DB Networks ADF-4200
– advanced database threat protection

DATABASE PROTECTION

The ADF-4200 uses complex behavioral analysis to immediately identify advanced SQL injection and database DoS attacks. A potentially critical database access vulnerability from Web applications is eliminated.

ADAPTIVE TECHNOLOGY

The DB Networks ADF-4200 capabilities far exceed traditional “black lists” and “white lists” database security products. Our patent pending behavioral analysis technology enables the ADF-4200 to quickly identify and protect against advanced database threats.

FEW FALSE POSITIVES

Using a multi-dimensional analysis of each SQL statement provides an accurate determination if the SQL is a threat: SQL Injection attacks are quickly identified, while false positives are very rare.

- Advanced database threats are real, they are growing, and their effect on an organization can be devastating.
- SQL injection is one of the most common attack mechanisms used against Web applications and is responsible for well over 90% of the records stolen.
- The DB Networks ADF-4200 is purpose built to detect the newest generation of weaponized SQL injection as well as database DoS attacks.

DB Networks ADF-4200 detects even the stealthiest of advanced SQL injection and database DoS attacks. This is accomplished through our highly accurate SQL behavioral analysis technology. The ADF-4200 immediately identifies any injection of hostile SQL commands on the network.

Once installed, the ADF-4200 rapidly learns the specific environment in which it's operating. From that learning it builds a behavioral model. Each SQL statement is then subjected to a thorough lexical analysis and SQL semantic comparison analysis. The result is that rogue SQL statements are immediately identified and a predefined alarm procedure is invoked.

The ADF-4200 is easily implemented and can be deployed without changes to either existing applications or databases. Flexible deployment options include passive monitoring and in-line proxy.

DB NETWORKS

11440 West Bernardo Ct :: Suite 300 :: San Diego, CA 92127
www.dbnetworks.com

Requirements and Specifications

BEYOND ACL

DB Networks ADF-4200 is able to identify advanced SQL injection and database DoS attacks that can bypass Web Application Firewalls (WAF).

LEGACY SYSTEM SUPPORT

Mature applications, which have been repeatedly patched over the years, are particularly vulnerable to SQL Injection attacks. DB Networks ADF-4200 is able to seamlessly and effectively protect even these legacy applications from advanced SQL Injection exploitation.

- Oracle server release 8i (8.1.7) or later

  OR
- MS SQL version 2000 or later
- Bi-directional span port or passive tap to connect to 10/100/1000 Mbit/sec capture ports

- System Specifications
  - Platform
    - 2U x 28 inch rack mount form factor
    - Dual redundant power supplies - 750W max (280W nominal consumption)
  - Security
    - Encrypted data
    - Operator authentication
    - Role based permissions to limit access to sensitive data
  - Connectivity
    - Four x 10/100/1000 Mbit/sec Ethernet capture ports
    - One x 10/100/1000 Mbit/sec Ethernet admin port
    - One x 10/100/1000 Mbit/sec Ethernet customer service
  - Capacity
    - 320 GB High performance SSD
    - 2 TB Achival storage

Operating at the database tier, directly in front of the database server, the ADF-4200 is a critical countermeasure against advanced database attacks. DB Networks ADF-4200 is unique in that it's able to quickly adjust to changing advanced SQL Injection and database DoS threats.

We recommend you contact us for additional information and to arrange an online demonstration of the DB Networks ADF-4200. This will help you better understand the product and how it would seamlessly integrate into your environment to immediately protect your mission critical applications from advanced database attacks.

DB NETWORKS

11440 West Bernardo Ct :: Suite 300 :: San Diego, CA 92127
www.dbnetworks.com