

DB Networks® DBN-6300

Asset Discovery and Tracking Features

Nonintrusive Database Discovery | User and Application Discovery

DATABASE INSIGHTS

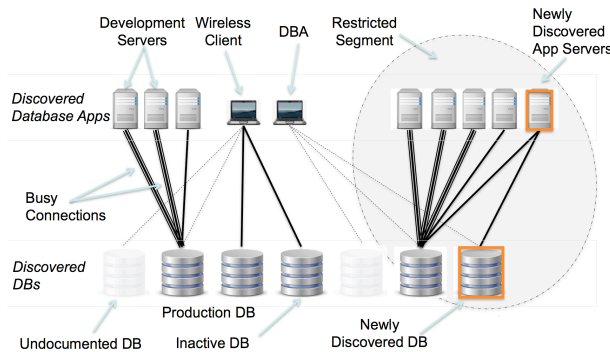
The DBN-6300 is a highly intelligent security appliance that not only immediately identifies database attacks but also provides new insights into your database infrastructure activities through deep protocol analysis.

DATABASE DISCOVERY

The DBN-6300 is able to non-intrusively and automatically discover databases on the network, including undocumented or non-compliant databases that could potentially pose a security threat.

APPLICATION MAPPING

DB Networks non-intrusively maps the interactions of users and applications to their connected databases. Activities from Advanced Persistent Threats (APTs) create new or altered user/application interactions. The DBN-6300 application-interaction mapping is able to immediately identify APTs.



- Nonintrusively discovers all databases (including the undocumented ones)
- Provides deep visibility into your database infrastructure including the interactions between applications and their connected databases
- Identifies core network policy violations
- Purpose-built to detect advanced database attacks through machine learning and behavioral analysis
- Compliant with requirements in NIST 800-53, PCI DSS, COBIT DS5.5, HIPAA, & GLBA

DB Networks' DBN-6300 "shines a light" on your database infrastructure. Through deep protocol analysis the DBN-6300 analyzes your database traffic to provide you with new insights and situational awareness of your database infrastructure.

Some of the unique insights the DBN-6300 offers include:

- Database discovery
- Application and database interaction details
- Monitoring core network policies
- Immediate identification of database attacks

These capabilities are achieved through deep protocol

extraction and the mapping of interactions between database clients/applications and the databases to which they are connected. Through this level of analysis you can:

- Reconcile your CMDB data
- Proactively manage your database licenses
- Monitor database accesses to ensure compliance with policy
- Understand what individual users are doing inside your critical database infrastructure

This critical information is provided immediately upon deployment of the DBN-6300 and updated continuously as changes in the network occur to keep you up to date.



POLICY MONITORING

Application to database interactions identify policy violations such as restricted databases being exposed to unrestricted network segments.

NO PLACE TO HIDE

Since the DBN-6300 Discovery capability decodes traffic as it transits the network it does not rely on IP address or port numbers to identify a database. This ensures that databases appearing on atypical ports are not missed. In addition, you'll have a clear picture of who is using each database so that ownership and responsibility can be easily established.

CONTINUOUS MONITORING

Unlike traditional solutions that scan the network periodically in an attempt to find databases, the DBN-6300 Discovery capability continuously monitors your network for changes. Any changes are immediately reported via syslog to ensure that there is always an up-to-date view of the network topology. This includes changes in the databases as well as the users and applications associated with those databases.

How it works

Network traffic decoding engine

The DBN-6300 is a network appliance (or a virtual machine) that listens to network traffic via a tap or SPAN port. Through a highly efficient network traffic-decoding engine it dissects all traffic and feeds the SQL conversations to the system. This patented traffic analysis technology is uniquely different from traditional full packet capture engines. The DBN-6300 analysis engine automatically performs filtering, categorization, statement assembly, and other functions required to separate, reconstruct and analyze the database traffic without any manual configuration. The decoding does not rely on TCP port numbers and will therefore also detect databases using atypical ports.

Relational Database Interactions Modeling

Relational modeling records all relationships between users, machines, applications, and databases. The DBN-6300 continuously discovers databases and maps the interactions of each database client. This process allows the DBN-6300 to build, and continuously update, an interactive topological map of the database environment monitored on the network. This visual map forms a foundation for security operations to visualize and analyze observed database interactions in multiple dimensions such as: from what network the traffic originates and in what network segment it terminates, to how many database services each client connects to; how many clients interact with each database service, etc.

Requirements and Specifications

Supported DBMS platforms:

- Oracle server release 8i (8.1.7) or later
- Microsoft SQL Server version 7 or later
- SAP Sybase ASE version 12.5 or later

10GigE or 10/100/1000 Mbit/sec capture ports (physical or virtual) connect to network tap or SPAN interface

Physical appliance

Platform

- 2U 19 inch wide x 28 inch deep rack mount form factor
- Dual redundant power supplies - 750W max (280W nominal consumption)

Connectivity

- Two 10GigE capture ports
- Four Gigabit Ethernet capture ports
- One Ethernet admin port

Virtual machine specifications

DBN-6300v is delivered as an OVF that comes in two different sizes / capacities:

	B (Base model)	E (Enterprise)
RAM (GB)	4	12
CPU cores	Up to 2	Up to 6
Disk space (GB)	50	200

Supported VM infrastructure: VMware ESXi 5.1, 5.5

Supported Networking environments: VMware vSwitch, dvSwitch as well as any SDN platform that is configured to allow network tapping.

