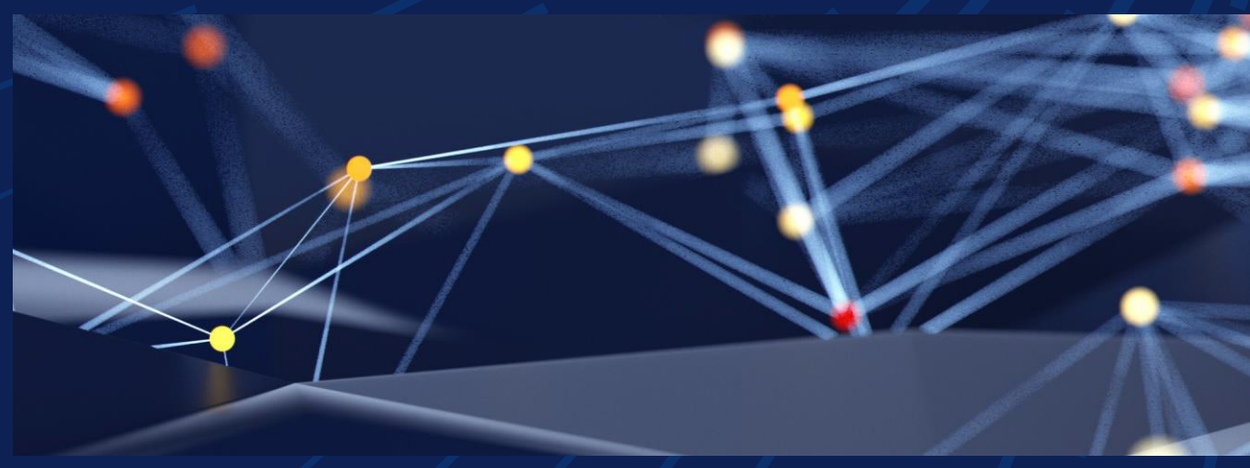
DELL Technologies

La cybersécurité de demain :

S’adapter à une nouvelle ère numérique



Bien que les professionnels de la cybersécurité se dévouent souvent entièrement à la prévention des attaques et à l’élaboration de plans de récupération, l’environnement de sécurité global évolue en permanence. Il est donc important de planifier vos prochaines étapes.

Lorsque nous nous penchons sur les perspectives d’avenir, trois domaines se distinguent : la cryptographie post-quantique, l’évolution du paysage réglementaire et les menaces émergentes. Les entreprises doivent agir dès maintenant en planifiant et en mettant en œuvre des solutions dès qu’elles sont disponibles.

À l’aube de la cryptographie post-quantique

L’informatique quantique porte la promesse de révolutionner tous les secteurs, en offrant une puissance de calcul apte à résoudre des problèmes que les ordinateurs classiques sont incapables d’appréhender. Cependant, cette même puissance pourrait rendre obsolètes les méthodes cryptographiques actuelles. Des algorithmes tels que RSA et ECC, qui sous-tendent la plupart des communications sécurisées à l’heure actuelle, pourraient être piratés en quelques secondes par un ordinateur quantique suffisamment avancé. Cette menace imminente a accru l’urgence de la cryptographie post-quantique.

La cryptographie post-quantique tourne autour du développement d’algorithmes cryptographiques qui restent sécurisés à l’ère de l’informatique quantique. Le National Institute of Standards and Technology (NIST) a reconnu l’imminence de ce risque et se démène pour normaliser les algorithmes de résistance quantique.

Pour les entreprises, se préparer à cette transition est non négociable. L’adoption précoce des solutions de cryptographie post-quantique garantira la sécurité des données lorsque les pirates mettront la main sur l’informatique quantique.

Comme le souligne Bobbie Stempfley, VP of Cybersecurity et Business Unit Security Officer chez Dell, les entreprises doivent faire leurs premiers pas en se concentrant sur deux domaines clés :

Identifier et recenser tous les modèles cryptographiques actuellement utilisés.

Prenez les données en cours de transfert et pas seulement les données au repos. Pensez à la gestion des clés, à la signature du code, à l’identification des appareils, à l’accès sécurisé et à la télémétrie. Dressez un inventaire complet, puis élaborez une feuille de route.

Comprendre le statut des fournisseurs.

Parce que les entreprises modernes font parfois appel à des milliers de fournisseurs, soyez conscient des risques que ces derniers représentent. Veillez à ce qu’ils planifient également le changement.

Ces points de départ ne suffisent pas. Menez des évaluations des risques pour identifier les systèmes vulnérables, envisagez la mise en œuvre de modèles cryptographiques hybrides pour rester opérationnel pendant la transition et collaborez avec les fournisseurs qui explorent déjà des solutions quantiques sécurisées, sans jamais perdre de vue qu’aucun fournisseur ou technologie n’offrira de solution clé en main.

Changements réglementaires et mondialisation

L’évolution de l’environnement réglementaire est un autre facteur déterminant dans l’avenir de la cybersécurité. Les réglementations vont désormais bien au-delà de la conformité : elles deviennent un cadre clé pour responsabiliser, favoriser les mises à niveau technologiques et protéger les citoyens dans un monde interconnecté et axé sur les données. Toutefois, elles évoluent rapidement et varient considérablement d’une région à l’autre, devenant un véritable casse-tête.

Cela dit, ces réglementations ne se limitent pas à de simples sanctions en cas de non-conformité. En effet, elles servent de catalyseurs pour mettre en place de meilleures pratiques de cybersécurité. Les entreprises qui alignent activement leurs politiques sur les exigences réglementaires instaurent un véritable climat de confiance et gagnent en efficacité opérationnelle. Pour ce faire, elles doivent établir des cadres de gouvernance suffisamment flexibles pour les adapter aux changements juridiques, mener des audits de conformité régulièrement et investir dans la formation des employés afin qu’ils apprennent à gérer les informations sensibles conformément aux normes les plus récentes.

Tout au long du chemin, les responsables de la sécurité doivent absolument s’assurer que tout le monde les comprend. Trop souvent, les professionnels de la sécurité communiquent en termes techniques qui n’interpellent pas les clients, les organismes de réglementation et les autres parties prenantes. Il leur incombe donc de vérifier qu’ils sont compris, et non à ceux qui les écoutent de les interpréter.

DELL Technologies

> « Passer à la cryptographie post-quantique, c'est un peu comme déplacer une maison entièrement meublée d'un point A à un point B. C'est au moins aussi complexe, et le défi est de ne rien casser pendant le processus. »
>
> ***Bobbie Stempfley***
> *VP, Cybersecurity et Business Unit Security Officer, Dell Technologies*

L'évolution des menaces (et des défenses)

L'IA révolutionne les entreprises, augmente la productivité et ouvre la voie à de nouvelles opportunités en matière de potentiel humain. Dans le domaine de la cybersécurité, l'IA profite à la fois aux pirates et à ceux qui tentent de s'en défendre :

Utilisation pirate : l'IA complexifie les attaques, parmi lesquelles l'hameçonnage ciblé et les deepfakes très convaincants.

Utilisation défensive : l'IA aide les équipes qui veulent s'en protéger grâce à :

- Traitement rapidement de grandes quantités de données de sécurité.
- Hiérarchisation plus efficace des menaces.
- Amélioration des capacités de détection et de réponse.

Cela dit, les outils de sécurité ne cesseront de s'améliorer. Le traitement du langage naturel permet par exemple aux professionnels de la sécurité d'interagir plus directement avec leurs systèmes et de prendre des mesures correctives de manière proactive.

Les entreprises doivent s'efforcer de tirer parti de ces capacités tout en veillant à ce que leurs formations et autres mécanismes de défense soient toujours à jour. En effet, la formation est le meilleur moyen d'éviter que les employés ne soient victimes d'attaques plus sophistiquées.

Abandonner les mots de passe

Les mots de passe ne sont plus la méthode de gestion des identités et des accès la plus sécurisée.

Les systèmes traditionnels basés sur des mots de passe présentent des vulnérabilités importantes, ce qui en fait une solution de plus en plus inadaptée aux besoins de cybersécurité modernes. Les mots de passe sont à la merci de nombreuses menaces, comme le bourrage d'identifiants, l'hameçonnage et les attaques par force brute, exposant souvent les entreprises à des risques inutiles. De plus, les mauvais comportements des utilisateurs qui réutilisent les mots de passe ou créent des mots de passe peu sécurisés aggravent ces vulnérabilités.

Les méthodes d'authentification sans mot de passe, comme la biométrie, les certificats et les jetons matériels, offrent une alternative plus solide et plus sécurisée en écartant d'office des catégories entières de menaces liées aux mots de passe. L'adoption de systèmes sans mot de passe représente une évolution cruciale dans la gestion des identités et des accès, en alignant les mesures de sécurité sur la sophistication croissante des cybermenaces.

Les technologies sans mot de passe offrent également de nombreux avantages : réduction de la surface d'attaque, amélioration de l'expérience utilisateur grâce à une connexion plus rapide et plus fluide, et réduction des coûts IT en diminuant le nombre d'incidents liés aux mots de passe. L'utilisation de méthodes avancées garantit une posture de sécurité renforcée et aide les entreprises à se conformer aux normes réglementaires. La transition vers des systèmes sans mot de passe n'est pas qu'une tendance : c'est un impératif absolu pour créer un écosystème numérique plus sûr et plus efficace, autant à destination des particuliers que des entreprises.

Conclusion

La cybersécurité entre dans une ère transformatrice, façonnée par l'informatique quantique, l'évolution des réglementations et des menaces toujours plus complexes. Pour garder une longueur d'avance, les entreprises doivent adopter certaines innovations, comme la cryptographie post-quantique, les défenses optimisées par l'IA et l'authentification sans mot de passe. En donnant la priorité à la préparation, à la collaboration et à l'investissement stratégique, elles peuvent créer un environnement numérique plus sécurisé et plus résilient. Il est temps d'agir.

Produits et solutions Dell qui peuvent vous aider

Solutions Dell disponibles	Description
Cybersecurity Advisory Services	Conseils d'experts qui peuvent vous aider à planifier l'évolution du paysage des menaces, y compris les menaces actuelles et émergentes.
vCISO	Responsable de la sécurité virtuelle des systèmes d'information et expert en cybersécurité qui peut vous aider à identifier et gérer les risques mais aussi à prendre des décisions stratégiques.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **dell.com/cybersecuritymonth**

DELL Technologies