DATA SHEET

AppDetectivePRO

EVALUATION GUIDE

AppDetectivePRO is an in-depth database security assessment solution offered by Trustwave. This Evaluation Guide provides information for the installation of the software, how to run scans that provide database security diagnostics data, how to review the data, and how to run reports.

This basic evaluation should take 30 minutes. After completing it, you may want to explore more of what AppDetectivePRO has to offer, including how policies can be customized and all the other controls available in the Trustwave Database Security Knowledgebase (ShatterKB).

1 Download

Get a copy of AppDetectivePRO for evaluation

Download AppDetectivePRO by completing the web form found at: https://www.trustwave.com/en-us/resources/security-resources/trial-software/appdetectivepro-trial. You will receive instructions on how to install the self-extracting executable to your test box.

A typical system for AppDetectivePRO is configured with Windows 10, dual core processor 1.60 GHz, 3GB of RAM, and 5GB of hard disk. The default install is recommended to streamline your evaluation.

If you received an evaluation or promotional license file to scan more than one asset, follow the instructions in section 7 of this guide

Notes:

Notes for installation:

- You must run the install as an Administrator.
- Even if you are the Administrator, use the "Run as administrator" option.
- Microsoft .NET Framework 4.6 is a required component. If it is not installed already, the AppDetectivePRO installer will install it.
- After installation add any Windows account that needs access to the application by going to System Settings > User Configuration. The application will not open for any user not configured.

Notes on trial limitations:

- AppDetectivePRO is limited to the following if an evaluation license is not installed:
- Only one asset can be scanned (Pen Test/Audit/URR).
- A single policy is only available for use. (Download Built-In policy).
- Policy Editor feature is locked and not viewable.
- Reports are watermarked with Evaluation.
- Functionality is valid for only 30 days from when the application is first opened. After that period, the application will not run.
- ASAP Updater functionality is not available.

2 Discover or Add New Asset

Scan a segment of the network and see what databases are present

After creating a new session, click the "Discover" button. A wizard will help you through the process of entering information to run the discovery scan. When the discovery is complete, Assets will appear in the grid. You can expand any of the newly discovered Assets (click the '+' next to the Asset) to view banner information collected in the Asset Information Section.

Notes:

- Scanning a Class C network (255 addresses) with 12 live hosts, looking at the default ports of all Asset types will take approximately 6 minutes.
- Scanning a larger network segment or a more extensive list of ports will take longer. The number of dead IP/Port combinations and network latency also can impact the Discovery scan time.
- Some databases cannot be discovered based on their security configurations (i.e. Oracle 10g or greater)
- Some databases do not provide banner information based on their security configurations.
- Cloud databases (e.g. AWS Aurora) are not supported with discovery and should be added manually.
- You can view all the details of the discovery scan in the History section.
- If you do not want to run the Discovery, you have the option of manually adding a database by clicking the 'New Asset' button. A form will be available to add the database information. There is also an option to import a list of Assets (target databases) by clicking on the "Import" button.

3 Policy Scan

Scan an asset to perform a comprehensive database security diagnostic review from a zero-knowledge perspective and via authenticated access

1. Select an asset from the grid and click the "Run Policy" button. The Download – Audit (Built-in) policy will be enabled.
2. Click the "Next" button.
3. Enter the database account credentials for the asset you chose to scan.
4. Click the "Test Connection" button. This will test the database account credentials you entered to make sure it can connect to the database and that it has sufficient privileges to perform the policy scan.
5. Once the test is complete, click the "Go" button and the scan will perform.

Notes:

- For details of what privileges are needed for the database account needed for an Audit policy, refer to the following user creation scripts available: C:\Program Files\Trustwave\AppDetectivePRODataComponent\Resources\ShatterKnowledgebase\UserCreationScripts
- To run an Audit policy against IBM DB2 LUW, Sybase ASE, MySQL, and Teradata, you must have the appropriate client drivers installed on your test box where AppDetectivePRO is installed.
- The Download – Audit (Built-in) policy is a lightweight policy that does not include all the controls available within the product.

After the results are gathered from the scan, click the "Run Policy" button again. Choose "Pen Test" and the Download – Pen Test (Built-in) policy will be enabled. Click the "Go" button and the scan will perform.

Notes:

- Pen Test policies perform a zero knowledge, unauthenticated and non-intrusive scan.
- Some controls available test against password attacks and may lock out accounts.
- The Download - Pen Test (Built-in) policy is a lightweight policy that does not include all the controls available within the product.

4 Rights review scan

Scan an asset to gain a detailed view of all the data ownership, access controls, and privileges to sensitive information

Select the same asset from the grid and click the "Run User Rights" button. Like the policy scan for audit, enter the database account credentials. If you want to use the same account, click the "Use Policy Credentials" button. This will populate the fields with the information. Click the "Test" button. This will test the database account credentials you entered to make sure it can connect to the database and that it has sufficient privileges to perform the rights review scan. Once the test is complete, click the "Go" button and the scan will perform.

Notes:

- Rights Review scans are only supported against Oracle, Microsoft SQL Server, Sybase ASE, IBM DB2 LUW, Teradata and PostgreSQL.
- For details of what privileges are needed for the database account needed for Rights Review, refer to the following user creation scripts available: C:\Program Files\Trustwave\AppDetectivePRODataComponent\Resources\ShatterKnowledgebase\UserCreationScripts
- To run a Rights Review scan against Sybase ASE, IBM DB2 LUW and Teradata, you must the appropriate client drivers installed on your test box where AppDetectivePRO is installed.

5 Review Results

Analyze the results from your comprehensive database security diagnostics review

Start by going to "Policy Results". You will see, by default, all checks that resulted in a "Finding" within the Check Results view. To see the occurrence details of the finding, click the 'arrow' for each one. The layout of the results is grouped by Asset and Policy Ran. The findings of the Audit policy scan and the Pen Test policy scan will be grouped accordingly. Expand the Knowledgebase Article on the right to view more information about each check. Use the "Filter" to add or remove certain groups of checks by "Risk" or by "Result Status".

If you want to review the policy results where you can suppress occurrence findings and add any notes about any of the findings, choose the Control Review view.

Notes:

- You can view more information about checks with result status of 'Failed' and 'Skipped' in the "History" section.
- The Control Review view allows you to answer manual process controls that policies, like the DISA-STIG may contain.

Next review the "User Rights Results". This section is grouped by three views: objects, roles, users. These groupings allow you to pinpoint certain data ownership and privileges. To see the details of data ownership and privileges, click the 'arrow' to the left of each of the rows you want to view. You can then select from different tabs that present various data.

Notes:

- If you want to examine which users have rights to a sensitive table, use the 'Objects' view and filter down to the table.
- If you want to examine the privileges for a role, user the Roles view and filter down to the specific role.
- If you want to examine the privileges for a user, use the Users view and filter down to the specific user.

6 Generate Reports

Produce actionable reports to determine next steps

Generate reports in either the Policy Results or User Rights Results sections.

For a quick report on all the database findings from the Policy Results, generate the Vulnerability Summary report. If you are looking to export the details of each finding straight to a .csv file, generate the Check Results report.

Notes:

- Reports will generate with data set you filtered down to in the Policy Results section. If you filtered to just the Audit policy scan with High Risk and Result Finding, then the report will contain the data for that.

To report on User Rights Results, click on the "Report" button and choose the different types of options based on the view you are in. Mark off the check box in the grid to include the specific data for the object(s), role(s), or user(s).

7 Applying a Promotional License File

1. Select the gear icon in the upper right corner of the screen
2. Select "Licensing" in the left-hand menu
3. Click the "Add a License" button
4. Navigate to where the promotional AppDetectivePRO license resides on your computer
5. Select the license file and click open
6. Upon completion, the promotional license will be applied.
7. Click OK on the text box

You are now able to scan the additional assets based on the scope of the promotional license

AppDetectivePRO is limited to the following if you installed the extended evaluation license:

- Policy Editor functionality is available and other built-in policies are available to be used.
- Reports are watermarked with "Evaluation".
- Functionality is valid until the end of the extended evaluation license. After that period, the application will not run.
- ASAP Updater functionality is available where you are able to download the latest Knowledgebase update.

For more information: www.trustwave.com