INTEGRIGY

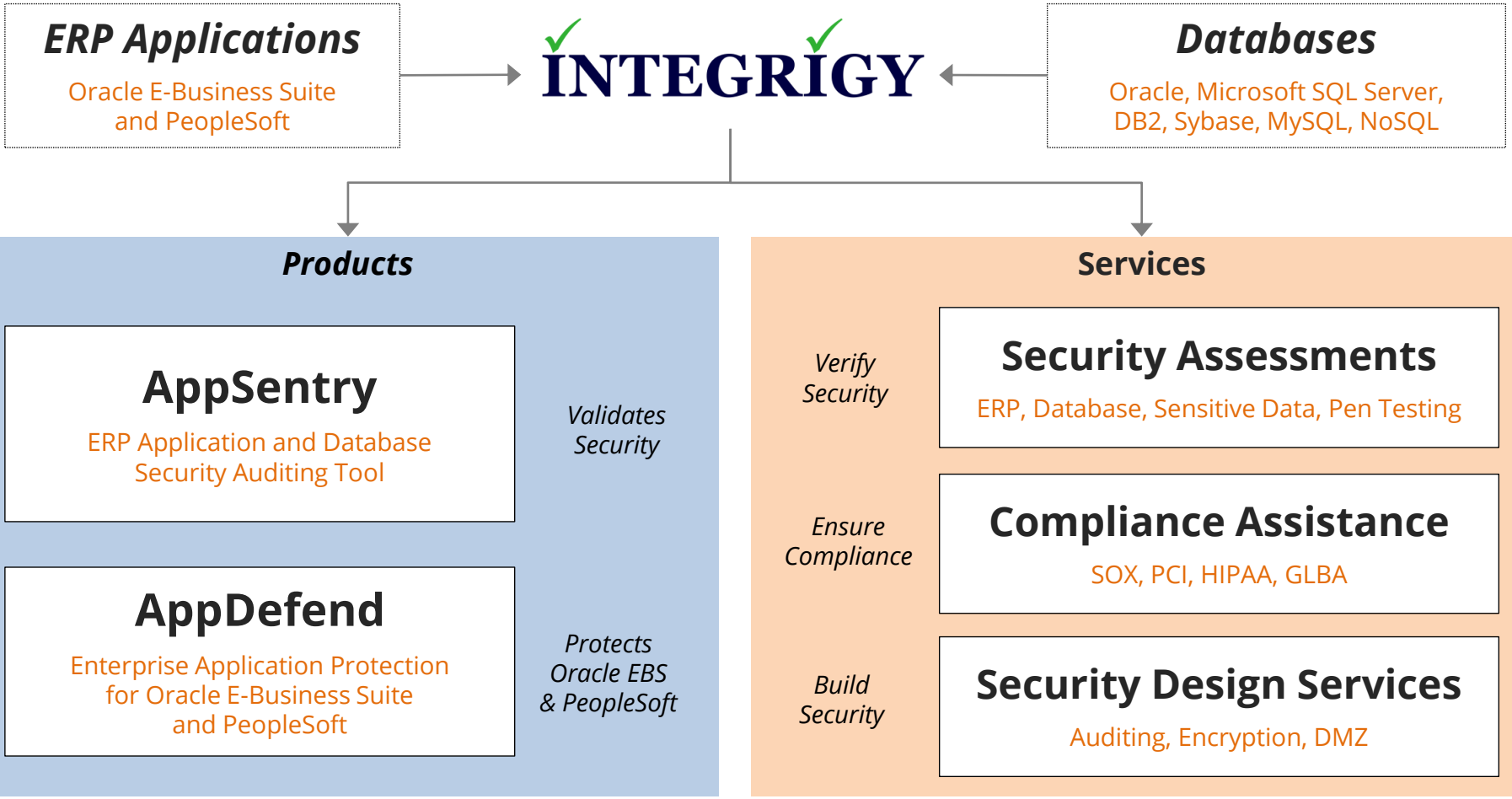
AppSentry

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

ORACLE Gold Partner

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'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 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

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 (SOX, GDPR, PCI, HIPAA, ...)

Using AppSentry

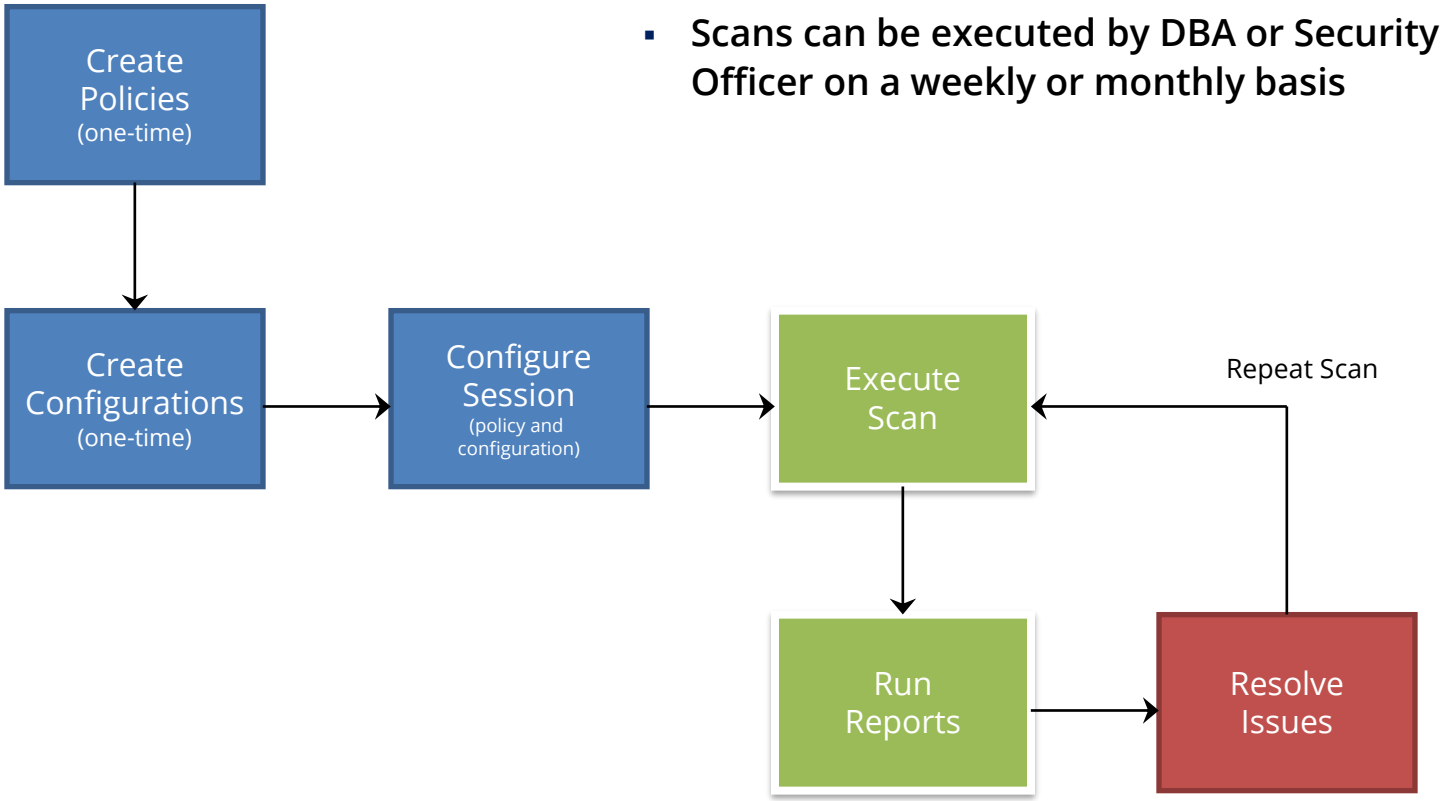
- **Simple to use – task-oriented GUI**
- **Comprehensive descriptions and solutions for identified vulnerabilities**
- **AppSentry Users**
  - IT Security
  - Internal Audit
  - Oracle DBAs
  - Oracle Project Team – IT
  - Oracle Project Team – Functional/Business Owner

AppSentry – Automated Audit

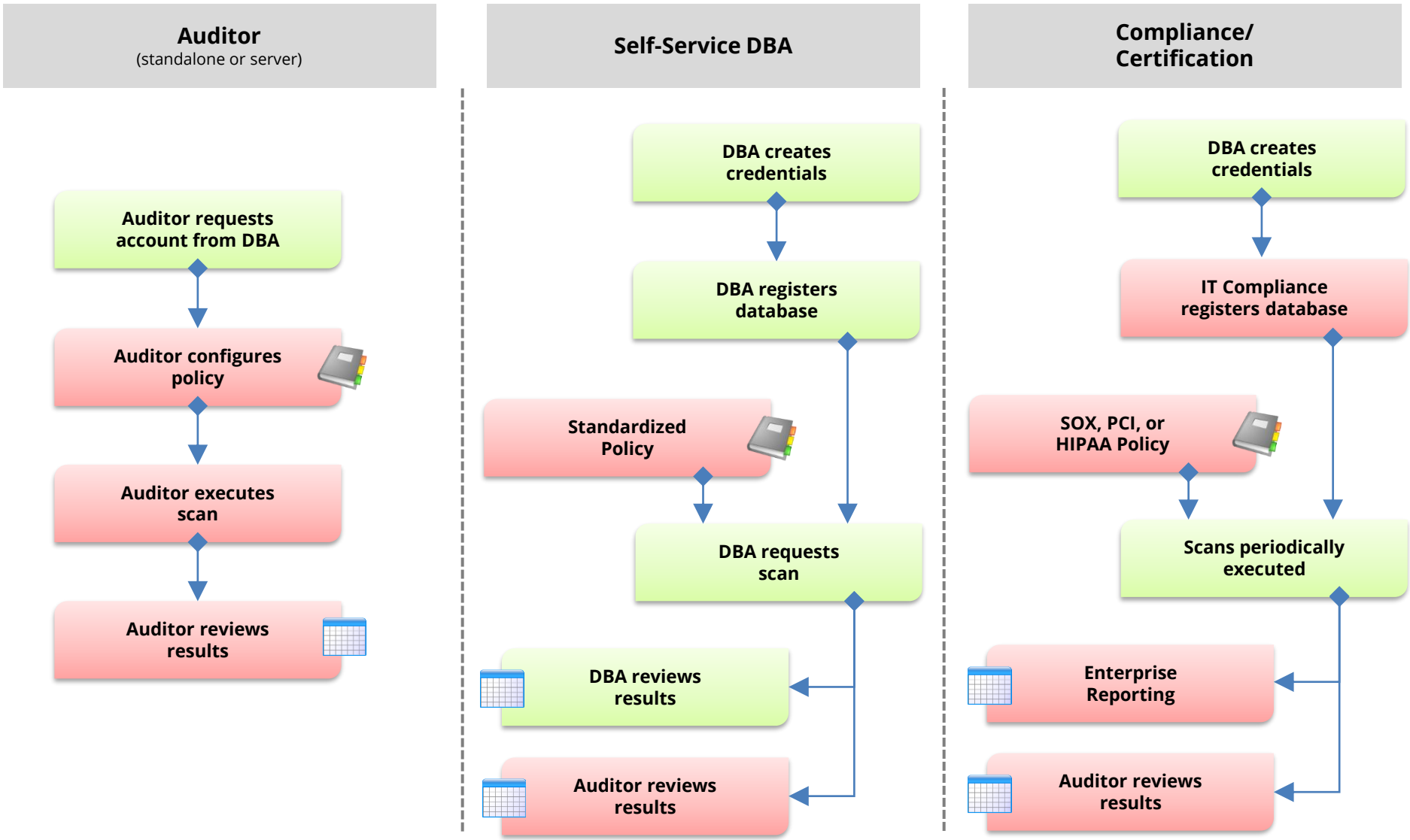
- **Confidence**
  - Audits all layers from operating system to application
  - Downloads updates before every scan
- **Breadth**
  - Performs both security and control audits
- **Productivity**
  - Simple to use
  - Automates auditing and reporting
  - Auditor can focus on more important tasks (e.g.,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

AppSentry Workflow

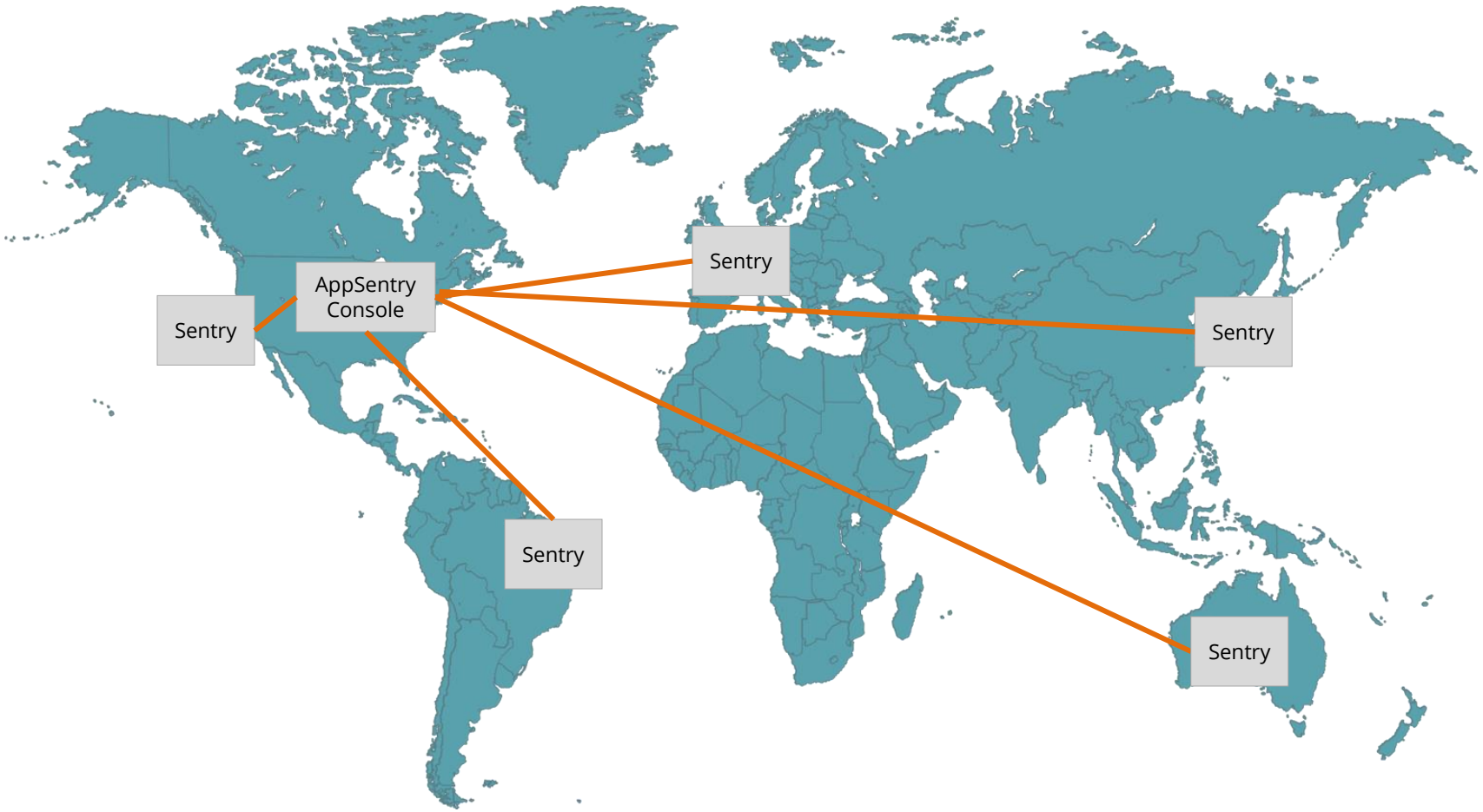
- Quick and simple workflow
- Policies and configurations are created once by DBA, Security Officer, or Internal Audit
- Scans can be executed by DBA or Security Officer on a weekly or monthly basis



AppSentry Standard Usage Models



AppSentry Distributed



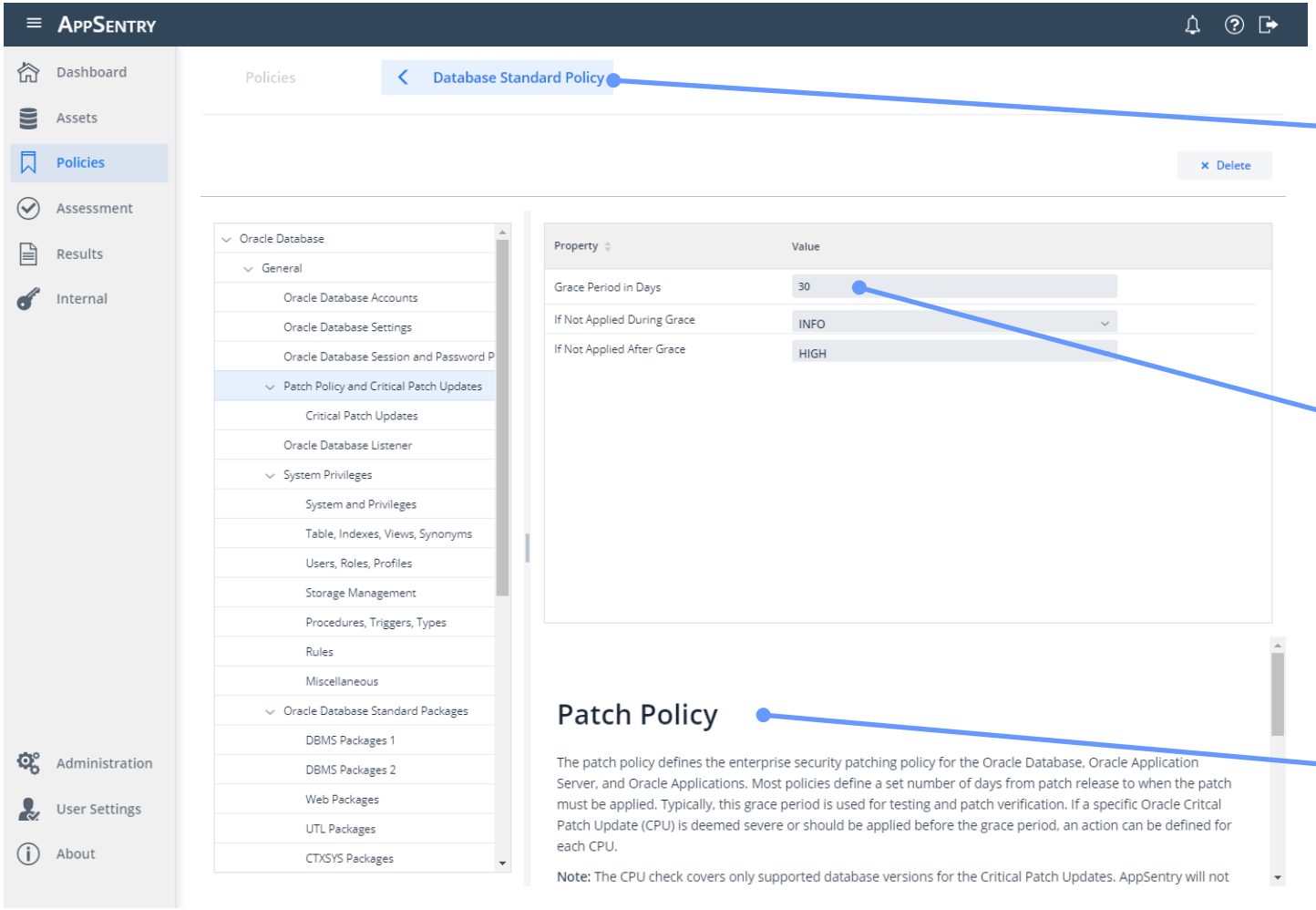
Access and Network Requirements

- **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	**Physical or Virtual Server**	▪ Multi-user solution on dedicated hardware ▪ Operating system Linux or Windows
	Virtual Appliance	▪ Docker image ▪ Open Virtualization Format (OVF) appliance
Cloud	**Private Cloud**	▪ Java-capable cloud solutions (Amazon, Google, Oracle, ...)
	Public Cloud (demonstration)	▪ Integrigy hosted solution at Amazon AWS

AppSentry – Policies

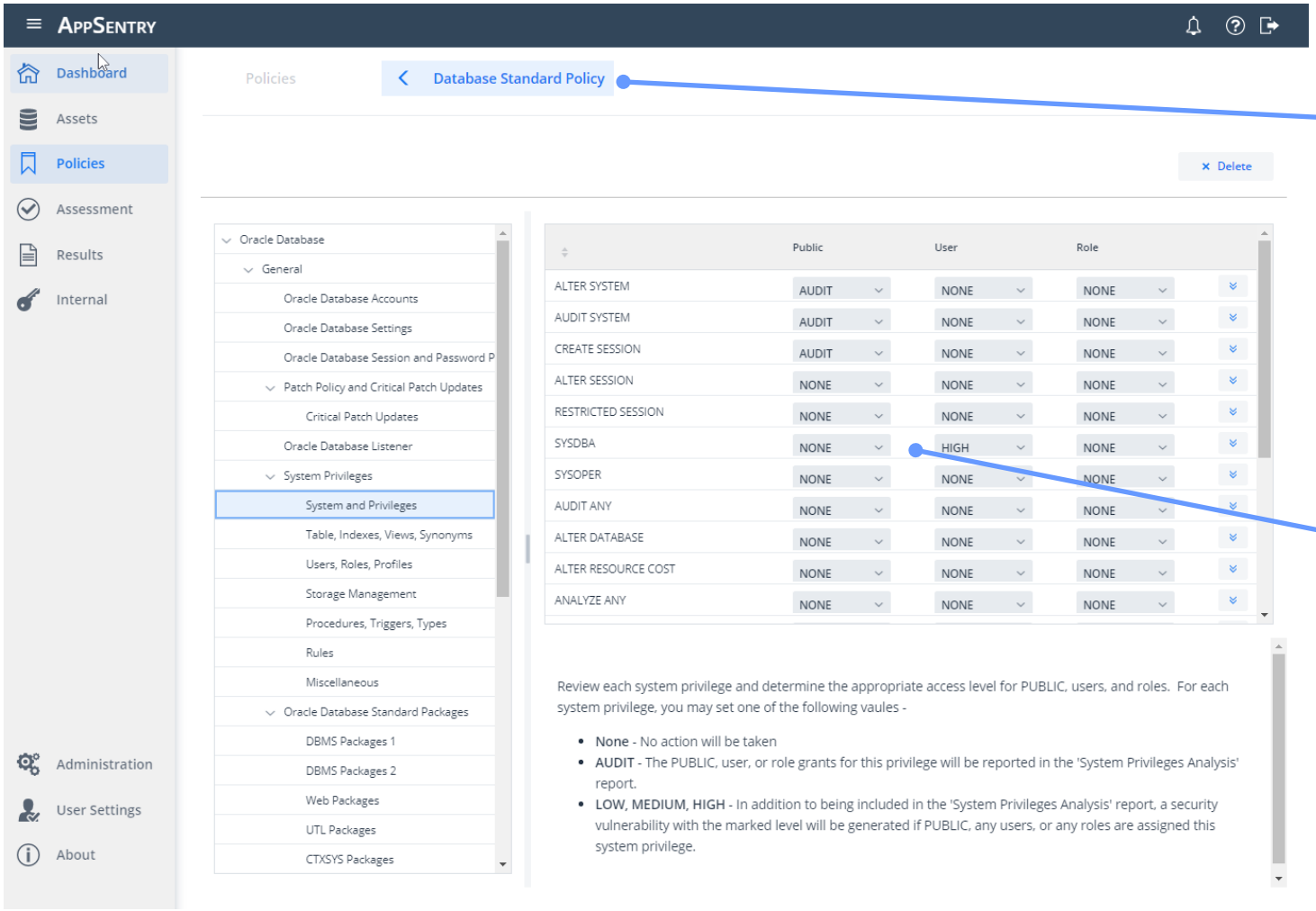


Policies can be defined for different scenarios such as HIPAA, month-end scan, a level of security, or a checklist

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

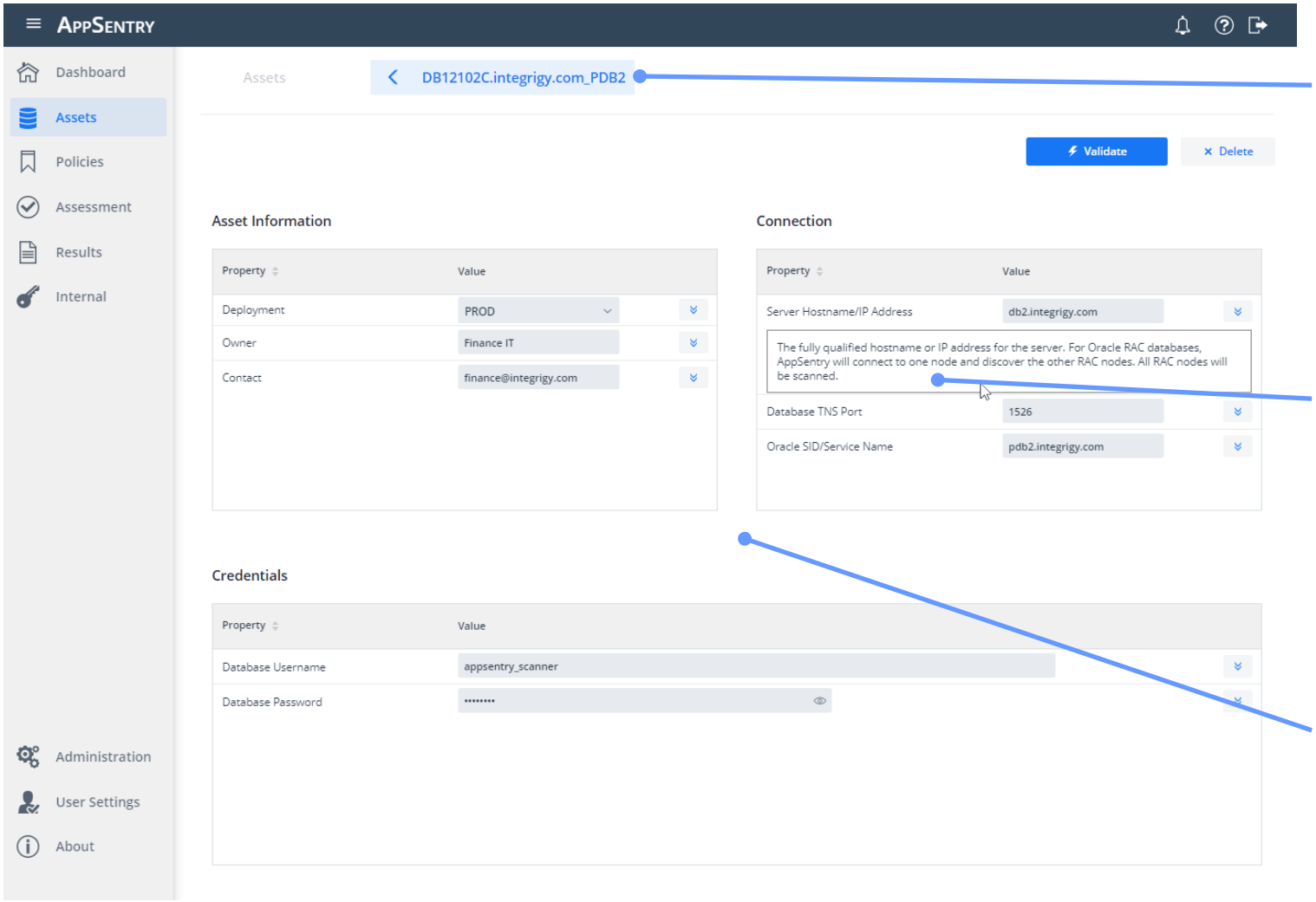
AppSentry – Policies



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

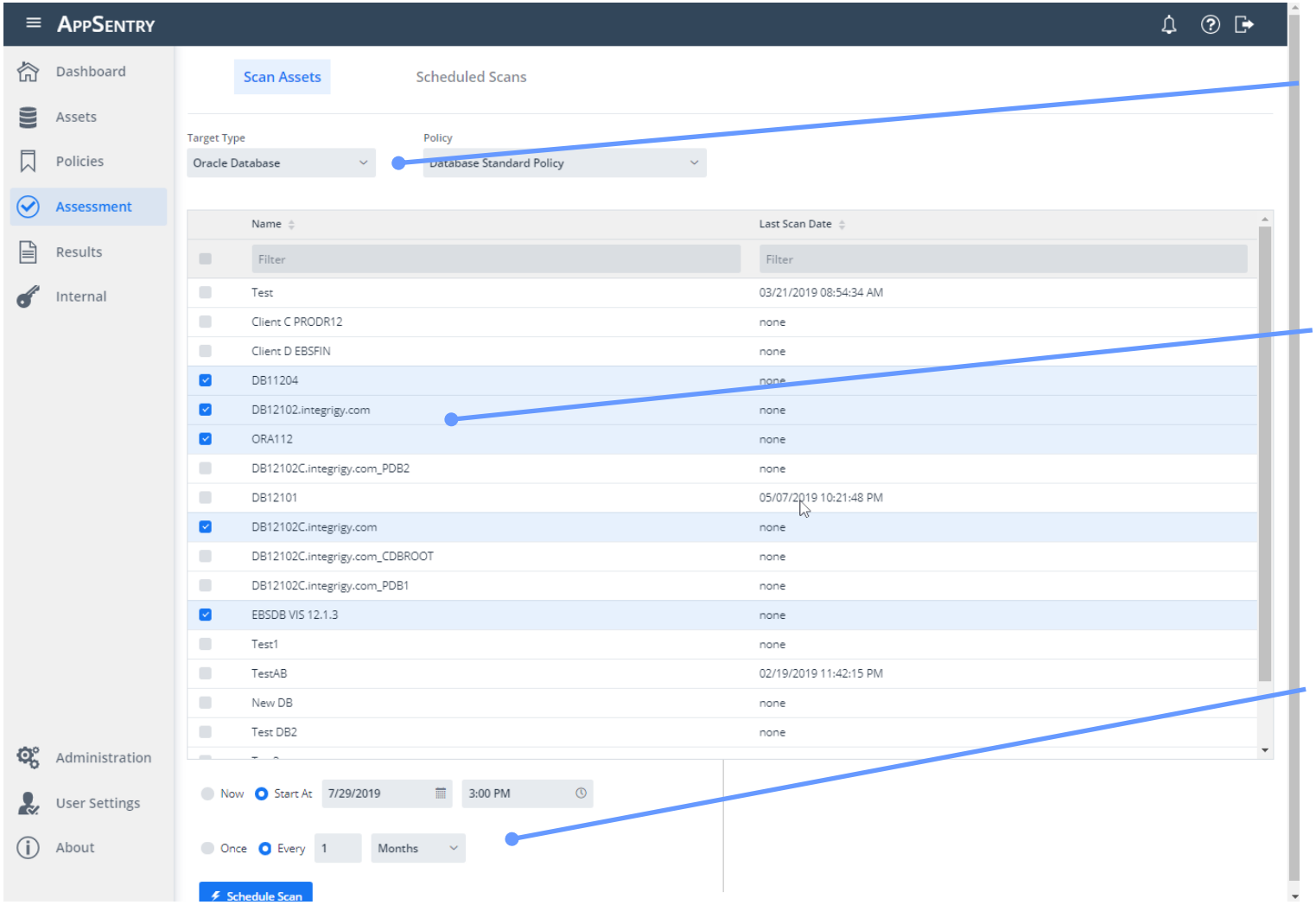


Configurations are defined for different environments including Oracle database, Oracle Application Server, and Oracle E-Business Suite

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

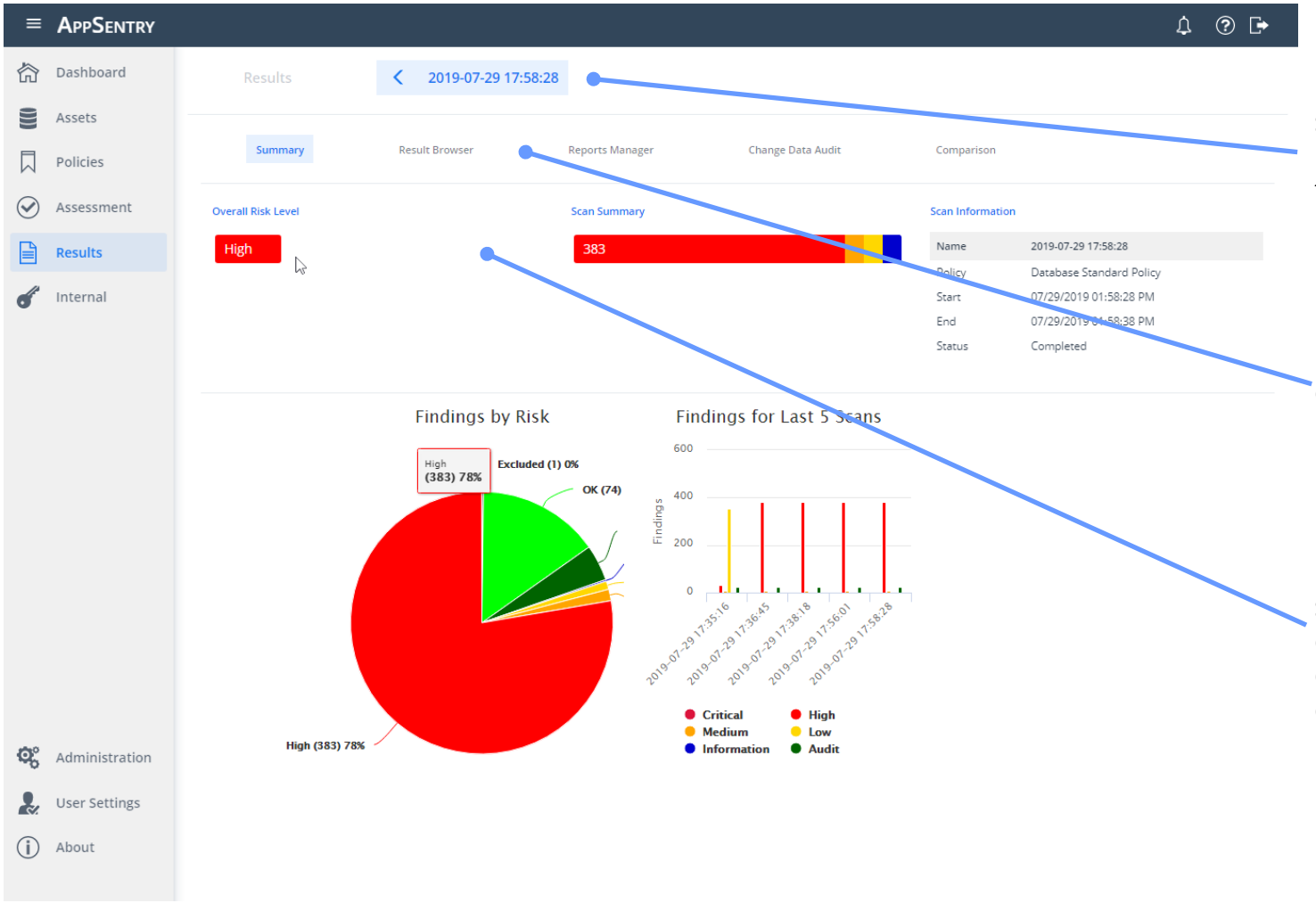


Running an assessment is as simple as choosing a configuration and policy and clicking start

Multiple assests may be included an assessement

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

AppSentry – Results

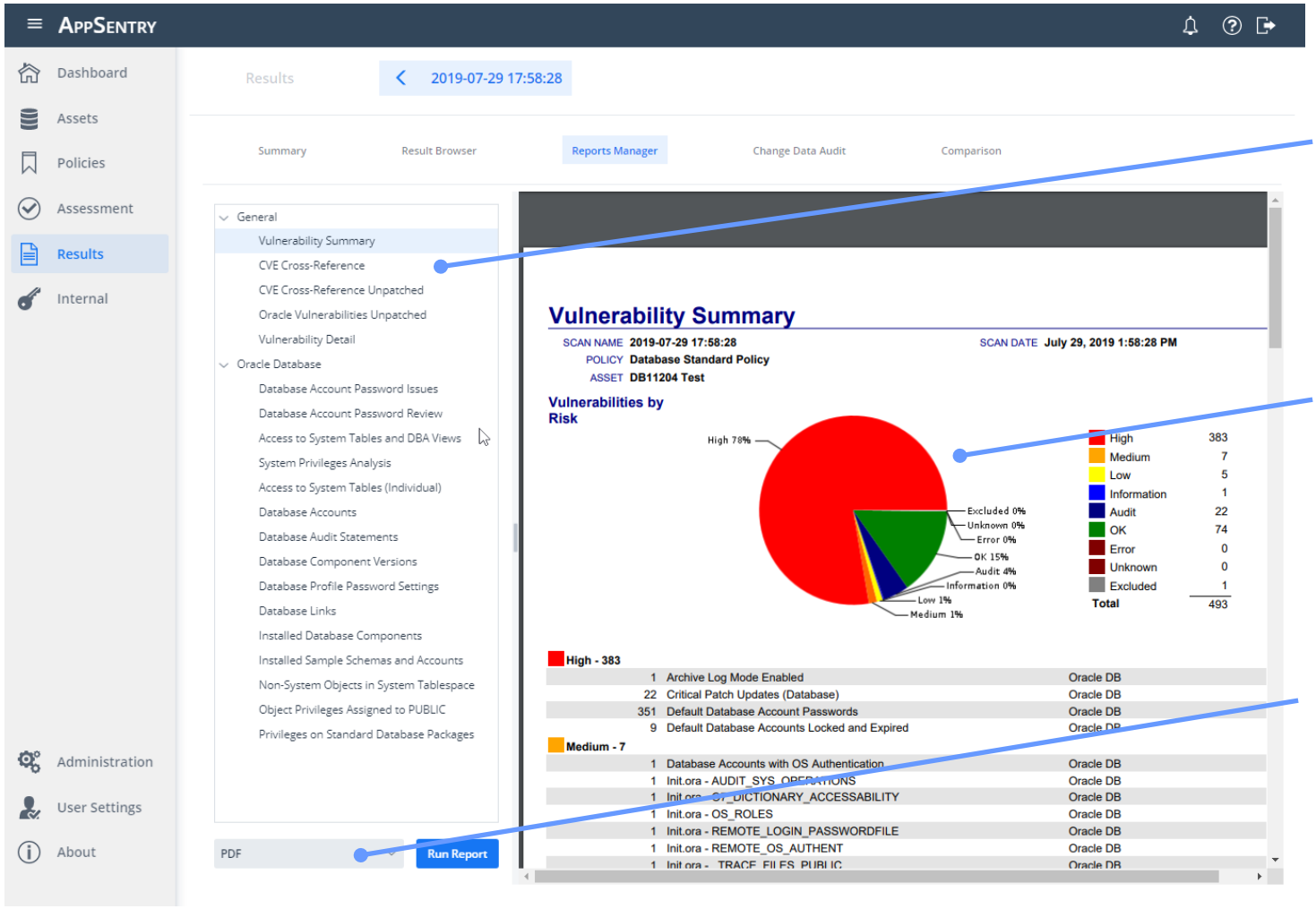


Results from all scans can be reviewed at any time.

Results can be browsed or reports run

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

AppSentry – Reporting

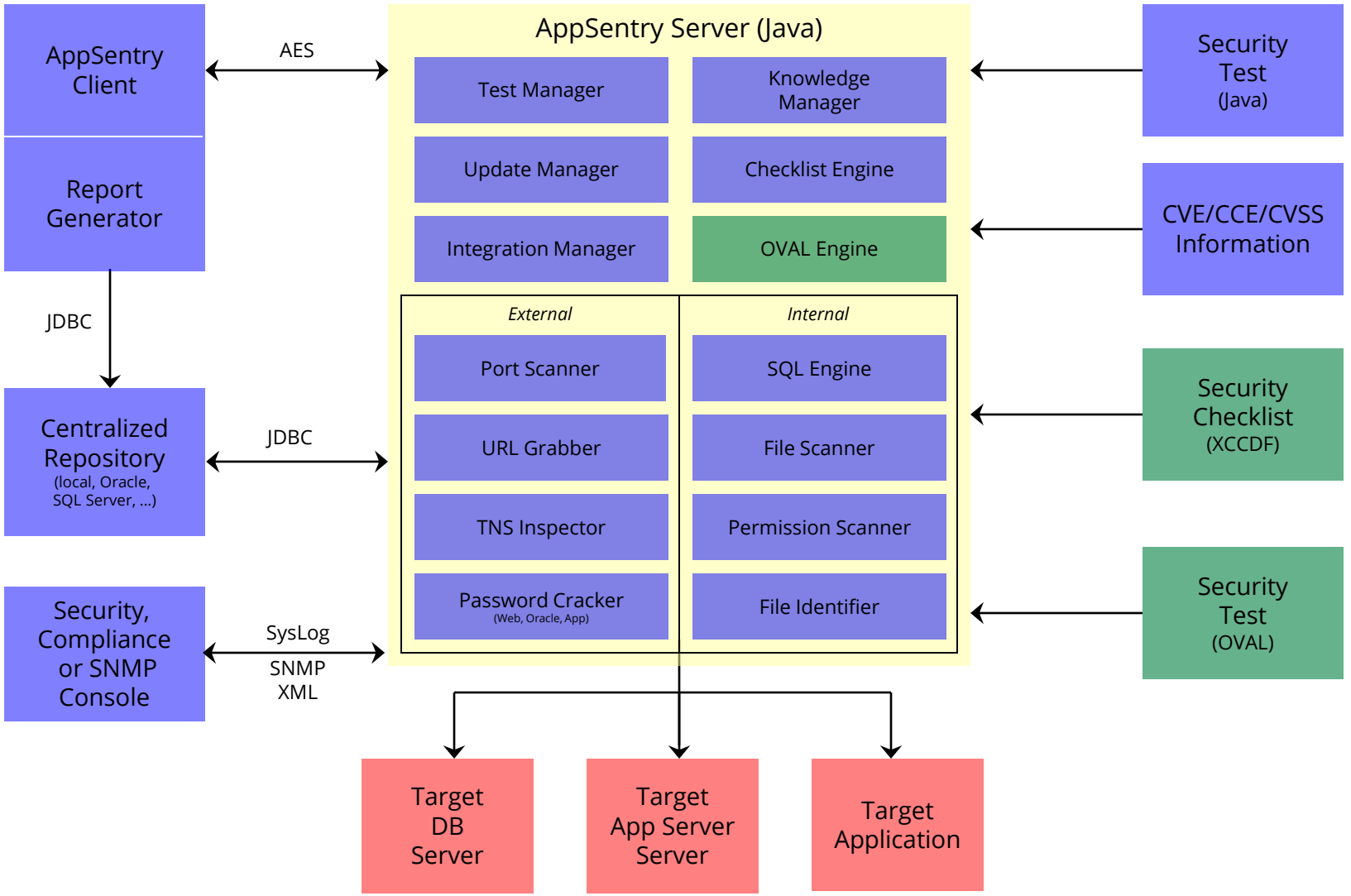


Reports are interactive and some allow drill-down into detailed information

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



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

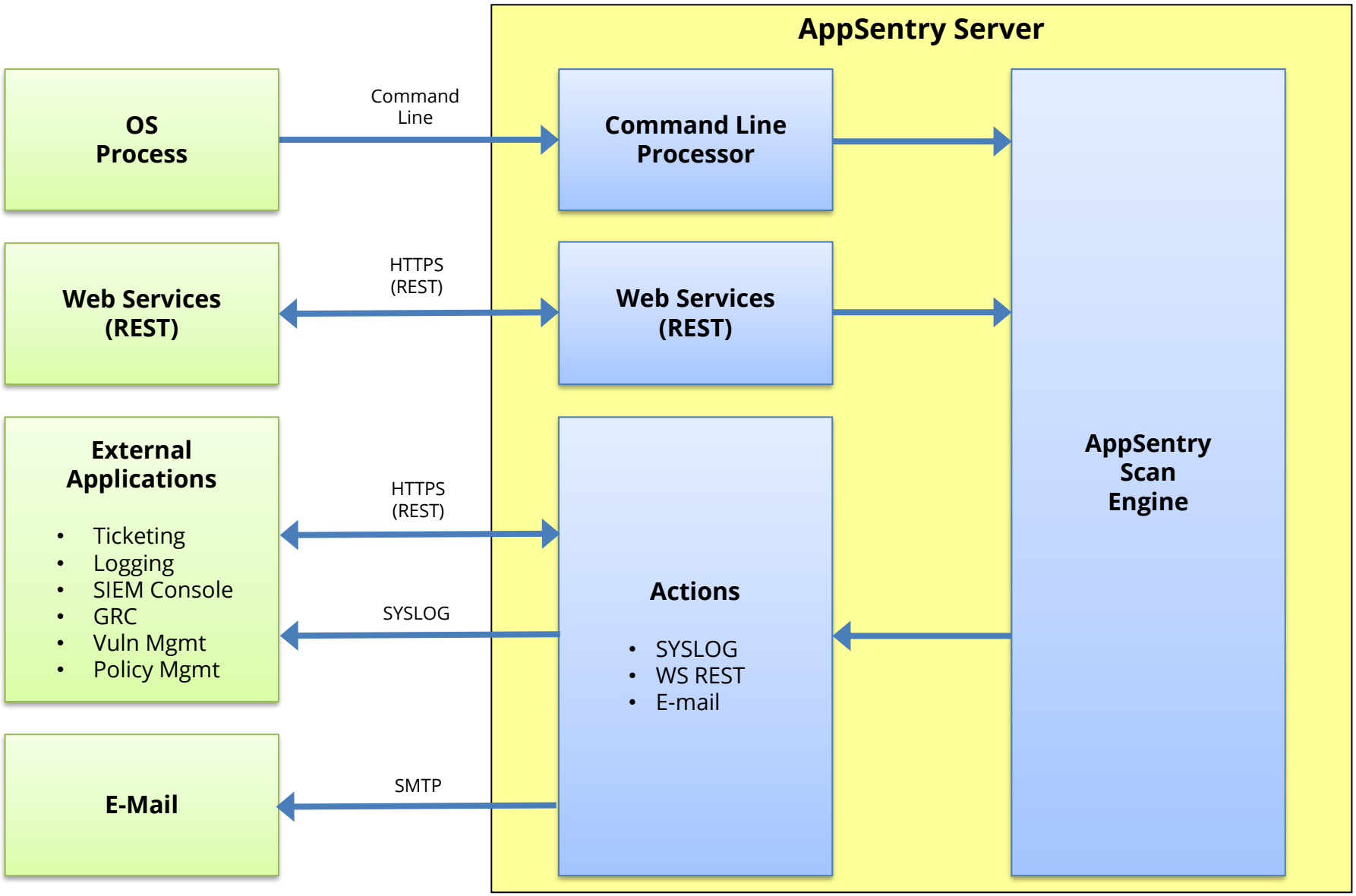
AppSentry Modules in Development or Planned

Databases	Cloud Databases	Applications and Application Servers
Relational Oracle MySQL * MariaDB * Sybase ASE IBM DB2 (LUW) * PostgreSQL * Teradata * Informix **No SQL** Cassandra * MongoDB * Hadoop	**Relational** 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 **No SQL** AWS DynamoDB Azure CosmosDB	Oracle Business Intelligence (OBIEE) ^ Oracle APEX ^ Oracle ERP Cloud Oracle WebLogic ^ Oracle Fusion Middleware ^

* Available with base security configuration and vulnerability scanning

^ 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 • [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**