DB Networks Adaptive Database Firewall – next generation SQL Injection protection

**DATABASE PROTECTION**
DB Networks Adaptive Database Firewall detects and stops SQL injection attacks, eliminating a critical security vulnerability of your Web applications.

**ADAPTIVE TECHNOLOGY**
While DB Networks Adaptive Database Firewall supports "black lists" and advanced "white lists", it goes well beyond with our exclusive SQL Threat Assessment Technology. This technology enables the DB Networks Adaptive Firewall to quickly adjust to, and protect against, rapidly changing SQL injection attacks.

**FEW FALSE POSITIVES**
Our SQL Threat Assessment Technology initiates a multi-pronged analysis against each SQL statement to accurately evaluate and determine if it's an attack or not. As a result, actual SQL Injection attacks are quickly identified while false positives are kept to a minimum.

- The SQL injection threat is real, it's growing, and its 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 90% of the records stolen.
- A single SQL injection attack can result in the compromise or destruction of an entire database of confidential records.
- The DB Networks Adaptive Database Firewall is able to thwart even the most complex SQL injection attacks.

DB Networks Adaptive Database Firewall is engineered to detect and stop even the stealthiest of SQL injection attacks. This is accomplished through three integrated countermeasures. These include "black lists", advanced "white lists", and also our exclusive SQL Threat Assessment Technology. SQL Threat Assessment Technology performs a multi-pronged analysis on each SQL statement in real-time to accurately determine if the SQL statement is an attack on the database or not. DB Networks SQL Threat Assessment Technology offers you unprecedented accuracy in identifying and stopping SQL injection attacks all while making false positives a thing of the past.

DB Networks Adaptive Database Firewall is completely nonintrusive and is easily installed in your new or legacy installations. Once installed, the firewall enters a "learning mode". During this short period, the firewall creates a unique model of proper SQL behavior for your particular environment. SQL statements which subsequently deviate from the model are identified, evaluated, and assigned a threat severity for further action.
Requirements and Specifications

- Oracle server release 8i (8.1.7) or later
- Bi-directional mirrored port or passive tap to connect to 10/100/1000 Mbit/sec capture ports

System Specifications

Platform
- 2U x 23 inch rack mount form factor
- Dual redundant power supplies - 300W

Security
- Encrypted data
- Operator authentication
- Role based permissions to limit access to sensitive data
- Support for encrypted database interfaces

Connectivity
- Four x 10/100/1000 Mbit/sec Ethernet capture ports
- Two x 10/100/1000 Mbit/sec Ethernet administration ports
- One x 10/100/1000 Mbit/sec Ethernet customer service port to limit access to sensitive data
- Support for encrypted database interfaces

Capacity
- 2 TB of RAID10 storage for captured workloads

Database firewalls are a critical countermeasure against SQL Injection attacks. DB Networks Adaptive Database Firewall is unique in that it can quickly adjust to changing SQL Injection techniques. It’s often suggested that a solution would be to rewrite all of your Web applications, based on improved coding practices. In reality, that’s simply not practical. It would be very costly, time consuming, and in the end may not be completely effective as SQL Injection attacks evolve.

We recommend you contact us for additional information and to arrange an online demonstration of the DB Networks Adaptive Database Firewall. This will help you better understand the product as well as how it would seamlessly integrate into your environment to immediately protect your mission critical applications from SQL Injection attacks.