

Comblant les lacunes des opérations de sécurité avec la solution MDR

À mesure que le risque de cyberattaque dévastatrice augmente et monopolise l'attention et le budget qui devraient être consacrés aux objectifs métier essentiels, les organisations doivent réagir en renforçant les programmes de cybersécurité. Les opérations de sécurité (SecOps), responsables de la surveillance et de la protection de tous les aspects de la surface d'attaque numérique, sont au cœur de tous les programmes de cybersécurité.

Malgré les investissements, les opérations de sécurité gagnent en complexité

PLUS DE LA MOITIÉ des personnes interrogées pensent que les SecOps **ont gagné en complexité** au cours des deux dernières années.

» Voici les cinq principales raisons pour lesquelles les SecOps ont gagné en complexité.

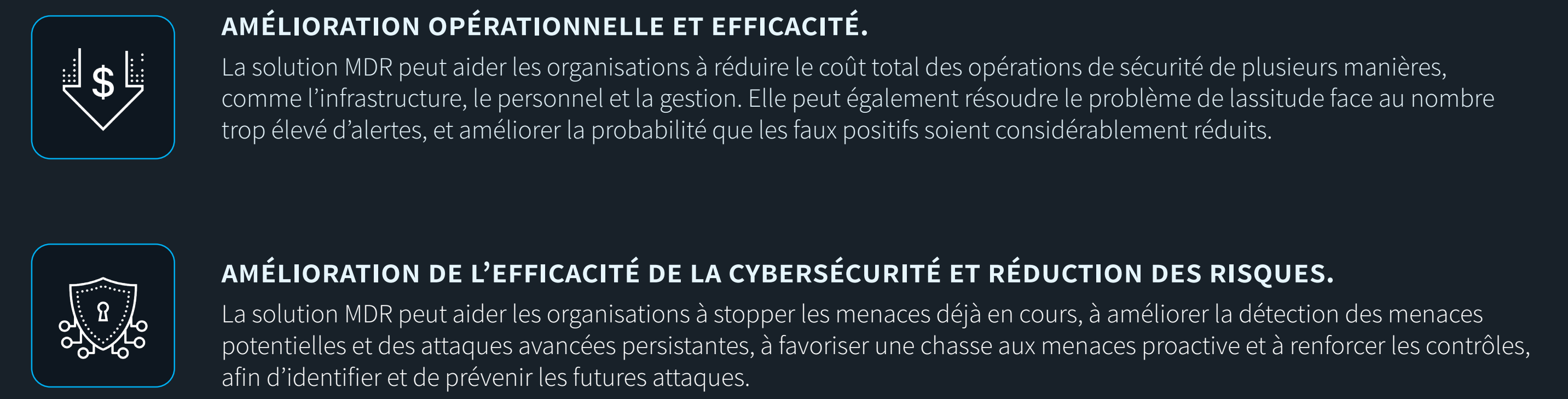


Repenser les stratégies du programme

La taille et la complexité des surfaces d'attaque et du paysage des menaces ont augmenté, tout comme l'utilisation des contrôles de sécurité, ce qui génère des milliers d'alertes et des quantités massives de données de sécurité. Les équipes de sécurité repensent les opérations globales du programme afin d'intégrer davantage les données, issues des équipes IT et de direction opérationnelle, sur les ressources et les risques. Elles peuvent ainsi se concentrer sur les menaces qui représentent le risque le plus important pour les objectifs organisationnels.



» Principaux moteurs de valeur pour l'engagement MDR.



» Principales raisons pour lesquelles votre organisation utilise ou prévoit d'utiliser des services managés.

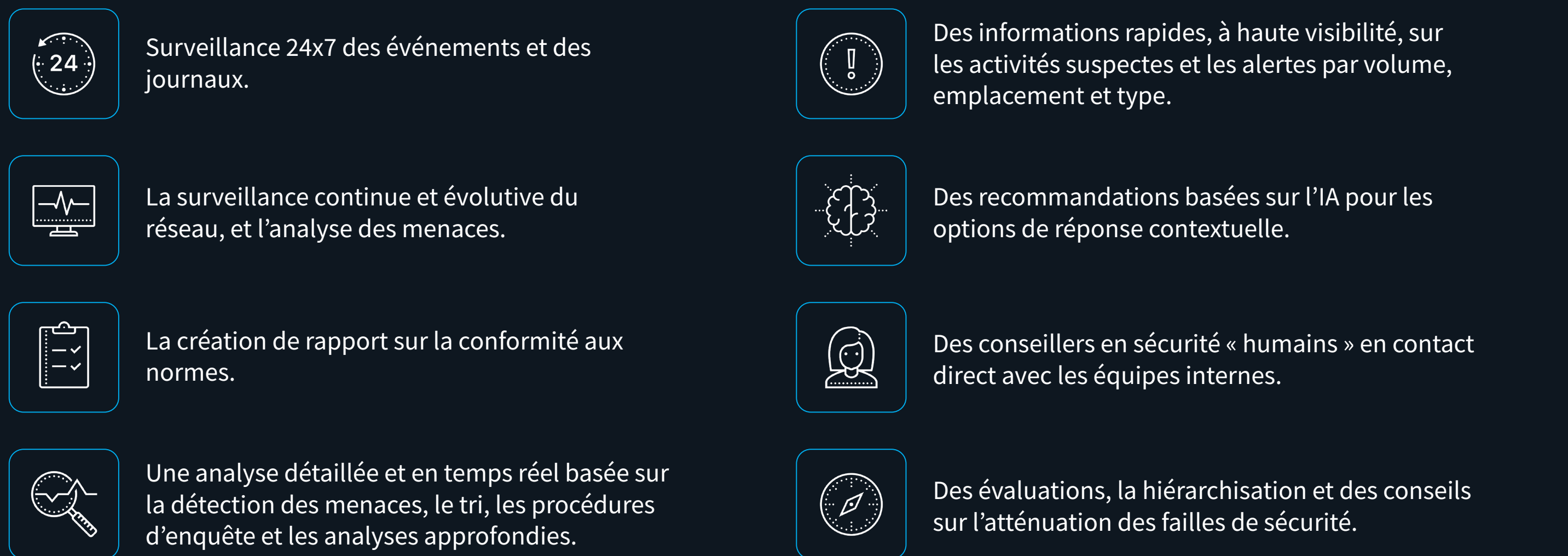


De nombreuses solutions MDR de première génération ont été conçues et implémentées pour une autre époque : il y avait moins de données, moins de menaces et les détections étaient plus simples."

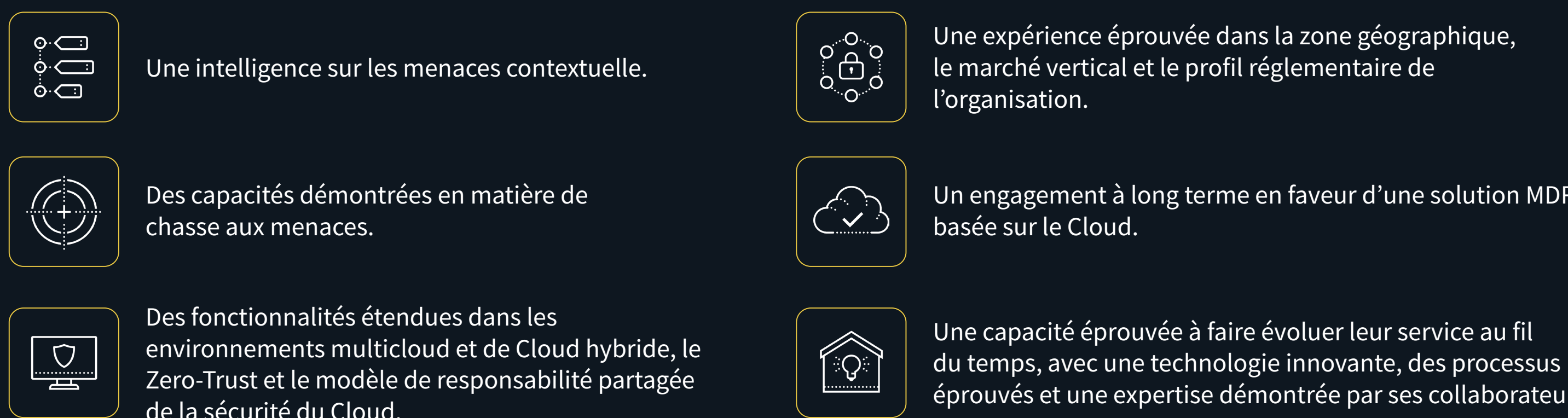
- Dave Gruber, ESG Principal Analyst

Nouvelles exigences pour la solution MDR

De nombreuses solutions MDR de première génération ont été conçues et implémentées pour une autre époque : il y avait moins de données, moins de menaces et les détections étaient plus simples. La nouvelle génération de solutions MDR doit être équipée pour protéger une surface d'attaque plus diversifiée, détecter des menaces plus complexes et tirer parti d'une approche plus axée sur les risques en vue de hiérarchiser et d'atténuer les risques.



Face au grand nombre de prestataires de services potentiels qui peuvent fournir une partie, la plupart, voire la totalité des fonctionnalités MDR sous-traitées, **les organisations doivent rechercher des partenaires capables de fournir les fonctions suivantes:**



Ce qu'il faut retenir

À mesure que le risque de cyberattaque dévastatrice augmente et monopolise l'attention et le budget qui devraient être consacrés aux objectifs métier essentiels, les organisations doivent renforcer les programmes de cybersécurité. Bien que les cas d'utilisation varient, la plupart d'entre elles s'appuient sur des prestataires de services MDR pour développer et faire évoluer leurs programmes.

L'approche de Dell Technologies en matière de détection et de réponse managées associe des technologies flexibles, intelligentes et évolutives à des professionnels expérimentés de la cybersécurité. Elle aide ainsi les organisations de toutes tailles et de tous profils de ressources à accélérer et à renforcer les programmes de sécurité.

EN SAVOIR PLUS

DELLTechnologies