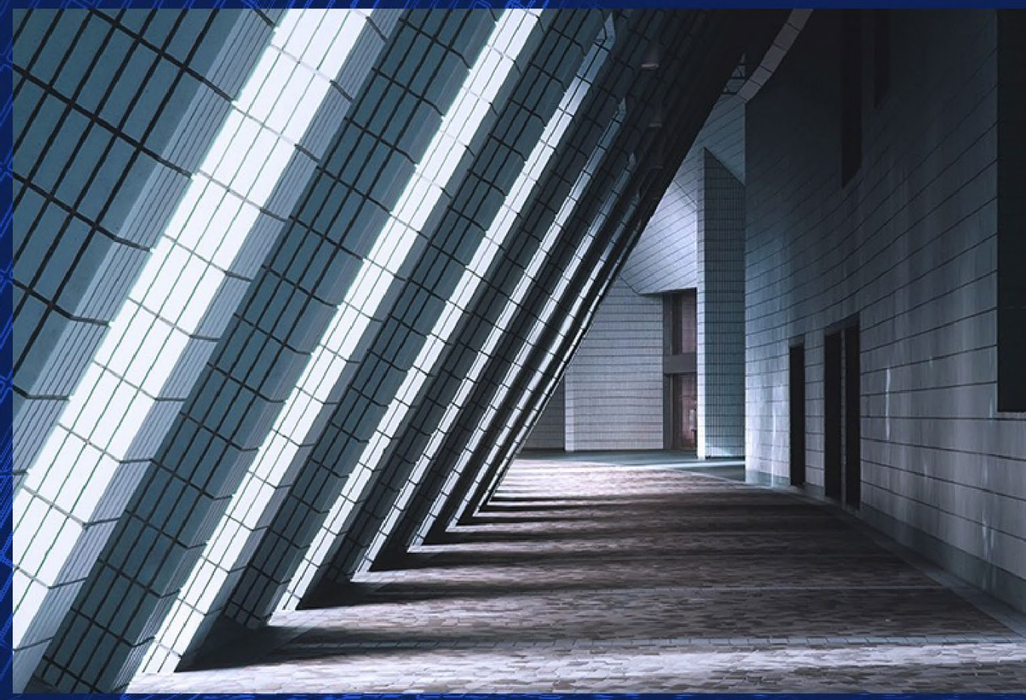
DELL Technologies



Cybersécurité plus mature

L’infrastructure technologique est le cœur battant de toute entreprise moderne

La sécurité et la résilience sont essentielles pour maintenir le bon fonctionnement de ces organes vitaux. Cependant, de nombreuses entreprises ont du mal à suivre le rythme de l’évolution des menaces. En effet, selon une de nos études récentes, 93 % des organisations reconnaissent que leurs stratégies de sécurité doivent être améliorées.

La question n’est plus de savoir si votre organisation sera confrontée à une cybermenace, mais quand et comment. En tant que dirigeant(e) d’entreprise, vous devez agir comme si une violation était inévitable, voire imminente. Vous devez cependant veiller à ce que les risques de sécurité n’entravent pas la capacité d’innovation de votre organisation. Notre étude suggère que 79 % des personnes interrogées ont du mal à trouver l’équilibre entre sécurité et innovation.

En raison des cybermenaces de plus en plus sophistiquées et de la prolifération rapide de technologies telles que l’intelligence artificielle (IA), il est plus que jamais indispensable d’adopter une attitude proactive en matière de sécurité. Les mesures de renforcement de la sécurité doivent se concentrer sur trois domaines prioritaires. Les entreprises doivent disposer de solides fonctionnalités pour :

- **réduire leur surface d’attaque ;**
- **détecter et répondre aux cybermenaces ; et**
- **se remettre d’une cyberattaque.**

93 %

des organisations reconnaissent que leurs stratégies de sécurité doivent être améliorées.

Réduction de la surface d'attaque

La surface d'attaque d'une organisation est très dynamique et évolue rapidement. Au cours des dix dernières années, la surface d'attaque des organisations a augmenté d'environ 1 000 %, ce qui illustre la complexité croissante de la sécurité des environnements numériques modernes.

Chaque nouveau progrès technologique crée des failles de sécurité potentielles. L'IA générative (GenAI), par exemple, présente de nouveaux risques liés à l'exposition des données, à la manipulation des résultats, à la divulgation d'informations sensibles, à l'injection d'instructions, etc. Cependant, les défis de sécurité ne se limitent pas aux implémentations de l'IA. En effet, 67 % des dirigeants d'entreprise redoutent que les nouvelles innovations augmentent leur surface d'attaque.

La réduction de cette surface d'attaque exige une approche multidimensionnelle. Cela nécessite dans un premier temps de réaliser des tests d'intrusion approfondis et d'évaluer les vulnérabilités afin d'identifier et de combler les failles de sécurité potentielles à traiter en priorité. La segmentation complète du réseau, l'isolement des données stratégiques, l'application de contrôles d'accès stricts, ainsi que la mise à jour et l'application de correctifs réguliers sur les systèmes et les applications sont également essentiels.

En outre, la cybersécurité étant un processus continu et non une activité ponctuelle, les évaluations de vulnérabilité et les tests de pénétration initiaux doivent être effectués régulièrement, car l'organisation et le paysage des menaces évoluent en permanence.

Dell Technologies applique le principe de « sécurité intégrée ». Cela passe par la mise en place d'une chaîne logistique sécurisée et l'adoption de principes Zero-Trust tels que la gestion des accès et des identités via l'authentification multifacteur (MFA) et le contrôle d'accès basé sur les rôles (RBAC), inclus dans nos principaux produits. Dell illustre la puissance de ces fonctionnalités en proposant les PC IA professionnels les plus sécurisés du marché.

85 %

des dirigeants d'entreprise s'accordent à dire que la chaîne logistique joue un rôle essentiel dans leur posture de sécurité.

54 % des organisations mettent en œuvre l'IA générative ou prévoient de la déployer dans les 12 prochains mois.

56 % des décideurs IT s'inquiètent des risques liés à l'IA générative (GenAI).

32 % des décideurs IT estiment que l'IA générative a le potentiel de renforcer la sécurité.

Détection/réponse face aux cybermenaces

Dans le domaine de la cyberdéfense, la vitesse et l'intelligence vont de pair. Les entreprises doivent chercher à identifier et à traiter activement les incidents de sécurité potentiels et les activités malveillantes dès les premiers stades d'une violation de la sécurité.

C'est là que les technologies de détection des menaces optimisées par l'IA et les algorithmes d'apprentissage automatique révèlent toute leur utilité. Ces systèmes surveillent le trafic réseau, les schémas de données et le comportement des utilisateurs en temps réel, à l'aide de l'IA, afin d'identifier les menaces de sécurité potentielles.

Un partenaire de sécurité idéal doit également disposer d'une expertise de pointe en matière d'intelligence sur les menaces et de réponse aux incidents. Dell intègre directement la sécurité dans ses PC et ses produits d'infrastructure. Des services optionnels tels que MDR (Managed Detection and Response) facilitent l'identification des menaces et leur traitement.

80 %

des organisations reconnaissent qu'elles pourraient améliorer leurs capacités de détection et de réponse face aux cybermenaces.

Récupération à la suite d'une cyberattaque

Dans le pire scénario, l'objectif principal doit être un retour à la normale dans les plus brefs délais, avec une interruption minimale. Toutefois, dans notre récente enquête, 64 % des organisations admettent qu'elles auraient du mal à se remettre d'une cyberattaque tout en respectant leurs contrats de niveau de service (SLA).

Même si vous créez les défenses les plus solides possibles, vous devez partir du principe qu'une attaque est inévitable. Par conséquent, il est essentiel de disposer d'un plan et de fonctionnalités de récupération efficaces. Il est important de conserver des sauvegardes sécurisées des données et des systèmes stratégiques, et de mettre en place un stockage hors site immuable, isolé et/ou sécurisé à l'aide du chiffrement. Cela exige également d'établir des protocoles clairs de réponse aux incidents qui définissent les rôles et responsabilités de chacun en cas d'attaque, et d'identifier des canaux permettant une coordination fluide entre les équipes internes et les partenaires. Enfin, il est nécessaire de tester régulièrement les procédures de récupération, en simulant notamment différents scénarios d'attaque afin de garantir la préparation de l'organisation.

Les produits de Dell intègrent des fonctionnalités de récupération. Le retour à la normale des entreprises est notre première priorité en cas d'incident.

Grâce à des solutions telles que nos serveurs PowerEdge dotés de la fonction de récupération automatique du système (ASR), les systèmes PowerStore et PowerMax intégrant une fonctionnalité avancée de snapshot pour un stockage immuable et le coffre-fort PowerProtect Cyber Recovery, vous avez l'assurance que vos données les plus stratégiques restent intactes.

65 %

des organisations admettent qu'elles auraient du mal à se remettre d'une cyberattaque tout en respectant leurs contrats de niveau de service.

Renforcez votre posture de sécurité grâce à des partenariats stratégiques

La maturité de la cybersécurité et de la résilience est un processus continu qui nécessite une vigilance et une évolution constantes. Une posture de sécurité et de résilience solide permet aux organisations de réduire considérablement leur exposition aux risques, de minimiser les pertes financières, d'améliorer l'efficacité opérationnelle et de renforcer la confiance des clients.

Un partenaire expérimenté peut vous guider dans ce paysage en constante évolution. En collaborant avec des leaders de la sécurité comme Dell, les entreprises bénéficient de compétences et de connaissances spécialisées dont elles ne disposent peut-être pas en interne, telles que des informations sur les risques émergents, des techniques d'attaque avancées et les toutes dernières stratégies et pratiques d'excellence en matière de sécurité.

En adoptant une approche adaptée pour réduire les surfaces d'attaque, détecter les menaces et y répondre, et rétablir leur activité après un incident, les organisations peuvent développer la résilience nécessaire pour prospérer dans l'ère numérique actuelle et innover afin de relever les défis de demain en toute sérénité.

En savoir plus sur les solutions de sécurité de Dell.

DELL Technologies

À propos de Dell Technologies

Dell Technologies (NYSE : DELL) aide les organisations 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.
Plus d'infos sur Dell.com

Toutes les données de cet e-book proviennent d'une enquête réalisée en février 2025 par Dell Technologies auprès de 750 décideurs d'entreprise et IT aux États-Unis, au Royaume-Uni, en Allemagne, en France et au Japon, tous segments confondus. Pour découvrir les résultats complets, cliquez ici.