DoSGuard là một dịch vụ được tích hợp trong cơ sở hạ tầng mạng của Azure SQL Database để giảm thiểu các cuộc tấn công từ chối dịch vụ (DoS). DoSGuard hoạt động bằng cách theo dõi và phản ứng đối với các hoạt động đáng ngờ hoặc không bình thường trên mạng, đặc biệt là các yêu cầu kết nối không hợp lệ hoặc thất bại.

Dưới đây là cách mà DoSGuard giảm tấn công mạng:

1. **Phát hiện và theo dõi**: DoSGuard liên tục theo dõi lưu lượng mạng đến cơ sở dữ liệu SQL Azure để phát hiện các hoạt động không bình thường hoặc đáng ngờ. Điều này bao gồm việc theo dõi các yêu cầu kết nối không hợp lệ, quá nhiều yêu cầu từ cùng một địa chỉ IP hoặc từ một số lượng lớn các địa chỉ IP khác nhau trong một khoảng thời gian ngắn.
2. **Phản ứng tự động**: Khi phát hiện các hoạt động đáng ngờ, DoSGuard sẽ tự động thực hiện các biện pháp phản ứng để giảm thiểu tác động của cuộc tấn công. Điều này có thể bao gồm việc chặn các yêu cầu từ địa chỉ IP cụ thể, tạm thời chặn toàn bộ một dải địa chỉ IP hoặc thậm chí chặn các yêu cầu từ một khu vực địa lý cụ thể.
3. **Bảo vệ khỏi quá tải**: Bằng cách ngăn chặn hoặc giảm thiểu lưu lượng mạng không mong muốn, DoSGuard giúp bảo vệ cơ sở dữ liệu khỏi tình trạng quá tải. Điều này giúp duy trì hiệu suất và sẵn sàng của dịch vụ cho người dùng cuối, ngay cả trong khi đang chịu tác động của một cuộc tấn công.

Tóm lại, DoSGuard là một công cụ quan trọng trong việc bảo vệ cơ sở dữ liệu SQL Azure khỏi các cuộc tấn công từ chối dịch vụ bằng cách phát hiện, theo dõi và tự động phản ứng đối với các hoạt động không mong muốn trên mạng.