INTEGRIGY

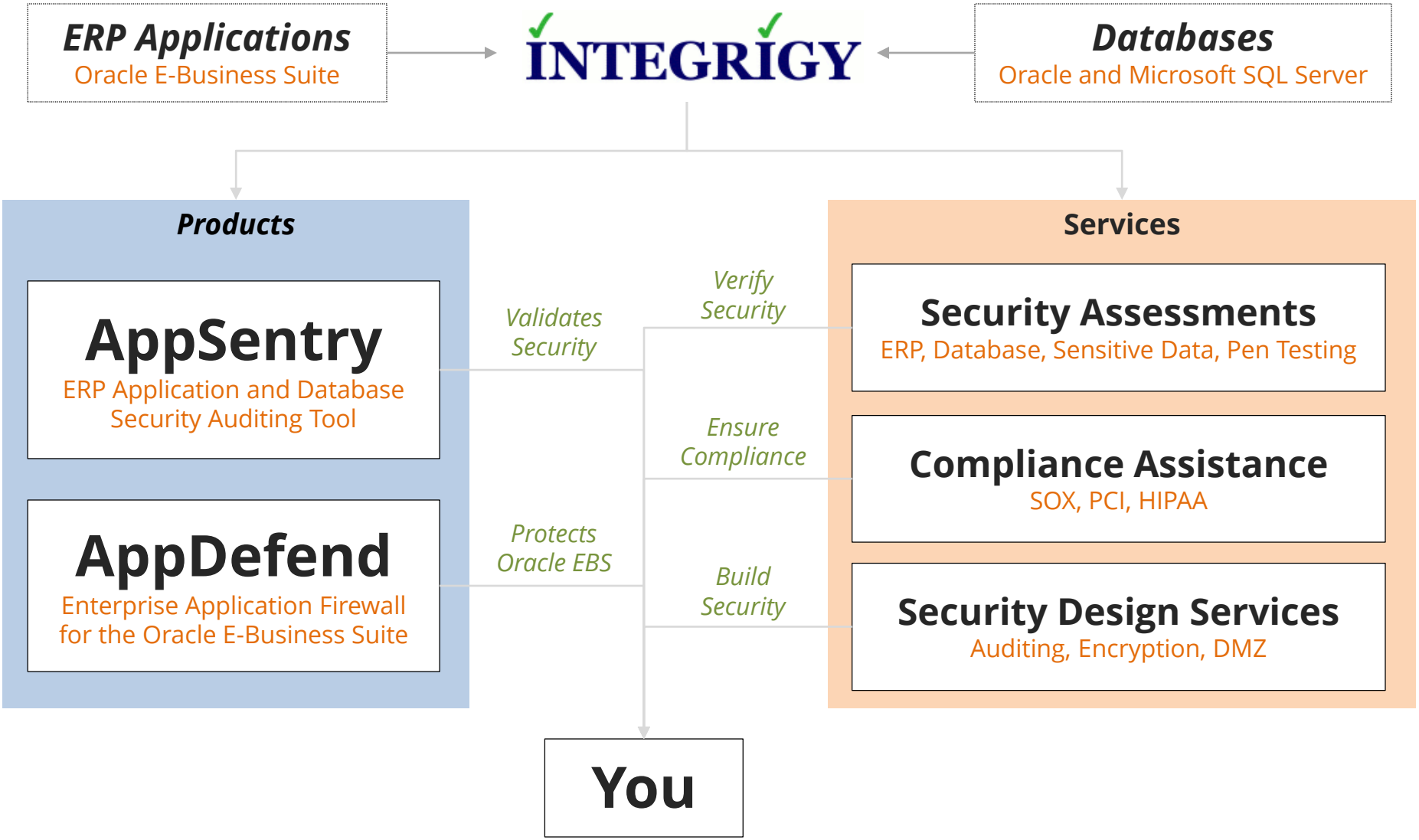
AppSentry

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
Critical Patch Update July 2012	11.5.10 – 12.1.x	▪ Oracle E-Business Suite XSS
Critical Patch Update July 2011	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security configuration issue
Critical Patch Update October 2010	11.5.10 – 12.1.x	▪ 2 Oracle E-Business Suite security weaknesses
Critical Patch Update July 2008	Oracle 11g 11.5.8 – 12.0.x	▪ 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	▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update July 2007	12.0.x 11.5.1 – 11.5.10	▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update October 2005	11.0.x, 11.5.1 – 11.5.10	▪ Default configuration issues
Critical Patch Update July 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update April 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update Jan 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities
Oracle Security Alert #68	Oracle 8i, 9i, 10g	▪ Buffer overflows ▪ Listener information leakage
Oracle Security Alert #67	11.0.x, 11.5.1 – 11.5.8	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	11.0.x, 11.5.1 – 11.5.8	▪ Buffer overflow in FNDWRR.exe
Oracle Security Alert #55	11.5.1 – 11.5.8	▪ 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	▪ 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

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, 3rd party integration, automatic updates, no agents, network and operating system included
- **Database Security**
  Accounts, patches, permissions (e.g. APPS, APPLSYSPUB), 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

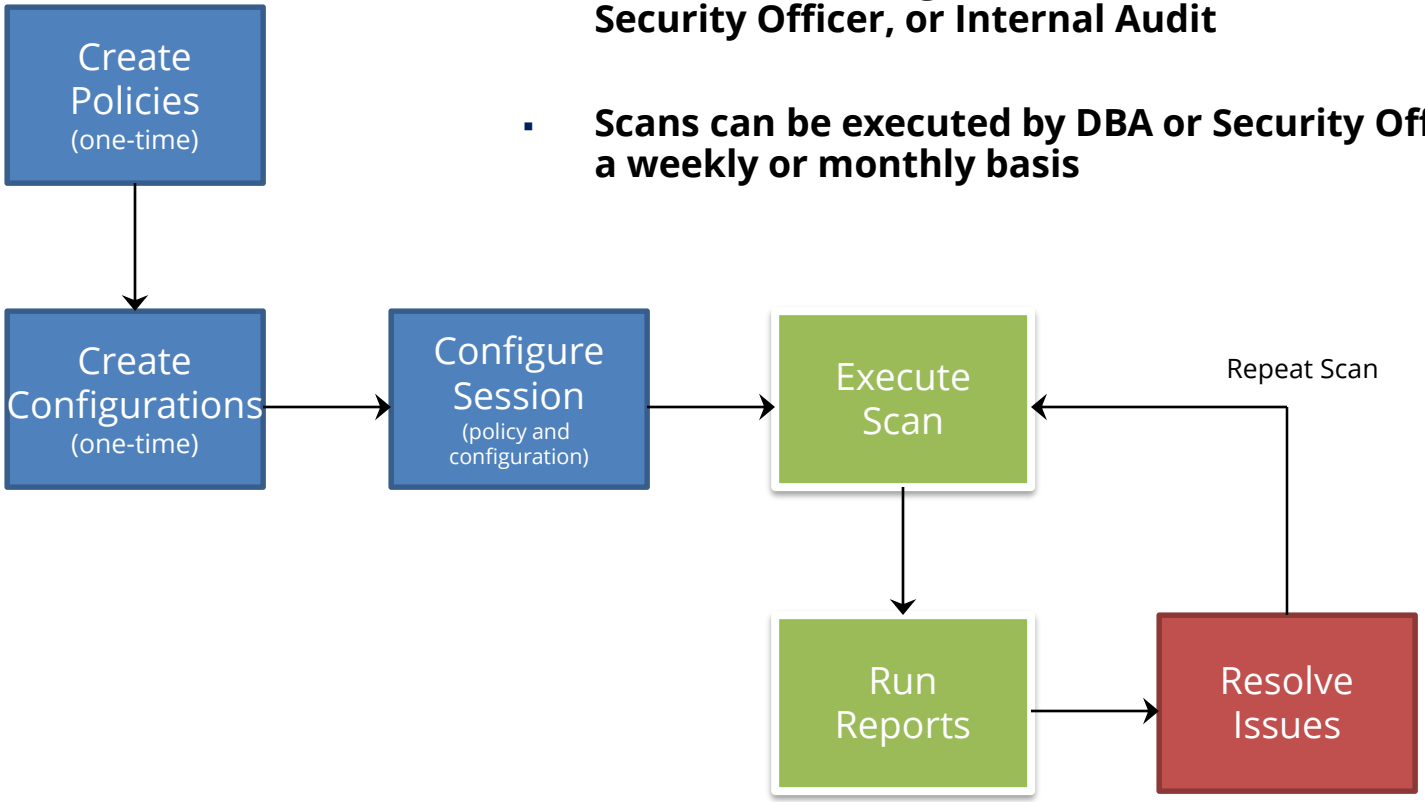
- **Simple to use – task oriented GUI**
- **Comprehensive descriptions and solutions for identified vulnerabilities**
- **AppSentry Users**
  - IT Security
  - Internal Audit
  - Oracle DBAs
  - Oracle Project Team – IT
  - Oracle Project Team – Functional/Business Owner

AppSentry – Automated Audit

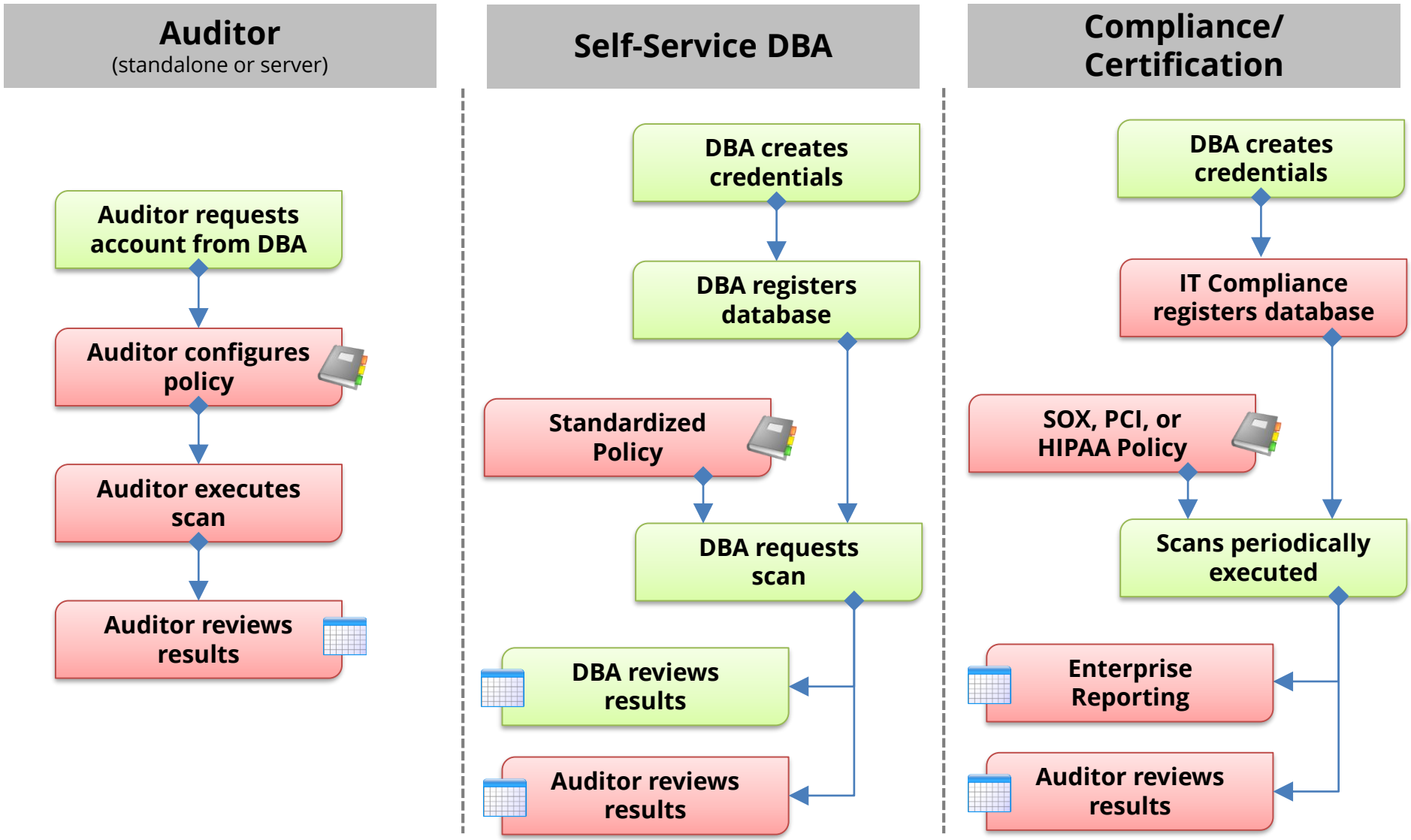
- **Confidence**
  - Audits all layers from operating system to application
  - Downloads updates before every scan
- **Breadth**
  - Performs both security and control audits
- **Productivity**
  - Simple to use
  - Automates auditing and reporting
  - Auditor can focus on more important tasks (e.g., 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



Access and Network Requirements

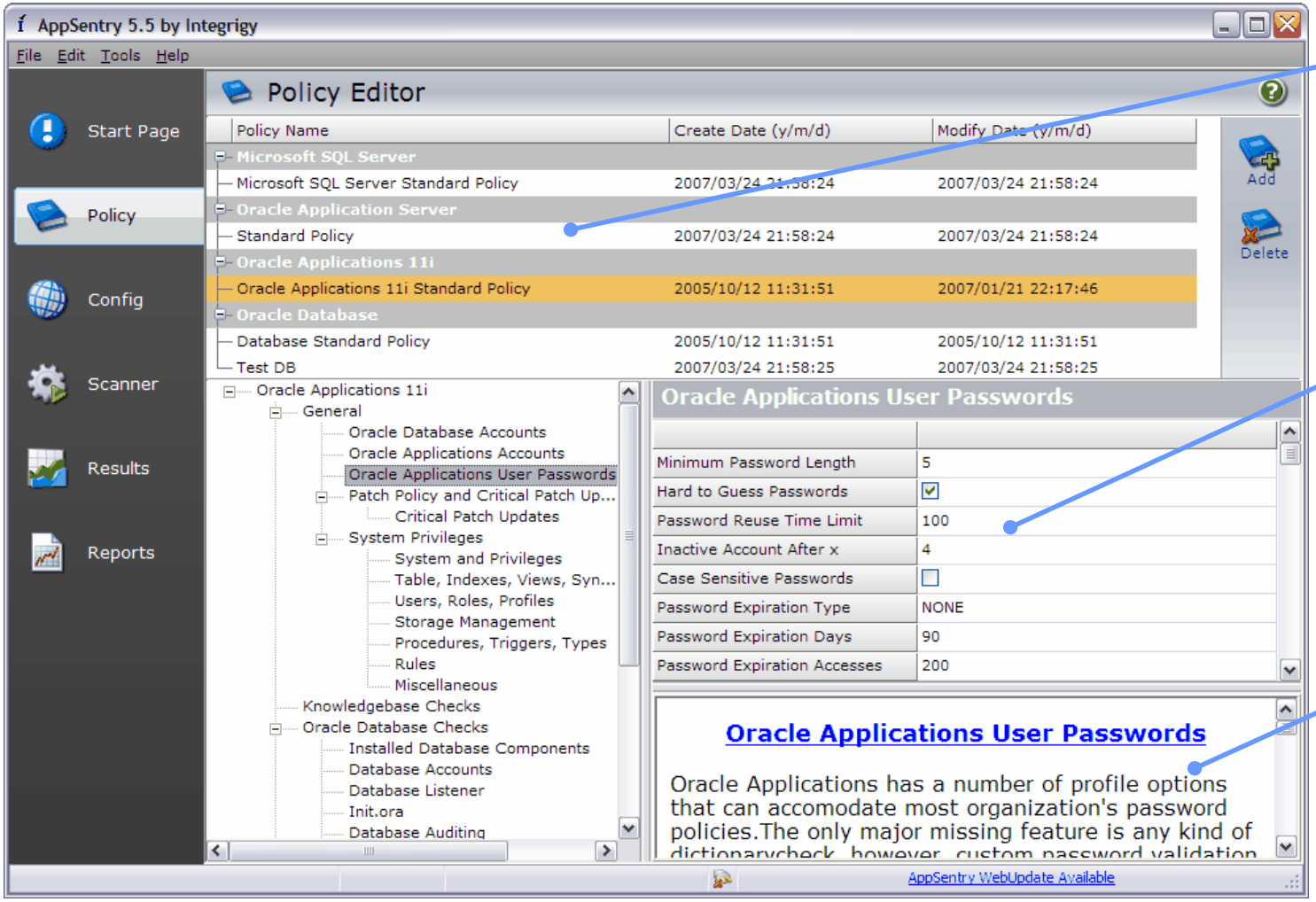
- **AppSentry is a credentialed scanner**
  - A database account is required
  - Oracle = CREATE SESSION, SELECT ANY DICTONARY
  - SQL Server = VIEW ANY DEFINITION, multiple views
  - SQL Server may use an Active Directory account

- **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**	▪ For auditors travelling ▪ Synchronize or archive to central server
	Desktop/ Laptop	▪ Single user, local installation
Server	**Server**	▪ Multi-user solution on dedicated hardware ▪ Operating system Linux or Windows
	Virtual Machine	▪ Multi-user solution on virtualized hardware ▪ Operating system Linux or Windows
	Virtual Appliance (planned)	▪ VMWare packaged (OVF) appliance running Linux JEOS OS
Cloud	**Private Cloud** (planned)	▪ Java-capable cloud solutions with database support
	Public Cloud (demonstration)	▪ Integrigy hosted solution at Amazon AWS

AppSentry – Policy Editor

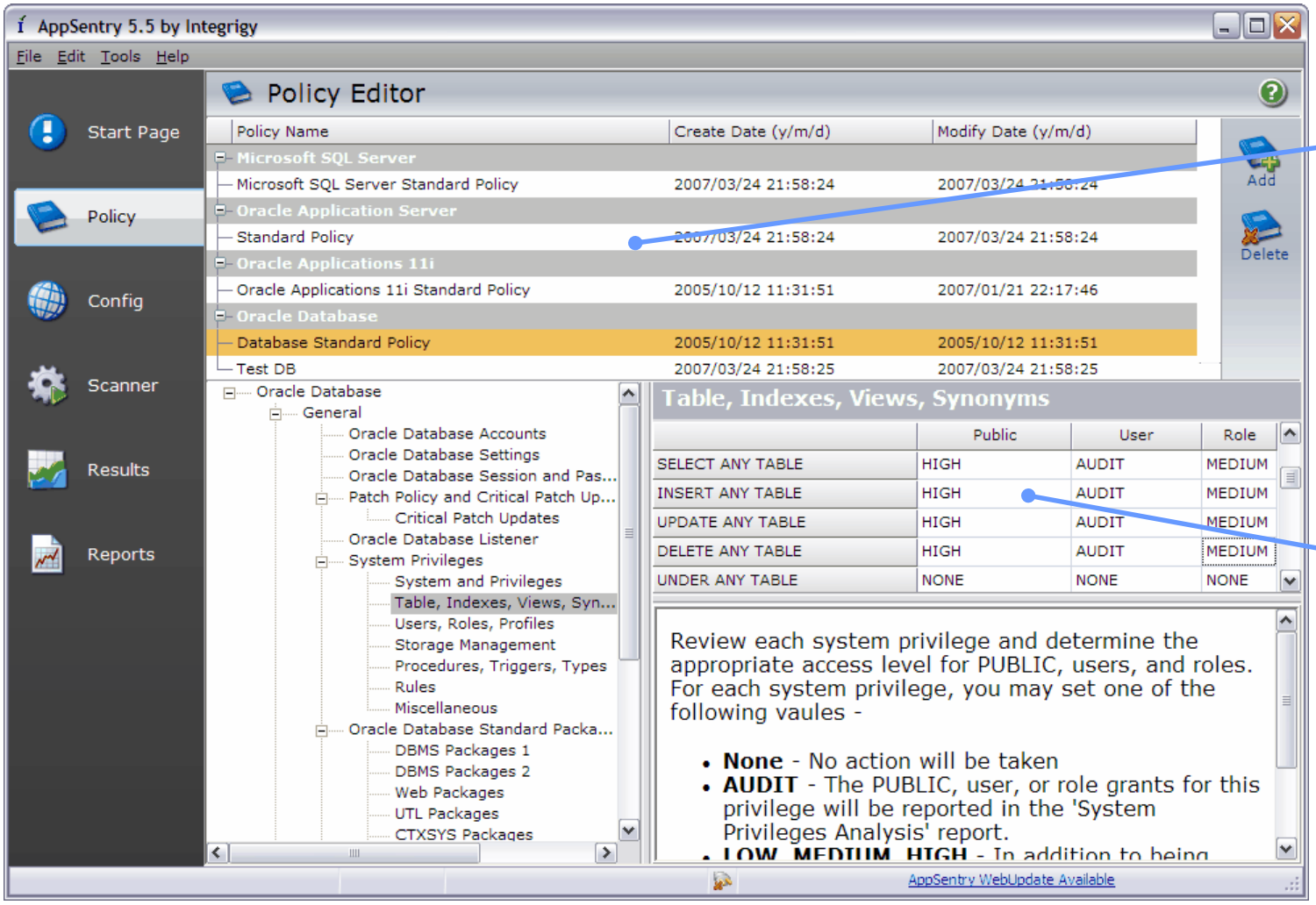


Policies can be defined for different scenarios such as HIPAA, month-end scan, a level of security, or a checklist

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

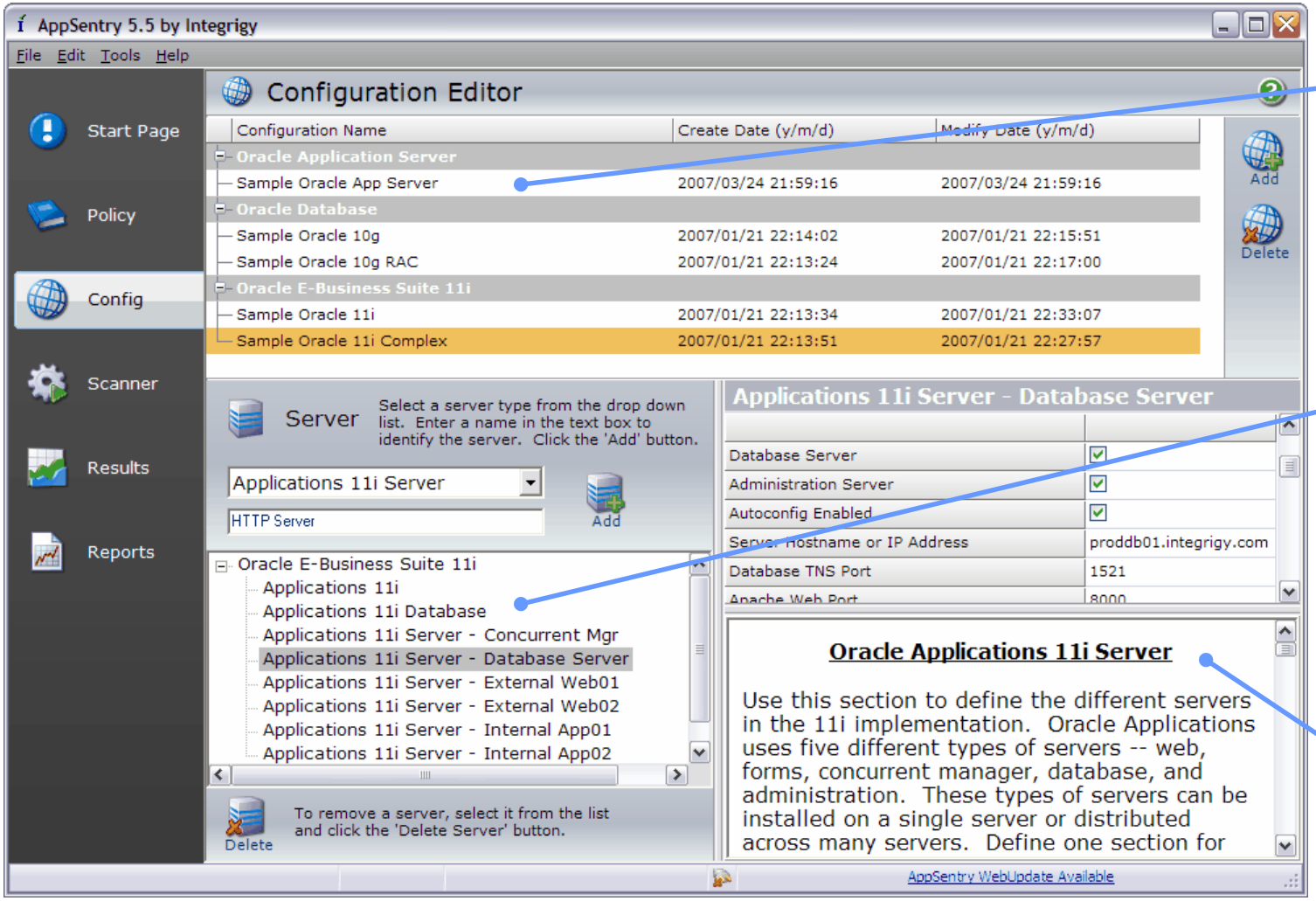
AppSentry – Policy Editor



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

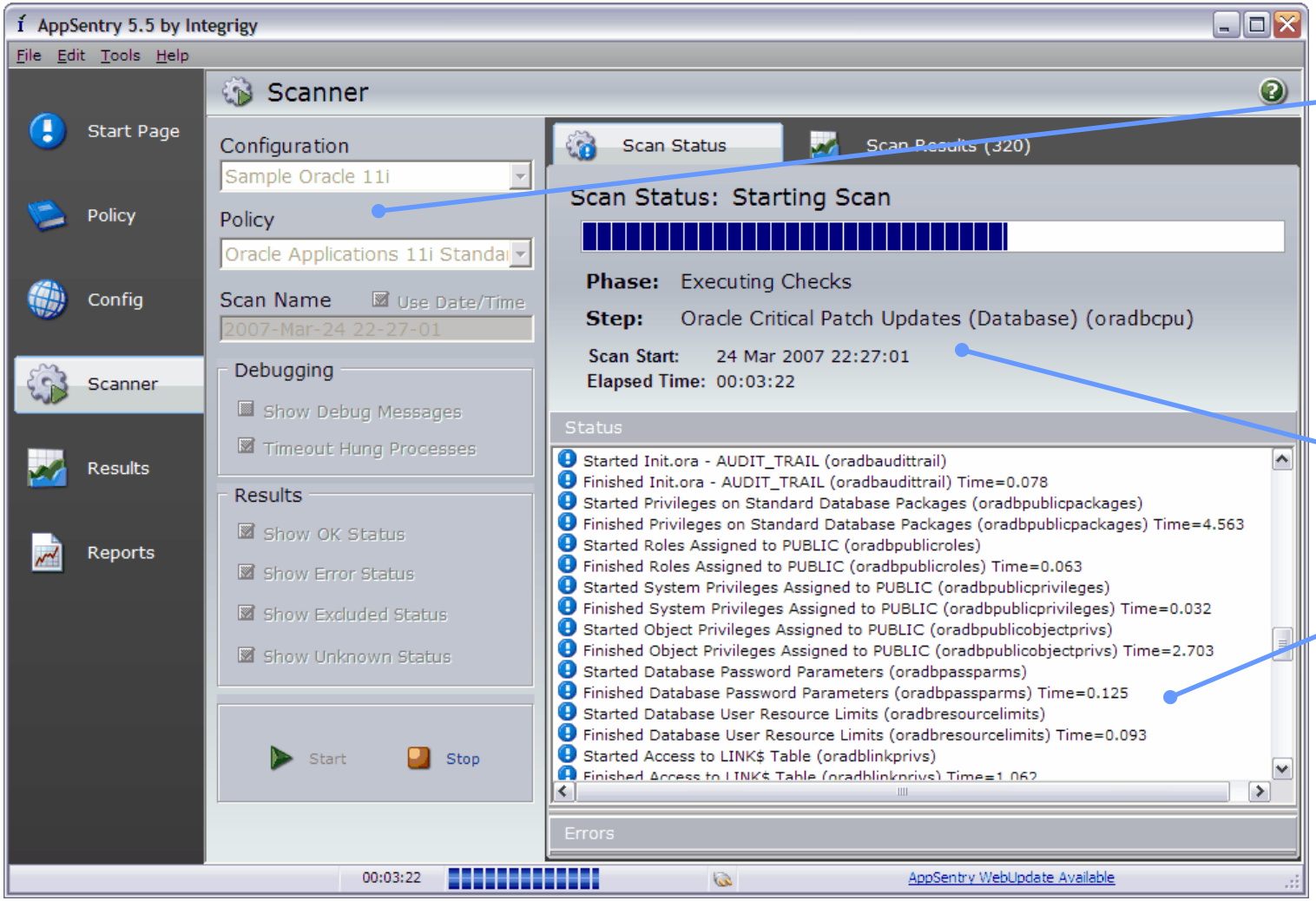


Configurations are defined for different environments including Oracle database, Oracle Application Server, and Oracle E-Business Suite

Complex configurations can be created to handle environments like RAC

Detailed information is included for each configuration setting

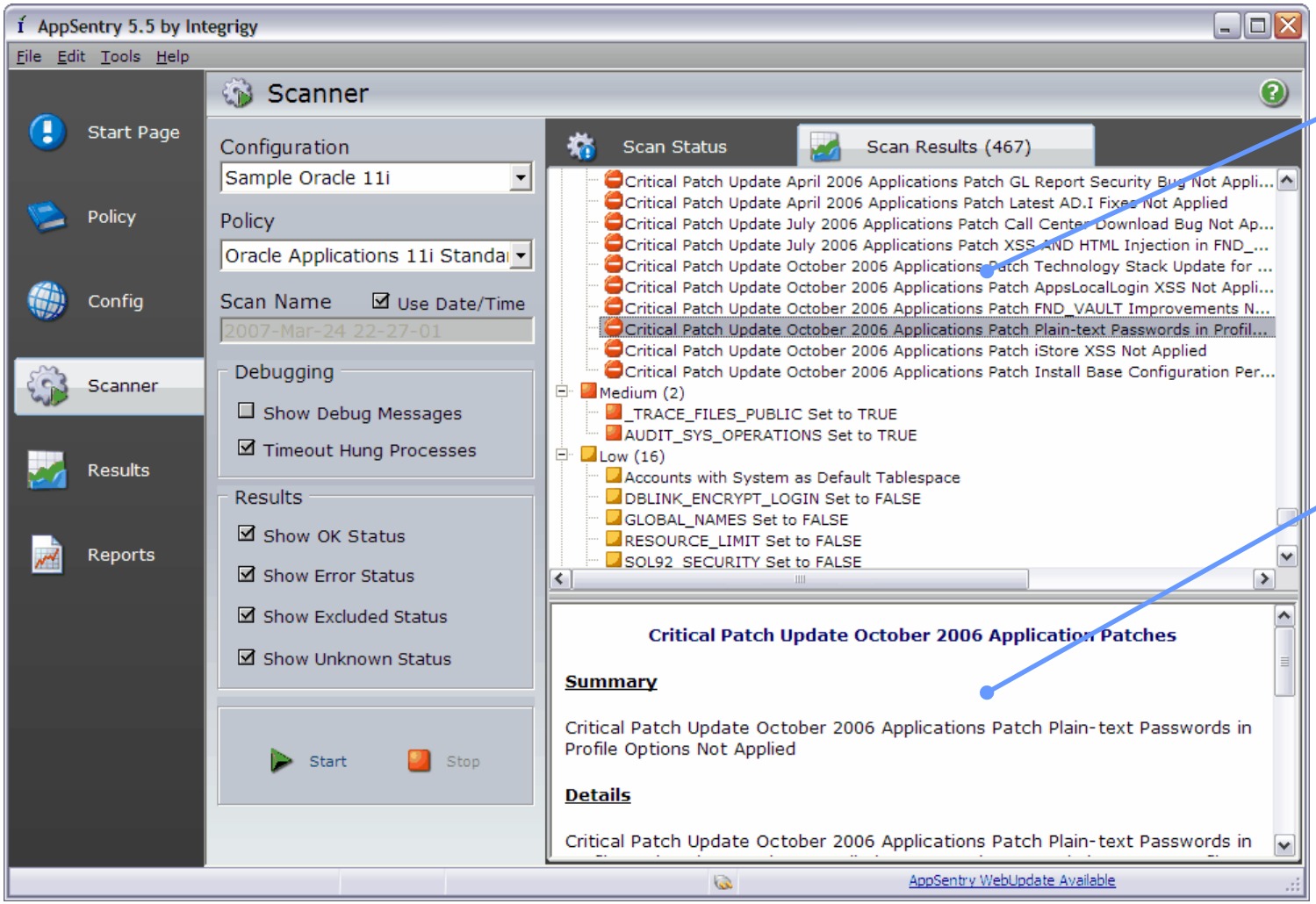
AppSentry – Scan



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

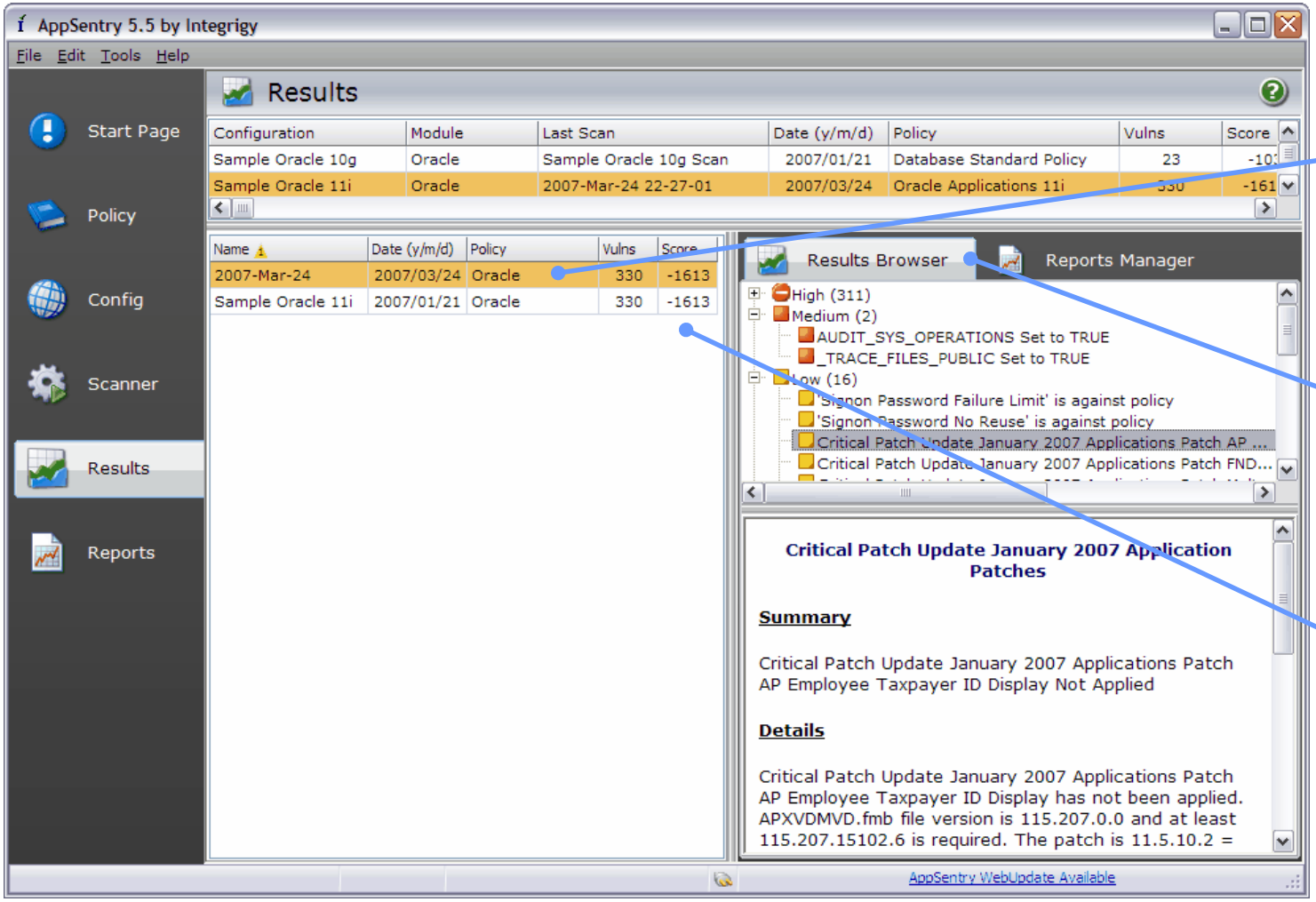
AppSentry – Scan



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

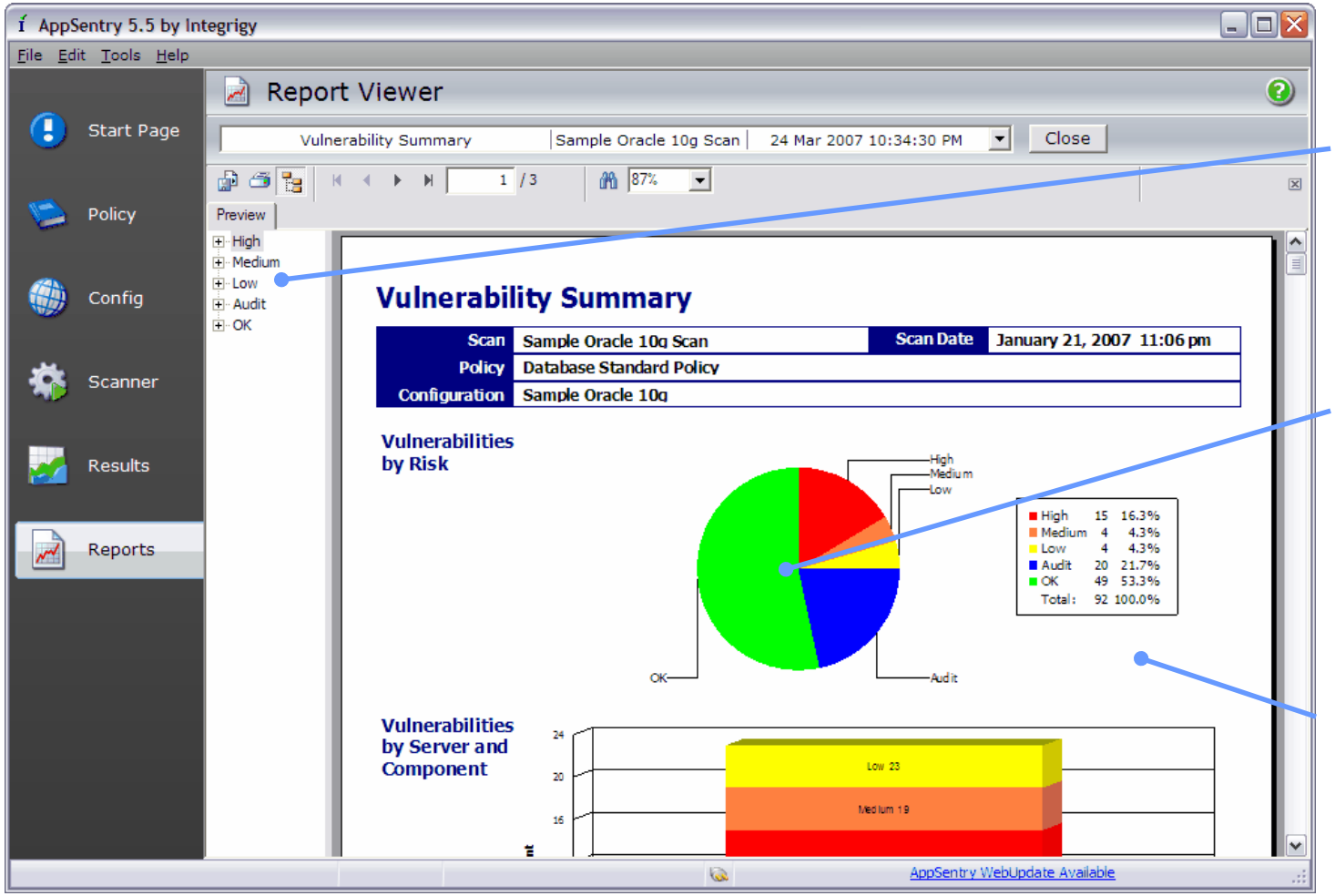


Results from all scans can be reviewed at any time.

Results can be browsed or reports run

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

AppSentry – Reporting

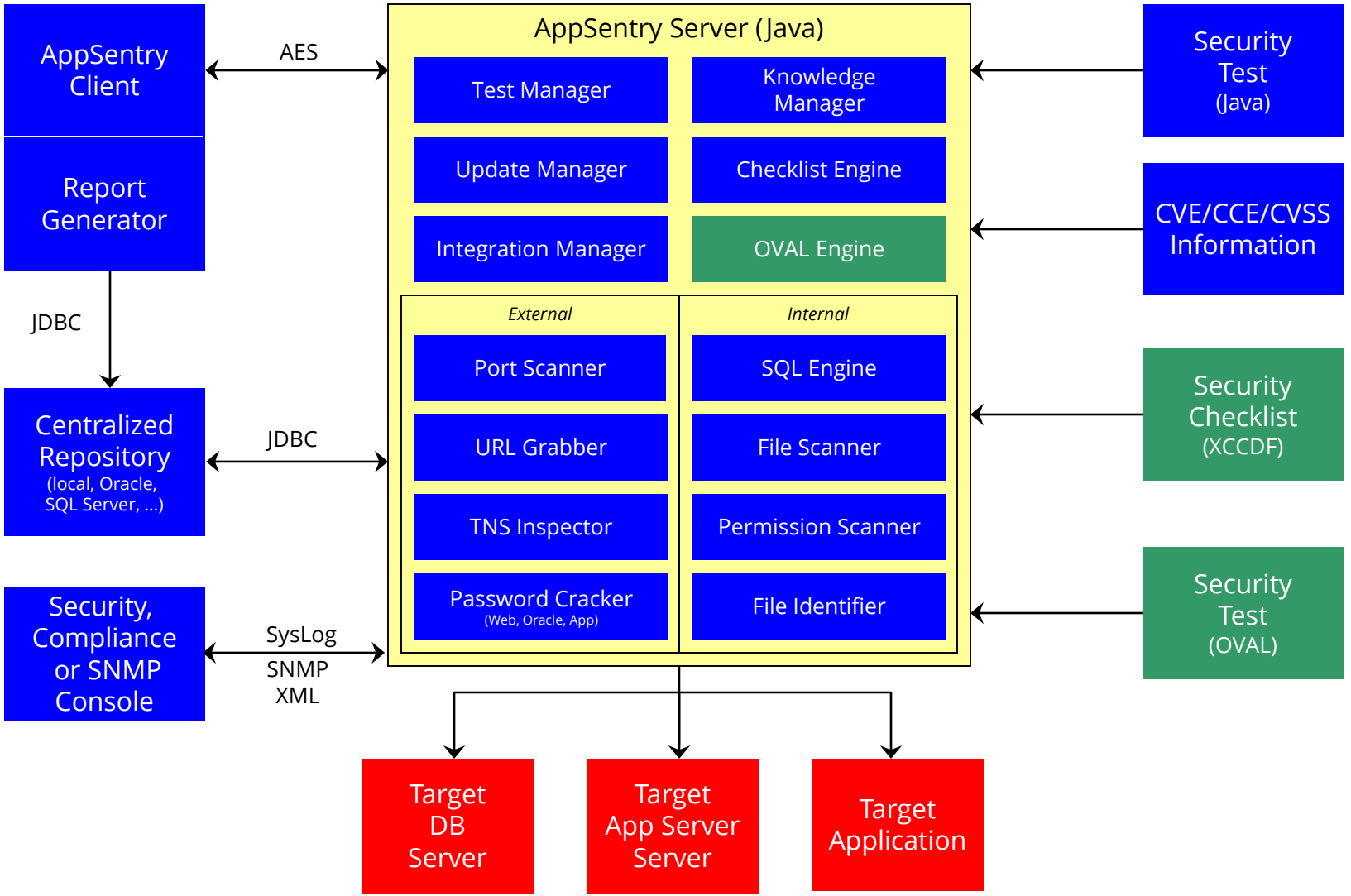


Reports are interactive and some allow drill-down into detailed information

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

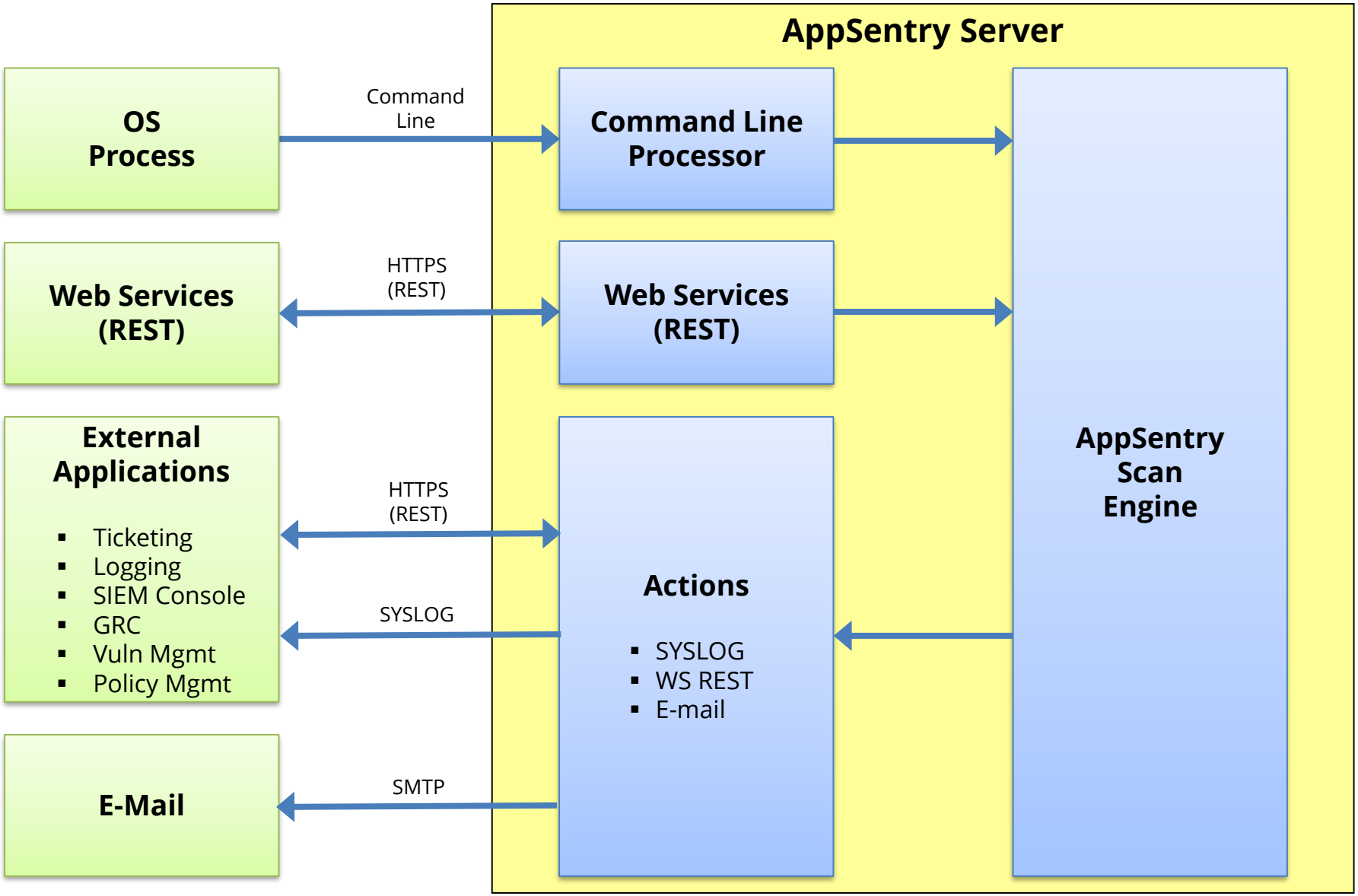
Oracle Database	▪ 8i (8.1.7) ▪ 9i (9.0.1, 9.2.0) ▪ 10g (10.1, 10.2) ▪ 11g (11.1, 11.2) ▪ 12c (12.1)
Oracle E-Business Suite	▪ 11i (11.5.1 – 11.5.10 CU2) ▪ R12 (12.0, 12.1, 12.2)
Oracle Application Server	▪ 9iAS (1.0.2, 9.0.2, 9.0.3) ▪ 10g (9.0.4, 10.1) ▪ 11g (11.1)
Microsoft SQL Server	▪ 2000 ▪ 2005 ▪ 2008, 2008 R2 ▪ 2012 ▪ 2014 ▪ 2016 (under development)

AppSentry Modules in Development or Planned

Databases	Applications	Application Servers
Relational ▪ Oracle MySQL* ▪ MariaDB* ▪ Sybase ASE* ▪ IBM DB2 (LUW) * ▪ PostgreSQL ▪ Teradata ▪ Informix ▪ Apache Derby ▪ SAP MaxDB **No SQL** ▪ Cassandra ▪ MongoDB ▪ Hadoop	▪ Oracle Business Intelligence (OBIEE) * ▪ Oracle Fusion Applications* ▪ PeopleSoft ▪ SAP	▪ Oracle WebLogic* ▪ Oracle Fusion Middleware* ▪ Apache ▪ Tomcat ▪ IBM WebSphere

* 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.

Assets	▪ 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)	▪ XCCDF - Extensible Configuration Checklist Description Format ▪ OVAL - Open Vulnerability and Assessment Language ▪ OCIL - Open Checklist Interactive Language
Security Data	▪ 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	▪ List Policies (/policy/list)
Assets	▪ List Assets (/asset/list) ▪ Add Asset (/asset/add)
Scans	▪ 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 @Out

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

Protocols	▪ Syslog ▪ Web Service - REST ▪ E-mail (smtp) ▪ SNMP trap ▪ File ▪ JDBC ▪ Socket/SSLSocket ▪ Custom Logback appenders
Formats	▪ XCCDF - Extensible Configuration Checklist Description Format ▪ ArcSight CEF ▪ OpenFISMA ▪ [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

Contact Information

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

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

phone: **888-542-4802**