AppDetectivePro™
The De-Facto Standard for Corporate Auditors and IT Advisors

By an overwhelming margin, corporate auditors, IT advisors, and Federal Government OIGs have made AppDetectivePro their database scanning and vulnerability assessment solution of choice. Deployed in over 130 countries, AppDetectivePro has been used to assess hundreds of thousands of databases in every vertical market. A thorough examination of the databases that store and process critical business information is a critical component of any IT audit; AppDetectivePro enables auditors and advisors to complete the task quickly, reliably, and cost effectively.

DATABASE SECURITY AND COMPLIANCE EFFORTS START WITH A SCAN
Manually assessing the security posture of a database is a complex task that requires expertise and significant resources. Manually measuring and demonstrating compliance with industry and government regulations is even more difficult. By equipping your staff with AppDetectivePro™, you will immediately and significantly reduce the complexity of these tasks. IT auditors and advisors, regardless of skill level, will be enabled to perform easy and repeatable database security assessments, capture all results for manual control checks, and generate compliance reports. AppDetectivePro leverages Application Security, Inc.’s (AppSec) SHATTER knowledgebase, the industry’s most complete collection of database vulnerability and misconfiguration checks to ensure the most comprehensive database assessment possible. The solution consists of three distinct functional modules:

• Database Discovery
• Database Vulnerability Assessment
• User Rights Review

DATABASE DISCOVERY
The critical first step in any IT audit is to identify all assets and applications residing on the network. AppDetectivePro’s Database Discovery module provides complete visibility into the inventory of databases on any network. Simply connect a laptop running AppDetectivePro to the network, and without agents, database logins, or other knowledge, the solution will scan and identify every database by vendor and release level.

DATABASE VULNERABILITY ASSESSMENT
AppDetectivePro has been the vulnerability assessment standard since the product was launched in 2002. With a policy-driven scanning engine, AppDetectivePro identifies vulnerabilities and misconfigurations. Issues identified include default or weak passwords, missing patches, poor access controls, and a host of other conditions. A flexible assessment framework allows auditors to choose between an outside-in, “hackers eye view” of the database which requires no credentials, or a more thorough inside-out scan which is facilitated through a read-only database account. AppDetectivePro includes built-in templates to satisfy the requirements of security best practices and various regulatory compliance initiatives. Compliance standards covered include: DISA STIG, NIST 800-53 (FISMA), PCI DSS, HIPAA, GLBA, Sarbanes-Oxley, ISO 27001, CoBIT, and Canada’s MITS.

Pen Test
AppDetectivePro’s unique Pen Test scan provides the outside-in view of a database’s security posture that is safe for use on production systems. The functionality does not perform intrusive tests or risky attack simulations. AppDetectivePro’s Pen Test gathers a detailed view of vulnerabilities that could allow an outsider access into a database system and provides awareness to the organization before the vulnerabilities are exploited. The Pen Tests are executed without the need to schedule downtime and can operate in a tight maintenance window. Pen Tests
require no database login information or passwords. Point the application at any database, and within seconds, results will be delivered.

Security Audit
For a more detailed, “inside-out” perspective of vulnerabilities and a complete assessment of database configuration settings, AppDetectivePro offers its Audit scan. Audits require minimal access to the databases being scanned; a read-only account with no access to sensitive user data is all that is required to perform a complete analysis. Audits extend beyond the capabilities of a Pen Test, identifying all the security holes that could allow an outsider access to a database. In addition, audits provide a detailed view of potential avenues of insider privilege abuse. Insiders can abuse their privileges to gain inappropriate access to data or functionality. AppDetectivePro Audit scans allow, organizations to protect sensitive information residing in database applications, guard against unauthorized outsider and insider access, and seamlessly demonstrate compliance to relevant requirements.

Vulnerability Knowledgebase, Up-to-Date Support
AppDetectivePro is based on the industry’s largest known collection of database-specific vulnerabilities. Compiled by TeamSHATTER, AppSec’s world-class threat research organization, the SHATTER knowledgebase is the most extensive set of database vulnerability and misconfiguration checks and rules on the market today. The knowledgebase is updated on a regular basis through AppSec’s ASAP Updates, ensuring that the most recent vulnerabilities can be identified and remediated.

KEY BENEFITS:
- Automated database discovery and inventory
- Database-specific vulnerability assessment
- Compliance work plans and policies
- Industry leading database vulnerability knowledgebase
- Automated information gathering and analysis
- Concurrent database scanning
- Deep analysis of user and role permissions
- Advanced, customizable reporting
- Easy to deploy, configure and use

in database applications, guard against unauthorized outsider and insider access, and seamlessly demonstrate compliance to relevant requirements.

USER RIGHTS REVIEW
A key component of nearly every regulatory initiative that addresses protection of data is a comprehensive analysis of which users have access to each system, which data and functionality they can access, and verification that the level of access that has been granted is appropriate based on the user’s business function or need to know. Traditionally, auditors have been forced to perform this analysis for database systems manually, consuming up to two weeks per database and often resulting in incorrect or incomplete information. AppDetectivePro User Rights addresses this problem by providing a scan-based review of user entitlements that automatically determines each user’s effective privileges. The automated User Rights Review significantly reduces the time and resources required to determine who has access to which data, what type of access rights they have (read, write, delete) and how they were granted that access.

WORK PLAN AND POLICY QUESTIONNAIRE
A thorough database assessment is more than just the scan. It consists of checking controls beyond database configurations and parameter settings. Understanding the business process, how the application interacts with the database, and procedural operations (like backup and audit log review policies) round out a complete database assessment. AppDetectivePro work plan management capabilities extends the auditor’s ability to capture all control information formulated in a questionnaire. It allows auditors to input password policy controls, run scans against password parameters, and independently conclude if a control is within compliance or not.

With the Work Plan Manager, IT auditors, consultants, and assessors can now centralize and automate their existing audit procedures. AppDetectivePro provides a work plan framework that simplifies audits and reduces the time to compliance by integrating the full audit findings results reporting into a single process.

APPDTECTIVEPRO REPORTING
AppDetectivePro’s reporting system allows organizations to easily report all database and application intelligence to appropriate stakeholders. Reporting options include: Inventory reports, Vulnerability Details and Summary reports, User Rights reports, Policy reports, and various others. Reports can be output in multiple formats including: PDF, Excel, Word, Crystal, HTML, XML and Text.
AppDetectivePro™

A 30-day evaluation copy of AppDetectivePro is available for download at: www.appsecinc.com/products/appdetective/

SYSTEM REQUIREMENTS

- Operating System: Microsoft Windows XP Professional SP2 or greater, Microsoft Windows Vista
- Browser: Internet Explorer version 7 or later
- Processor: 750 MHZ or 1 GHZ
- RAM: 1 GB or more
- Hard Drive: 300 MB of free disk space with additional space required to store vulnerability information
- Database: (Optional for storing AppDetectivePro results) Microsoft SQL Server 2008, 2005, 2000 or MSDE 2000 SP4

Vulnerability Summary


Application: Microsoft SQL Server 2008 (GHOSTDB_2K) on 172.16.32.15, port 1433

A security review has been run on a number of applications on your network. This review consisted of probing the application and comparing the results to a knowledge base of application security vulnerabilities.

This report displays a summary list of all vulnerabilities found including a summary analysis of the problem. To review a more detailed list of vulnerabilities and a comprehensive description of each vulnerability found, refer to the Vulnerability Details report.

AppDetectivePro enables auditors, IT advisors, security personnel and database administrators to implement database security, risk, and compliance best practices by continuously tracking and managing database vulnerabilities. With robust reporting capabilities and a customizable work plan manager and policy editor, AppDetectivePro arms enterprises with ready to deploy technology to manage security risk and extend compliance policies to the database.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

Application Security, Inc. (AppSec) is the leading provider of cross platform database security, risk and compliance solutions for the enterprise. Application Security, Inc.’s products – DbProtect and AppDetectivePro – deliver the industry’s most comprehensive database security solution and are used in the most demanding environments around the world. With over 2,500 customers, AppSec was named to Inc. Magazine’s 2007 (Inc. 500) and 2009 list of America’s Fastest Growing Companies, and was also named to the 2009 Deloitte Technology Fast 50. For more information, please visit www.appsecinc.com or follow AppSec on Twitter at www.twitter.com/appsecinc.

ABOUT TEAMSHATTER

TeamSHATTER is AppSec’s world-renowned research team, specializing in application vulnerability assessment and mitigation. The team conducts ongoing research into threats and vulnerabilities, identifying and reporting on security alerts. This intense focus and effort has resulted in the industry’s premier knowledgebase of vulnerabilities, patches, and remediation best practices. AppSec provides frequent product updates for the purpose of ensuring that DbProtect customers are able to proactively secure their systems against the latest database vulnerabilities and threats using ASAP Updates. All of the security alerts and checks developed by TeamSHATTER are integrated into our security solutions. Follow TeamSHATTER on Twitter at www.twitter.com/teamshatter.