

**Application and Database Security Auditing,
Vulnerability Assessment, and Compliance**

AppSentry™

Product Overview

Integrigy Overview

- **Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. Integrigy Consulting offers comprehensive security assessment services for leading ERP and CRM applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.**
- **Corporate Details**
 - Founded December 2001
 - Privately Held
 - Based in Chicago, Illinois

Integrigy Background

- **Extensive experience with Oracle**
 - Founded by former Big-6 consultants with significant experience on Oracle implementations in Fortune 500 companies
 - Founders recognized a major gap in all implementations – little or no security auditing done on projects
 - Integrigy has found more security bugs in Oracle Applications than anyone else inside or outside of Oracle
- **Both an ERP/CRM company and a security company**
 - Products developed to support and enhance an ERP/CRM implementation – Integrigy understands the issues and risks challenging large ERP/CRM implementations
 - Integrigy bridges the gap between applications, databases, and security

Integrigy Security Alerts

Security Alert	Versions	Security Vulnerabilities
Critical Patch Update July 2008	Oracle 11g 11.5.8 – 12.0.x	<ul style="list-style-type: none"> 2 Issues in Oracle RDBMS Authentication 2 Oracle E-Business Suite vulnerabilities
Critical Patch Update April 2008	12.0.x 11.5.7 – 11.5.10	<ul style="list-style-type: none"> 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update July 2007	12.0.x 11.5.1 – 11.5.10	<ul style="list-style-type: none"> 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update October 2005	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> Default configuration issues
Critical Patch Update July 2005	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> SQL injection vulnerabilities Information disclosure
Critical Patch Update April 2005	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> SQL injection vulnerabilities Information disclosure
Critical Patch Update Jan 2005	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> SQL injection vulnerabilities
Oracle Security Alert #68	Oracle 8i, 9i, 10g	<ul style="list-style-type: none"> Buffer overflows Listener information leakage
Oracle Security Alert #67	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> 10 SQL injection vulnerabilities
Oracle Security Alert #56	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> Buffer overflow in FNDWRR.exe
Oracle Security Alert #55	11.5.1 – 11.5.8	<ul style="list-style-type: none"> Multiple vulnerabilities in AOL/J Setup Test Obtain sensitive information (valid session)
Oracle Security Alert #53	10.7, 11.0.x 11.5.1 – 11.5.8	<ul style="list-style-type: none"> No authentication in FNDFS program Retrieve any file from O/S

Integrigy's Products

AppSentry™

- Security scanner for databases, application servers, and ERP packages
- Performs advanced penetration testing and in-depth security and controls auditing
- Performs over 300+ audits and checks on Oracle products
- Runs on any Windows PC and requires no software to be installed on the target servers

AppDefend™

- Application firewall and intrusion prevention system for ERP packages
- Blocks common attacks like SQL injection, session hijacking, and cross site scripting
- Blocks access to unimplemented Oracle Applications modules
- Runs as an Apache modules and scans all incoming web requests

Manual Auditing Issues

- **Massive applications with many layers**
 - Very time consuming to check everything – hundreds of items to check and analyze
 - Auditor's knowledge must be extensive and broad
 - Technical (security) and functional (control) auditing skills required
- **Audits are static and need to be performed routinely**
 - Difficult and expensive to conduct a 2 week audit every year
- **Few tools exist to automate audit process**
 - Multiple tools required to automate entire process
 - Tools are usually a conglomeration of SQL scripts and shell scripts
- **New exploits and vulnerabilities are discovered frequently in operating system, web server, application server, database, app**
 - Difficult to keep accurate inventory of new security issues

AppSentry Overview

- **Security Scanner for databases, application servers, and ERP/CRM Applications**
 - Validates security of network, operating system, web server, database, and application
 - Modular design with distributed GUI and centralized server
 - Security checks written in XML and Java
 - Automatic program and security check updates

 - In-depth security and controls auditing
 - Advanced penetration testing
 - Scanning of open network ports for well-known and application specific vulnerabilities
 - Validation of application and technology stack configuration by analyzing configuration files, logs, and file versions
 - Analysis of users and roles to isolate segregation of duty issues
 - Transaction auditing to detect possible fraud

Using AppSentry

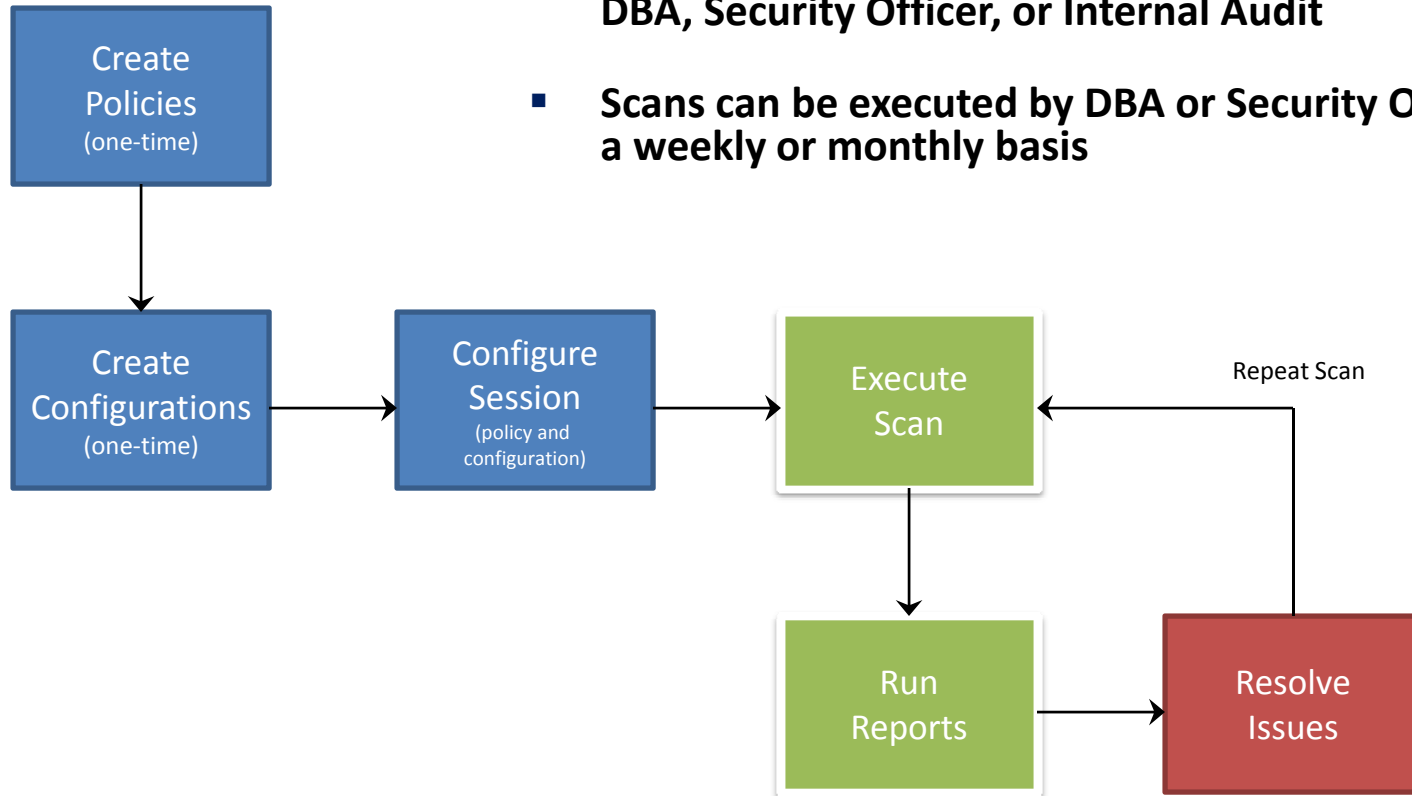
- **Simple to use – task oriented GUI**
- **Comprehensive descriptions and solutions for identified vulnerabilities**
- **AppSentry Users**
 - IT Security
 - Internal Audit
 - Oracle DBAs
 - Oracle Project Team – IT
 - Oracle Project Team – Functional/Business Owner

AppSentry – Automated Audit

- **Confidence**
 - Audits all layers from operating system to application
 - Downloads updates before every scan
- **Breadth**
 - Performs both security and control audits
- **Productivity**
 - Simple to use
 - Automates auditing and reporting
 - Auditor can focus on more important tasks (e.g., process controls)
 - Fast – audit can be accomplished in less than 1 hour

AppSentry Workflow

- Quick and simple workflow
- Policies and configurations are created once by DBA, Security Officer, or Internal Audit
- Scans can be executed by DBA or Security Officer on a weekly or monthly basis



Third-Party Integration

- **Security Management System and SNMP Management Systems**
 - Result data sent to Security Management Systems (Event and Incident Consoles) or SNMP Management Systems
 - Supports Syslog, SNMP Trap, or ArcSight CEF

AppSentry – Policy Editor

Policy Name	Create Date (y/m/d)	Modify Date (y/m/d)
Microsoft SQL Server		
Microsoft SQL Server Standard Policy	2007/03/24 21:58:24	2007/03/24 21:58:24
Oracle Application Server		
Standard Policy	2007/03/24 21:58:24	2007/03/24 21:58:24
Oracle Applications 11i		
Oracle Applications 11i Standard Policy	2005/10/12 11:31:51	2007/01/21 22:17:46
Oracle Database		
Database Standard Policy	2005/10/12 11:31:51	2005/10/12 11:31:51
Test DB	2007/03/24 21:58:25	2007/03/24 21:58:25

Configuration Item	Value
Minimum Password Length	5
Hard to Guess Passwords	<input checked="" type="checkbox"/>
Password Reuse Time Limit	100
Inactive Account After x	4
Case Sensitive Passwords	<input type="checkbox"/>
Password Expiration Type	NONE
Password Expiration Days	90
Password Expiration Accesses	200

Oracle Applications User Passwords

Oracle Applications has a number of profile options that can accommodate most organization's password policies. The only major missing feature is any kind of dictionary check, however, custom password validation

Policies can be defined for different scenarios such as HIPAA, month-end scan, a level of security, or a checklist

Policy items are general security policy settings (e.g., minimum password length) and individual audit and check settings

Detailed information is provided for each policy item including best practices and references

AppSentry – Policy Editor

AppSentry 5.5 by Integrity

File Edit Tools Help

Policy Editor

Policy Name	Create Date (y/m/d)	Modify Date (y/m/d)
Microsoft SQL Server		
Microsoft SQL Server Standard Policy	2007/03/24 21:58:24	2007/03/24 21:58:24
Oracle Application Server		
Standard Policy	2007/03/24 21:58:24	2007/03/24 21:58:24
Oracle Applications 11i		
Oracle Applications 11i Standard Policy	2005/10/12 11:31:51	2007/01/21 22:17:46
Oracle Database		
Database Standard Policy	2005/10/12 11:31:51	2005/10/12 11:31:51
Test DB	2007/03/24 21:58:25	2007/03/24 21:58:25

Oracle Database

- General
 - Oracle Database Accounts
 - Oracle Database Settings
 - Oracle Database Session and Pas...
 - Patch Policy and Critical Patch Up...
 - Critical Patch Updates
 - Oracle Database Listener
 - System Privileges
 - System and Privileges
 - Table, Indexes, Views, Syn...
 - Users, Roles, Profiles
 - Storage Management
 - Procedures, Triggers, Types
 - Rules
 - Miscellaneous
 - Oracle Database Standard Packa...
 - DBMS Packages 1
 - DBMS Packages 2
 - Web Packages
 - UTL Packages
 - CTXSYS Packages

Table, Indexes, Views, Synonyms

	Public	User	Role
SELECT ANY TABLE	HIGH	AUDIT	MEDIUM
INSERT ANY TABLE	HIGH	AUDIT	MEDIUM
UPDATE ANY TABLE	HIGH	AUDIT	MEDIUM
DELETE ANY TABLE	HIGH	AUDIT	MEDIUM
UNDER ANY TABLE	NONE	NONE	NONE

Review each system privilege and determine the appropriate access level for PUBLIC, users, and roles. For each system privilege, you may set one of the following values -

- **None** - No action will be taken
- **AUDIT** - The PUBLIC, user, or role grants for this privilege will be reported in the 'System Privileges Analysis' report.
- **LOW MEDIUM HIGH** - In addition to being

AppSentry WebUpdate Available

Policy items can be tailored to a specific environment, security standard, or checklist. As an example, AppSentry allows any Oracle database system privilege to be checked. Other areas include access to standard packages, roles, etc.

Any Oracle database system privilege can be checked and return either AUDIT, HIGH, MEDIUM, LOW results.

AppSentry – Configuration Editor

AppSentry 5.5 by Integrity

File Edit Tools Help

Configuration Editor

Configuration Name	Create Date (y/m/d)	Modify Date (y/m/d)
Oracle Application Server		
Sample Oracle App Server	2007/03/24 21:59:16	2007/03/24 21:59:16
Oracle Database		
Sample Oracle 10g	2007/01/21 22:14:02	2007/01/21 22:15:51
Sample Oracle 10g RAC	2007/01/21 22:13:24	2007/01/21 22:17:00
Oracle E-Business Suite 11i		
Sample Oracle 11i	2007/01/21 22:13:34	2007/01/21 22:33:07
Sample Oracle 11i Complex	2007/01/21 22:13:51	2007/01/21 22:27:57

Server Select a server type from the drop down list. Enter a name in the text box to identify the server. Click the 'Add' button.

Applications 11i Server

HTTP Server

Add

Applications 11i Server - Database Server

Database Server	<input checked="" type="checkbox"/>
Administration Server	<input checked="" type="checkbox"/>
Autoconfig Enabled	<input checked="" type="checkbox"/>
Serv. Hostname or IP Address	proddb01.integrity.com
Database TNS Port	1521
Apache Web Port	8000

Oracle Applications 11i Server

Use this section to define the different servers in the 11i implementation. Oracle Applications uses five different types of servers -- web, forms, concurrent manager, database, and administration. These types of servers can be installed on a single server or distributed across many servers. Define one section for

Delete To remove a server, select it from the list and click the 'Delete Server' button.

AppSentry WebUpdate Available

Configurations are defined for different environments including Oracle database, Oracle Application Server, and Oracle E-Business Suite

Complex configurations can be created to handle environments like RAC

Detailed information is included for each configuration setting

AppSentry – Scan

The screenshot displays the AppSentry 5.5 Scanner application window. The interface is divided into several sections:

- Configuration:** Includes dropdown menus for 'Sample Oracle 11i' and 'Oracle Applications 11i Standal', a 'Scan Name' field with '2007-Mar-24 22-27-01', and checkboxes for 'Use Date/Time', 'Show Debug Messages', and 'Timeout Hung Processes'.
- Scan Status:** Shows 'Scan Status: Starting Scan' with a progress bar, 'Phase: Executing Checks', and 'Step: Oracle Critical Patch Updates (Database) (oradbcpu)'. It also displays 'Scan Start: 24 Mar 2007 22:27:01' and 'Elapsed Time: 00:03:22'.
- Status Log:** A list of scan events with timestamps, such as 'Started Init.ora - AUDIT_TRAIL (oradbaudittrail)', 'Finished Privileges on Standard Database Packages (oradbpublicpackages) Time=4.563', and 'Finished Access to LINK\$ Table (oradblinkprivs) Time=1.062'.
- Results:** Contains checkboxes for 'Show OK Status', 'Show Error Status', 'Show Excluded Status', and 'Show Unknown Status'.
- Controls:** 'Start' and 'Stop' buttons are located at the bottom of the configuration section.

Blue arrows point from the text annotations to the 'Policy' dropdown, the 'Scan Status' section, and a specific log entry in the 'Status' list.

Running a scan is as simple as choosing a configuration and policy and clicking start

Detailed information is presented on the current status of the scan, including the current check running, the timing of all executed checks, and any errors encountered during the scan

AppSentry – Scan

The screenshot displays the AppSentry 5.5 by Integriqy application window. The interface is divided into several sections:

- Left Sidebar:** Contains navigation icons for Start Page, Policy, Config, Scanner (selected), Results, and Reports.
- Configuration Panel:** Shows 'Sample Oracle 11i' selected in the Configuration dropdown, 'Oracle Applications 11i Stand...' in the Policy dropdown, and a Scan Name of '2007-Mar-24 22-27-01' with 'Use Date/Time' checked.
- Debugging Panel:** Includes checkboxes for 'Show Debug Messages' (unchecked) and 'Timeout Hung Processes' (checked).
- Results Panel:** Includes checkboxes for 'Show OK Status', 'Show Error Status', 'Show Excluded Status', and 'Show Unknown Status' (all checked).
- Start/Stop Buttons:** A green 'Start' button and a red 'Stop' button are located at the bottom of the configuration area.
- Scan Status Panel:** Shows 'Scan Results (467)' with a tree view of findings. The tree is expanded to show 'Medium (2)' and 'Low (16)' categories. A specific result is highlighted: 'Critical Patch Update October 2006 Applications Patch Plain-text Passwords in Profil...'. Below the tree, a detailed view of this result is shown, including a 'Summary' and 'Details' section.

Results are available in real-time as the scan is running in an easy to use tree navigator

Each result includes detailed information including Summary, Details, Target (host, database, application), Description, Solution, Risk, Type, and References

AppSentry – Results

The screenshot displays the AppSentry 5.5 by Integrity application window. The interface includes a menu bar (File, Edit, Tools, Help), a sidebar with navigation icons for Start Page, Policy, Config, Scanner, Results, and Reports, and a main content area. The main area is divided into several panes:

- Results Table:** A table showing scan configurations and results.
- Results Browser:** A tree view showing the hierarchy of scan results, including High, Medium, and Low severity categories.
- Reports Manager:** A pane for managing reports.
- Report Content:** A detailed report for a specific scan, including a summary and details.

Configuration	Module	Last Scan	Date (y/m/d)	Policy	Vulns	Score
Sample Oracle 10g	Oracle	Sample Oracle 10g Scan	2007/01/21	Database Standard Policy	23	-10
Sample Oracle 11i	Oracle	2007-Mar-24 22-27-01	2007/03/24	Oracle Applications 11i	330	-161

Name	Date (y/m/d)	Policy	Vulns	Score
2007-Mar-24	2007/03/24	Oracle	330	-1613
Sample Oracle 11i	2007/01/21	Oracle	330	-1613

Results Browser

- High (311)
- Medium (2)
 - AUDIT_SYS_OPERATIONS Set to TRUE
 - _TRACE_FILES_PUBLIC Set to TRUE
- Low (16)
 - 'Signon Password Failure Limit' is against policy
 - 'Signon Password No Reuse' is against policy
 - Critical Patch Update January 2007 Applications Patch AP...
 - Critical Patch Update January 2007 Applications Patch FND...

Critical Patch Update January 2007 Application Patches

Summary

Critical Patch Update January 2007 Applications Patch AP Employee Taxpayer ID Display Not Applied

Details

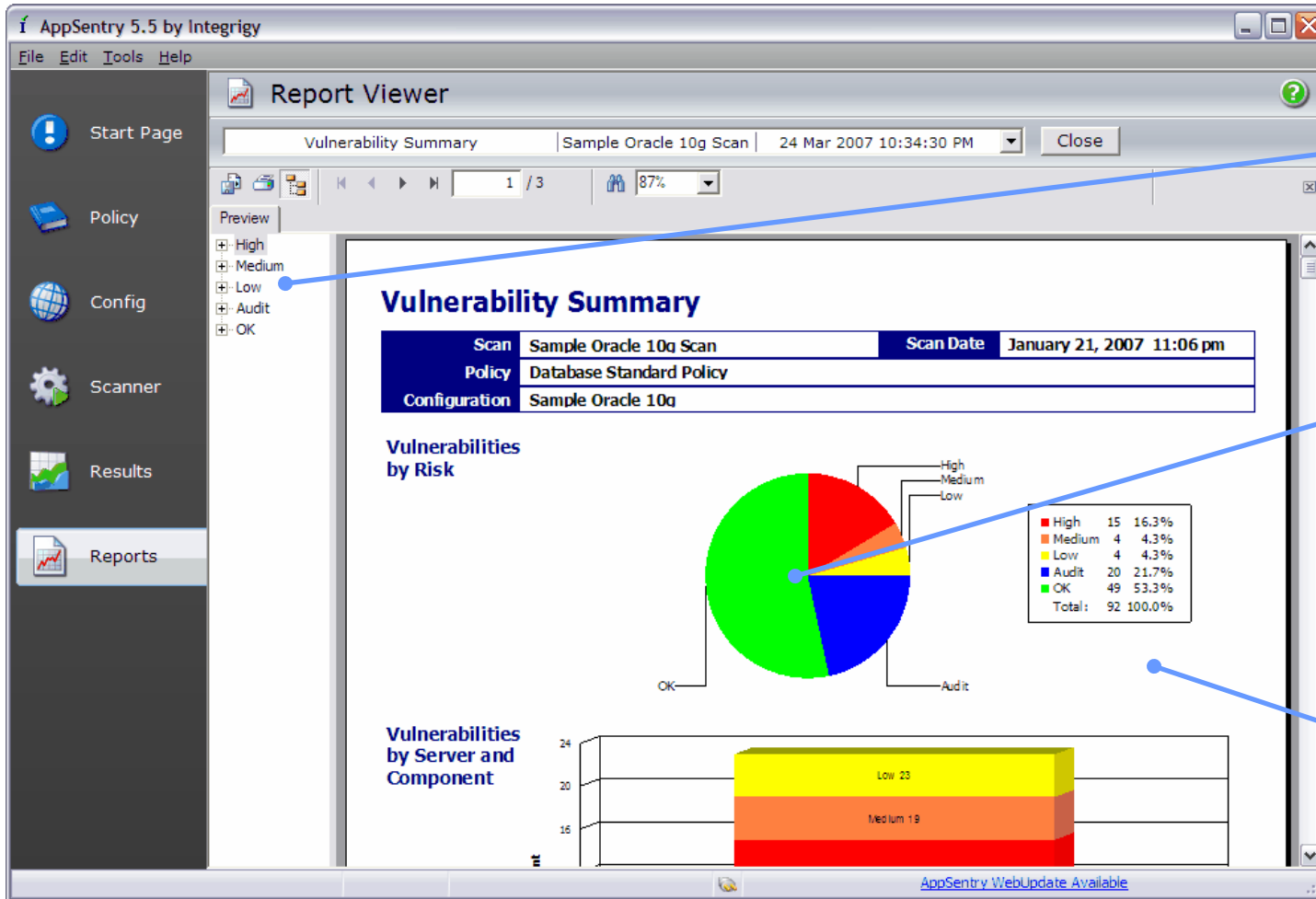
Critical Patch Update January 2007 Applications Patch AP Employee Taxpayer ID Display has not been applied. APXVDMVD.fmb file version is 115.207.0.0 and at least 115.207.15102.6 is required. The patch is 11.5.10.2 =

Results from all scans can be reviewed at any time.

Results can be browsed or reports run

Each scan includes a score based on a custom formula defined for each customer.

AppSentry – Reporting

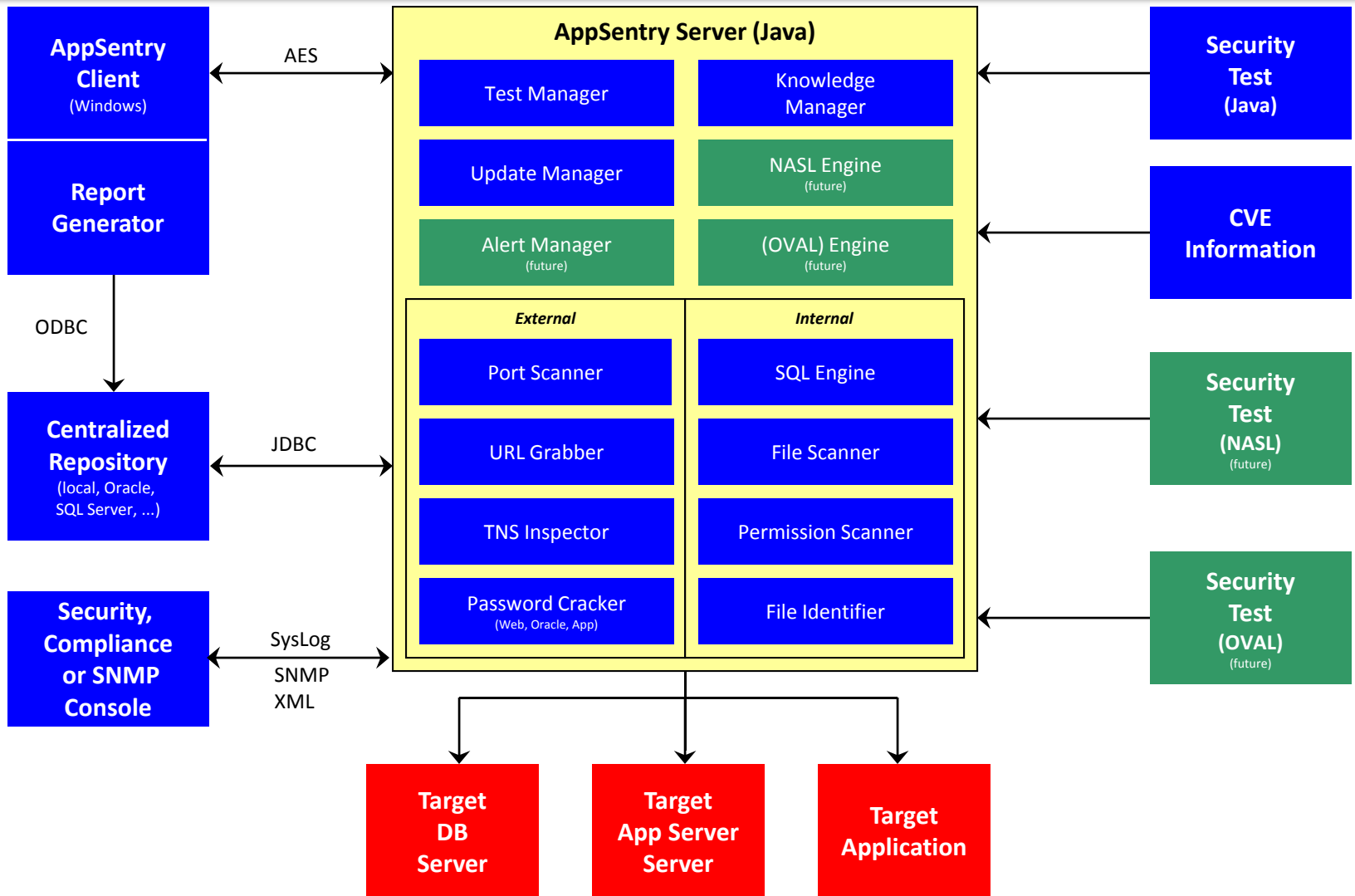


Reports are interactive and some allow drill-down into detailed information

Reports include charts and graphs, which are interactive and allow drill-down

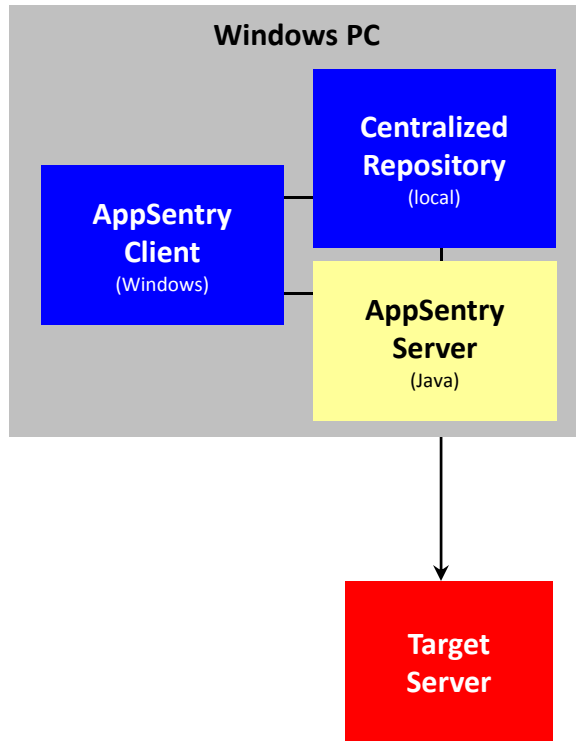
Reports can be viewed, printed, or exported into multiple formats including Acrobat (PDF), Word, Excel, HTML

AppSentry Architecture

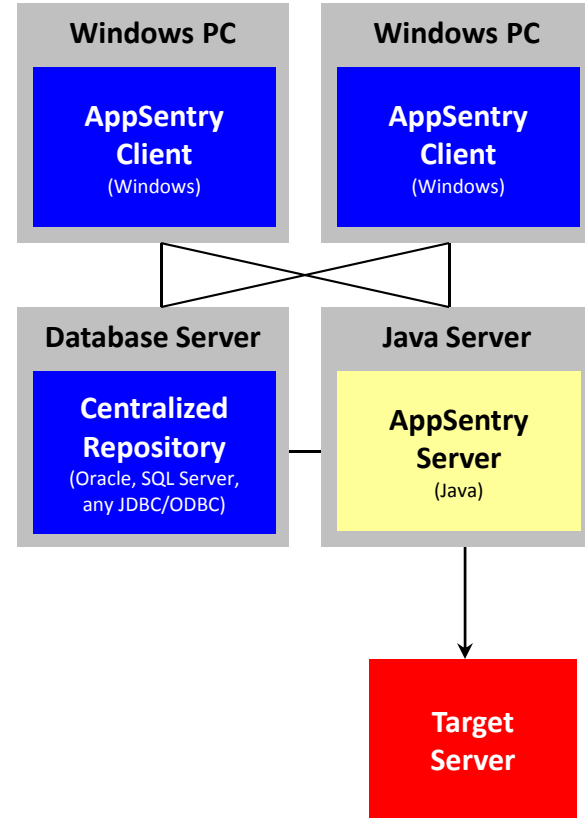


AppSentry Deployment

Standard



Distributed



Distributed deployments require support from Integrity Consulting

Current AppSentry Modules

Oracle E-Business Suite

- 11i (11.5.1 – 11.5.10 CU2)
- R12 (12.0, 12.1)

Oracle Database

- 8i (8.1.7)
- 9i (9.0.1, 9.2.0)
- 10g (10.1, 10.2)
- 11g (11.1, 11.2)

Oracle Application Server

- 9iAS (1.0.2, 9.0.2, 9.0.3)
- 10g (9.0.4, 10.1)
- 11g (11.1)

Microsoft SQL Server

- 2000
- 2005
- 2008

AppSentry Modules in Development

Database/Web Server/Application	Estimated Release Date
Oracle PeopleSoft	Q4 2010
SAP	Q1 2011
Oracle Collaboration Suite	Q1 2011
Oracle Clinical	Q1 2011
Oracle Retail	Q2 2011
Oracle Siebel	Q2 2011
IBM DB2	Q1 2011
Sybase	Q1 2011
Apache and MySQL (AppSentry Open-Source Edition)	Q3 2011
Oracle WebLogic	Q4 2010

Integrigy Contact Information

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681
888/542-4802

Website: www.integrigy.com

Sales: sales@integrigy.com

Development: development@integrigy.com

Support: support@integrigy.com

Security Alerts: alerts@integrigy.com

Copyright © 2010 Integrigy Corporation. All rights reserved.

