DELL Technologies

Protégez vos charges applicatives Cloud contre les attaques réseau

Implementation Services for Microsoft Azure Network Security

Comment protégez-vous vos réseaux Cloud ?

Dans le paysage numérique moderne, Azure a connu une augmentation significative des efforts de migration, principalement en raison de ses fonctionnalités d'évolutivité, d'adaptabilité et de rentabilité. Néanmoins, la préoccupation majeure reste la sécurité. Une sécurité réseau Azure inadéquate représente une menace directe pour la protection des données et des charges applicatives essentielles résidant au sein d'environnements Cloud.

En l'absence de protocoles de sécurité du réseau solides, le risque de violation de données, de cybermenaces et de failles de sécurité ne fait qu'augmenter, ce qui compromet l'intégrité, l'accessibilité et la confidentialité des ressources vitales. Souvent, les organisations n'ont pas les outils nécessaires pour mettre en œuvre des mesures de sécurité complètes et établir une stratégie bien définie, ce qui les expose à d'éventuelles attaques DDoS et aux menaces de logiciels malveillants.

50 %
plus de tentatives de cyberattaques des organisations par semaine[1]

62 %
des employeurs signalent que les équipes de cybersécurité sont en sous-effectif[3]

200 %
plus d'attaques DDoS au cours de l'année écoulée entre 2022 et 2023[2]

72 %
des entreprises déclarent que plus de 40 % de leurs données sur le Cloud sont classées comme sensibles[4]

Des services visant à créer un environnement réseau structuré et sécurisé

Avec Dell Technologies Implementation Services for Microsoft Azure Network Security et notre stratégie de défense multicouche axée sur la segmentation du réseau, le contrôle des accès et le chiffrement, les organisations peuvent améliorer la sécurité de leur réseau Cloud pour relever leurs défis d'implémentation. Nos meilleurs experts en sécurité travailleront avec votre organisation pour comprendre votre environnement réseau Azure actuel et le sécuriser de manière robuste et personnalisée, afin de protéger vos charges applicatives stratégiques dans le Cloud. Ainsi, vous aurez confiance en votre capacité à réduire les risques de propagation latérale, d'attaque DDoS, de ransomware et de violation de la sécurité.

- **Bénéficiez de services sur mesure adaptés aux besoins uniques de votre entreprise**
- **Tirez parti d'une stratégie de défense multicouche pour réduire les risques**
- **Confiez la gestion à des experts en sécurité**
- **Limitez le risque d'erreurs de configuration lors du déploiement**

Implementation Services for Microsoft Azure Network Security

Des services permettant de créer un environnement réseau structuré et sécurisé au sein d'Azure

- Atelier permettant d'identifier et d'examiner la région Azure en vue d'une segmentation
- Appliquer la segmentation du réseau pour isoler et organiser les charges applicatives spécifiques
- Déployer des pare-feu pour inspecter, contrôler et protéger le trafic Internet
- Améliorer la sécurité du trafic interne entre les utilisateurs et les applications grâce au chiffrement
- Développer le réseau avec des fonctions de sécurité améliorées alignées aux besoins métier

Plus de 35 ans de partenariat avec Microsoft

Nos solutions, nos services et notre expertise technique co-conçus vous fournissent un partenariat plus complet pour générer des résultats et accélérer la transformation numérique.

- ✓ Partenaire mondial Microsoft FastTrack
- ✓ Plus de 47 000 certifications Microsoft détenues par les techniciens Dell
- ✓ 7/7 compétences de solutions Microsoft
- ✓ Membre de l'Association de sécurité intelligente de Microsoft

Passez à la vitesse supérieure sur le chemin de la modernisation

La division Dell Technologies Services propose une gamme complète de services adaptés aux technologies Microsoft pour donner à vos équipes les moyens de travailler et vous aider à atteindre les résultats opérationnels ciblés.

Explorer les services de conseil

Contacter un expert Dell Technologies

Voir plus de ressources

Prendre part à la conversation avec #DellTechnologies

50 % plus par semaine, petites et moyennes entreprises : https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=4f9a64186b61
62 % signalent que les équipes de cybersécurité sont en sous-effectif : https://www.computerweekly.com/news/252515016/Hiring-and-retention-challenges-in-cyber-security-persist
https://cybermagazine.com/cyber-security/zayo-group-confirms-ddos-attacks-in-2023-are-up-200
https://www.backblaze.com/blog/the-2022-backup-survey-54-report-data-loss-with-only-10-backing-up-daily/Ransomware attacks have increased by 232% since 2019, https://www.supplychainquarterly.com/articles/6268-report-ransomware-attacks-on-networks-soared-in-2021#:~:text=The%20company's%202022%20Cyber%20Threat,files%2C%20databases%2C%20or%20applications.