Databases often contain sensitive and confidential information and are attractive targets for cyber criminals. They also need to meet stringent compliance, regulatory and audit requirements. Conducting regular database health checks ensures that their security meets their standards. They also help identify gaps and how to remediate them.

The Database Risk Assessment (DRA) program is a key component of the Trustwave Database Security Process. The goal of the DRA is to identify risk exposure and compliance posture on the databases, prioritize them and understand how a continuous process would improve the organization’s database security & compliance program effectiveness. This program is ideal for organizations in the following situations:

- Preparing for an audit and need expertise to assess their current database security program
- Need to conduct database inventory as they don’t know where all their databases are located
- Need external verification of their database security program
- Lack of in-house database security expertise and seek an expert assessment

Overview

Databases contain an organization’s valuable information, but the complexity of database functionality and the lack of technical awareness regarding database security results in database applications being one of the most commonly misconfigured applications. A Database Risk Assessment (DRA) discovers database platforms within your infrastructure and then assesses their risk exposure.

During a Database Risk Assessment, a Trustwave consultant performs testing in three phases:

1. Identify discoverable database instances within a defined IP range or domain within your infrastructure
2. Assess representative database(s) against industry best practices. A vulnerability assessment scan using credentials is configured to assess the database instance and to access the information needed to complete the audit. This approach provides actionable information on inherent vulnerabilities and database configuration elements that may make your databases vulnerable to attack, lead to regulatory compliance issues, or make them fail to comply with your information security policy.
3. Conduct a User Entitlement Review against a handful of objects that contain sensitive data to identify who has access to this data and how those rights were obtained.
At the end of a Database Risk Assessment a comprehensive presentation and documentation are created that outlines key vulnerabilities and configuration issues, prioritization of each by risk level, as well as explanations of what they are, their impact and appropriate next steps. Trustwave will provide deep analysis on the top five to ten issues, the root causes or enablers of those issues and detailed findings reports on them. As part of the Database Risk Assessment we additionally provide a 30-day license of AppDetectivePRO so that you can retest and ensure a more secure database.