Service Details

The Imperva Database Discovery and Analysis (dDnA) service is the first step in the successful discovery and classification of database assets and provides a proven way to identify and classify data to enable compliance with frameworks, standards and regulatory requirements.

Most companies understand how and where sensitive data should reside within the environment, but due to inter-connectivity between supporting groups and the requirements of business processes, data tends to be replicated and reside in systems and databases that are not fully catalogued.

The Imperva dDnA service helps eliminate the gaps, providing detailed data inventories and classification. This understanding helps reduce the overall information risk, and precisely the danger of noncompliance and subsequent regulator imposed financial or operational penalties. Building a database asset register helps clarify what is valuable in your company and who is accountable and responsible for it.
Imperva Methodology

Imperva utilizes the proven Data Security Risk and Compliance Life Cycle. The dDnA focuses on a pragmatic execution of the service across the Discover and Classify cycles.

<table>
<thead>
<tr>
<th>LIFE CYCLE</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover</td>
<td>Locate all known and unknown databases, produce an asset inventory</td>
</tr>
<tr>
<td>Classify</td>
<td>Find sensitive data, determine business value and associated governance requirements</td>
</tr>
<tr>
<td>Assess</td>
<td>Scan database servers for vulnerabilities, misconfigurations, configuration changes, and user entitlements</td>
</tr>
<tr>
<td>Prioritize</td>
<td>Combine information from Classify and Assess phases to determine what items to fix, what to mitigate through compensating controls (i.e. monitoring policies), and in what order to do the work</td>
</tr>
<tr>
<td>Fix</td>
<td>Create and run fix scripts, apply patches, create monitoring policies to implement compensating controls</td>
</tr>
<tr>
<td>Monitor</td>
<td>Audit access to sensitive data and privileged user activities, monitor for exploits and suspicious or unusual behavior</td>
</tr>
</tbody>
</table>

Deliverables

The service will deliver an overall asset register and control recommendations covering:

- Identify database assets
- Identify data owner(s)
- Identify custodian(s)
- Provide information sensitivity classification
- Deliver control recommendations
Why Are Discovery and Analysis So Important?

IT Security needs to support the securing of information systems and management of business risk. The dDnA deliverables will ensure clarity on the database asset owners, custodians, and sensitive data – a prerequisite for the application of security controls.

The dDnA will support four key drivers for sensitive data management:
- Compliance
- Information risk management
- Security optimization
- Business enablement

Learn More

Imperva consultants follow best practice methodologies leveraging our expertise and experience. We work flexibly to meet the needs of your organization and have experience in data security. Customers trust our consultants to deliver projects in line with best practices and good governance. Please direct questions regarding Imperva Services to Proserv-requests@imperva.com.