Trustwave AppDetectivePRO Scanning FAQ

1. **Why do I need AppDetectivePRO when I already have a Vulnerability Scanner like Nessus?**

AppDetectivePRO is purpose built for database scanning. Scanners like Nessus provide a broad coverage of scanning for the network, OS, and web applications and specifically focus on known vulnerabilities (CVE's). While some scanners may identify database vulnerabilities, they do not provide the in-depth security testing AppDetectivePRO provides.

AppDetectivePRO is an agentless scanning solution that examines databases for configuration issues, vulnerabilities, identity and access control issues, excessive permissions, and underlying operating system issues impacting database security. Broad coverage vulnerability scanners do not test for the extensive and specific database security issues that AppDetectivePRO does. And AppDetectivePRO is utilized by many of the largest commercial and government IT Audit firms to assess millions of databases each year.

2. **What is Discovery scan and is it required?**

A Discovery scan is a systematic approach for searching your network for databases and database components. It performs an IP/Port scan and is comparable to a Nmap scan but is more limited in scope. A Discovery scan is configurable and can be performed against a specific set of IP addresses and ranges. Only default database ports are probed during a discovery scan. When a discovery scan is complete it adds databases as assets into your session in AppDetectivePRO.

Note: Databases may not be identified via a Discovery scan as newer versions of databases provide more secure configurations that prevent their ability to be detected in this scan. Additionally, discovery of databases in public clouds (AWS, Azure, Google Cloud Platform) is not supported.

A Discovery scan is not required to add assets to your session in AppDetectivePRO. Assets can be added in manually using the UI and can also be bulk imported into AppDetectivePRO. Documentation is provided in the ADP User Guide.

3. **What is a Pen Test policy scan?**

A Pen Test policy scan is non-credentialed scan of the database. It is a security test that identifies how unauthorized users or attackers can access your database. Pen Test scans take an "outside-in" approach and simulates how attackers could exploit vulnerabilities assuming they only had IP connectivity towards the database assets and no credentials.

4. **What is an Audit policy scan?**

An Audit policy scan provides an in-depth examination of the configuration and potential security holes within your database. Audit scans take an "inside-out" approach to testing the security of the database. Audit scans

require credentials to be supplied. During an audit scan, AppDetectivePRO provides an assessment of possible configuration issues, user access issues, and vulnerabilities.

5. **What is a User Rights scan?**

A User Rights scan is a deep examination of all the users, roles, objects and their relationships within the database. The scan produces results that help you understand user and role entitlements. You can review to see if a user or role has excessive permissions based on the business requirements and also quickly understand what users have access granted to a sensitive object, like a table that contains PII, credit card information, intellectual property or other sensitive data. Through User Rights scans, you are able to identify orphaned access rights from previous employees and contractors who no longer need access. Most important, User Rights scans enable you to adjust access rights to ensure a policy of Least Privilege.

6. **What is a Web Application (Application Scan) policy scan?**

An Application Scan, or commonly referred to as App Scan for short, is a policy scan performed against a web application. You can add a web application as an asset into a session. An Application Scan policy will run the checks included in the policy against the pages of the web application. Application Scan policy scanning is currently in technology preview in AppDetectivePRO 9.3.

7. **What is a policy and can I choose what controls/checks I want to run in a policy scan?**

A policy is a collection of controls/checks that are used to examine the security posture of a database. Controls can have a one-to-many mapping for checks. Checks are individual assessment tests that inspect the database for configuration issues, security weaknesses, vulnerabilities, and user access issues.

While AppDetectivePRO comes with built-in policies (i.e. CIS Benchmarks, DISA STIG, GDPR, Best Practices), you can create your own custom policies. Using the Policy Editor, you can create a new policy from scratch or clone an existing policy and modify the policy by adding or removing controls/checks. The Policy Editor displays what controls/checks are included in a policy and what controls/checks can be added .

8. **What privileges are needed to run a scan?**

AppDetectivePRO does not require database privileges for running a Discovery or Pen Test policy scan. To run authenticated scans, both an Audit policy scan and a User Rights scan, you need READ ONLY privileges on system tables. AppDetectivePRO comes with User Creation Scripts available in the product installation directory:

<installation folder>Trustwave>AppDetectivePRODataComponent>Resources

If a check requires escalated privileges, it is documented in the “CheckPermissions.txt” file located in that directory. For example, the audit check for Oracle “_TRACE_FILES_PUBLIC undocumented configuration parameter is NOT set to FALSE” requires SYSDBA privileges, as this setting can only be verified by that role. As policies are customizable, that check can simply be left out. If that check is included in the policy and the credentials provided are not sufficient enough to assess that configuration parameter, it will simply result back an error (i.e. check failed) due to lack of permissions.

9. **Do all scans require credentials? If they require scan credentials how are they stored?**

Some scans in AppDetectivePRO require credentials and some do not. Audit policy scans and User Rights scans require credentials, while Discovery, Pen Test policy scans do not. Web application (Application Scan) policy scans also do not require credentials but may optionally allow for them in the future.

Scan credentials are only cached once a successful test connection is established and are available to use while AppDetectivePRO is open. Scan credentials are protected using the Windows Data Protection API. Once the application is closed, any credentials cached are removed.

10. Why do I need Operating System (OS) credentials for Audit policy scans?

AppDetectivePRO has checks that examine the underlying OS integrity issues of a database installation. OS credentials are needed for these checks to run successfully. Documentation on what specific privileges are needed for the OS credentials are provided.

11. Does AppDetectivePRO provide auto-remediation of the issues it finds?

AppDetectivePRO does not provide auto-remediation to the issues it finds. AppDetectivePRO does not make any changes to the databases it scans. Remediation guidance is provided in each Knowledgebase article for every check. Additionally, a Fix Scripts report can be generated for any issues found. A Fix Scripts report is a detailed report of possible SQL statements to fix findings uncovered during an Audit policy scan.

Note: Not all issues found have a corresponding Fix Scripts as each issue is different. For example, a finding issue of a missing patch cannot be remediated via a Fix Script.

12. How long does it take for scans to run?

Discovery – Depending on the IP & port number ranges, the number of database types and other discovery scan options you have selected, a Discovery scan can complete in seconds or can take up to several hours. The wider the scope of scan options selected the longer the scan may take to complete. A discovery of a Class C subnet, checking default ports, typically completes in less than 2-3 minutes.

Policy Scans (Pen Test and Audit) – The length of the scan is contingent on the policy. For example, if you include some account password checking in a Pen Test policy, this may take longer to complete than that of a policy without those checks. Audit policies can be very comprehensive in reviewing configuration and integrity checks. Some checks may assess every single user and a group of administrative permissions. If a database has thousands of users, the scan will take longer than that of a database with dozens of users. For guidance, the built-in DISA STIG audit policy run against an Oracle 12c database with 50 users typically completes in 6-8 minutes.

User Rights – The length of the scan is contingent on the number of users, roles, and objects in the database which can exponentially grow based on these numbers. For guidance, a user rights scan run against a default Microsoft SQL Server 2016 database typically runs for about 1 minute.

13. Does a Discovery, Pen Test, Audit, or User Rights scan affect my system in any way? Are the scans intrusive?

A **Discovery** is a fairly innocuous process and does not seriously affect the performance of your network any more than copying a large file. A Discovery is less intrusive than scans performed by typical network security

assessment tools because the AppDetectivePRO Discovery is restricted in the ports it probes. AppDetectivePRO does **not** discover all ports (unless you specifically configure it that way, which is not recommended) as other tools do. Instead, AppDetectivePRO only probes ports likely to have a databases on them.

AppDetectivePRO does **not** perform a traditional Penetration Test. Instead, it performs a non-intrusive scan without authenticating to the database; which we refer to as a **"Pen Test**" scan. During this scan, AppDetectivePRO uses fingerprinting techniques to determine an exact database version and patch level. From there, it refers to a matrix that details which vulnerabilities exist at each patch level. This matrix is used to determine which vulnerabilities exist in your database. AppDetectivePRO does **not** change or alter your database in any way.

An **Audit policy scan** is non-intrusive and works by authenticating user-provided credentials to the database. The Audit then gathers information and examines your database for security vulnerabilities and misconfigurations. This "gathering of information" does **not** affect your database or its performance, any more than a READ ONLY query on a table will do.

Like an Audit, the **User Rights scan** is also non-intrusive and collects information out of the database and does **not** affect your database or its performance, any more than a READ ONLY query on a table will do.

14. Are passwords identified in scans captured and protected?

Passwords can be identified by scans if the policy contains controls/checks that examine for this. By default, all passwords identified are masked. They are stored and presented as results in the UI and reports masked. If it is acceptable by corporate security policy, passwords identified can be displayed in clear text. This requires a change to the Password Scan Settings configuration in the System Settings of AppDetectivePRO. Only new scans performed after the configuration is changed will make this possible. At any time, the configuration can be reverted back to the default setting making any passwords identified in new scans also masked. Any previous results will have passwords stored as masked.

15. What is a Framework?

A framework is a container of total controls possible to be added to policies. AppDetectivePRO has some built-in frameworks available: SHATTER, CIS, and DISA STIG.

The **SHATTER framework** is the default framework which comes with controls and checks that can be used within policies. This framework is maintained by Trustwave's research and development group, SpiderLabs. The SHATTER framework and policies associated with it are updated monthly via ASAP Updates. It is the only framework that can be cloned. The CIS and DISA STIG frameworks cannot be cloned because they represent content from outside organizations.

The **CIS and DISA STIG frameworks** are frameworks associated to their respective industry specific guidance standards. CIS is associated with the Center for Internet Security, and DISA STIG is associated with the Defense Information Systems Agency.

Within Frameworks, you can create your own custom frameworks or view the current built-in ones. You can further customize a user-created framework as described in the following sections.

16. What is Control Review?

Control Review is a way of viewing Policy Scan results in AppDetectivePRO. This view is used by users that want to review policy scan results mapped to controls for a specific framework (i.e. DISA-STIG or CIS). Results are presented with the specific framework control language and the checks mapped to those controls. Users can add notes and suppress at all levels of the control (control, check result, or check result occurrence).

17. **As an external consultant should I install AppDetectivePRO on my laptop or on my client's workstation?**

This depends on what your client finds acceptable based on their corporate security policy. In many instances, clients will require that AppDetectivePRO be installed in their environment and run on their workstation. The AppDetectivePRO license in this case would then need to be installed on that workstation. Other times, clients may permit you to run AppDetectivePRO from your laptop and provide you with the credentials needed for the scans.