Comment protéger les données des entreprises et des clients contre les cybercriminels

8 stratégies de cybersécurité pour les petites et moyennes entreprises.

À propos de ce guide électronique

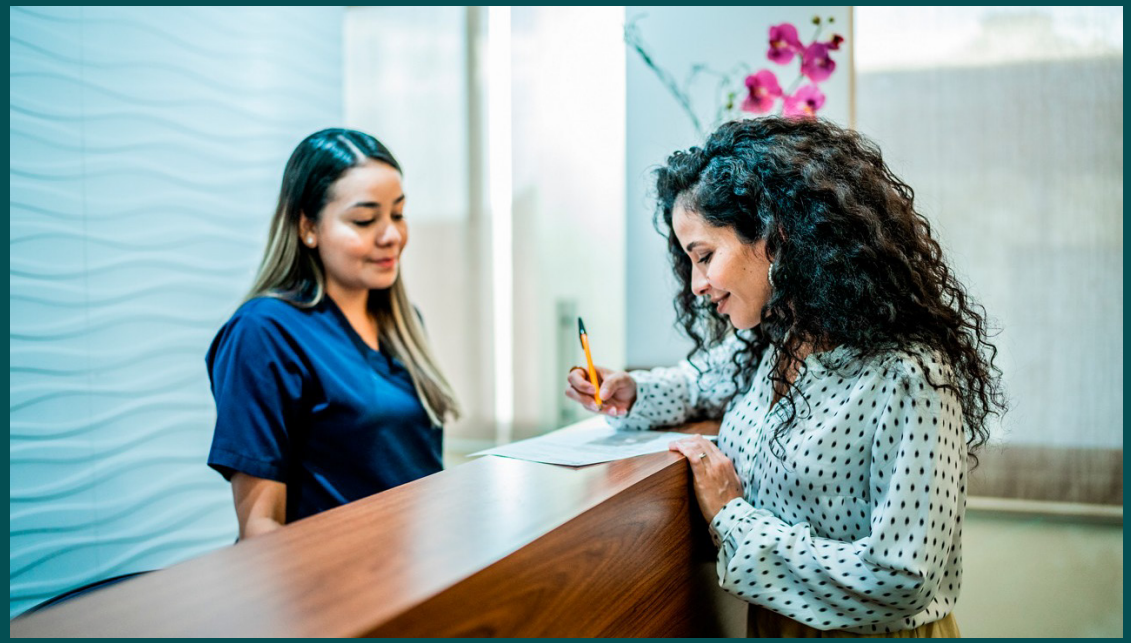
En tant que partenaire IT et de sécurité de confiance pour les entreprises de toutes tailles, Dell Technologies comprend les défis quotidiens de cybersécurité auxquels les petites et moyennes entreprises (PME) sont confrontées. Dans ce guide électronique, nous vous présentons huit stratégies intelligentes pour vous aider à protéger les données de votre entreprise et de vos clients contre les cybermenaces.

Sommaire

Introduction

Nous avons tous vu des titres de journaux sur les cyberattaques qui sont de plus en plus fréquentes et touchent les entreprises de toutes tailles. Pour les PME, la cybersécurité est désormais incontournable. Les cybercriminels ciblent souvent les petites et moyennes entreprises, car ils pensent que leur sécurité est plus facile à contourner. Alors que les grandes entreprises disposent souvent d'équipes et de ressources IT et de sécurité dédiées, les PME peuvent ne pas en disposer. Dans les faits, des études montrent que 35 % des petites entreprises dans le monde estiment que leur cyberrésilience est inadéquate. Elles sont sept fois plus nombreuses qu'en 2022. Il suffit d'une erreur (les correctifs de sécurité les plus récents non installés sur un PC, des informations sensibles non protégées, un clic sur un e-mail de phishing) pour exposer une entreprise à une multitude de problèmes, des difficultés financières à la perte de données en passant par la perte de confiance des clients.

La bonne nouvelle, c'est qu'il suffit de quelques mesures proactives pour faire une grande différence. Protéger les données de votre entreprise et de vos clients vous aide à rester confiant, compétitif et prêt pour l'avenir. ►



Notions de base sur les auteurs de cyberattaques

Avant d'expliquer *comment* vous pouvez assurer votre protection, il est important de connaître l'état d'esprit des attaquants eux-mêmes. Les attaquants utilisent une approche stratégique : ils recherchent des points d'entrée faciles tels que des PC sans correctifs appliqués, des mots de passe faibles et des réseaux non sécurisés. Ils étudient souvent le comportement des utilisateurs, ciblent les identités et tirent parti des vulnérabilités négligées. En connaissant leurs tactiques, les PME peuvent mieux hiérarchiser leurs défenses, détecter les activités suspectes à un stade précoce et élaborer une stratégie de sécurité proactive et non réactive. ►

Qui sont les attaquants ?

Il peut s'agir de criminels ordinaires (pirates mal intentionnés) ou encore d'États-nations. Des e-mails ou des SMS mal écrits permettent d'identifier facilement certains attaquants. Ils disposent parfois de moyens financiers suffisants pour lancer des attaques très sophistiquées.

Pourquoi attaquent-ils ?

L'argent est un facteur de motivation clé. La cybercriminalité mondiale continue de croître chaque année, les experts prédisant que les coûts annuels atteindront 10,5 000 milliards de dollars en 2025. Il va sans dire que le gain potentiel d'une attaque réussie est trop important pour être ignoré.

Comment les attaquants procèdent-ils ?

Les cybercriminels ne s'arrêtent jamais et réalisent des attaques plus sophistiquées grâce à l'IA, désormais à portée de main. Voici quelques méthodes qu'ils utilisent :

- Les attaques sur les « points de terminaison » tels que les PC constituent un problème croissant. Dans le rapport Perspectives du marché de la sécurité des points de terminaison de Forrester Research, Inc. daté de mars 2025, la société explique que « les points de terminaison sont parmi les principales cibles des attaques externes pour les entreprises qui ont subi une violation au cours des 12 derniers mois. »
- Les attaques basées sur l'identité sont également en plein essor. Le phishing reste une menace majeure. Il s'agit de l'une des attaques les plus courantes. Elle est souvent utilisée pour voler des informations d'identification et diffuser des logiciels malveillants.
- Les attaques réseau comme les rançongiciels continuent de faire des ravages. Des recherches récentes montrent que les petites entreprises ont été plus durement touchées que les grandes entreprises : 88 % des violations les visant impliquent des rançongiciels.

En résumé, les cyberattaques sont lucratives. En moyenne, les attaques par rançongiciels réussies rapportent 2 millions de dollars aux cybercriminels. La persistance fait donc partie de leur stratégie, et la protection doit faire partie de la vôtre.

Risques majeurs de cybersécurité pour les PME

Compromission des appareils

Compromission des identités

Compromission des réseaux

1 Identifiez les éléments à protéger

Les attaquants s'attaquent aux données sensibles des clients et des collaborateurs, mais vous ne pouvez pas protéger ce que vous ignorez. Inventoriez toutes les ressources et données IT de votre entreprise. Où les données sont-elles stockées ? Qui a accès ? Quels appareils sont présents sur votre réseau ? À l'aide de ces informations, prenez des mesures. Assurez-vous que le stockage des données est sécurisé et limitez l'accès aux informations confidentielles. Connaître vos données est une première étape essentielle pour les protéger. ►

2 Collaborez avec des fournisseurs sécurisés

Prenons l'histoire du cheval de Troie. Les Grecs ont dissimulé des soldats dans un cadeau apparemment inoffensif, que les Troyens ont apporté à l'intérieur de leur ville fortifiée. Au moment opportun, les attaquants ont frappé de l'intérieur. Les cybercriminels ont recours à des tactiques similaires. Ils s'introduisent par le biais de fournisseurs de confiance, de mises à jour logicielles ou de matériel. Souvent, les PME s'appuient sur de nombreux fournisseurs, ce qui les rend vulnérables en cas de compromission. Par exemple, le contrôle des fournisseurs, la surveillance de l'intégrité des logiciels et la visibilité des détails des expéditions sont essentiels à une stratégie de cybersécurité solide. ►

3 Bénéficiez de PC dotés d'une sécurité intégrée

Chaque PC est un point d'entrée potentiel pour les auteurs de cyberattaques. Des fonctionnalités de sécurité intégrées, telles que la protection du matériel, le démarrage sécurisé et la protection de l'identité, vous aident à vous protéger contre les menaces dès l'installation. Les PC sécurisés simplifient la gestion IT et offrent une protection renforcée contre les logiciels malveillants, le phishing et les accès non autorisés. En outre, gardez à l'esprit que les attaquants ne frappent pas toujours à distance. Un PC laissé sans surveillance dans un espace public ou partagé peut être physiquement accessible et exploité par un autre utilisateur ou une personne se faisant passer pour un membre du personnel ou un technicien de maintenance. Avec des ressources limitées et des risques physiques et numériques toujours plus nombreux, la sécurité intégrée est aujourd'hui indispensable. ►

4 Mettez les PC à jour

Les cybercriminels exploitent souvent les failles connues de systèmes obsolètes, comme s'ils se faufilaient par une porte déverrouillée. Ignorer les alertes des PC et reporter les mises à jour peut vous rendre vulnérable. Les mises à jour logicielles et les correctifs agissent comment des verrous : ils corrigent les bugs et les failles de sécurité que les attaquants pourraient exploiter. Des correctifs et mises à jour réguliers corrigent ces vulnérabilités, ce qui vous aide à protéger les données de votre entreprise et de vos clients. Pour les PME, il s'agit d'une étape simple qui permet d'éviter de graves problèmes. ►

5 Détectez les problèmes et résolvez-les rapidement

Ce n’est pas parce que vous disposez de PC sécurisés et que vous les tenez correctement à jour qu’un cybercriminel n’attaquera pas. Des attaquants peuvent tenter d’utiliser un seul appareil des dizaines de fois. Ils peuvent effectuer plusieurs attaques par phishing via des e-mails ou des SMS. Cela augmente les chances d’entrer par effraction et d’accéder à des données sensibles. Il est donc essentiel de disposer d’une visibilité sur l’ensemble des PC professionnels, de votre réseau et de tous les environnements Cloud que vous utilisez. C’est là qu’une couche logicielle peut vous aider à tout voir et, surtout, à agir rapidement lorsque vous constatez une activité suspecte. ►

6 Utilisez des mots de passe complexes et activez la MFA

Vous utilisez toujours « 123456 » ou « motdepasse » ? Vous n'êtes pas seul, mais c'est risqué. Le vol d'informations d'identification génère de nombreuses failles. Des mots de passe complexes sont indispensables comme première ligne de défense. Cela étant dit, les attaquants persistants trouvent des moyens de les contourner. L'authentification multifacteur (MFA) est importante : elle permet d'ajouter une deuxième couche, ce qui réduit de 99 % les risques de piratage.

Tout d'abord, définissez des mots de passe complexes.

Combinez-les ensuite à une deuxième méthode de vérification de l'identité, comme les lecteurs d'empreintes digitales, les cartes à puce ou NFC. Pour une protection renforcée, stockez les informations d'identification des utilisateurs dans du matériel sécurisé, hors de portée des logiciels malveillants qui cherchent à les dérober. ►

7 Formez vos collaborateurs et testez leurs compétences

Votre sécurité dépend de votre maillon le plus faible. Malheureusement, l'erreur humaine continue d'être une cause majeure de failles. Les erreurs vont du report des mises à jour critiques de PC à l'exposition accidentelle de données sensibles en passant par la réutilisation des mots de passe. Les auteurs de cyberattaques comptent sur l'erreur humaine et la négligence pour s'emparer de votre entreprise. La formation à la cybersécurité est donc essentielle. Elle aide les collaborateurs à identifier les menaces et à suivre des pratiques sécurisées. Organisez régulièrement des formations et testez les compétences des participants. Sont-ils capables de repérer une attaque par phishing ? Réagissent-ils de manière appropriée ? Pourquoi ? Renforcez l'apprentissage et révélez les lacunes avant qu'il ne soit trop tard. Dotés des connaissances nécessaires, les collaborateurs constituent une première ligne de défense solide. ►

8 Mettez en place un plan en cas de violation

Anticipez toujours le pire scénario. Trop d'enjeux sont en jeu. Chaque seconde compte lorsque vous avez été victime d'une violation de sécurité, et la mise en place d'un plan d'intervention en cas d'incident permet à votre équipe d'obtenir un guide clair sur la marche à suivre en cas de problème. Une stratégie de réponse permet de détecter une violation, de limiter les dommages et d'assurer la récupération en toute sécurité. Vous pouvez ainsi réduire les interruptions et accélérer la reprise des activités. Une cybersécurité forte implique d'être proactif et préparé, quel que soit le problème. ►

Principaux points à retenir

La modernisation du lieu de travail est une priorité pour de nombreuses entreprises qui se tournent vers l'IA générative (GenAI) pour stimuler la productivité et améliorer l'expérience des collaborateurs. Dans une étude récente, 77 % des PME estiment que l'IA/IA générative est un élément clé de leur stratégie commerciale. Toutefois, une majorité d'entre elles craignent que les innovations augmentent leur surface d'attaque. C'est une préoccupation légitime.

Avec l'essor des PC IA et la fin de la prise en charge de Windows 10, **c'est le moment idéal pour effectuer une mise à niveau.** Optimisez les performances et la sécurité avec les PC IA les plus récents. ►

Récapitulatif des 8 meilleures pratiques et comment Dell peut aider

1 **Identifiez les éléments à protéger.**
Dell Services peut vous aider à faire l'inventaire de vos ressources IT, réseaux et données.

2 **Collaborez avec des fournisseurs sécurisés.**
Les contrôles de la chaîne logistique de Dell atténuent le risque d'altération. Une conception sécurisée des PC réduit les risques de failles de sécurité.

3 **Bénéficiez de PC dotés d'une sécurité intégrée.**
Les PC Dell sont équipés d'une sécurité intégrée sans frais supplémentaires.

4 **Mettez les PC à jour.**
Dell assure la sécurité des PC grâce à des correctifs en temps opportun. Besoin d'aide ? Essayez une évaluation des failles de sécurité avec Dell Security Services.

5 **Détectez les problèmes et résolvez-les rapidement.**
Appuyez-vous sur des logiciels de partenaires Dell pour surveiller les activités suspectes sur les PC, les réseaux et le Cloud.

6 **Utilisez des mots de passe complexes. Activez MFA.**
Passez au niveau supérieur avec Dell SafeID pour le stockage des informations d'identification basé sur le matériel.

7 **Formez vos collaborateurs et testez leurs compétences.**
Faites appel à Dell Services pour obtenir une formation gérée de sensibilisation à la sécurité pour les collaborateurs.

8 **Mettez en place un plan en cas de violation.**
Incident Response & Recovery de Dell peut vous aider.

Prêt à renouveler votre équipement ? Découvrez les PC adaptés à votre entreprise

Trouvez des PC IA qui répondent aux objectifs de sécurité de votre entreprise.
Dell propose plusieurs options.

Protégez-vous contre les attaques basées sur les appareils, les identités et les réseaux avec des PC IA sécurisés. Restez protégé et concentrez-vous sur vos activités quotidiennes. ►

--

1 Même si une fonctionnalité PC peut être disponible dans une gamme de produits, il n'est pas garanti qu'elle soit disponible sur toutes les plateformes.

2 Les PC IA professionnels les plus sécurisés : d'après une analyse interne réalisée par Dell en mars 2025. S'applique aux PC équipés de processeurs AMD. Toutes les fonctionnalités ne sont pas disponibles sur tous les PC. Certaines fonctionnalités sont vendues séparément.

3 Authentifiez-vous via un lecteur d'empreintes digitales avec des informations d'identification stockées en toute sécurité dans le module TPM.

4 Authentifiez-vous via un lecteur d'empreintes digitales, une carte à puce ou le NFC avec des informations d'identification stockées en toute sécurité dans ControlVault (exclusivité Dell).

5 Certaines offres sont disponibles par volume uniquement et nécessitent un nombre minimum de licences. Des options autorisées par FedRAMP sont disponibles.

			SÉCURITÉ INCOMPARABLE[2]
Sécurité disponible[1]	**Dell et Dell Plus**	**Dell Pro Essential**	**Dell Pro et Pro Max**
Assurance de la chaîne logistique	•	•	•
Assurance améliorée de la chaîne logistique			•
Obturateur de confidentialité	•	•	•
Logement antivol	•	•	•
Lecteur d'empreintes digitales	•	•	•
TPM 2.0	•	•	•
Protection des informations d'identification[3]			•
Protection améliorée des informations d'identification[4]			•
Alertes de sécurité des PC			•
Mises à jour logicielles et correctifs	•	•	•
Gestion PC			•
Silicium optimisé pour l'IA	•	•	•
Silicium optimisé pour la sécurité			•
Logiciel antivirus de nouvelle génération (NGAV)[5]	•	•	•
Logiciel antivirus de nouvelle génération et logiciel de détection des menaces (PC, réseau et Cloud)[5]			•
Logiciels d'autoréparation, de géolocalisation et de résilience pour PC			•
Support avancé des PC	•	•	•

Aller de l’avant

Actualisez vos PC.

La prise en charge de Windows 10 prend fin en octobre. De nombreuses PME se retrouveront donc avec des PC obsolètes et non pris en charge.

Passez aux PC IA Dell sécurisés sur les processeurs AMD Ryzen AI PRO.

Optez pour une couche logicielle.

Tenez les attaquants à distance grâce à plusieurs couches de défense.

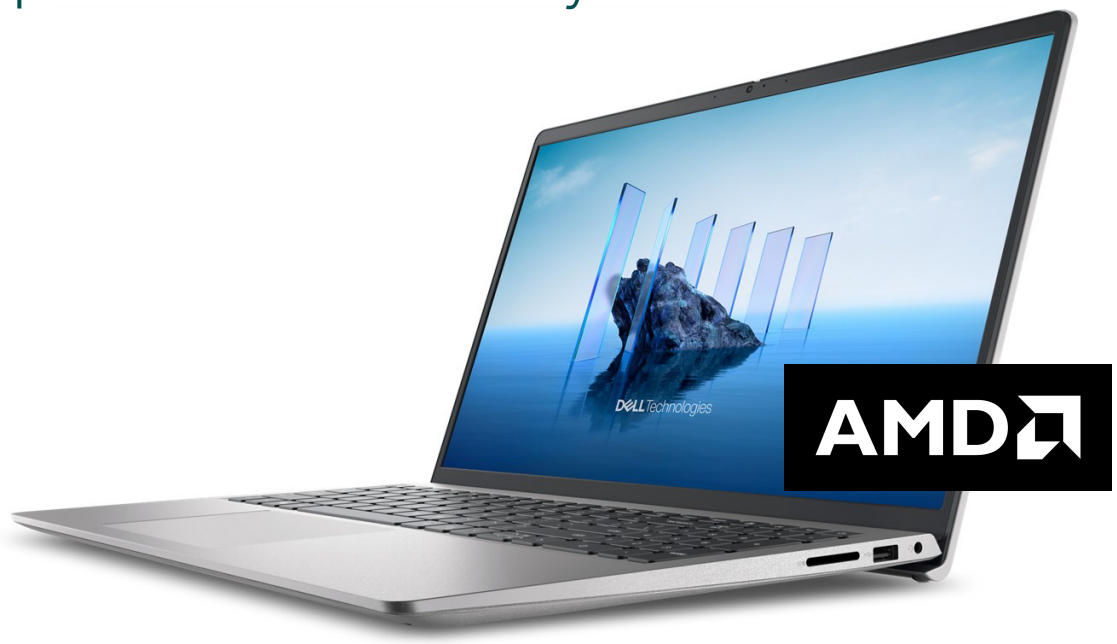
Ajoutez une protection logicielle pour les PC nouveaux et existants.

Besoin d’aide pour gérer la sécurité ?

Les opérations de sécurité dont vous avez besoin, avec les experts en cybersécurité Dell.

Découvrez les services de sécurité gérés.

Passez aux derniers PC IA Dell sur les processeurs AMD Ryzen AI PRO.



Pour en savoir plus :

Contactez-nous à l'adresse : Global.Security.Sales@Dell.com

Rendez-vous sur : Dell.com/Endpoint-Security

Suivez-nous : LinkedIn @DellTechnologies | X @DellTech

À propos de Dell Technologies

Disposant de ressources limitées, les PME doivent être proactives dans la protection des informations de l'entreprise et des données des clients. Investir dans la cybersécurité permet d'assurer la continuité de l'activité, de préserver la réputation et de renforcer la confiance des clients, ce qui en fait un élément intelligent et nécessaire de la gestion d'une entreprise moderne.

De la réduction des risques d'attaques par rançongiciels à la détection des activités suspectes et à la réponse aux menaces en temps réel, Dell est là pour vous aider à créer une stratégie de sécurité et à mettre en œuvre des solutions de sécurité adaptées aux besoins actuels et futurs de votre entreprise.