

Comment une approche de cybersécurité fondée sur des plateformes permet-elle de réduire les coûts et de simplifier les démarches de conformité?

EY

Travailler ensemble
pour un monde meilleur



Microsoft

Malgré le resserrement des conditions économiques et des compressions budgétaires, on s'attend à ce que les dirigeants protègent leur entreprise contre les cybermenaces persistantes en se conformant aussi pleinement à une liste croissante d'exigences réglementaires. Ces difficultés peuvent être exacerbées en cumulant des outils ultraspecialisés et

redondants qui augmentent les coûts et la complexité. Plutôt, les sociétés de pointe se tournent vers des plateformes intégrées de protection des données afin d'éliminer les outils redondants, réduire la dépendance à des ressources hautement spécialisées et renforcer l'agilité des programmes de sorte à pouvoir composer avec le flot permanent de nouvelles exigences réglementaires.

En bref

- ▶ Les entreprises de pointe dégagent une valeur commerciale substantielle en délaissant les troupes d'outils de cybersécurité fragmentées en faveur d'une plateforme intégrée de protection des données.
- ▶ Poser les bonnes questions est la première étape du renforcement de la cybersécurité d'entreprise et permet également de réduire les coûts, de simplifier la conformité réglementaire et de gagner en agilité.

D'après le [Forum économique mondial](#), la réglementation mondiale en matière de cybersécurité et de protection des renseignements personnels, quoiqu'elle soit bien intentionnée et cherche à contribuer à la lutte quotidienne contre les menaces émergentes, engendre des processus complexes et coûteux pour le respect des obligations de conformité dans tous les secteurs et sème des embûches sur la voie vers la cybersécurité chez les nouveaux innovateurs. Le coût de gestion d'une surface d'attaque sinieuse, l'ampleur et la complexité de la pile technologique de cybersécurité et la pénurie de compétences poussent les dirigeants à partir en quête de réponses.

Les coûts cachés de la spécialisation

Les importantes transformations du milieu des affaires et du milieu de la technologie ont mené les sociétés à cumuler les outils spécialisés pour gérer les nouveaux cas d'utilisation. En moyenne, les grandes entreprises utilisent couramment 100 produits de sécurité émanant de 35 fournisseurs ou plus. Il en découle une trousse d'outils fragmentée, souvent redondante, qui requiert une équipe opérationnelle considérable pour l'entretenir. Au moment de comparer des solutions ponctuelles, les outils hautement spécialisés paraissent avantageux de prime abord, mais en cherchant le *nec plus ultra*, on néglige souvent son incidence sur les coûts opérationnels indirects et totaux. Chaque outil supplémentaire ajoute de la complexité et des points de défaillance, accentue les exigences en matière de compétences et mine l'agilité des programmes. De fréquents changements opérationnels et réglementaires nécessitent une reconfiguration et un ajustement constants des outils, et mettent les organisations en face du coût réel de leur trousse d'outils hétérogène.

En moyenne, les grandes entreprises utilisent couramment 100 produits de sécurité émanant de 35 fournisseurs ou plus.



Améliorer l'efficacité et la sécurité grâce à la rationalisation des outils

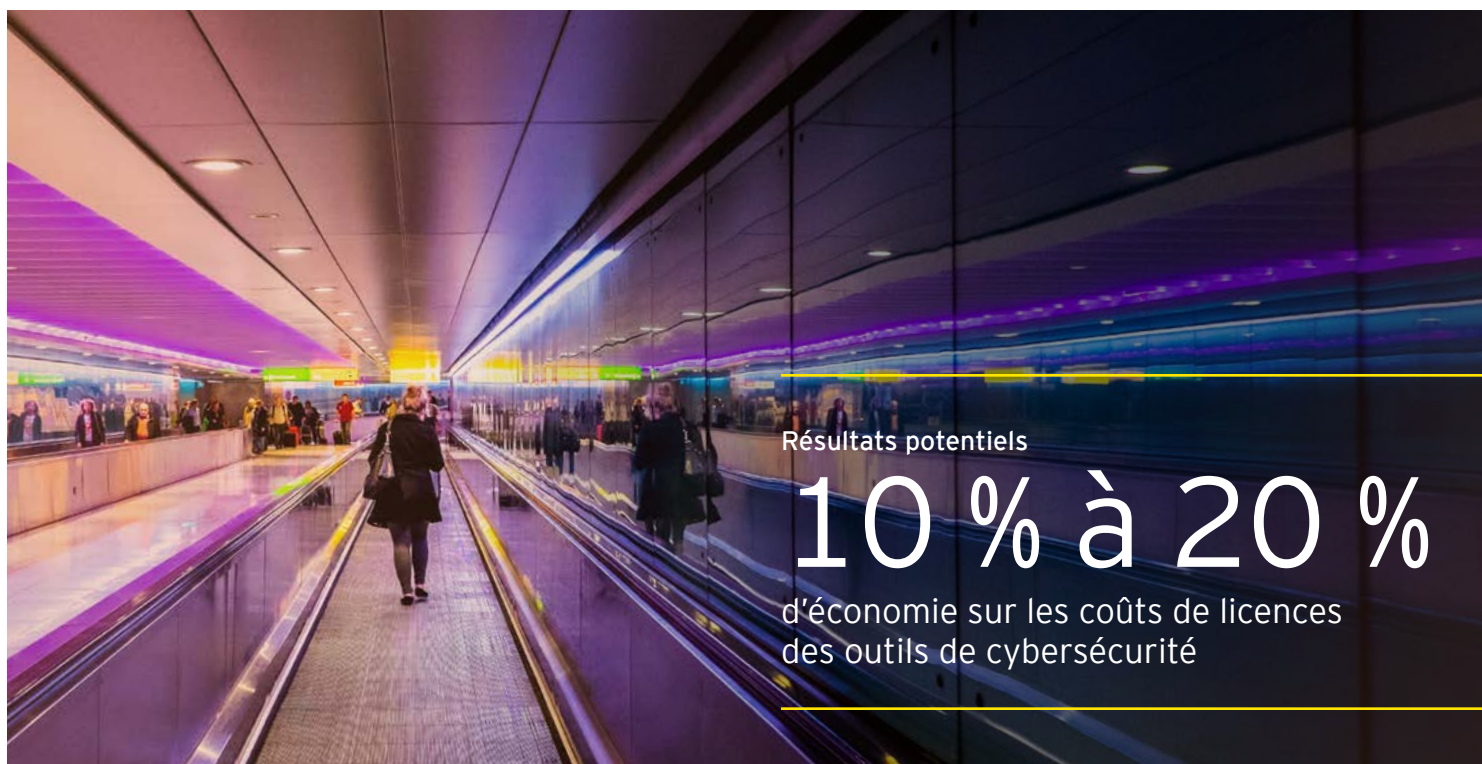
Toutefois, il y a une issue. EY a aidé des entreprises issues de multiples secteurs à réaliser des économies moyennes de 10 % à 20 % sur les coûts de licences des outils de cybersécurité et, dans certains cas, de 35 % par année. Chez un certain nombre de grandes entreprises, les réductions de coûts annuelles se situent même dans les millions de dollars. La rationalisation des outils de cybersécurité constitue un autre facteur clé. Au cours de mandats récents, nous avons aidé nos clients à réduire le nombre d'outils de 24 % en moyenne, tout en conservant le même niveau de sécurité.

Résultats potentiels

24 %

de réduction dans le nombre d'outils
en conservant le même niveau de sécurité

EY aide les entreprises à évoluer dans un environnement Microsoft 365 E3 ou E5 et à dégager des bénéfices en effectuant la transition d'une trousse d'outils de cybersécurité fragmentée à une stratégie de cybersécurité tirant parti de Microsoft Purview et d'autres technologies intégrées de Microsoft. EY est forte d'une équipe de cybersécurité spécialisée qui a fait ses preuves et qui possède une vaste expérience dans l'accompagnement des entreprises dans le processus de mise en œuvre de Purview, leur permettant ainsi de réduire les coûts et la complexité des programmes de cybersécurité, tout en maintenant la conformité. Munis d'une image claire des anciens outils en place et des plus récents développements dans le milieu de l'interconnexion de Microsoft, les professionnels d'EY fournissent une vue complète des fonctionnalités qui sont directement appariées, qui n'offrent qu'une couverture partielle ou qui sont véritablement lacunaires, pour assurer l'élaboration de plans de prise en charge des coûts réalistes et réalisables permettant d'éviter les surprises tout en améliorant la couverture complète de sécurité.



Résultats potentiels

10 % à 20 %

d'économie sur les coûts de licences
des outils de cybersécurité

Une transition harmonieuse

En collaboration avec le chef de la sécurité de l'information et le chef de la gestion des risques, les chefs d'entreprise doivent envisager une approche fondée sur les plateformes de manière objective en se posant les quatre questions suivantes :

1. **Dans la pile technologique de cybersécurité, quels sont les points les plus irritants pour mon organisation?** L'entretien d'une panoplie d'outils, la complexité d'intégration et la formation d'une équipe opérationnelle dotée des compétences adéquates peuvent représenter un défi. Les programmes à outils multiples nécessitent plus d'effort pour se conformer aux changements réglementaires et évoluer selon les initiatives de transformation d'entreprise. Purview simplifie les mises à jour en utilisant une bibliothèque de classement des données uniformisée pouvant s'appliquer à l'entièreté de la plateforme.
2. **À quel point mon entreprise incorpore-t-elle efficacement des produits Microsoft Security déjà assortis d'une licence?** Microsoft a continué d'améliorer ses capacités de cybersécurité et ses cas d'utilisation intégrés, et un nombre croissant d'entreprises ont intégré Microsoft dans leurs programmes de cybersécurité, en particulier Protection des données Microsoft Purview.
3. **Combien dépensons-nous actuellement pour nos outils de cybersécurité? Comment puis-je réduire le coût total de propriété?** Les coûts de licences et de maintenance, de mises à l'essai et d'intégration, et les coûts liés aux ressources humaines peuvent se démultiplier dans un environnement très hétérogène. Les organisations tirent parti de Purview pour simplifier et optimiser leurs trousseaux d'outils de cybersécurité et de protection des données.



4. **Nos capacités de cybersécurité correspondent-elles adéquatement à l'utilisation actuelle et future des données sur place et infonuagiques?** L'utilisation accrue de services infonuagiques et les nouveaux cas d'utilisation des données exigent des responsables des programmes de protection des données qu'ils revoient en permanence la couverture qu'ils offrent. Les capacités intégrées de protection des données de Microsoft Purview fournissent un portrait exhaustif du patrimoine de données. Ce portrait comprend les données structurées et non structurées, les processus de traitement des données, les données stockées sur place et les données stockées dans le nuage. En combinaison avec les autres suites de produits Microsoft, Defender et Intune, Purview est une suite de produits fondamentale dans le cadre du modèle à vérification systématique, qui aide à garantir une rigueur suprême dans l'approche en matière de gouvernance des données et de protection des renseignements.

Pour le chef de la sécurité de l'information, le chef des finances et le chef de la gestion des risques, une plateforme de cybersécurité uniformisée offre différentes formes de valeur ajoutée. Les coûts opérationnels et les besoins en ressources humaines sont réduits. Les délais de déploiement en cas de changement des exigences réglementaires sont raccourcis. De plus, l'équipe de cybersécurité peut surveiller et protéger la sécurité des données au moyen d'un seul tableau de bord. Point particulièrement important, la suite d'outils de conformité de Microsoft permet de satisfaire plus facilement aux règlements sur la protection des données et d'éviter toute amende ou perturbation potentielle.

Résumé

Les programmes de cybersécurité alliant rentabilité et conformité sont au cœur des préoccupations des conseils d'administration en matière de gouvernance et de responsabilité de l'entreprise. Les dirigeants axés sur les profits doivent considérer les programmes de cybersécurité non pas comme une dépense fixe, mais comme un coût pouvant être optimisé grâce à une solution de gouvernance et de conformité des données appropriée, comme Microsoft Purview. Les services qu'offre EY, alignés sur les fonctionnalités de Microsoft Purview, aident les entreprises à faire passer leur gouvernance et leur conformité en matière de données d'une tâche ardue à des possibilités d'économies de coûts, de production de rapports plus utiles, de responsabilisation et d'affectation des ressources de sorte à protéger leurs données les plus précieuses.

Personnes-ressources

Découvrez comment l'[alliance entre EY et Microsoft](#) simplifie la cybersécurité pour aider votre organisation à se transformer dans la confiance, la fiabilité et la résilience.



Melissa Tamblyn

Leader du groupe Microsoft
EY Canada
melissa.tamblyn@ey.com



Nick Galletto

Associé
Leader, Cybersécurité, EY Canada
nick.galletto@ey.com

EY | Travailler ensemble pour un monde meilleur

La raison d'être d'EY est de bâtir un monde meilleur, de créer de la valeur à long terme pour les clients, les gens et la société, et de renforcer la confiance envers les marchés financiers.

S'appuyant sur les données et la technologie, les équipes diversifiées d'EY présentes dans plus de 150 pays instaurent la confiance au moyen de la certification, et aident les clients à prospérer, à se transformer et à exercer leurs activités.

Que ce soit dans le cadre de leurs services de certification, de consultation, de stratégie, de fiscalité ou de transactions, ou encore de leurs services juridiques, les équipes d'EY posent de meilleures questions pour trouver de nouvelles réponses aux enjeux complexes du monde d'aujourd'hui.

EY désigne l'organisation mondiale des sociétés membres d'Ernst & Young Global Limited, lesquelles sont toutes des entités juridiques distinctes, et peut désigner une ou plusieurs de ces sociétés membres. Ernst & Young Global Limited, société à responsabilité limitée par garanties du Royaume-Uni, ne fournit aucun service aux clients. Des renseignements sur la façon dont EY collecte et utilise les données à caractère personnel ainsi qu'une description des droits individuels conférés par la réglementation en matière de protection des données sont disponibles sur le site ey.com/fr_ca/privacy-statement. Les sociétés membres d'EY ne pratiquent pas le droit là où la loi le leur interdit. Pour en savoir davantage sur notre organisation, visitez le site ey.com/fr_ca.

© 2024 Ernst & Young s.r.l./s.e.n.c.r.l. Tous droits réservés.
Société membre d'Ernst & Young Global Limited.

4420506

Le présent document a été préparé aux fins d'information générale uniquement et l'information qu'il contient n'est pas censée constituer un conseil de comptabilité, conseil de fiscalité ou autre conseil professionnel. Veuillez consulter vos conseillers pour obtenir des conseils particuliers.

ey.com/fr_ca