Research

Avec plus de trois décennies d'expérience dans les études de marché indépendantes et crédibles, Aberdeen Strategy & Research (une division de Spiceworks Ziff Davis) aide à **faire la lumière** sur les réalités du marché et à informer les stratégies d'entreprise. Notre approche de la recherche, basée sur les faits, impartiale et centrée sur les résultats, fournit des informations sur la technologie, la gestion de la clientèle et les opérations commerciales afin d'**inspirer** une réflexion critique et de **déclencher** des actions commerciales basées sur les données.