DBN-6300 Technical Brief
# Table of Contents

Overview .................................................................................................................. 3

Key Features and Benefits of the DBN-6300 .............................................................. 3

Key Database Security – The Risks ......................................................................... 4
- Insider Threat ...................................................................................................... 4
- Advanced Persistent Threat ............................................................................... 5
- Application Breaches ......................................................................................... 5
- Availability Loss (Downtime) ............................................................................. 6

The Challenges ....................................................................................................... 6

Intelligent Continuous Monitoring ....................................................................... 8
- Database Assets Discovery and Usage ............................................................. 9
- Audit and Compliance Monitoring ................................................................ 10
- Detection of Application Intrusions ............................................................... 10
- Runtime Vulnerability Detection .................................................................... 11
- Penetration Testing .......................................................................................... 12

How it Works ........................................................................................................ 8
- Network Traffic Decoding Engine ................................................................. 13
- Relational Database Interactions Modeling .................................................. 13
- Machine Learning Behavioral Profile Engine .............................................. 14
- Alerting and Reporting Engine ...................................................................... 14
- Behavioral and Topological Visualization & Analysis .................................. 15

Conclusion .......................................................................................................... 16

Learn More ......................................................................................................... 16
Overview
This technical brief introduces the security challenges associated with database systems and the benefits DB Networks DBN-6300 offers its customers to address these challenges.

Key Features and Benefits of the DBN-6300
The DBN-6300 is a new generation of Intelligent Continuous Monitoring system offering the following features:

Non-Intrusive Data Collection and Analysis
- Non-intrusive database service discovery using a passive network tap or span port in real time.
- Supports batch processing using PCAP files from network segments of interest.

Comprehensive Database Discovery and Asset Management
- Database service discovery that is not dependent on transport layer (Layer 4) TCP/UDP port numbers.
- Identifies databases at the services level not just which servers are running database applications.
- Identifies active undocumented and potentially rogue databases.

Application to Database Interactions Analysis
- Network traffic is analyzed at the application layer (Layer 7), providing rich context of which clients and applications are communicating with which databases, how frequently, and what is being communicated.
- Intelligent, non-intrusive, continuous monitoring of the nature, frequency, and content of the network traffic between users, applications, and databases.
- Visualization tools that efficiently analyze monitored interactions and provide the ability to drill-down into the nature of each interaction, including client and server IP address, amount and frequency of SQL traffic, and SQL statements exchanged.
- Real-time alerting of abnormal changes in client-database interactions.

Behavioral Analysis Based Database Security
- Machine learning behavioral engine requires no signature files or rules customization.
Multi-modal behavioral analysis includes textual, lexical, syntactic, and semantic analysis of each SQL statement against normal client and application behavior.

High accuracy violation alerting includes detail on threats, vulnerabilities and exploits by database clients with the corresponding details on the dataset under attack.

Real-time verification of effective reconnaissance allows SecOps to understand true exposure and spend ZERO wasted time on false positive alerts related to already mitigated or non-vulnerable targets.

SOC measures on average 15-second alert vetting and escalation process for real world clients.

**Policy Monitoring**

- Ability to define activity views focusing on regulatory or corporate policy compliance and violations.
- Drill down capabilities to further explore the nature of each security or regulatory policy violation, such as detection of access to monitored databases from new or unauthorized clients from network segments that are crossing trust boundaries.

**Key Database Security – The Risks**

When determining the risks associated with database security and compliance the focus is on the data itself. In this document we will focus on the most significant risk related to data, the risk of data loss.

An organization's most valuable data resides within database systems typically located in the corporate datacenter. Although often guarded behind several layers of security, the risk of losing data is significant and growing. We first need to map the risks and use cases contributing to data loss to later define the required solutions to the problem. Typically there are four primary categories of risks:

- Insider threat
- Advanced persistent threat (APT)
- Application breaches
- Availability loss (downtime)

**Insider Threat**

Insider threat is considered the top priority for many IT security organizations today. It pertains to the unauthorized use of internal user credentials to perform unauthorized or high-risk activities. It could be internal actors (employees,
contractors, etc.) violating corporate policies maliciously or unintentionally or malicious external agents who managed to get a hold of a legitimate users’ credentials, infiltrate into the corporate core network, and then access sensitive data. One of the most common targets for those risky or malicious activities is the sensitive data repositories within relational databases, where the most current and valuable information is stored and processed.

Cyber attacks involving insider activities are on the increase and are widely considered one of the top concerns for corporate IT security. Insider threats are therefore typically classified as top risk threats.

**Advanced Persistent Threat**

Advanced persistent threat occurs when malicious software is inadvertently loaded onto a system that has legitimate access to resources inside the perimeter of the network. Because this software has already made it inside, perimeter defenses can no longer offer any protection for your critical assets. The malicious software then attempts to access resources, including databases, across the network using a variety of techniques. Once it gains access it begins leaking the information it gets out of the organization, typically over an extended period of time.

**Application Breaches**

Application breaches are considered one of the most prevalent and impactful classes of risks. An attacker focuses in on finding vulnerabilities at the application layer, typically situated in front of many database systems to enable controlled access to data. Application servers are frequently granted escalated privileges in order to access data giving the application control to grant specific users privileges. Attackers target applications given their escalated privilege to access sensitive data. The attack itself is carried out by interacting with the application in a manner that allows the attacker to leverage the escalated privileges of the application to carry out the attack.

The specific attack vector varies greatly from exploit to exploit based on the application vulnerability and often include obfuscation techniques aimed at evading the perimeter defenses. Extensive reconnaissance is typically performed on the targeted organization in order to identify vulnerabilities that can be exploited undetected. One of the more popular and dangerous vulnerabilities exploited is carried out by manipulating the application to generate a query for sensitive data that would normally not be allowed. This is known as a SQL injection attack.

Since the vulnerability being exploited by the attacker is generally unknown to the target organization, most SQL injection attacks go undetected for weeks or
months. Such application breaches are typically classified as high risk due to an attacker’s ability to exfiltrate large amounts of sensitive data undetected.

**Availability Loss (Downtime)**

Availability loss refers to loss of the availability of data due to downtime originating from attacks on the database infrastructure. This can include destruction or alteration of data through an attack on the database that hosts the data. Another example is a denial of service attack, which could include SQL commands designed to consume excessive database resources thereby starving legitimate consumers and adversely affecting application performance. A malicious user abusing an application-level weakness typically generates these abnormal SQL commands. While the risk is not related directly to data loss, it can be significant due to the potential significant business disruption caused by a slowdown or an outage.

**The Challenges**

There are four primary challenges to address the risks identified above:

1. **Data assets discovery**: Identifying where sensitive data is located and which applications and users are accessing it – One of the first steps in protecting sensitive data is to know where it is located. In order to locate sensitive data, a discovery process is initiated to identify the location of all the active databases in an organization as well as the users and applications that interact with it and the nature of those interactions. Knowing where sensitive data is located is a common requirement of most security compliance mandates. With accurate information of the location of sensitive data, data security operations can ensure that all appropriate security practices (patches, credential and usage policies, etc.) are being applied. Analyzing interactions enables creation of a baseline of normal access to sensitive data and provides the information necessary to identify potentially risky anomalies. Ironically, this is also the first step an attacker will carry out during the reconnaissance phase of an APT in order to gain sufficient intelligence about the targeted environment.

Unfortunately, most companies lack sufficient tools to accurately and continuously keep track of the location of sensitive data repositories and how they’re being used. The process of gathering the data typically involves periodic, expensive, time consuming manual procedures, resulting in inaccurate not up-to-date information for where sensitive data resides. The information that is ultimately pulled together represents data that was collected at various points in time and rarely reflects the actual behavior of users and applications access to sensitive data. Coupled with the fact that
most customer environments are dynamic and changing all the time, makes it almost impossible to maintain a current and accurate view of the location of sensitive data and who is accessing it.

2. **Behavioral modeling**: A current understanding of normal and authorized access to sensitive data — Once the sensitive data is located and which users and applications are accessing it, the next step is to understand what normal behavior looks like. This has to do with the nature of each client and applications access to sensitive data. Context needs to be understood for each authorized interaction with sensitive data over time. Information such as:

- How frequently does each client connect to the database?
- From which clients and networks each database user connects to the database?
- What type of database client software is being used and is it changing?
- What is the nature of the interaction, specifically, what SQL queries are being requested and how frequently?
- Are the SQL queries the same or unique and how are they related to one another?
- How frequently are applications legitimately modified?

Gathering and effectively analyzing this type of context around the interactions for each client, application, and database over time builds a baseline for normal, authorized access to sensitive data, which can then be used to identify potentially harmful deviations.

3. **Identifying undesired behavioral anomalies**: Without knowing where sensitive data is located or establishing a baseline of related normal use of the data, it can become almost impossible to identify some of the more sophisticated new behavioral patterns that were crafted to go undetected by rules based defense systems. When executed by an attacker, such behaviors are often designed with the knowledge of the existing systems and enforced policies in mind to allow execution under the corporate radar. Some examples of such behaviors include:

- Internal malicious agent, running on a privileged user’s machine executing commands that are within the scope of the user privileges and normal operations at a low enough rate to avoid any suspicion.
- Injected application variation that looks similar enough to the existing application functionality that produces harmful new SQL.
A new database or client host serving to collect pieces of data from multiple sources located on the same network as the target data sources.

In fact, the real challenge is that the infinite variability of such attacks renders existing security systems that rely on a relatively static policy and pre-set rules ineffective. Without effective monitoring of sensitive data for behavioral anomalies, cyber attacks run undetected for ridiculously extended periods of time. It is only through detecting behavioral changes on top of an ever-morphing environment that an effective protection against potential cyber attacks becomes possible.

4. **Effective detection of application intrusion attempts**: most IT organizations today suffer from a severely insufficient ability to detect application-level intrusions. The ever-growing complexity of application interfaces and logic provides a fertile ground for hackers to launch more highly evasive attacks carried out undetected by perimeter security. Once past the application layer detection capacity drops even further because the attack is introduced by a trusted entity, the application servers. Using this method attackers are able break in the front gate to the corporate network and launch their attacks undetected.

**Intelligent Continuous Monitoring**

DB Networks has introduced a new approach to database and application security with the DBN-6300. It utilizes intelligent continuous monitoring and deep protocol analysis of every SQL conversation on the network. It records each application and client connection and uses structural, lexical and syntactical analysis of each SQL access to the database to build behavioral profiles for each connecting client. These behavioral profiles are used as a baseline to analyze each new SQL conversation, thereby allowing detection of any significant and potentially harmful deviation from the baseline. The DBN-6300 is designed to address the challenges listed above by offering effective visibility into core network database activities, insider threats detection and mitigation, and gaps in application security practices today.

A matrix of how the DBN-6300 Intelligent Continuous Monitoring solution aligns with current security best practice is explained in the figure below.
**Intelligent Continuous Monitoring**

**Database Assets Discovery and Usage**

An effective monitoring and analysis process of core database activity offers multiple essential values. Primarily it offers an always up-to-date inventory of databases and their consumers (database clients – users or applications). This may sound trivial, yet it appears to be a common gap in today’s corporate IT. Lacking this visibility on a continuous basis results in an inability to effectively protect corporate data assets as well as meet a variety of tightening regulatory compliance requirements that are shifting emphasis towards continuous compliance.

From an ROI perspective, an ongoing effective discovery process significantly contributes to inventory management processes and data center consolidation initiatives by providing information that aids in enabling decommissioning and consolidation of under-utilized database services. It also facilitates capacity management of network infrastructure and database services by detecting over-subscribed networks, database services or ultra-chatty application consumers.

Through non-intrusive continuous monitoring of traffic, the DBN-6300 collects and analyzes every database-related interaction. In doing so, it provides essential intelligence about the activity patterns on multiple dimensions:

- Detect and inform about every new database service, database client, and database interaction it discovers on the network.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Primary Benefit</th>
<th>Security Assessment</th>
<th>Insider Threat</th>
<th>APT Detection</th>
<th>SQL Injection Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Discovery</td>
<td>Know where your databases are to determine if adequate safeguards exist</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Applications / Clients Discovery</td>
<td>Provides insights into which clients (Apps, Tools, Users) are accessing each database. Highlights security risks associated with the characteristics of these users and ensures proper segmentation is occurring.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications / Clients to Database Interactions</td>
<td>Gain insights into the interaction of applications / clients &amp; database. Identify usage patterns that are atypical. Are DBA’s accessing more frequently than they should, are desktops suddenly exhibiting application like behavior?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Behavioral Analysis</td>
<td>Immediately identify applications expressing vulnerability behaviors or behaviors that they’ve been compromised</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Map the relationship between discovered database services and the corresponding application clients, indicating which application client(s) are talking to which database service(s).

• Provides insight about connectivity behavioral patterns, including service up/down periods, traffic volume statistics, complexity of interaction and quality (e.g. indicating which are the most chatty database services), application clients, physical/virtual hosts, as well as inactive/intermittent database services.

• Enables easy identification of the web-facing database clients, DBA accounts, and web-facing database services among the potentially large number of total database services and clients.

• Identification of retired databases so they can be decommissioned and the data archived securely.

Audit and Compliance Monitoring
Using deep analysis of every SQL conversation, the DBN-6300 offers a unique insight into the nature of each interaction it captures on the network. The insight provided is helpful for the audit activities around maintaining compliance with security policies.

An example is the use of administrative credentials. Earlier security policies allowed for the usage of shared credentials for deployment and management of applications. Current policy disallows this practice and requires DBA users to have unique credentials tied to their corporate ID. This policy is easier mandated than enforced. The DBN-6300 facilitates an audit of the usage of these credentials on network assets. Additionally, the DBN-6300 can alert SecOps when a future violation occurs in real-time.

Another example is in monitoring and enforcing internal network segmentation. Most organizations establish policies inside the core network, such as – no data connection should be established between production systems and non-production (e.g. development) systems. Another example is data segmentation and governance driven by industry regulations such as PCI DSS, PII, PHI, or SOX. In most cases the enforcement and maintenance of those rules is too demanding, and therefore goes unenforced other than educating personnel on corporate code of conduct policy. The DBN-6300 implemented as a compliance control offers intelligent continuous monitoring to identify such policy violations instantly and alert SecOps as soon as they occur.

Detection of Application Intrusions
The DBN-6300 is highly effective even against zero-day threats. Leveraging the unique multi-modal behavioral approach that does not rely on simple pattern
matching (signatures), the profile created by the DBN-6300 of normal application behavior enables effective and accurate detection of each application intrusion attempt. Internal experts evaluate each unique SQL statement generated by the application against the baseline to determine whether it is a legitimate application variant or a potential threat, resulting in outstanding accuracy in detecting actual attacks (extremely low false positive rates), threats, or weaknesses.

Moreover, as a unique value, the system is designed to help detect Advanced Persistent Threats (APTs). As application intrusions tend to continue over an extended period of time, the DBN-6300 builds an overall logical map where a sequence of malicious behavior is visualized as an APT in progress which, in turn, can be used to mitigate a threat in short order.

**Comprehensive Visibility & Control**

**Runtime Vulnerability Detection**

Using the behavioral profile built for every application and database service, the DBN-6300 can identify anomalies that may be a result of:

- Legitimate application code changes. Those are typically added to the DBN-6300 baseline behavioral profile.
- Poorly-designed applications exposing a vulnerability that requires a code-fix. Such a vulnerability may be discovered as part of a normal
operation (staging or production) or during a penetration-testing process, discussed below.

• Penetration testing process where one of the test cases (a potential attack) penetrates the application and reaches the database layer, indicating application design flaws that needs to be addressed.

• An attack in progress. A malicious activity is discovered between the application server and the database requiring immediate preventative action. This case is reviewed as a separate, primary use case as discussed below.

Penetration Testing

With its ability to detect runtime vulnerabilities, the DBN-6300 can be used as an instrument to improve the effectiveness of penetration testing.

The penetration testing process simulates an external hacking attempt involving launching attacks against the application web front-end. The penetration tester evaluates an application as vulnerable or immune based on the response from the application. Unfortunately this approach falls short when a hacking attempt successfully reaches the database layer, particularly if no response is sent back to the tester. This may occur for a variety of reasons. If no response is seen, the pen tester can gather no awareness of an actual vulnerability his test may have otherwise revealed.

By analyzing the traffic between the application server and the database, the DBN-6300 is able to detect every “successful” intrusion attack (an attack that manages to reach the database layer) regardless of the feedback the application sends back to the tester. Moreover, it may point to discovered application vulnerabilities that were not part of the penetration testing agenda. Lastly, it provides useful information including the base SQL statement that was compromised to pinpoint the origin of the vulnerability inside the application code to facilitate the remediation process.

Using the DBN-6300 in conjunction with a penetration test provides immediate feedback when SQL injection attacks eventually make it through the application and reach the database tier on their first successful attempt. The penetration tester can submit the detailed information provided by the DBN-6300 with the vulnerability report to assist in remediation. The DBN-6300 detects every successful SQL injection attempt thereby significantly reducing the amount of time required by the pen-tester to vet each application’s vulnerability, resulting in lower total costs for the process.
How it Works

The following figure depicts the DBN-6300 being deployed on a network for non-intrusive monitoring of the access to sensitive data.

Non-intrusive Database Security

Network Traffic Decoding Engine

The DBN-6300 listens for network traffic via a network tap or span port through a highly efficient network traffic-decoding engine to dissect all network traffic and feed SQL conversations to the appliance. This traffic analysis technology is patent-pending and uniquely different from traditional full packet capture engines, in that the DBN-6300 analysis engine automatically performs the filtering, categorization, statement assembly, and other functions required to separate out, reconstruct and analyze the database traffic without any manual configuration or policy creation. The decoding does not rely on TCP port numbers and will therefore detect databases using custom ports.

Relational Database Interactions Modeling

Relational modeling records the legitimate relationships between users, machines, applications, and databases. This modeling is then used to analyze database activities and surface anomalous behaviors that are considered risky or a violation of corporate policies.

The DBN-6300 continuously discovers databases and maps the interactions of each database client. This process allows the DBN-6300 to build and continuously

DBN-6300 Technical Brief Copyright © DB Networks® 2017 www.dbnetworks.com
update an intelligent and interactive topological map of the database environment monitored on the network. This topological map is a starting point for security operations to perform an analysis of all the 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, what bandwidth each interaction uses over time and to what extent each interaction evolves. Such a multi-dimensional analysis enables the user to quickly visualize outlying data patterns and then focus in on and drill down into exceptional network behavioral patterns, highlight interactions not allowed by corporate policy, risky boundary crossing between networks, and suspicious activities based on capacity and quality.

**Machine Learning Behavioral Profile Engine**

The DBN-6300 behavioral analysis engine analyzes every SQL statement seen on the wire. It does so by using multiple views, including among others lexical, semantic, and syntactical algorithms. Each database client that is interacting with a monitored database is profiled to the point where the appliance develops a baseline behavioral profile of the user and applications normal usage. This profile is composed of every structurally unique SQL query observed by the DBN-6300. Every new query is evaluated by comparing it to the existing profile. Any deviation from the learned set is then further analyzed. The magnitude and the nature of the difference allow the DBN-6300 to determine the risk level of each deviant behavior. The algorithms utilized are intelligent enough that the DBN-6300 can differentiate between normal, legitimate user or application variation versus malicious behavior and intent.

Unlike most other rules based technology, the DBN-6300 does not need constant updates for every application change. The DBN-6300 behavioral analysis engine understands normal application variation vs. malicious behavior, allowing it to continuously learn and add to the profile new legitimate behavioral elements. Most new applications can be learned in under a week. The DBN-6300 includes specific tools that enable vetting new applications and discovery of possible risks before any incremental learning is committed to the learned set.

**Alerting and Reporting Engine**

DBN-6300 reporting includes flexible out of the box reports to display database activity, client activity, and application to database mapping, new service discovery, inactivity and availability, behavioral profiles and more. The lexical analysis displays SQL statement grouping with visualization of statement relations for fast review of application behavior in a highly intuitive presentation useful for vetting of new applications. This process speeds up the on boarding of
new applications orders of magnitude faster than any other method. The DBN-6300’s alerting functions integrate with any SIEM and detail threats as they relate to true vulnerabilities. Alerts can be written to SYSLOG or be submitted to the SIEM using the Common Event Format (CEF). Alerts include threat data, the exploit functions, and the database under attack.

**Behavioral and Topological Visualization & Analysis**

Advanced visualization tools provide dynamic topology mapping of assets interacting with the database tier. Drillable views provide context from high-level views of global communications with indicators of anomalies, policy violations, and security risks and breaches, down to the nature and SQL content of a single interaction of interest.

The following figure depicts the database client to database interaction mapping.

![Visualization Diagram](image)

**Visualization Tools Assist with Identifying Policy Issues**

**Conclusion**

The DBN-6300 introduces an innovative approach to database security through intelligent continuous monitoring. It provides a practical solution to many of the most significant security challenges associated with application and database security today. Behavioral analysis of each database interaction introduces a major leap forward in the level of visibility and awareness of core network activity, essential for advanced cyber threat mitigation as well as meeting regulatory requirements. Behavioral profiling and machine learning are key technologies to identify behavioral anomalies and analyze their risk level. The
operational benefits in turn provide significant risk mitigation against cyber threats.

Learn More
To find out more about how the DBN-6300 provides actionable insights into the attack surface of your core network and can improve your overall database infrastructure security posture through Intelligent Continuous Monitoring, contact us at +1-800-598-0450 or email info@dbnetworks.com.

DB Networks®
15015 Avenue of Science Suite 150
San Diego, CA 92128-3434
Tel: +1-800-598-0450
www.dbnetworks.com
Copyright © 2017 DB Networks, Inc. All rights reserved.

*DB Networks is a registered trademark of DB Networks, Inc.*
*All other brand or product names are trademarks or registered trademarks of their respective holders.*