

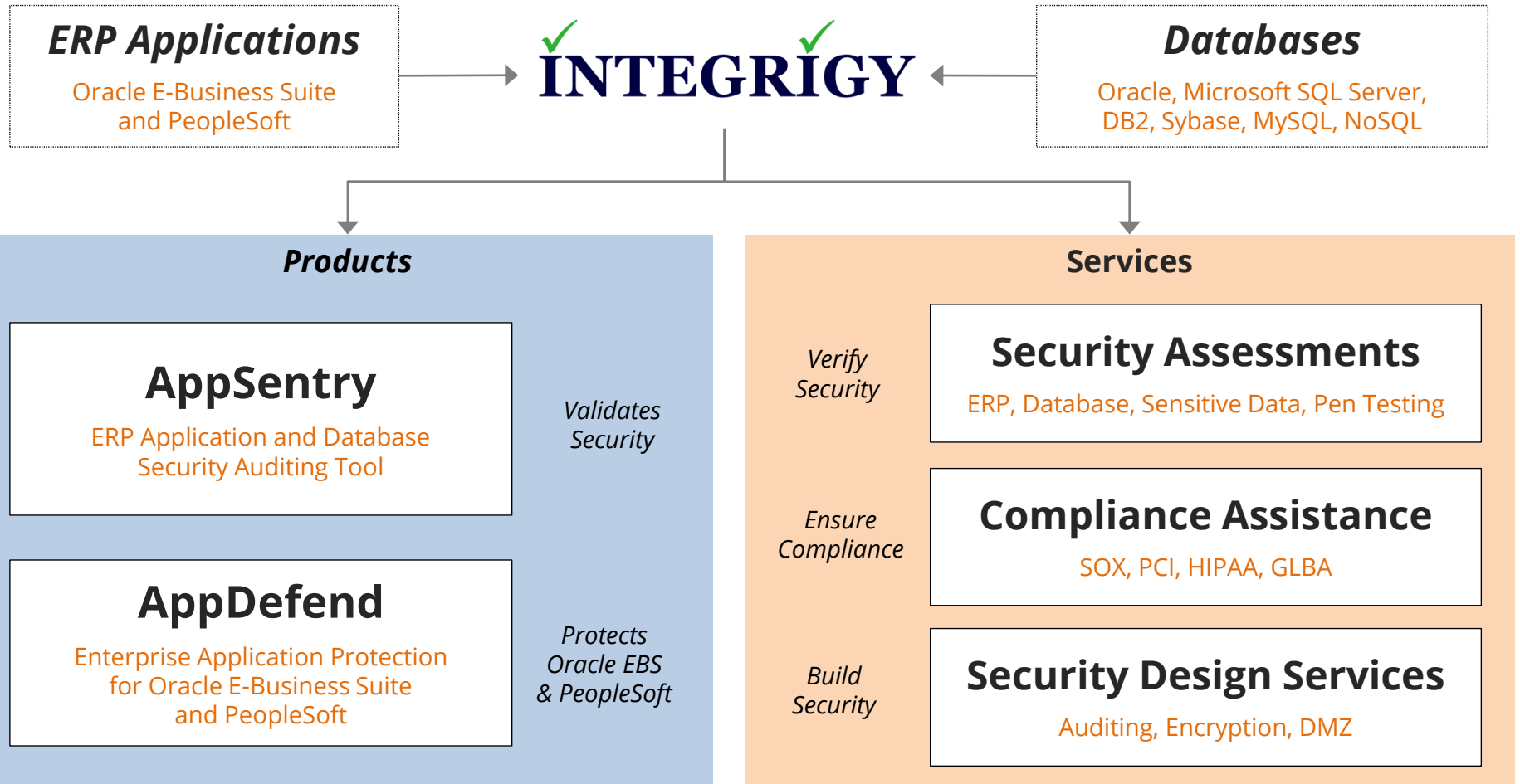
AppSentry

ERP Application and Database Security Auditing

June 2021

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

About Integrigy



Integrigy Research Team

ERP Application and Database Security Research



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 Integriqy's products remains at the sole discretion of Integriqy.

AppSentry

Security scanner for databases, application servers, and ERP packages

- Performs advanced penetration testing and in-depth security and controls auditing
- Performs over 1,000+ 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 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, 3rd party integration, automatic updates, no agents, network and operating system included

Oracle EBS Security

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

Database Security

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

Security Reports

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

Using AppSentry

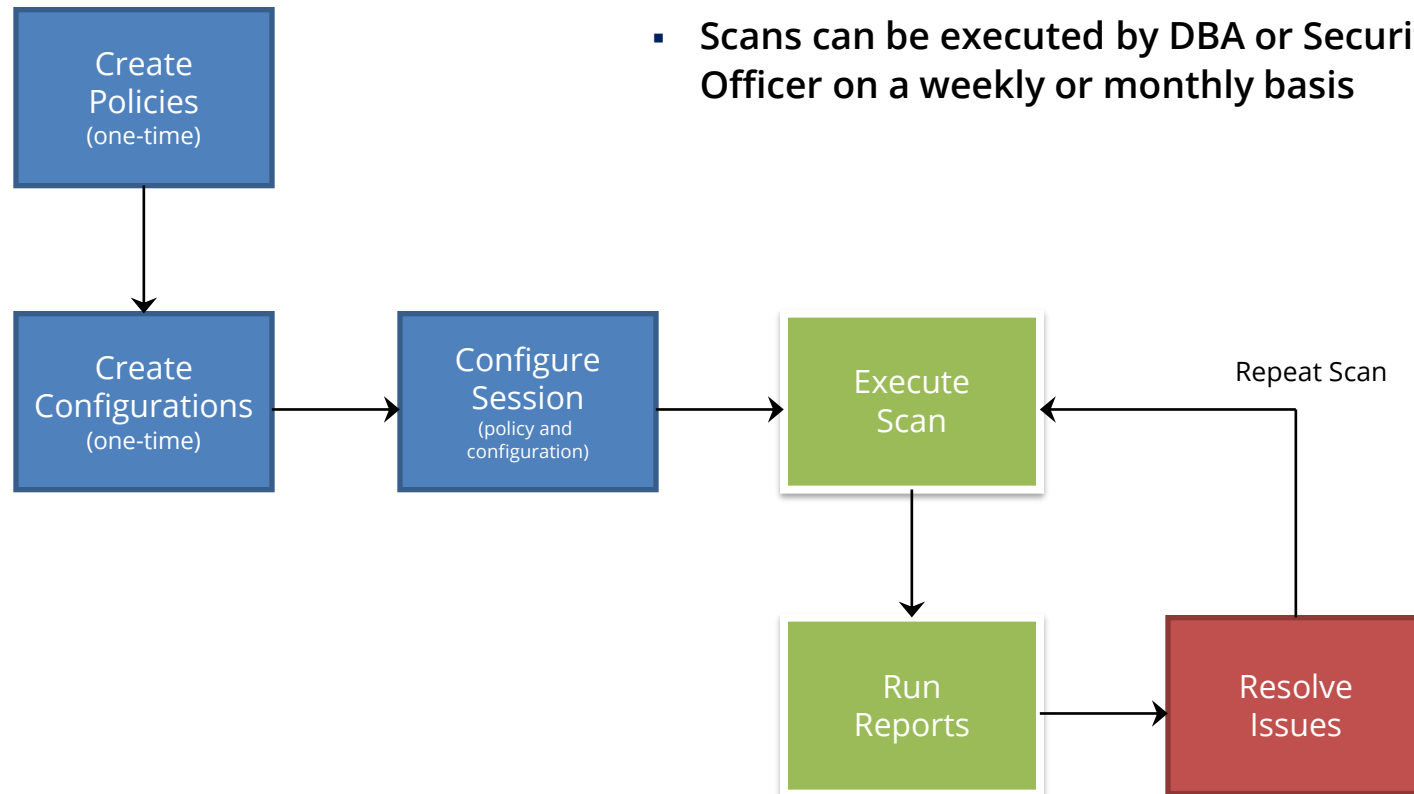
- Simple to use – task-oriented GUI
- Comprehensive descriptions and solutions for identified vulnerabilities
- AppSentry Users
 - IT Security
 - Internal Audit
 - Oracle DBAs
 - Oracle Project Team – IT
 - Oracle Project Team – Functional/Business Owner

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

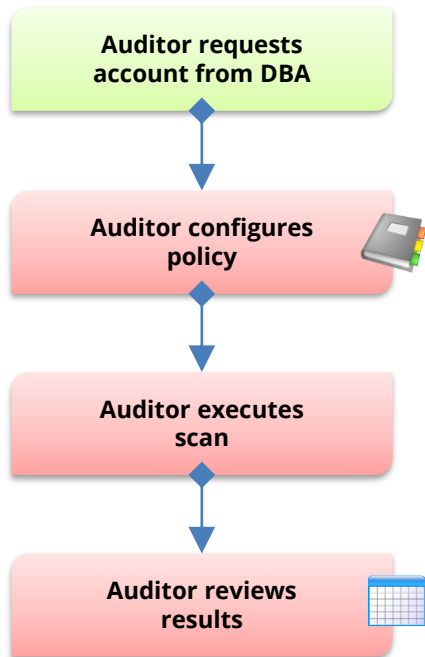
AppSentry Workflow

- 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

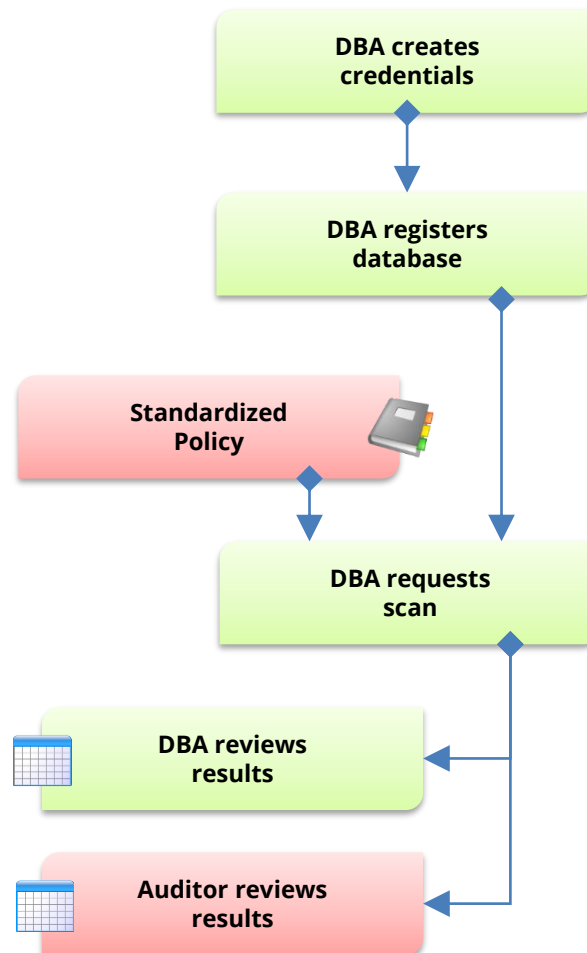


AppSentry Standard Usage Models

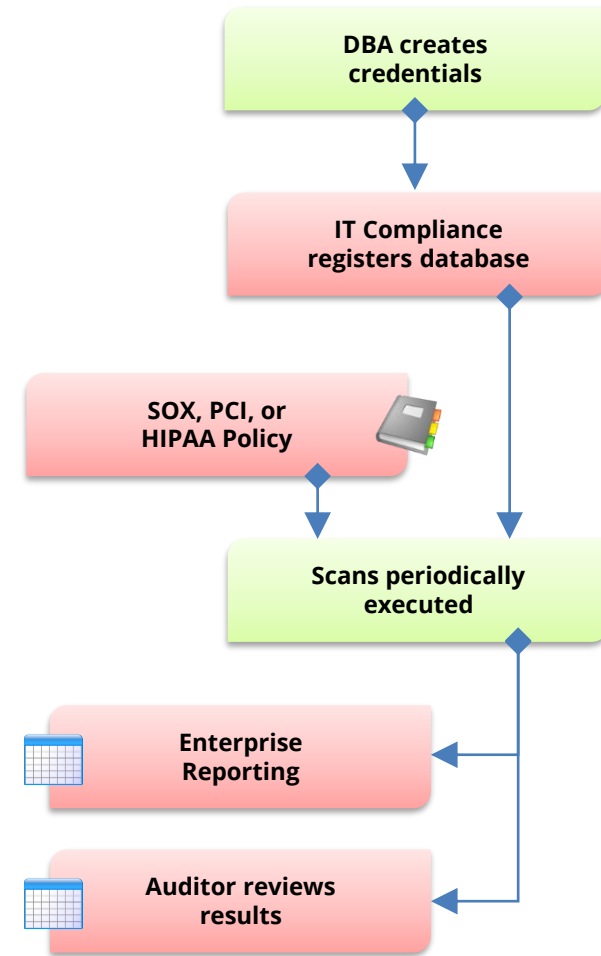
Auditor (standalone or server)



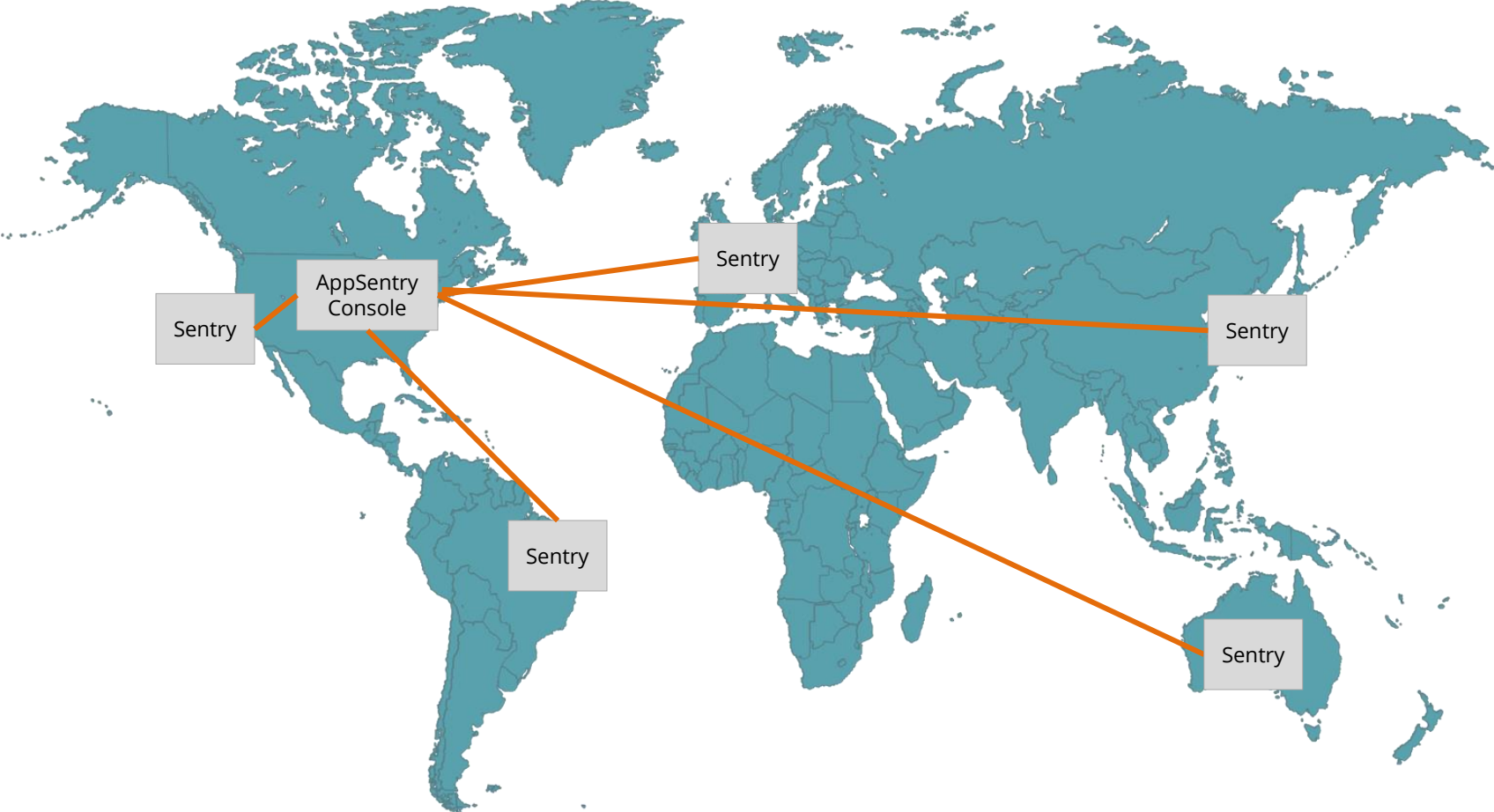
Self-Service DBA



Compliance/ Certification



AppSentry Distributed



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	USB	<ul style="list-style-type: none">▪ For auditors travelling▪ Synchronize or archive to central server
	Desktop/ Laptop	<ul style="list-style-type: none">▪ Single user, local installation
Server	Physical or Virtual Server	<ul style="list-style-type: none">▪ Multi-user solution on dedicated hardware▪ Operating system Linux or Windows
	Virtual Appliance	<ul style="list-style-type: none">▪ Docker image▪ Open Virtualization Format (OVF) appliance
Cloud	Private Cloud	<ul style="list-style-type: none">▪ Java-capable cloud solutions (Amazon, Google, Oracle, ...)
	Public Cloud (demonstration)	<ul style="list-style-type: none">▪ Integrigy hosted solution at Amazon AWS

AppSentry – Policies

The screenshot shows the AppSentry interface with a sidebar on the left containing navigation items: Dashboard, Assets, Policies (highlighted), Assessment, Results, and Internal. The main content area is titled 'Policies' and shows a breadcrumb trail for 'Database Standard Policy'. A 'Delete' button is visible in the top right. A left-hand navigation pane lists various policy categories under 'Oracle Database', with 'Patch Policy and Critical Patch Updates' selected. The main configuration area displays a table of properties and values:

Property	Value
Grace Period in Days	30
If Not Applied During Grace	INFO
If Not Applied After Grace	HIGH

Below the table, the 'Patch Policy' section is expanded, showing a detailed description of the policy and a note.

Patch Policy

The patch policy defines the enterprise security patching policy for the Oracle Database, Oracle Application Server, and Oracle Applications. Most policies define a set number of days from patch release to when the patch must be applied. Typically, this grace period is used for testing and patch verification. If a specific Oracle Critical Patch Update (CPU) is deemed severe or should be applied before the grace period, an action can be defined for each CPU.

Note: The CPU check covers only supported database versions for the Critical Patch Updates. AppSentry will not

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 – Policies

The screenshot shows the AppSentry interface with the 'Policies' section selected. The 'Database Standard Policy' is active, and the 'System and Privileges' category is expanded. The table below shows the configuration for various Oracle database system privileges.

	Public	User	Role	
ALTER SYSTEM	AUDIT	NONE	NONE	⌵
AUDIT SYSTEM	AUDIT	NONE	NONE	⌵
CREATE SESSION	AUDIT	NONE	NONE	⌵
ALTER SESSION	NONE	NONE	NONE	⌵
RESTRICTED SESSION	NONE	NONE	NONE	⌵
SYSDBA	NONE	HIGH	NONE	⌵
SYSOPER	NONE	NONE	NONE	⌵
AUDIT ANY	NONE	NONE	NONE	⌵
ALTER DATABASE	NONE	NONE	NONE	⌵
ALTER RESOURCE COST	NONE	NONE	NONE	⌵
ANALYZE ANY	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 included in the 'System Privileges Analysis' report, a security vulnerability with the marked level will be generated if PUBLIC, any users, or any roles are assigned this system privilege.

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 - Assets

Assets < DB12102C.integrity.com_PDB2

Validate Delete

Asset Information

Property	Value
Deployment	PROD
Owner	Finance IT
Contact	finance@integrity.com

Connection

Property	Value
Server Hostname/IP Address	db2.integrity.com
Database TNS Port	1526
Oracle SID/Service Name	pdb2.integrity.com

The fully qualified hostname or IP address for the server. For Oracle RAC databases, AppSentry will connect to one node and discover the other RAC nodes. All RAC nodes will be scanned.

Credentials

Property	Value
Database Username	appentry_scanner
Database Password	*****

Administration User Settings About

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

Detailed information is included for each configuration setting

AppSentry will load configuration information from environment such as RAC nodes or all EBS servers (app, web, etc.) from single database connection

AppSentry - Assessments

APPSENTRY

Dashboard Assets Policies Assessment Results Internal Administration User Settings About

Scan Assets Scheduled Scans

Target Type: Oracle Database Policy: Database Standard Policy

Name	Last Scan Date
Test	03/21/2019 08:54:34 AM
Client C PRODR12	none
Client D EBSFIN	none
<input checked="" type="checkbox"/> DB11204	none
<input checked="" type="checkbox"/> DB12102.integrity.com	none
<input checked="" type="checkbox"/> ORA112	none
DB12102C.integrity.com_PDB2	none
DB12101	05/07/2019 10:21:48 PM
<input checked="" type="checkbox"/> DB12102C.integrity.com	none
DB12102C.integrity.com_CDBROOT	none
DB12102C.integrity.com_PDB1	none
<input checked="" type="checkbox"/> EBSDB VIS 12.1.3	none
Test1	none
TestAB	02/19/2019 11:42:15 PM
New DB	none
Test DB2	none

Now Start At: 7/29/2019 3:00 PM

Once Every 1 Months

Schedule Scan

Running an assessment is as simple as choosing a configuration and policy and clicking start

Multiple assets may be included in an assessment

Assessments may be scheduled and repeated by days, weeks, or months

AppSentry - Results

The screenshot displays the AppSentry Results interface. The left sidebar contains navigation options: Dashboard, Assets, Policies, Assessment, Results (selected), Internal, Administration, User Settings, and About. The main content area shows the Results page for a scan on 2019-07-29 17:58:28. The overall risk level is High. The scan summary shows 383 findings. The findings are categorized by risk: High (383) 78%, OK (74), Excluded (1) 0%, Medium, Information, Low, and Audit. A bar chart shows findings for the last 5 scans, and a table provides scan information.

Scan Information	
Name	2019-07-29 17:58:28
Policy	Database Standard Policy
Start	07/29/2019 01:58:28 PM
End	07/29/2019 01:58:38 PM
Status	Completed

Findings for Last 5 Scans	
2019-07-29 17:35:16	High (383) 78%
2019-07-29 17:36:45	High (383) 78%
2019-07-29 17:38:18	High (383) 78%
2019-07-29 17:56:01	High (383) 78%
2019-07-29 17:58:28	High (383) 78%

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

Results < 2019-07-29 17:58:28

Summary Result Browser Reports Manager Change Data Audit Comparison

General

- Vulnerability Summary
- CVE Cross-Reference
- CVE Cross-Reference Unpatched
- Oracle Vulnerabilities Unpatched
- Vulnerability Detail

Oracle Database

- Database Account Password Issues
- Database Account Password Review
- Access to System Tables and DBA Views
- System Privileges Analysis
- Access to System Tables (Individual)
- Database Accounts
- Database Audit Statements
- Database Component Versions
- Database Profile Password Settings
- Database Links
- Installed Database Components
- Installed Sample Schemas and Accounts
- Non-System Objects in System Tablespace
- Object Privileges Assigned to PUBLIC
- Privileges on Standard Database Packages

Vulnerability Summary

SCAN NAME 2019-07-29 17:58:28 SCAN DATE July 29, 2019 1:58:28 PM
POLICY Database Standard Policy
ASSET DB11204 Test

Vulnerabilities by Risk

Risk Level	Count
High	383
Medium	7
Low	5
Information	1
Audit	22
OK	74
Error	0
Unknown	0
Excluded	1
Total	493

High 76%
Medium 1%
Low 1%
OK 15%
Audit 4%
Information 0%
Excluded 0%
Error 0%

High - 383

1	Archive Log Mode Enabled	Oracle DB
22	Critical Patch Updates (Database)	Oracle DB
351	Default Database Account Passwords	Oracle DB
9	Default Database Accounts Locked and Expired	Oracle DB

Medium - 7

1	Database Accounts with OS Authentication	Oracle DB
1	Init.ora - AUDIT_SYS_OPERATIONS	Oracle DB
1	Init.ora - CT_DICTIONARY_ACCESSABILITY	Oracle DB
1	Init.ora - OS_ROLES	Oracle DB
1	Init.ora - REMOTE_LOGIN_PASSWORDFILE	Oracle DB
1	Init.ora - REMOTE_OS_AUTHENT	Oracle DB
1	Init.ora - TRACF_FILES_PLURIC	Oracle DB

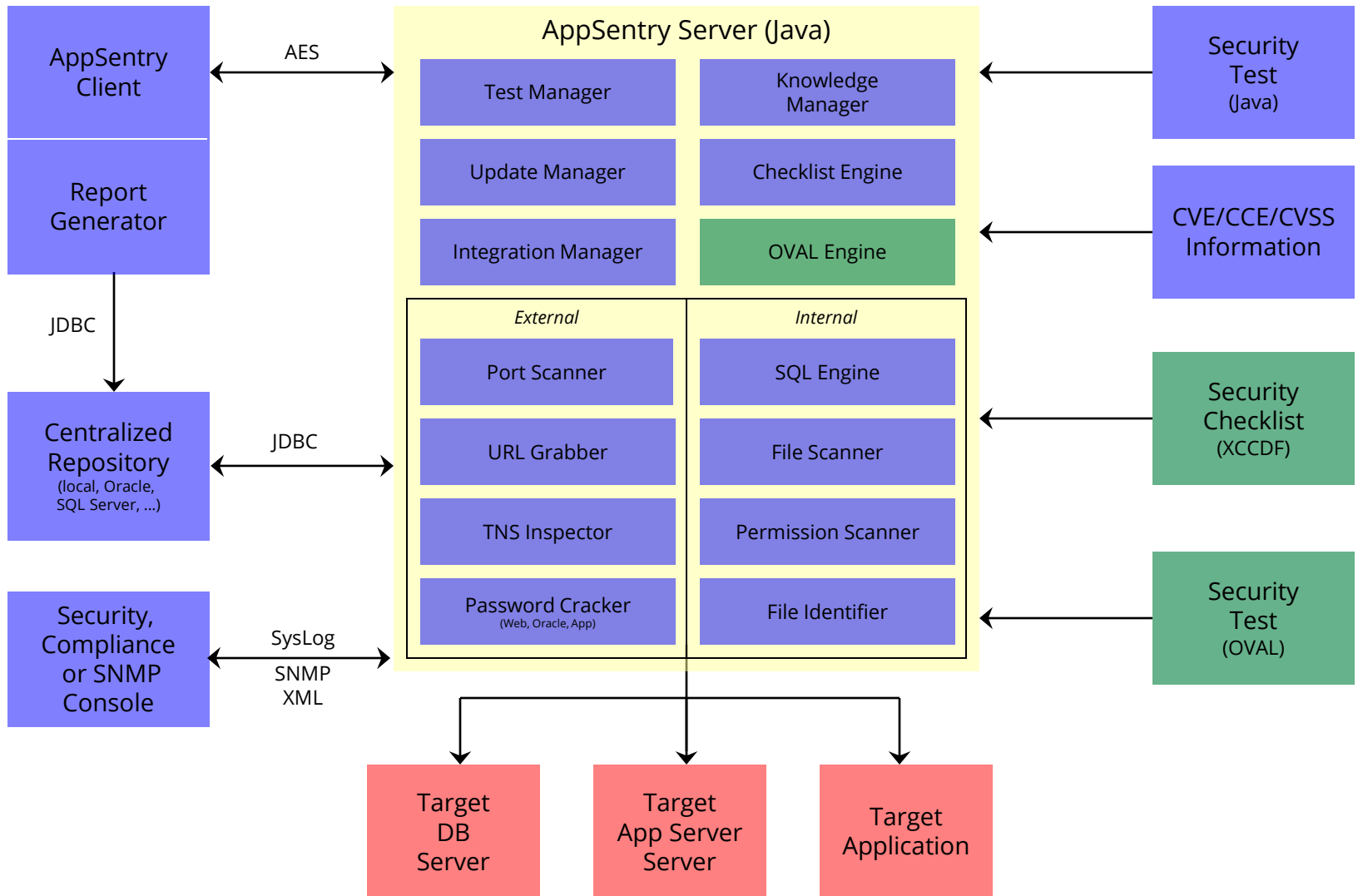
PDF Run Report

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 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, 12.2) 18c (18.x) 19c (19.x)
Oracle E-Business Suite	11i (11.5.1 – 11.5.10 CU2) R12 (12.0, 12.1, 12.2)
Oracle PeopleSoft	9.1, 9.2 PeopleTools 8.53 – 8.58
Microsoft SQL Server	2000 2005 2008, 2008 R2 2012 2014 2016 2017 2019

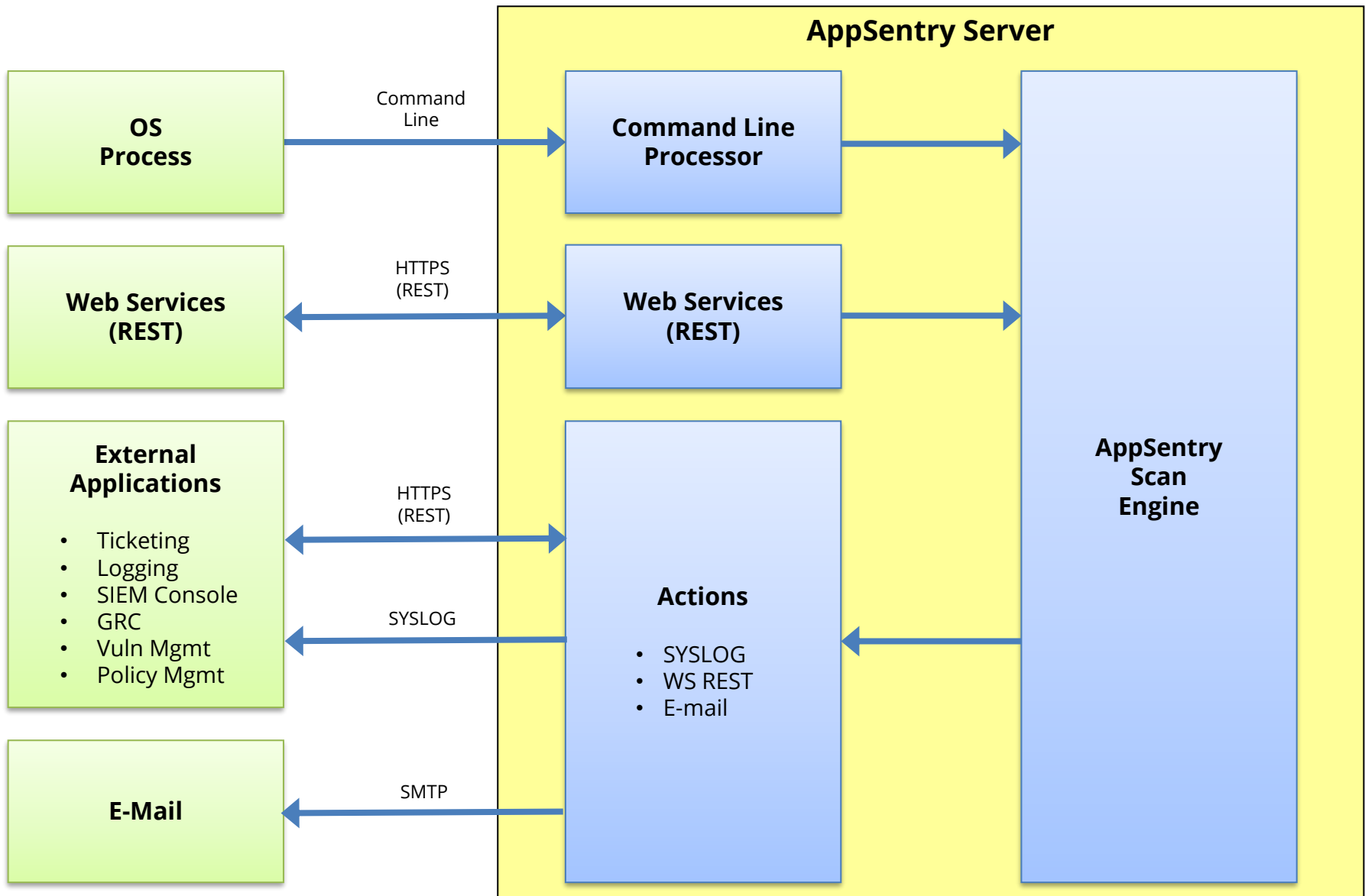
AppSentry Modules in Development or Planned

Databases	Cloud Databases	Applications and Application Servers
<p><u>Relational</u> Oracle MySQL * MariaDB * Sybase ASE IBM DB2 (LUW) * PostgreSQL * Teradata * Informix</p> <p><u>No SQL</u> Cassandra * MongoDB * Hadoop</p>	<p><u>Relational</u> AWS RDS – Oracle * AWS RDS – SQL Server * AWS RDS – MySQL * AWS RDS – MariaDB * AWS RDS – PostgreSQL * AWS Aurora ^ AWS Redshift ^ Azure SQL Database Azure MySQL/PostgreSQL</p> <p><u>No SQL</u> AWS DynamoDB Azure CosmosDB</p>	<p>Oracle Business Intelligence (OBIEE) ^ Oracle APEX ^ Oracle ERP Cloud</p> <p>Oracle WebLogic ^ Oracle Fusion Middleware ^</p>

* Available with base security configuration and vulnerability scanning

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

AppSentry Integration Architecture



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

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

AppSentry – Web Services (REST)

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

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

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

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

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

Integrigy Contact Information

Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**