DELL Technologies

Améliorez la maturité de la cybersécurité et de la résilience

La maturité de la cybersécurité est un levier stratégique pour chaque entreprise moderne

Le paysage actuel des cybermenaces est plus dynamique et exigeant que jamais, avec des attaques pilotées par l'IA gagnant en fréquence et en sophistication. Les entreprises ne peuvent plus se contenter de défenses fragmentées ni de mises à jour progressives.

En tant que dirigeant(e) d'entreprise, vous devez agir comme si une violation était inévitable, voire imminente. Chez Dell Technologies, nous aidons nos clients à accroître leur maturité en cybersécurité, c'est-à-dire leur niveau de confiance pour opérer face aux cyberrisques. Nous y parvenons en faisant évoluer une approche globale et multicouche de la cybersécurité et de la résilience, structurée autour de trois domaines d'action essentiels.

Les entreprises doivent disposer de fonctionnalités pour :

- **Réduire leur surface d'attaque**
- **Détecter et répondre aux cybermenaces**
- **Effectuer une récupération après une cyberattaque**

Une cybersécurité efficace commence par une évaluation honnête de votre posture de sécurité actuelle et de votre niveau de maturité. Cette clarté vous permet de prioriser les améliorations pertinentes et d'investir dans un avenir plus sécurisé.

Réduire la surface d’attaque

La surface d’attaque d’une entreprise est dynamique et évolue rapidement, l’IA introduisant de nouveaux vecteurs d’attaque. Avec le télétravail et les systèmes hérités, la surface d’attaque s’élargit, créant davantage de points d’entrée pour les acteurs malveillants. Réduire cette surface devient une nécessité stratégique pour diminuer les risques, respecter les obligations de conformité, protéger la résilience organisationnelle et instaurer une confiance de base.

Améliorer la maturité de la cybersécurité et de la résilience

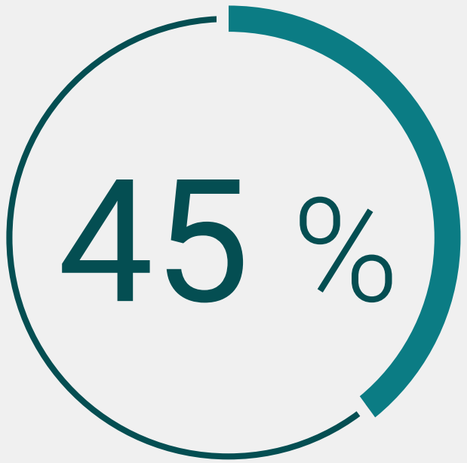
Réduire la surface d'attaque permet de diminuer le risque global en limitant les points d'entrée exploitables par les attaquants. Cela renforce votre maturité en matière de sécurité et simplifie vos démarches de conformité. Résultat : une résilience renforcée, des coûts réduits grâce à la prévention des incidents et la capacité d'innover plus librement et d'entrer sur de nouveaux marchés en sachant que la sécurité est intégrée dès le départ. Tout commence par l'adoption des principes Zero-Trust (ne jamais faire confiance, toujours vérifier) et l'application du moindre privilège pour les utilisateurs, appareils et applications.

Dell Technologies applique le principe de « sécurité dès la conception ». La cybersécurité est intégrée à tout ce que nous faisons, depuis notre chaîne d'approvisionnement mondiale sécurisée jusqu'aux protections intégrées dans nos produits phares. Ces protections commencent au niveau matériel afin de garantir que les appareils démarrent et exécutent uniquement des logiciels de confiance. Nous alignons nos solutions sur ces principes Zero-Trust, vous aidant à éliminer les vulnérabilités avant qu'elles ne soient exploitées. Nos PC IA professionnels les plus sécurisés au monde[1], par exemple, offrent des défenses fondamentales pour l'espace de travail moderne.

Réduire la surface d'attaque augmente votre maturité en matière de sécurité en éliminant les incertitudes : moins d'inconnues, moins de points d'entrée, moins de surprises.

Principaux résultats pour les clients :

- **Réduction des vulnérabilités :** en renforçant de manière proactive les points de terminaison, l'infrastructure et les applications, vous pouvez réduire considérablement les opportunités pour les attaquants.
- **Gestion de la sécurité simplifiée :** moins d'actifs exposés signifient moins de contrôles à gérer, pour une posture de sécurité plus rationalisée et efficace.
- **Une base plus solide pour l'innovation :** avec des points de terminaison fiables et des données protégées, vous pouvez adopter de nouvelles technologies comme l'IA et l'edge computing avec davantage de confiance.



Les entreprises qui se concentrent sur la réduction de leur surface d'attaque constatent une baisse de 45 % du risque de cyberviolation lorsqu'elles gèrent les expositions externes[2].

Détecter et répondre aux cybermenaces

Dans le domaine de la cybersécurité, la vitesse et l'intelligence vont de pair. Une détection et une réponse efficaces permettent d'identifier et de contenir rapidement les menaces, réduisant le temps de d'arrêt et limitant les dégâts. Le résultat : des coûts réduits, moins d'interruptions et une confiance opérationnelle accrue permettant à votre entreprise de fonctionner en toute sécurité, même sous une menace constante.

Améliorer la maturité de la cybersécurité et de la résilience

Cependant, de nombreuses entreprises manquent de visibilité sur leurs environnements hybrides et doivent gérer un volume d'alertes écrasant. Les attaquants restent désormais en moyenne 11 jours dans les réseaux avant d'être détectés. Pour contrer ce problème, vous avez besoin d'une visibilité en temps réel sur les points de terminaison, les réseaux et les systèmes grâce à la surveillance continue, l'intelligence sur les menaces et l'automatisation.

Un partenaire de sécurité idéal dispose d'une expertise de pointe en matière d'intelligence sur les menaces et de réponse aux incidents. Dell associe l'analyse avancée, la détection de menaces pilotée par l'IA/le ML et les services managés 24 h/24 et 7 j/7 à une base matérielle sécurisée afin d'identifier et de contenir les menaces avant qu'elles ne provoquent des perturbations. Des services optionnels comme notre Managed Detection and Response (MDR) offrent une expertise en sécurité pour élargir la visibilité et répondre rapidement aux menaces.

De puissantes capacités de détection et de réponse renforcent votre maturité en matière de sécurité en réduisant le temps d'arrêt et en donnant aux équipes la confiance nécessaire pour agir rapidement lorsque des menaces apparaissent.

Principaux résultats pour les clients :

- **Détection plus rapide et temps d'arrêt réduit :** MDR (Managed Detection and Response) peut réduire le temps moyen de détection et de réponse de 25 à 49 %, diminuant ainsi la probabilité qu'une attaque devienne plus grave.
- **Réduction de la charge opérationnelle :** s'associer à des experts pour la recherche proactive des menaces et la surveillance continue, allège la pression sur les équipes internes, qui peuvent se concentrer sur des initiatives stratégiques.
- **Résilience renforcée :** les capacités de détection et de réponse matures permettent de réduire le nombre d'incidents de sécurité et d'éviter une augmentation des coûts liés aux violations de sécurité.

4,44 M $

Le coût moyen d'une violation de données a atteint 4,44 millions de dollars en 2025[3].

Effectuer une récupération après une cyberattaque

Dans le pire scénario, l'objectif principal est un retour à la normale dans les plus brefs délais, avec une interruption minimale. La reprise après une cyberattaque garantit que vous pouvez restaurer rapidement des données et des systèmes propres, réduisant les dommages réputationnels et vous donnant la certitude que votre récupération est fiable et exempte de réinfection.

Améliorer la maturité de la cybersécurité et de la résilience

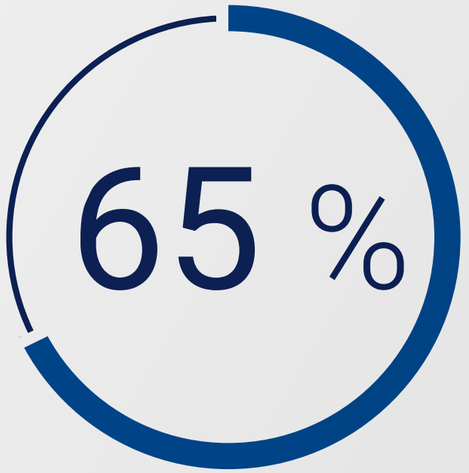
Même si vous créez les défenses les plus solides possibles, vous devez partir du principe qu'une attaque est inévitable. Il est essentiel de disposer d'un plan et de fonctionnalités de récupération complets. Cela inclut le maintien de sauvegardes propres et immuables des données essentielles dans un coffre-fort de récupération isolé, ainsi que l'utilisation d'environnements de salle blanche pour valider que les systèmes restaurés sont exempts de logiciel malveillant avant leur remise en ligne.

Les produits de Dell intègrent des fonctionnalités de récupération. Le retour à la normale des entreprises est notre première priorité en cas d'incident. Des solutions telles que notre coffre-fort PowerProtect Cyber Recovery isolent et protègent les copies propres des données critiques pour une récupération rapide, limitant les pertes et rendant les attaques de ransomware inefficaces. Cette architecture vous aide à remettre rapidement en service les charges applicatives essentielles, afin que vous puissiez avancer en toute confiance.

La phase de récupération est souvent celle où la maturité en matière de sécurité est réellement mise à l'épreuve, lorsque la confiance dépend de la rapidité et de la propreté avec lesquelles l'entreprise peut revenir à un fonctionnement normal.

Principaux résultats pour les clients :

- **Impact métier réduit :** les entreprises disposant d'un plan de réponse aux incidents bien rodé peuvent réduire les coûts liés aux violations d'environ 61 %.
- **Reprise plus rapide des opérations :** privilégier un retour rapide à l'activité, et pas seulement l'élimination de la menace, permet de restaurer les opérations avec un minimum d'interruptions et de coûts.
- **Amélioration de l'intégrité des données :** isoler les données critiques, utiliser des copies immuables et valider l'intégrité avant une restauration renforce la confiance dans le processus de récupération.



des entreprises admettent qu'elles auraient du mal à se remettre d'une cyberattaque en respectant leur contrat de niveau de service[4].

Renforcer votre maturité en matière de sécurité grâce à des partenariats stratégiques

Des partenaires expérimentés sont essentiels pour naviguer dans un paysage de cybersécurité complexe et en constante évolution. Les cybermenaces gagnent en sophistication et en fréquence, rendant presque impossible pour une seule entreprise de maintenir l'expertise, les ressources et la technologie nécessaires pour garder une longueur d'avance. En collaborant avec des leaders de la sécurité comme Dell, les entreprises accèdent à des compétences spécialisées, à des technologies de pointe et à un réseau de partenaires de confiance. Ces partenariats fournissent le support et l'expertise nécessaires pour détecter, prévenir et répondre efficacement aux menaces, garantissant ainsi une protection des entreprises dans un environnement numérique en constante évolution.

En adoptant une approche appropriée dans ces trois domaines de pratique, les entreprises renforcent leur maturité en matière de sécurité, ce qui leur permet de fonctionner, d'innover et de se développer en toute confiance malgré la pression constante du cyberespace. Dell réunit une infrastructure fiable, un espace de travail de confiance, des services avancés et un écosystème de partenaires pour aider votre entreprise à rester sécurisée, évolutive et résiliente, prête pour l'avenir.

Explorer les solutions de sécurité

DELL Technologies

Questions fréquentes

1. Pourquoi la cybersécurité doit-elle être une priorité pour mon entreprise ?
La cybersécurité ne se limite pas à une simple protection : elle constitue la base sur laquelle une entreprise peut innover et se développer tout en faisant face au paysage dangereux de la cybersécurité. Une posture de sécurité solide ne se limite pas à la défense, elle vise aussi à permettre l'innovation. Les entreprises disposant de cadres de cybersécurité matures peuvent évoluer plus rapidement, innover plus librement et pénétrer de nouveaux marchés en toute confiance. Elles sont mieux préparées à gérer les évolutions réglementaires, les attentes des clients et la pression concurrentielle.

2. Comment concilier sécurité stricte et liberté d'innover ?
Vous ne devriez pas avoir à choisir entre sécurité et innovation. Nous sommes convaincus qu'une sécurité robuste favorise réellement l'innovation. À partir d'une base sécurisée, où la sécurité est intégrée dès le départ à vos appareils, à votre infrastructure et à vos données, vos équipes peuvent adopter de nouvelles technologies telles que l'IA et l'edge computing en toute confiance.

3. Pourquoi la sécurité de la chaîne d'approvisionnement est-elle si essentielle ?
La sécurité réelle commence bien avant d'appuyer sur le bouton d'alimentation. À mesure que votre empreinte numérique s'étend, votre exposition augmente, et la confiance devient votre première ligne de défense. Chaque maillon de la chaîne d'approvisionnement doit être protégé, car un seul composant compromis peut affaiblir même le logiciel le plus avancé. C'est pourquoi nous intégrons la sécurité dès la conception, en protégeant chaque étape, de la production au déploiement. De l'usine jusqu'à votre entreprise, votre technologie arrive fiable, vérifiée et prête à fonctionner en toute confiance.

4. Comment Dell peut nous aider à nous remettre d'une cyberattaque ?
Minimiser les interruptions de service et les perturbations est essentiel en cas d'incident. Une bonne préparation est fondamentale. Notre coffre-fort PowerProtect Cyber Recovery isole une copie propre et immuable de vos données les plus essentielles, séparée en toute sécurité de votre environnement principal. En cas d'incident, vous pouvez restaurer les opérations rapidement et en toute confiance, sans compromis et sans payer de rançon.
Dell propose un large éventail de produits et de services conçus pour vous aider à mettre en œuvre une stratégie de récupération complète. Des services de conseil pour élaborer un plan de récupération et de formation, ainsi que des fonctionnalités de protection des données qui permettent de sécuriser les données critiques. Dell adopte une approche centrée sur les personnes et la technologie, en veillant à ce que les collaborateurs et la technologie travaillent ensemble pour vous aider à récupérer rapidement.

5. Dell peut-elle m'aider à détecter les menaces en temps réel ?
Absolument, Courtney. La rapidité est essentielle pour stopper une cybermenace. Nous associons des fonctionnalités de sécurité intégrées avec des services avancés comme Managed Detection and Response (MDR) pour surveiller votre environnement 24 h/24, 7 j/7. À l'aide d'informations issues de l'IA/le ML et de l'expertise humaine, nous vous aidons à détecter instantanément les anomalies et les menaces potentielles, ce qui vous permet de réagir et de contenir les problèmes avant qu'ils n'affectent votre activité.

Sources

[1] D'après une analyse interne réalisée par Dell en octobre 2024 (Intel) et mars 2025 (AMD). S'applique aux PC équipés de processeurs Intel et AMD. Toutes les fonctionnalités ne sont pas disponibles sur tous les PC. Certaines fonctionnalités sont vendues séparément. PC Intel validés par Principled Technologies, juillet 2025 Infographie : Anatomie d'un appareil de confiance

[2] Forrester Consulting, « The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight », octobre 2024.

[3] IBM et le Ponemon Institute, « Cost of a Data Breach Report 2025: The AI Oversight Gap », 2025.

[4] Dell Technologies, « Advance Cybersecurity Maturity: Technology Infrastructure is the Heartbeat of Every Modern Business », février 2025.

À propos de Dell Technologies

Dell Technologies (NYSE : DELL) aide les entreprises et les personnes à construire leur futur numérique et à transformer leur façon de travailler, de vivre et de se divertir. L'entreprise propose à ses clients la gamme de technologies et de services la plus complète et innovante du secteur à l'ère de l'IA.

Apprenez-en plus sur Dell.com