De quelle façon la rationalisation des outils de cybersécurité permet-elle de renforcer l'efficacité des mesures de sécurité?

EY
Travailler ensemble pour un monde meilleur

Microsoft

En cybersécurité, les vases clos ne sont pas évolutifs. La complexité entraîne des coûts et des risques. La simplification permet de renforcer la cybersécurité de votre entreprise et d'appuyer les activités internes.

En bref

- Les entreprises renforcent leur posture de cybersécurité et optimisent leurs investissements en passant à une plateforme d'outils de cybersécurité intégrés.
- Les chefs de la sécurité de l'information peuvent devenir des moteurs d'innovation tout en maintenant la sécurité nécessaire dans un contexte où les menaces sont de plus en plus pernicieuses.

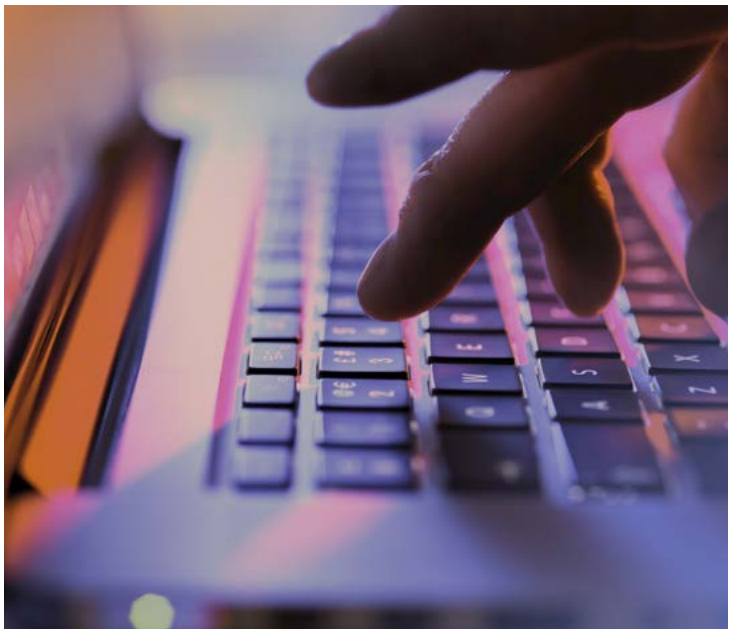
D'après notre expérience, nombre de grandes entreprises déploient une panoplie d'outils de fournisseurs différents et disposent souvent de 100 outils provenant de 35 fournisseurs ou plus. En plus d'augmenter les coûts, cet étalement nuit à l'agilité et affecte le profil de risque de l'entreprise. De fait, beaucoup d'organisations consacrent une portion importante de leur budget de TI et de cybersécurité à des outils redondants, peu performants et surchargés. Simplifier le portefeuille d'outils de cybersécurité est un levier essentiel de l'augmentation de la valeur que les chefs de la sécurité de l'information peuvent ajouter à l'entreprise.

D'où provient toute cette complexité?

La cause de cette complexité se trouve souvent dans l'approche traditionnelle du rattrapage, dans laquelle les équipes des opérations de sécurité ajoutent des outils et des processus de cybersécurité aux technologies déjà en place pour répondre aux exigences que les dirigeants croient nécessaires à leur mission. Nous observons régulièrement des unités fonctionnelles réaliser des investissements parallèles en TI pour l'acquisition d'un logiciel-service sans évaluer pleinement les besoins de cybersécurité adéquate ou son intégration dans la plateforme de cybersécurité de l'entreprise.

La conséquence involontaire de répondre aux besoins de l'entreprise est d'offrir une courtepointe de technologies qui a pour but de fournir une couverture de cybersécurité pour tout ce qui touche à l'informatique, mais sans y parvenir dans un contexte où les cyberattaques pullulent et où les délais d'intervention sont excessivement longs. Ces délais d'intervention prolongés font des raccords entre technologies des cibles de choix pour les agents malveillants.

Le contexte d'affaires actuel ne cesse de se complexifier pour les chefs de la sécurité de l'information. L'agilité est essentielle à la réussite d'une entreprise : toute équipe de cybersécurité devrait donc s'adapter au même rythme que l'entreprise. La courtepointe se complique et ses coutures sont de plus en plus attrayantes pour les agents malveillants. Les équipes de direction des grandes sociétés s'attendent à de meilleurs résultats, à un meilleur rendement de leurs investissements, à un meilleur bilan et à une plus grande résilience après les milliards de dollars investis dans les technologies, les effectifs et les programmes de cybersécurité.



Simplifier, une occasion d'affaires

À une époque de ralentissement économique et de compressions budgétaires accrues, le moment est idéal pour les chefs de la sécurité de l'information d'amorcer l'optimisation de l'efficacité en simplifiant la pile technologique de sécurité pour renforcer la protection. Les chefs de direction, les chefs des finances, les conseils d'administration et les organismes de réglementation poussent de plus en plus les équipes de cybersécurité à dégager de meilleurs résultats et de meilleurs rendements des investissements en cybersécurité. La règle proposée par la Securities and Exchange Commission, intitulée « Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure », exige des sociétés qu'elles divulguent périodiquement leurs directives de cybersécurité, leurs mesures de gestion du risque, l'expertise des membres de leur conseil d'administration et la surveillance des risques qu'effectuent ces derniers. Cette règle souligne l'importance d'une gestion proactive des risques de cybersécurité.

La réputation traditionnelle de contrôleurs d'accès des chefs de la sécurité de l'information s'estompe et se transforme. Les hautes directions recherchent leur expertise pour réaliser des progrès rapidement et s'attendent à ce qu'ils soient des moteurs d'agilité. Adopter la simplification permettra aux chefs de la sécurité de l'information de répondre à ces exigences et de contribuer au succès global de l'entreprise.

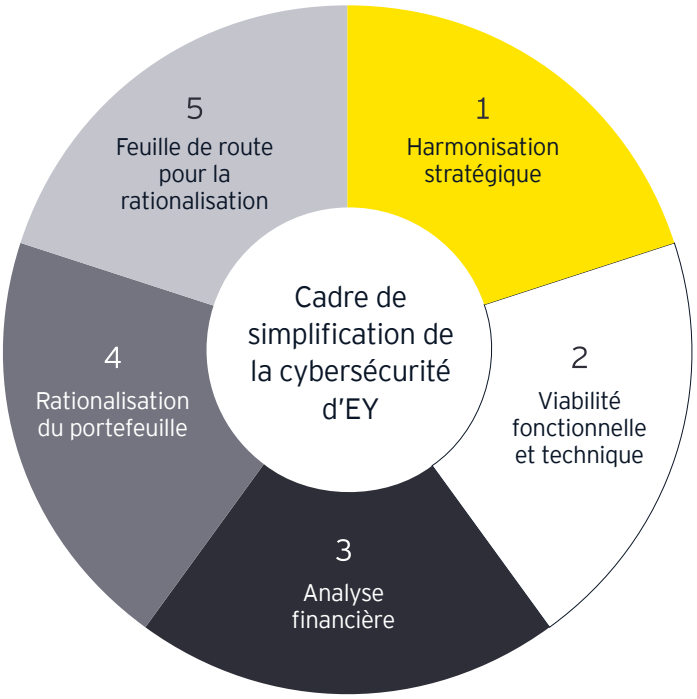
Le parcours de simplification

Le parcours de simplification de la cybersécurité ne se fera pas sans embûches; il est difficile de changer ses habitudes, particulièrement lorsque les cadres s'appuient sur une accumulation d'outils et croient que la complexité est gage d'une défense renforcée. Néanmoins, la complexité n'est pas nécessairement synonyme de cyberprotection améliorée et dépenser intelligemment vaut mieux que dépenser beaucoup.

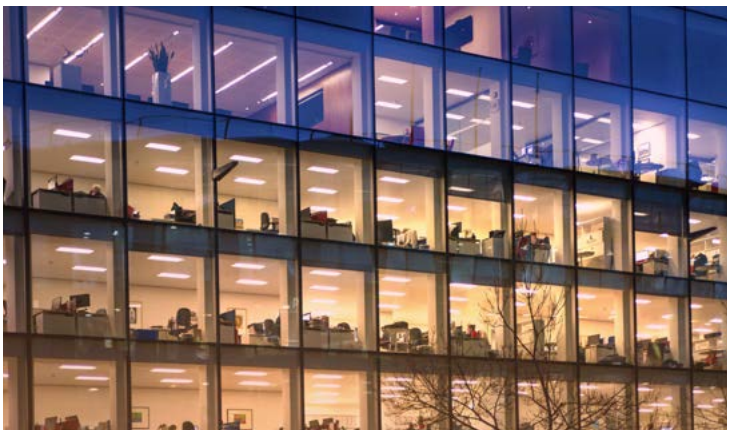
Des investissements sont nécessaires au cours de la période de transition vers une cybersécurité simplifiée, tandis que les anciens outils sont rationalisés et remplacés par une plateforme allégée. La surveillance et la mesure du rendement des investissements réalisés au cours de la transition sont une pratique exemplaire essentielle.

Le cadre de simplification de la cybersécurité d'EY offre une approche sûre en matière de simplification de la cybersécurité, comprenant cinq étapes clés fondées sur l'analyse des données, qui relève efficacement les possibilités d'optimisation dans tous les principaux secteurs d'activité.

1. Harmonisation stratégique : Établir un consensus entre la direction d'affaires, la direction des TI et le chef de la sécurité de l'information pour aligner les coûts de cybersécurité sur la stratégie d'entreprise en améliorant les bénéfices tout en servant les parties prenantes de manière efficace.
2. Viabilité fonctionnelle et technique : Évaluer les outils en place, les relier aux fonctionnalités souhaitées, relever les lacunes de sécurité et les comparer à l'aide d'une plateforme simplifiée, comme le Centre de sécurité et conformité Microsoft.
3. Analyse financière : Estimer le coût total de la propriété associé aux actifs de cybersécurité avant et après la migration, et évaluer l'efficacité future, la cyberrésilience et la flexibilité de l'entreprise.
4. Rationalisation du portefeuille : Utiliser un tableau de bord sur la cybersécurité fondé sur des critères stratégiques, techniques et opérationnels prédéfinis pour orienter les décisions de retrait d'outils et déterminer dans quelle mesure chaque outil correspond aux objectifs et aux exigences réglementaires.
5. Feuille de route pour la rationalisation : Établir un échéancier détaillé d'activités internes nécessaires pour tirer parti des possibilités de simplification, en ordre de priorité.



D'après notre expérience, les grandes entreprises à structure complexe connaissent un parcours fructueux lorsqu'un guide de confiance les y accompagne. Chez EY, nous aidons les clients à réussir leur migration d'une plateforme à l'autre dans une optique d'affaires, en gardant l'objectif de créer une valeur commerciale ajoutée. Au cours de la transition, nous collaborons étroitement avec les dirigeants des TI et des unités fonctionnelles afin de minimiser les perturbations opérationnelles et de veiller à ce que les nouvelles technologies soient adoptées dans le respect des règlements sur la cybersécurité et les données sectoriels, nationaux et régionaux.



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.

Contact

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.

4420506

ey.com/fr_ca