

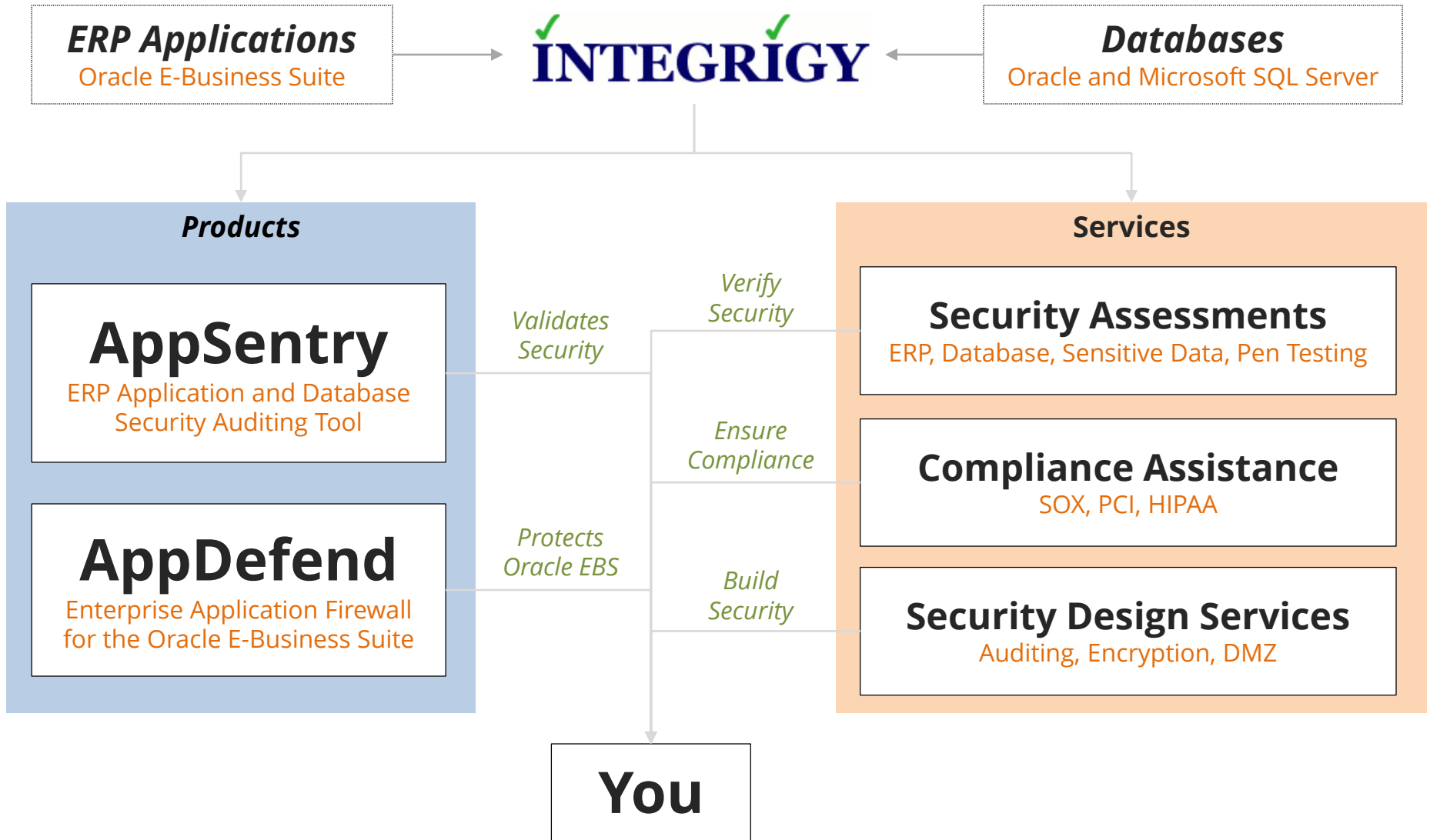
# AppSentry

## Application and Database Security Auditing

March 2016

*mission critical applications ...  
... mission critical security*

# About Integrigy



# Safe Harbor Statement

**The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Integrigy's products remains at the sole discretion of Integrigy.**

# Integrigy Published Security Alerts

Security Alert	Versions	Security Vulnerabilities
<b>Critical Patch Update July 2012</b>	11.5.10 – 12.1.x	<ul style="list-style-type: none"> <li>▪ Oracle E-Business Suite XSS</li> </ul>
<b>Critical Patch Update July 2011</b>	11.5.10 – 12.1.x	<ul style="list-style-type: none"> <li>▪ Oracle E-Business Suite security configuration issue</li> </ul>
<b>Critical Patch Update October 2010</b>	11.5.10 – 12.1.x	<ul style="list-style-type: none"> <li>▪ 2 Oracle E-Business Suite security weaknesses</li> </ul>
<b>Critical Patch Update July 2008</b>	Oracle 11g 11.5.8 – 12.0.x	<ul style="list-style-type: none"> <li>▪ 2 Issues in Oracle RDBMS Authentication</li> <li>▪ 2 Oracle E-Business Suite vulnerabilities</li> </ul>
<b>Critical Patch Update April 2008</b>	12.0.x 11.5.7 – 11.5.10	<ul style="list-style-type: none"> <li>▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update July 2007</b>	12.0.x 11.5.1 – 11.5.10	<ul style="list-style-type: none"> <li>▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update October 2005</b>	11.0.x, 11.5.1 – 11.5.10	<ul style="list-style-type: none"> <li>▪ Default configuration issues</li> </ul>
<b>Critical Patch Update July 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> <li>▪ Information disclosure</li> </ul>
<b>Critical Patch Update April 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> <li>▪ Information disclosure</li> </ul>
<b>Critical Patch Update Jan 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>▪ SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #68</b>	Oracle 8i, 9i, 10g	<ul style="list-style-type: none"> <li>▪ Buffer overflows</li> <li>▪ Listener information leakage</li> </ul>
<b>Oracle Security Alert #67</b>	11.0.x, 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ 10 SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #56</b>	11.0.x, 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ Buffer overflow in FNDWRR.exe</li> </ul>
<b>Oracle Security Alert #55</b>	11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ Multiple vulnerabilities in AOL/J Setup Test</li> <li>▪ Obtain sensitive information (valid session)</li> </ul>
<b>Oracle Security Alert #53</b>	10.7, 11.0.x 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>▪ No authentication in FNDFS program</li> <li>▪ Retrieve any file from O/S</li> </ul>

# 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

# Integrigy AppSentry

**AppSentry** is a **security scanner** designed and optimized for the Oracle Database, MS SQL Server, and ERP applications.

## ❖ **Security scanner**

1,000+ in-depth security audits and controls, 3<sup>rd</sup> party integration, automatic updates, no agents, network and operating system included

## ❖ **Database Security**

Accounts, patches, permissions (e.g. APPS, APPLSYS PUB), listener, links, auditing, exploits

## ❖ **Oracle EBS Security**

Apache, SSL, accounts, auditing, patches, privileges, auditing and security settings

## ❖ **Security Reports**

Findings, recommendations, exportable, compliance mappings (PCI, HIPAA, SOX...)

# 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**

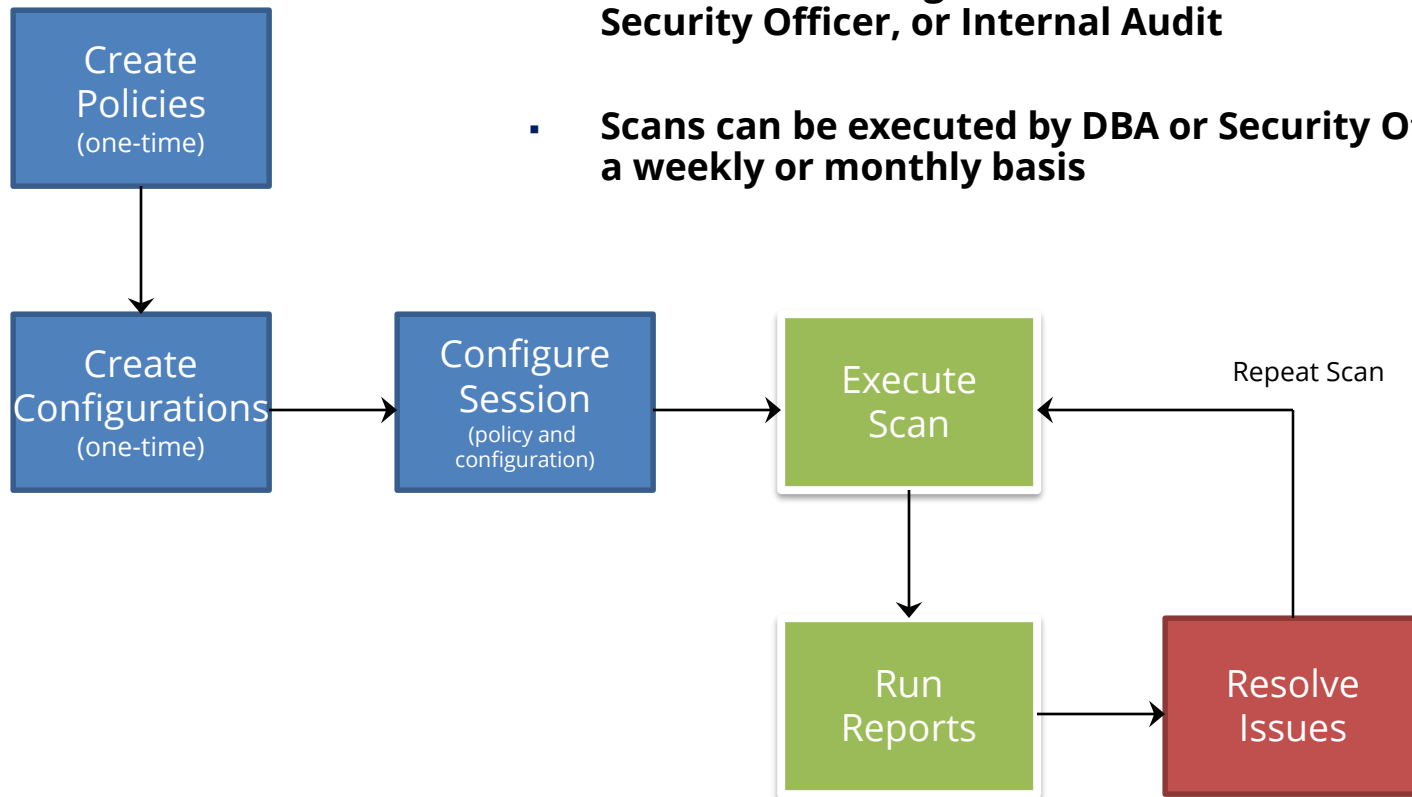
- Performs both security and control audits

- **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

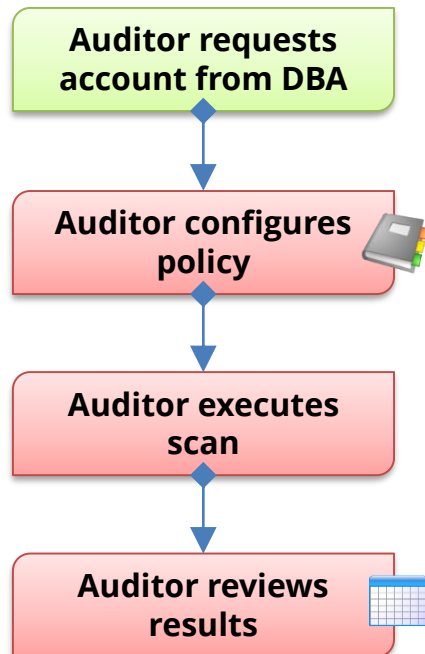
- **Quick and simple workflow**
- **Policies and configurations are created once by DBA, Security Officer, or Internal Audit**
- **Scans can be executed by DBA or Security Officer on a weekly or monthly basis**



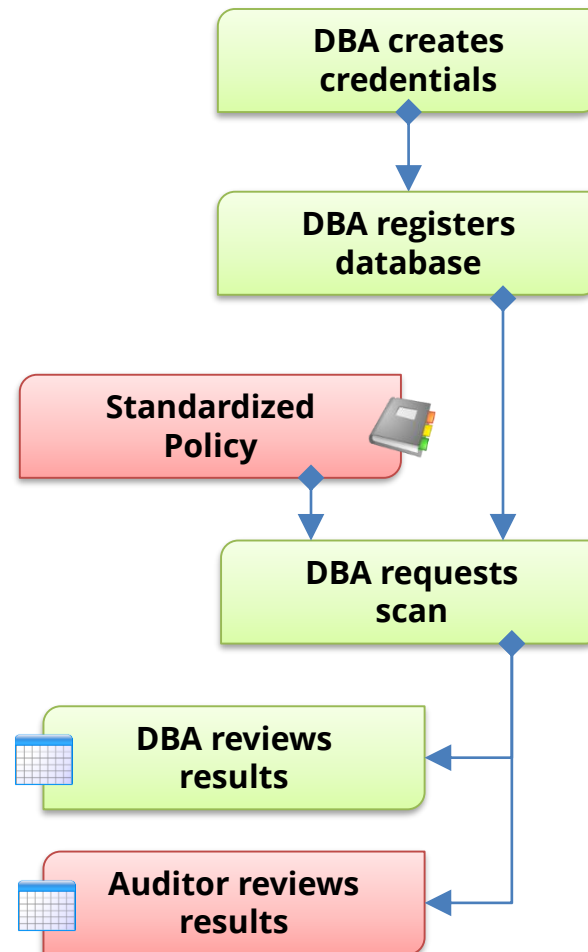
# AppSentry Standard Usage Models

## Auditor

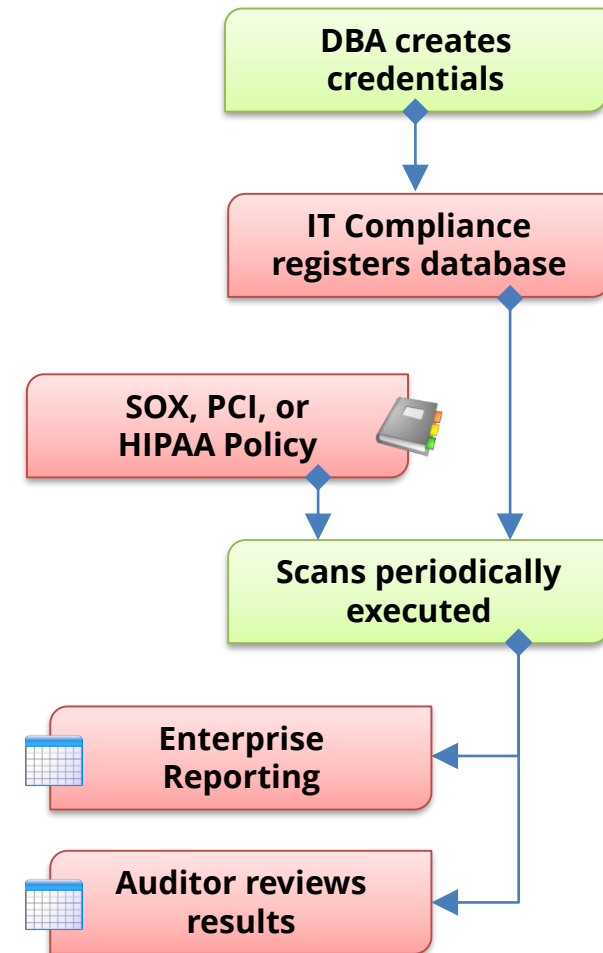
(standalone or server)



## Self-Service DBA



## Compliance/Certification



# Access and Network Requirements

- **AppSentry is a credentialed scanner**
  - A database account is required
  - Oracle = CREATE SESSION, SELECT ANY DICTIONARY
  - SQL Server = VIEW ANY DEFINITION, multiple views
  - SQL Server may use an Active Directory account
  
- **Direct database network access is required**
  - AppSentry server connects to database server
  - Oracle port = 1521 (default)
  - SQL Server port = 1433 (default)

# AppSentry Deployment Options

Standalone	<b>USB</b>	<ul style="list-style-type: none"><li>▪ For auditors travelling</li><li>▪ Synchronize or archive to central server</li></ul>
	<b>Desktop/ Laptop</b>	<ul style="list-style-type: none"><li>▪ Single user, local installation</li></ul>
Server	<b>Server</b>	<ul style="list-style-type: none"><li>▪ Multi-user solution on dedicated hardware</li><li>▪ Operating system Linux or Windows</li></ul>
	<b>Virtual Machine</b>	<ul style="list-style-type: none"><li>▪ Multi-user solution on virtualized hardware</li><li>▪ Operating system Linux or Windows</li></ul>
	<b>Virtual Appliance</b> (planned)	<ul style="list-style-type: none"><li>▪ VMWare packaged (OVF) appliance running Linux JEOS OS</li></ul>
Cloud	<b>Private Cloud</b> (planned)	<ul style="list-style-type: none"><li>▪ Java-capable cloud solutions with database support</li></ul>
	<b>Public Cloud</b> (demonstration)	<ul style="list-style-type: none"><li>▪ Integrigy hosted solution at Amazon AWS</li></ul>

# 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

Setting	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

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

Applications 11i Server - Database Server

Server Type	Checked
Database Server	<input checked="" type="checkbox"/>
Administration Server	<input checked="" type="checkbox"/>
Autoconfig Enabled	<input checked="" type="checkbox"/>
Server 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

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 by Integriqy 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:** A list of scan activities 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.

The status bar at the bottom shows the elapsed time '00:03:22', a progress bar, and a notification for 'AppSentry WebUpdate Available'.

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 Integrigy 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' in the Configuration dropdown, 'Oracle Applications 11i Stand...' in the Policy dropdown, and a Scan Name of '2007-Mar-24 22-27-01' with the 'Use Date/Time' checkbox 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 play button labeled 'Start' and a red stop button labeled 'Stop' are located at the bottom of the configuration area.
- Scan Status and Results:** The main area shows a tree view of scan results. The 'Scan Results (467)' tab is active, displaying a list of findings categorized by severity: Critical (9 items), Medium (2 items), and Low (16 items). A specific result is selected and expanded, showing a detailed view for 'Critical Patch Update October 2006 Application Patches'.

The detailed view for the selected result includes the following sections:

- Summary:** Critical Patch Update October 2006 Applications Patch Plain-text Passwords in Profile Options Not Applied
- Details:** Critical Patch Update October 2006 Applications Patch Plain-text Passwords in

At the bottom of the window, a status bar indicates 'AppSentry WebUpdate Available'.

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 main area is titled 'Results' and contains a table with the following data:

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

Below this table is another table with columns: Name, Date (y/m/d), Policy, Vulns, and Score. It shows two entries:

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

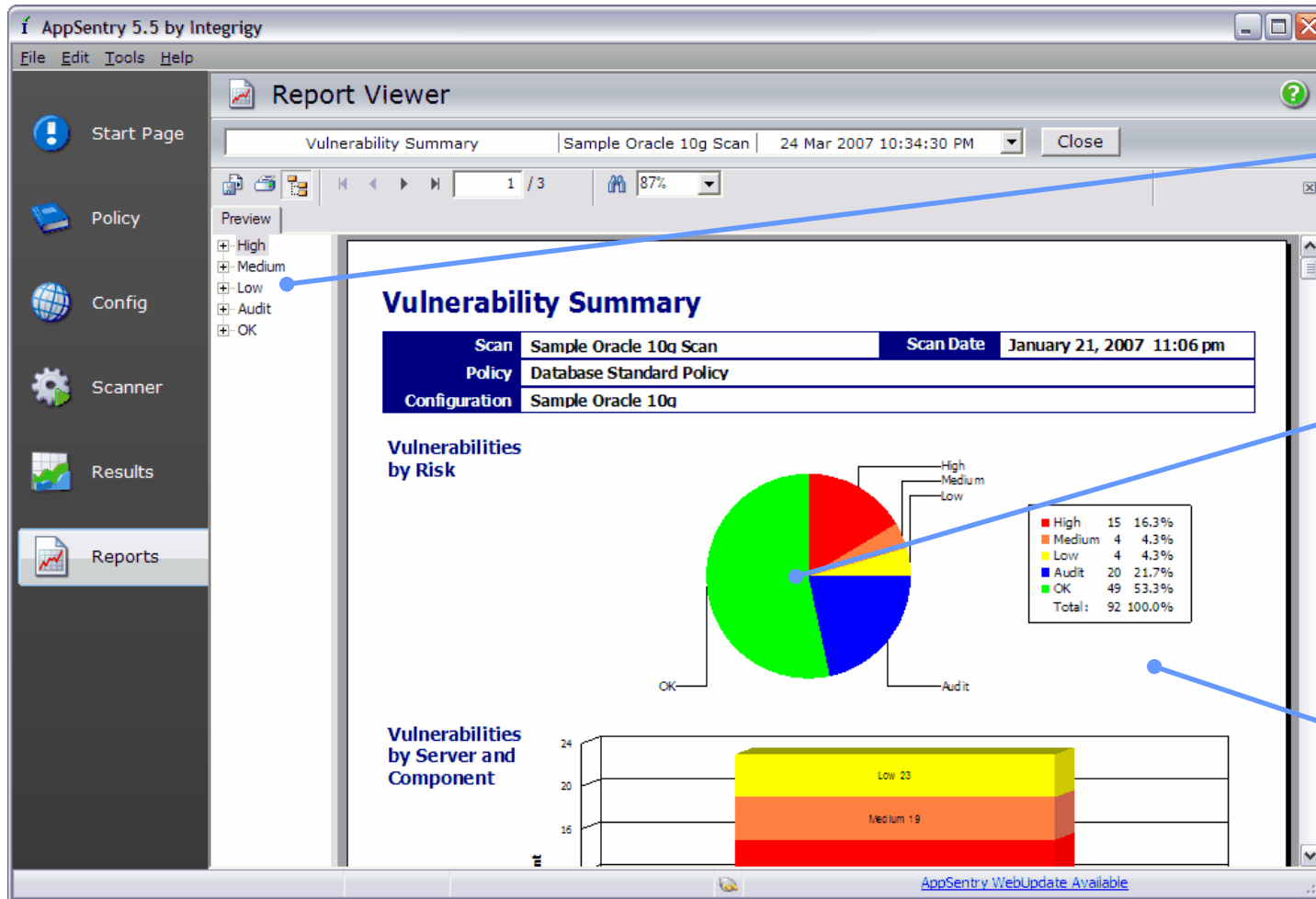
The 'Results Browser' pane on the right shows a hierarchical view of vulnerabilities, categorized by severity: High (311), Medium (2), and Low (16). The 'Medium' category is expanded, showing specific findings such as 'AUDIT\_SYS\_OPERATIONS Set to TRUE' and 'Critical Patch Update January 2007 Application Patches'. The 'Details' section for the selected patch update provides further information: 'Critical Patch Update January 2007 Applications Patch AP Employee Taxpayer ID Display Not Applied'. The 'Summary' section states: 'Critical Patch Update January 2007 Applications Patch AP Employee Taxpayer ID Display Not Applied'. The 'Details' section states: '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 ='. The bottom of the window indicates 'AppSentry WebUpdate Available'.

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

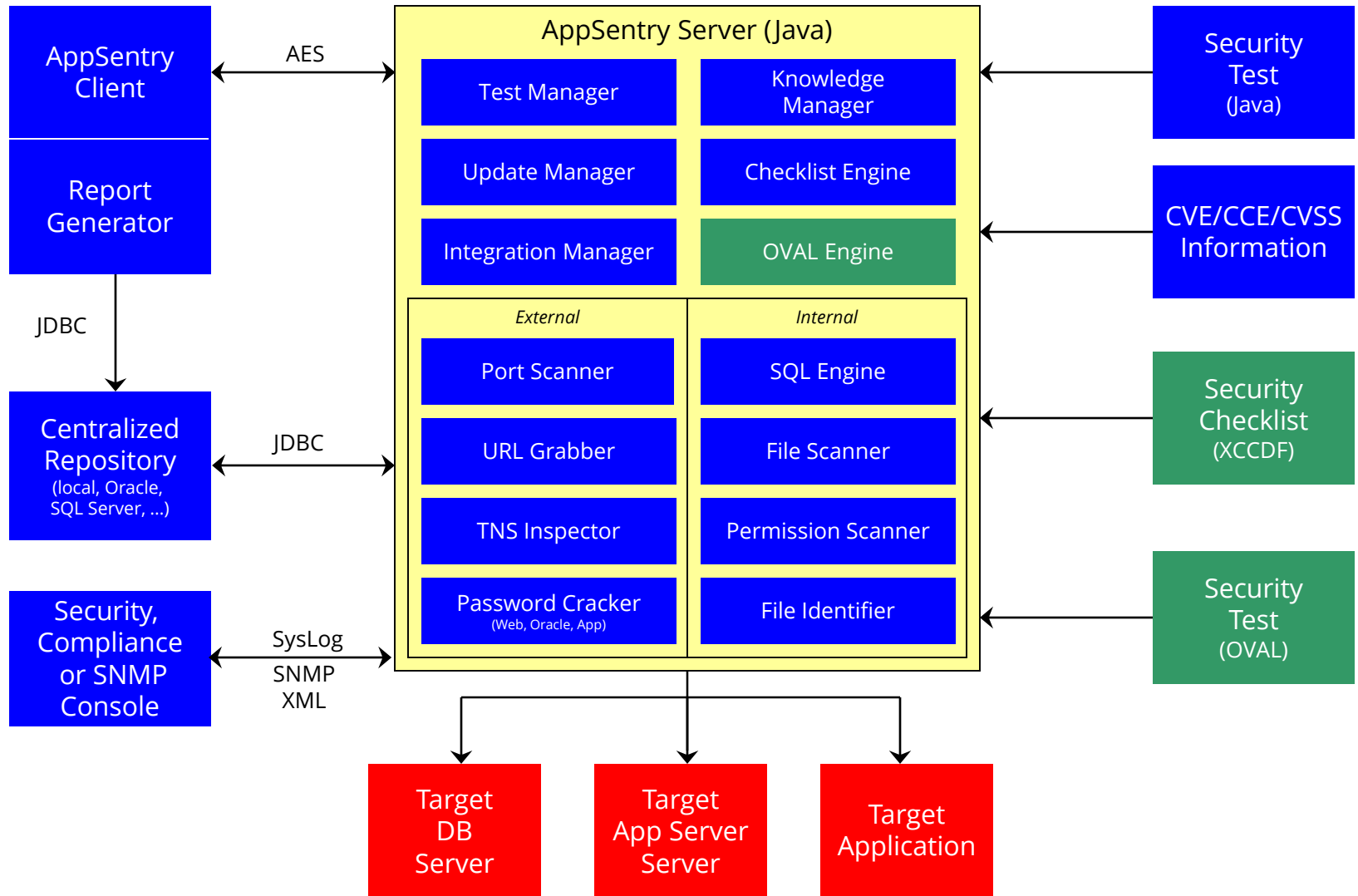


Reports are interactive and some allow drill-down into detailed information

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



# Current AppSentry Modules

## Oracle Database

- 8i (8.1.7)
- 9i (9.0.1, 9.2.0)
- 10g (10.1, 10.2)
- 11g (11.1, 11.2)
- 12c (12.1)

## Oracle E-Business Suite

- 11i (11.5.1 – 11.5.10 CU2)
- R12 (12.0, 12.1, 12.2)

## 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

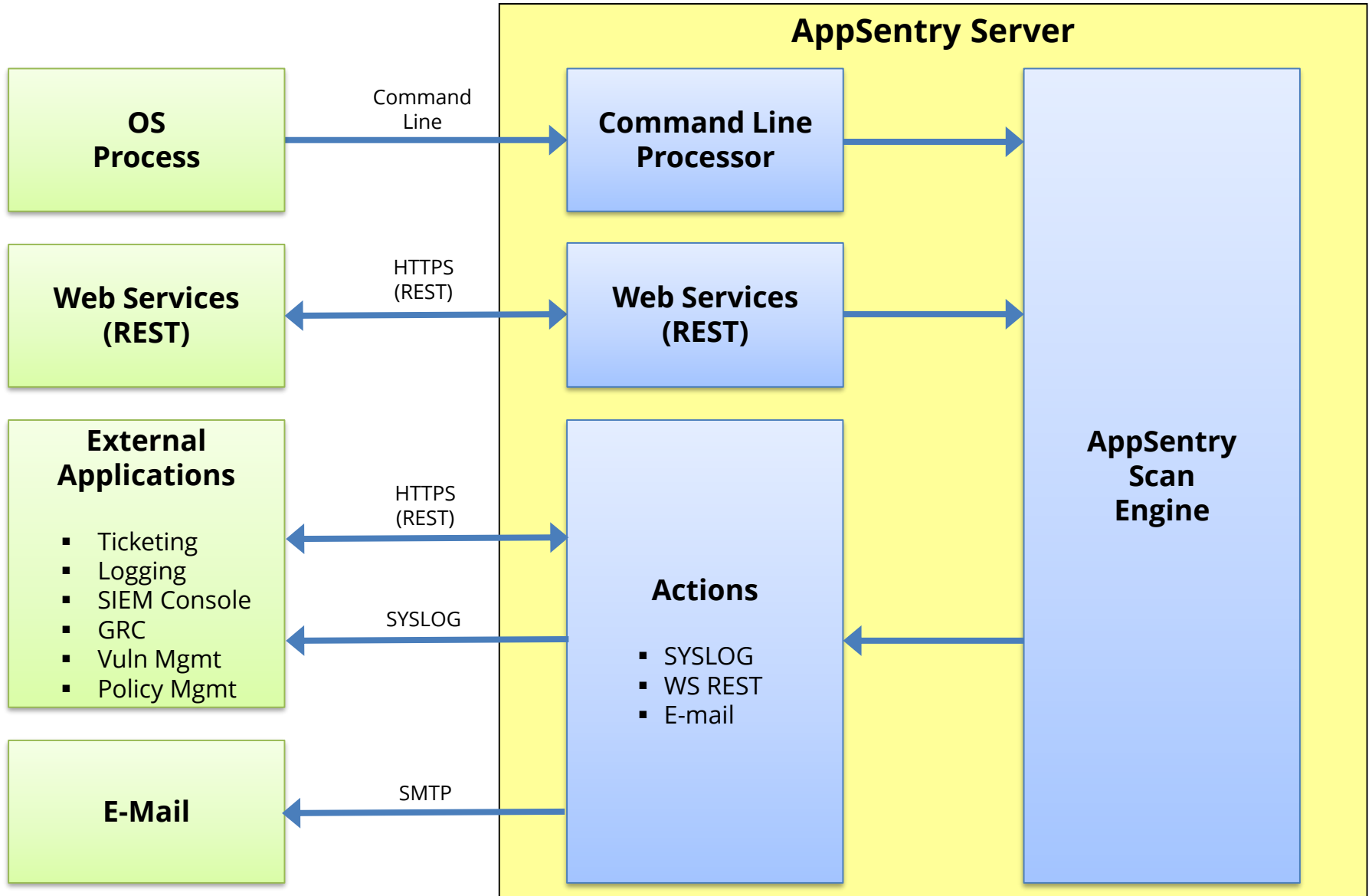
- 2000
- 2005
- 2008, 2008 R2
- 2012
- 2014
- 2016 (under development)

# AppSentry Modules in Development or Planned

Databases	Applications	Application Servers
<p><b><u>Relational</u></b></p> <ul style="list-style-type: none"><li>▪ Oracle MySQL*</li><li>▪ MariaDB*</li><li>▪ Sybase ASE*</li><li>▪ IBM DB2 (LUW)*</li><li>▪ PostgreSQL</li><li>▪ Teradata</li><li>▪ Informix</li><li>▪ Apache Derby</li><li>▪ SAP MaxDB</li></ul> <p><b><u>No SQL</u></b></p> <ul style="list-style-type: none"><li>▪ Cassandra</li><li>▪ MongoDB</li><li>▪ Hadoop</li></ul>	<ul style="list-style-type: none"><li>▪ Oracle Business Intelligence (OBIEE)*</li><li>▪ Oracle Fusion Applications*</li><li>▪ PeopleSoft</li><li>▪ SAP</li></ul>	<ul style="list-style-type: none"><li>▪ Oracle WebLogic*</li><li>▪ Oracle Fusion Middleware*</li><li>▪ Apache</li><li>▪ Tomcat</li><li>▪ IBM WebSphere</li></ul>

\* Available as a consulting engagement to automate organization's security standard

# AppSentry Integration Architecture





# AppSentry @In

**AppSentry** imports data from multiple sources and additional custom imports can be developed.

<b>Assets</b>	<ul style="list-style-type: none"><li>▪ Comma delimited (CSV)</li><li>▪ Oracle TNS Names</li><li>▪ [Future] ARF - Asset Reporting Format</li><li>▪ [Future] Oracle Enterprise Manager Import</li><li>▪ [Future] SQL Server management tools</li></ul>
<b>Policies and Security Checks (SCAP)</b>	<ul style="list-style-type: none"><li>▪ XCCDF - Extensible Configuration Checklist Description Format</li><li>▪ OVAL - Open Vulnerability and Assessment Language</li><li>▪ OCIL - Open Checklist Interactive Language</li></ul>
<b>Security Data</b>	<ul style="list-style-type: none"><li>▪ CVE - Common Vulnerabilities and Exposures</li><li>▪ CPE - Common Platform Enumeration</li><li>▪ CCE - Common Configuration Enumeration</li></ul>

# AppSentry – Web Services (REST)

**AppSentry** can be controlled through a REST web service to add assets, run scans, and retrieve reports

<b>Policies</b>	<ul style="list-style-type: none"><li>▪ List Policies (/policy/list)</li></ul>
<b>Assets</b>	<ul style="list-style-type: none"><li>▪ List Assets (/asset/list)</li><li>▪ Add Asset (/asset/add)</li></ul>
<b>Scans</b>	<ul style="list-style-type: none"><li>▪ Run Scan (/scan/run)</li><li>▪ Scan Status (/scan/status)</li><li>▪ Scan Summary (/scan/summary)</li><li>▪ Scan Finding (/scan/finding)</li><li>▪ Run Report (/report/run)</li></ul>

# AppSentry Reporting

- **Eclipse BIRT used for reporting**
- **Export reports**
  - PDF, Excel, Word, CSV, HTML, Open Document, ...
- **65 standard reports**
- **Ad-hoc and custom reports**
  - Columns, grouping and sort order
- **Customize report headers and footers**
  - Custom header and footer fields for all reports
  - Use open-source BIRT report designer for advanced customization of report templates
- **Develop new reports**
  - Use open-source BIRT report designer for new reports

# AppSentry Compliance Reports

- **Integrigy database security baseline**
- **Payment Card Industry (PCI-DSS)**
- **HIPAA**
- **FISMA NIST 800-53**
- **DoD DISA STIG**

# AppSentry @Out

**AppSentry** integrates with third-party security management systems and log management platforms

<b>Protocols</b>	<ul style="list-style-type: none"><li>▪ Syslog</li><li>▪ Web Service - REST</li><li>▪ E-mail (smtp)</li> <li>▪ SNMP trap</li><li>▪ File</li><li>▪ JDBC</li><li>▪ Socket/SSLSocket</li><li>▪ Custom Logback appenders</li></ul>
<b>Formats</b>	<ul style="list-style-type: none"><li>▪ XCCDF - Extensible Configuration Checklist Description Format</li><li>▪ ArcSight CEF</li><li>▪ OpenFISMA</li><li>▪ [Future] Archer GRC</li></ul>

# AppSentry @Out – Actions

**AppSentry** actions allow for scan results and findings to be integrated with ticketing, security, and logging systems.

- Supports SYSLOG, REST, and e-mail
- Executed after each scan and for each finding
- Action filter on risk level (high, medium, low, info, OK, error) or number of results
- Define action payload using scan fields – free form text with fields
- Authentication fixed per action

Scan Fields	
scan_name asset_name policy_name scan_start reference	
Summary	Finding
scan_status scan_start scan_end result_count result_count_risk	result_id result_key check_name risk_level server port title data description [CDATA] solution[CDATA] cve_id software version

# Contact Information

**Integrigy Corporation**

web: **[www.integrigy.com](http://www.integrigy.com)**

e-mail: **[info@integrigy.com](mailto:info@integrigy.com)**

blog: **[integrigy.com/oracle-security-blog](http://integrigy.com/oracle-security-blog)**

phone: **888-542-4802**