KEY BENEFITS
DBC Security enables security professionals to:

• Stop the loss of business-critical structured data before it happens
• Predictively identify behavior indicative of malicious intent
• Focus resources on threat analysis, not activity audit logs
• Continuously and non-intrusively monitor all structured data behavior

PREDICTIVE MACHINE LEARNING
DBC Security uses machine learning to:

• Automatically analyze the intent of each database query
• Pinpoint deviations from normal behavior that indicate compromised credentials and suspicious activity
• Provide the earliest possible warning – ahead of data loss
• Minimize security analyst work with intelligent anomaly clustering

CONTINUOUS MONITORING
As opposed to scanning and agent based technologies, DBC Security operates in real-time. Modeling and alerting are adaptive to change and always up to date with your structured data environment.

Threats against business-critical structured data present a unique combination of challenges for security professionals:

• The tell tale signs of attack may be removed from the original point of compromise
• The technology involved often spans separate domains of expertise – networking and databases
• The source, often an insider or posing as one, is a trusted member within the environment

Such threats pose a substantial business risk for loss of high-value and sensitive data. DBC Insider Threat uses predictive analytics to reduce your business risk of loss of high-value and sensitive data.

Major breaches that result in data loss are invariably preceded by days, and often weeks, of reconnaissance and other nefarious behavior. Rather than focusing on a narrow time window when the data was exfiltrated from the organization, DBC Security predictively identifies the behavior indicative of malicious intent. By proactively alerting you to such threats, DBC Security enables you to properly address data loss threat before it happens.

By spanning both the network and database domains, DBC Security shows threats in context.
INTELLIGENT BEHAVIORAL ANALYSIS

DBC Security uses deep SQL protocol decoding and semantic analysis to understand the structured data conversation in context:

- Which database was accessed?
- Which table was accessed?
- What kind of access was it (read, write, grant, etc.)
- Which client was used?
- When did it happen?
- What queries were used?

NON-INTRUSIVE OPERATION

DBC Security operates on a copy of network traffic. The solution is not inline, so there are no performance impacts on your structured data environment. In addition, it’s discovery capabilities require no scanning or configuration setup to locate and monitor structured data assets.

FLEXIBLE EXTENSIBLE POLICY

DBC Security includes an optional policy layer. This layer enables security professionals to build up a behaviorally-driven set of policies for alerting, or encode existing network and database policies for continuous monitoring.

Scanning based approaches are inherently out of date, limited to a subset of your environment, and have no visibility to data in motion. In contrast, DBC Security uses patented layer 7 extraction and deep SQL protocol decoding to identify, parse, and understand each database conversation in full detail. This occurs in real time ensuring DBC Security events are timely, high quality, and detailed for adjudication. You will see which client maliciously accessed which tables on a database, and exactly how they did it.

Underpinning DBC Security’s approach are a collection of predictive machine learning technologies. Since structured data threats cannot be identified based on their identity alone, DBC Security uses machine learning driven behavioral modeling to recognize anomalous behavior involving structured data. Related anomalies are grouped together using intelligent clustering to form easily adjudicated incidents. Incidents group behaviors such as abuse of credentials or distributed attacks on specific business-critical assets.

DBC Security operates off of a network SPAN or TAP. Therefore, it’s not inline and operates completely non-intrusively. Agent based solutions inherently limit the scope of what they monitor. When new structured data assets are accessed, the data they store, who has access, when and how is completely untracked until an agent is installed. In contrast, DBC Insider Threat is agnostic to the location of structured data assets in the environment, automatically monitoring and modeling the behavior around each and every one.

For additional information or to arrange for an online demonstration contact us at info@dbcybertech.com.

Requirements and Specifications

Supported Database Management Systems

- Oracle server release 8i (8.1.7) or later
- Microsoft SQL Server version 7 or later
- SAP Sybase ASE version 12.5 or later
- IBM Db2 Mainframe (DSN)
- IBM Db2 LUW (SQL)