

Proteja las cargas de trabajo de cloud frente a los ataques basados en la red

Implementation Services for Microsoft Azure Network Security

¿Cómo protege sus redes de cloud?

En el panorama digital moderno, las iniciativas de migración a Azure han aumentado significativamente, principalmente motivadas por sus capacidades de ampliación y adaptabilidad, y su rentabilidad. No obstante, acecha una preocupación crítica, la seguridad. Una seguridad inadecuada en la red de Azure representa una amenaza directa a la protección de los datos y las cargas de trabajo esenciales que residen en entornos de cloud.

Si carece de protocolos de seguridad sólidos, el riesgo de vulneraciones de datos, ciberamenazas y vulnerabilidades no hace más que crecer, hasta que, en última instancia, es capaz de poner en riesgo la integridad, accesibilidad y confidencialidad de recursos vitales. En muchas ocasiones, las organizaciones se percatan de que carecen de lo necesario para implementar medidas de seguridad completas y establecer una estrategia bien definida, lo que las deja expuestas a posibles ataques de denegación de servicio (DDoS) y amenazas de malware.

Servicios para crear un entorno de red estructurado y seguro

Gracias a Dell Technologies Implementation Services for Microsoft Azure Network Security, las organizaciones pueden mejorar la seguridad de la red de cloud a fin de abordar los desafíos de la implementación con nuestra estrategia de defensa multicapa centrada en la segmentación de la red, el control de acceso y el cifrado. Contamos con los mejores expertos en seguridad de su clase y colaboramos con su organización para comprender su actual entorno de red de Azure, así como implementar una seguridad de red sólida y personalizada capaz de proteger las cargas de trabajo críticas en la cloud. De este modo, puede confiar en su capacidad para reducir con éxito el riesgo de propagación lateral, ataques de DDoS, programas de secuestro y vulneraciones de la seguridad.

- ✓ **Obtenga servicios adaptados a sus necesidades empresariales únicas.**
- ✓ **Aproveche una estrategia de defensa multicapa para reducir riesgos.**
- ✓ **Deje la gestión en manos de expertos en seguridad.**
- ✓ **Mitigue el riesgo de sufrir errores de configuración durante la implementación.**

50 %

más intentos de ciberataque por semana contra organizaciones.¹

62 %

de los empleadores afirman que falta personal en los equipos de ciberseguridad.³

200 %

de aumento en los ataques DDoS el año pasado, de 2022 a 2023.²

72 %

de las empresas afirman que más del 40 % de los datos que almacenan en la cloud se clasificaría como "sensible".⁴

Implementation Services for Microsoft Azure Network Security

Servicios para crear un entorno de red estructurado y seguro en Azure

- Participe en un taller para identificar y revisar las regiones de Azure de cara a la segmentación.
- Aplique la segmentación de la red para aislar y organizar cargas de trabajo específicas.
- Implemente firewalls para inspeccionar, controlar y proteger el tráfico vinculado a Internet.
- Mejore la seguridad del tráfico interno entre usuarios y aplicaciones mediante cifrado.
- Amplíe la red con características de seguridad mejoradas adaptadas a los requisitos empresariales.

Más de 35 años colaborando con Microsoft

Nuestras soluciones codiseñadas, servicios y conocimientos técnicos le aportan una colaboración más completa, para que impulse los resultados y acelere la transformación digital.

- ✓ Socio FastTrack mundial de Microsoft
- ✓ Más de 47 000 certificaciones de Microsoft concedidas a técnicos de Dell
- ✓ 7 de 7 competencias de área de soluciones de Microsoft
- ✓ Miembro de la Microsoft Intelligent Security Association

Dé el siguiente paso en su camino hacia la modernización

Dell Technologies Services ofrece una amplia cartera de servicios para tecnologías de Microsoft, con el objetivo de capacitar a sus equipos y ayudarle a obtener resultados empresariales.



Explore los [servicios de asesoramiento](#).



[Póngase en contacto](#) con un experto de Dell Technologies



Consulte [más recursos](#).



Participe en la conversación con #DellTechnologies.

Aumento del 50 % a la semana en pequeñas y medianas empresas: <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022-a-fresh-look-at-some-very-alarming-stats/?sh=4f9a64186b61>

El 62 % afirman que falta personal en los equipos de ciberseguridad: <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/>, <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.>