INTEGRIGY

AppSentry

ERP Application and Database Security Auditing

October 2025

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

About Integrigy

ERP Applications

Oracle E-Business Suite and PeopleSoft

INTEGRIGY

Databases

Oracle, Microsoft SQL Server, DB2, Sybase, MySQL, NoSQL

Products

AppSentry

ERP Application and Database Security Auditing Tool

Validates Security

AppDefend

Enterprise Application Protection for Oracle E-Business Suite and PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, GDPR, PCI, HIPAA

Build Security

Security Design Services

Auditing, Encryption, DMZ

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

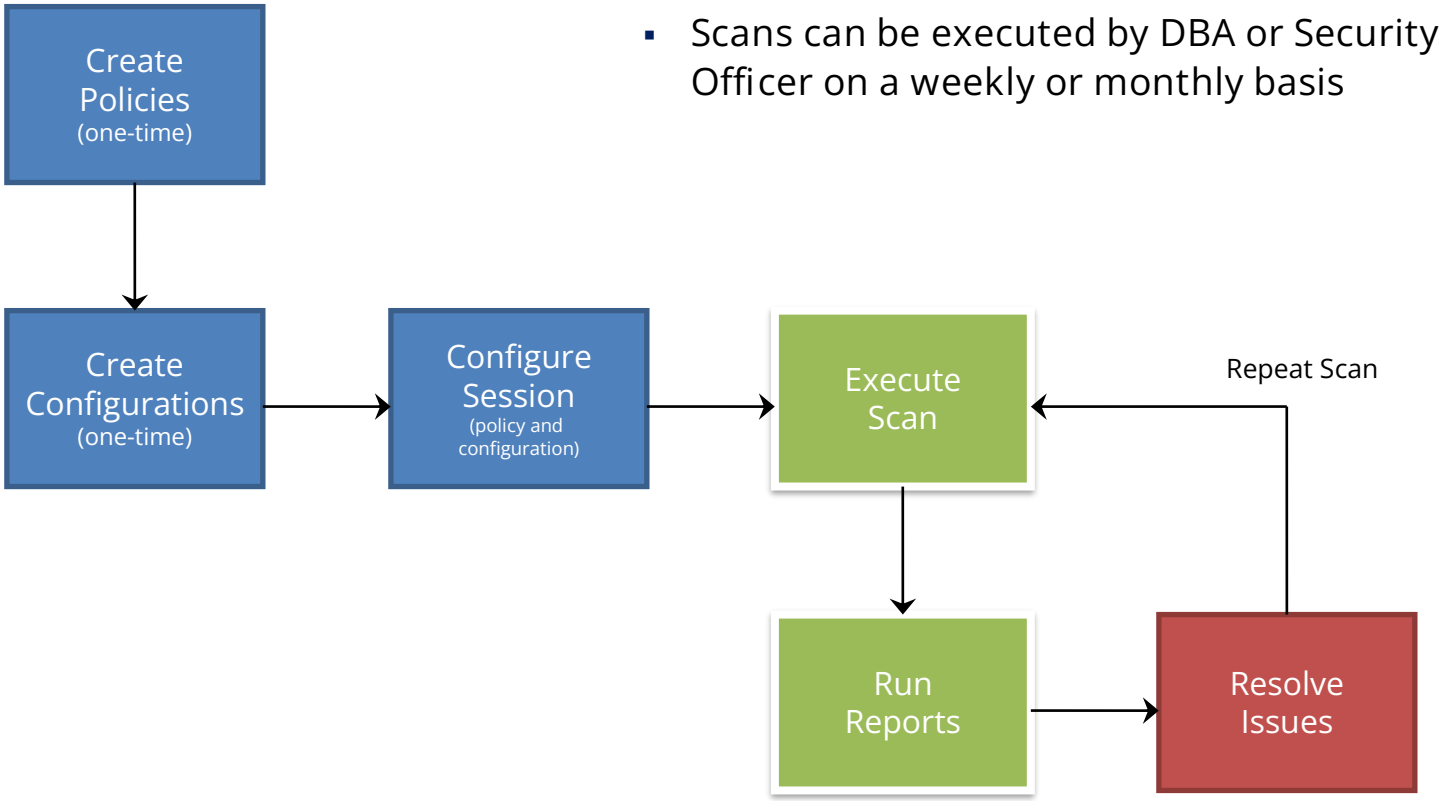
- Simple to use – task-oriented GUI
- Comprehensive descriptions and solutions for identified vulnerabilities
- AppSentry Users
  - IT Security
  - Internal Audit
  - Oracle DBAs
  - Oracle Project Team – IT
  - Oracle Project Team – Functional/Business Owner

AppSentry – Automated Audit

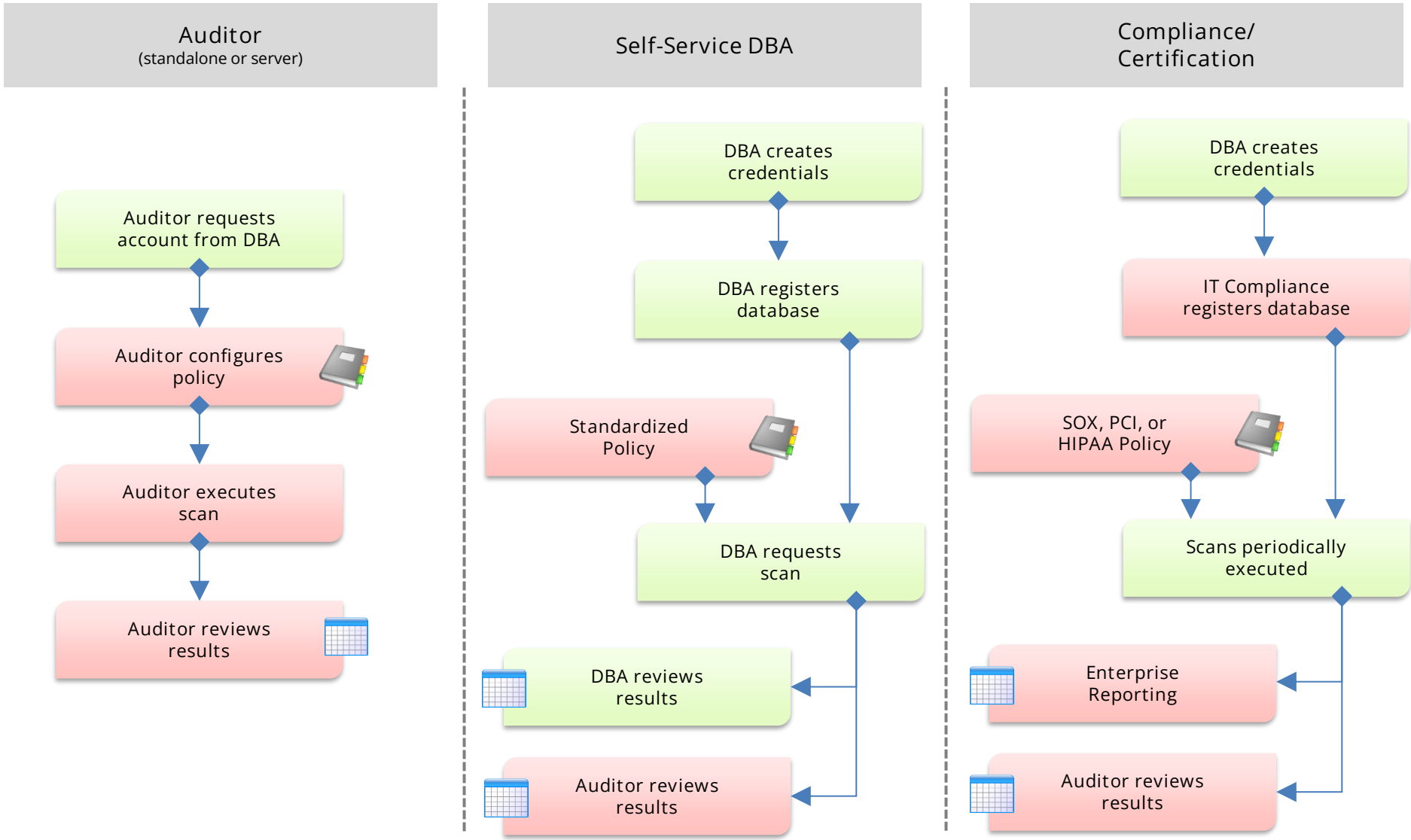
- Confidence
  - Audits all layers from operating system to application
  - Downloads updates before every scan
- Breadth
  - Performs both security and control audits
- Productivity
  - Simple to use
  - Automates auditing and reporting
  - Auditor can focus on more important tasks (e.g., process controls)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

AppSentry Workflow

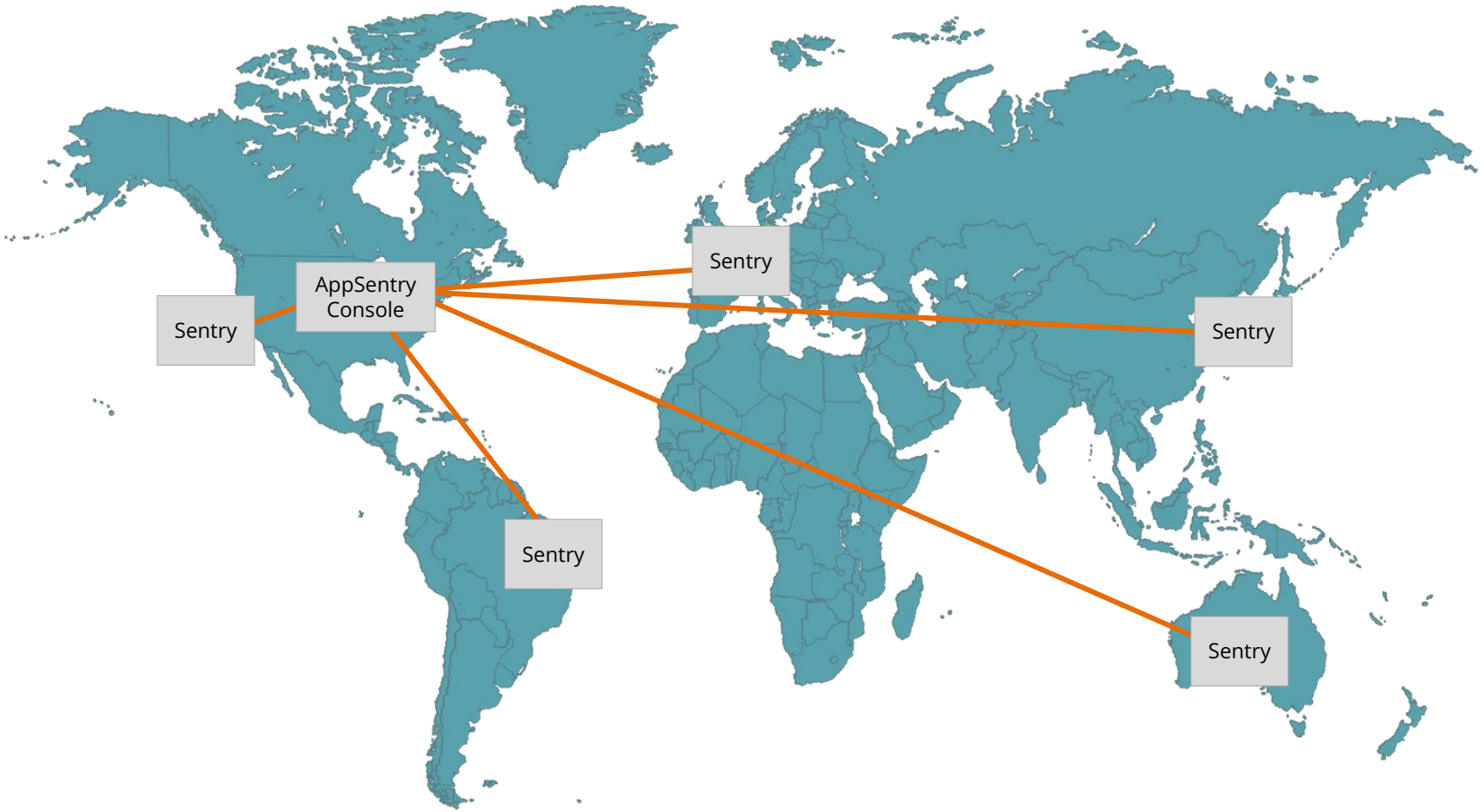
- Quick and simple workflow
- Policies and configurations are created once by DBA, Security Officer, or Internal Audit
- Scans can be executed by DBA or Security Officer on a weekly or monthly basis



AppSentry Standard Usage Models



AppSentry Distributed



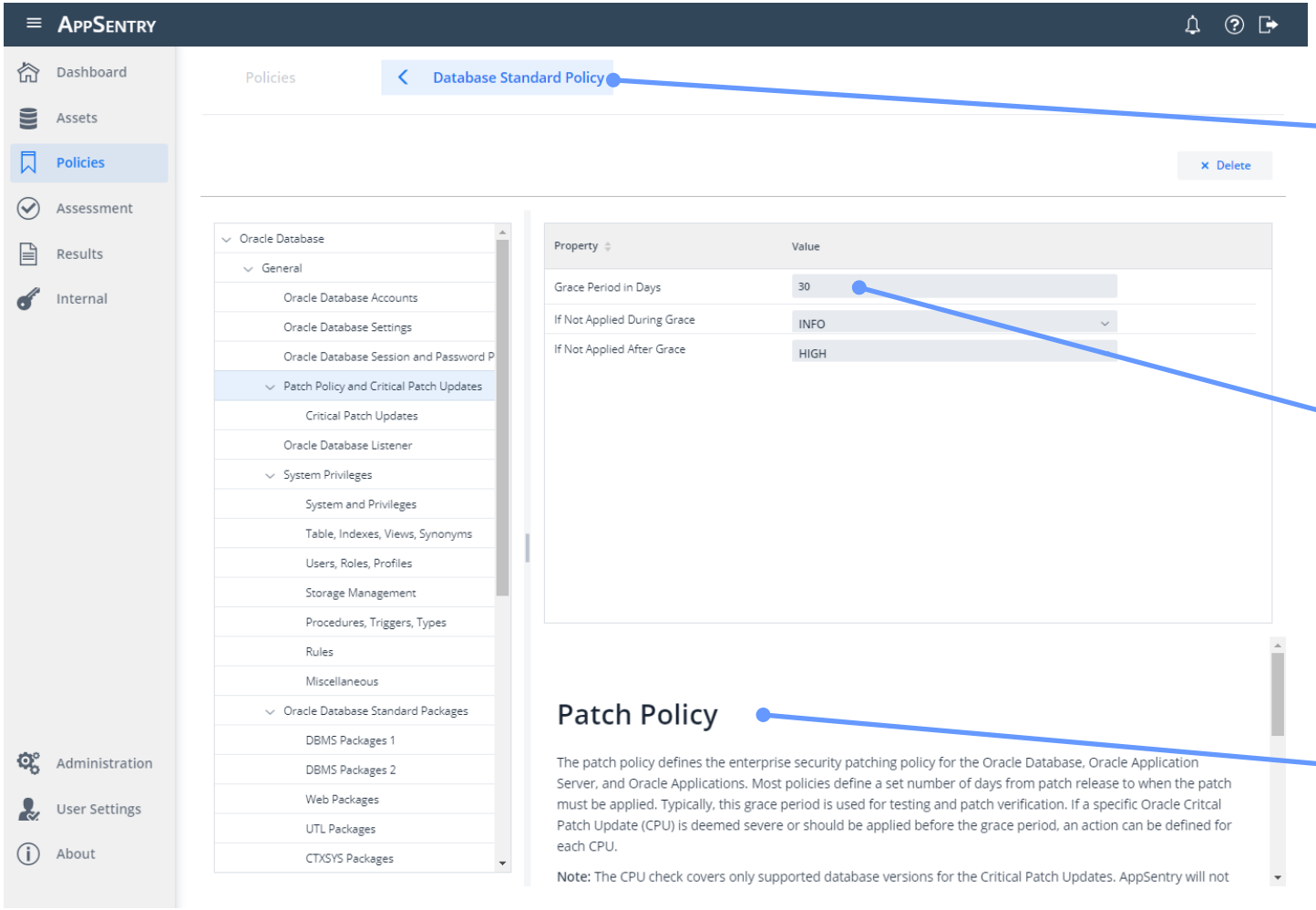
Access and Network Requirements

- 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 ▪ OCI 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

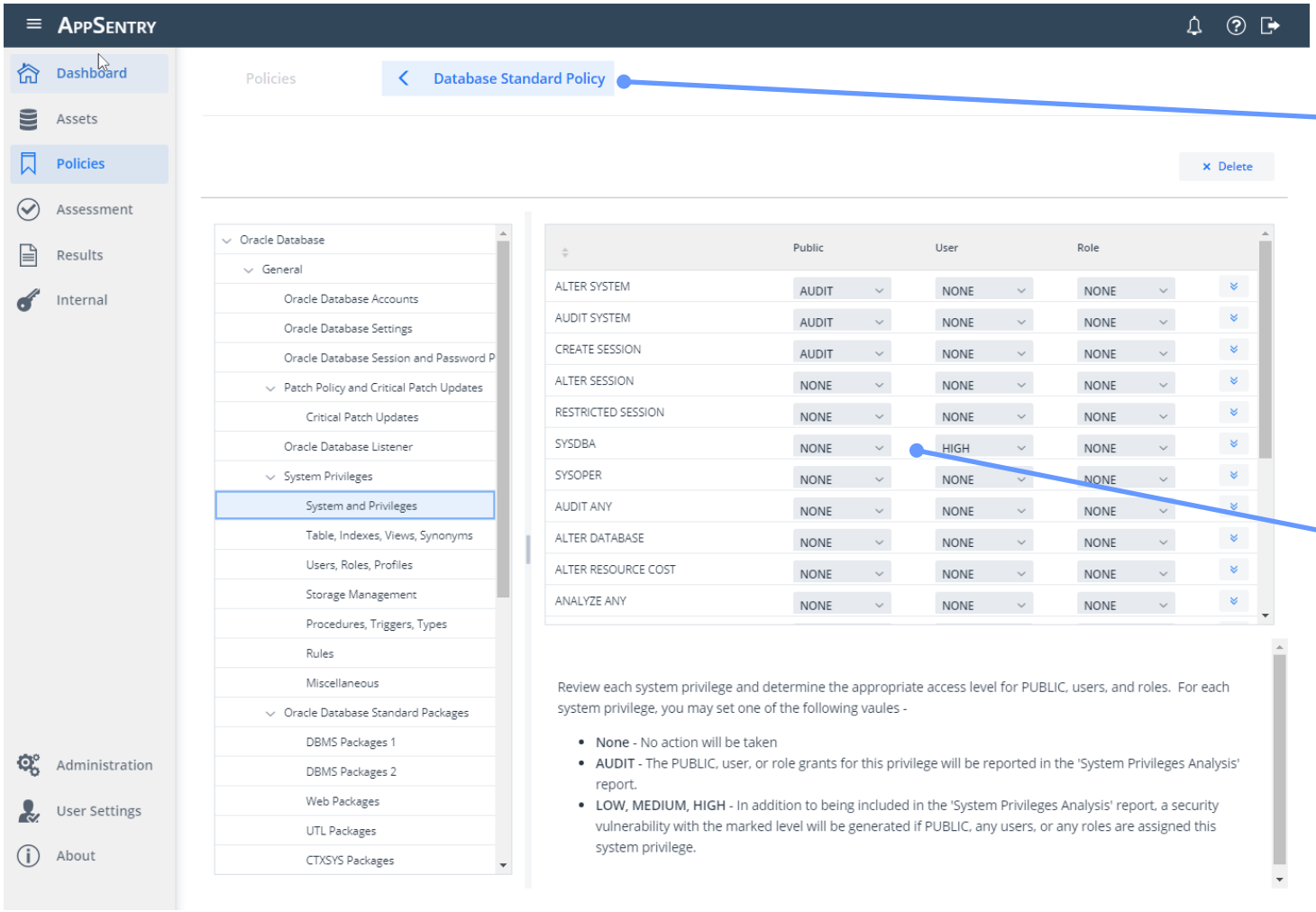


Policies can be defined for different scenarios such as HIPAA, month-end scan, a level of security, or a checklist

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

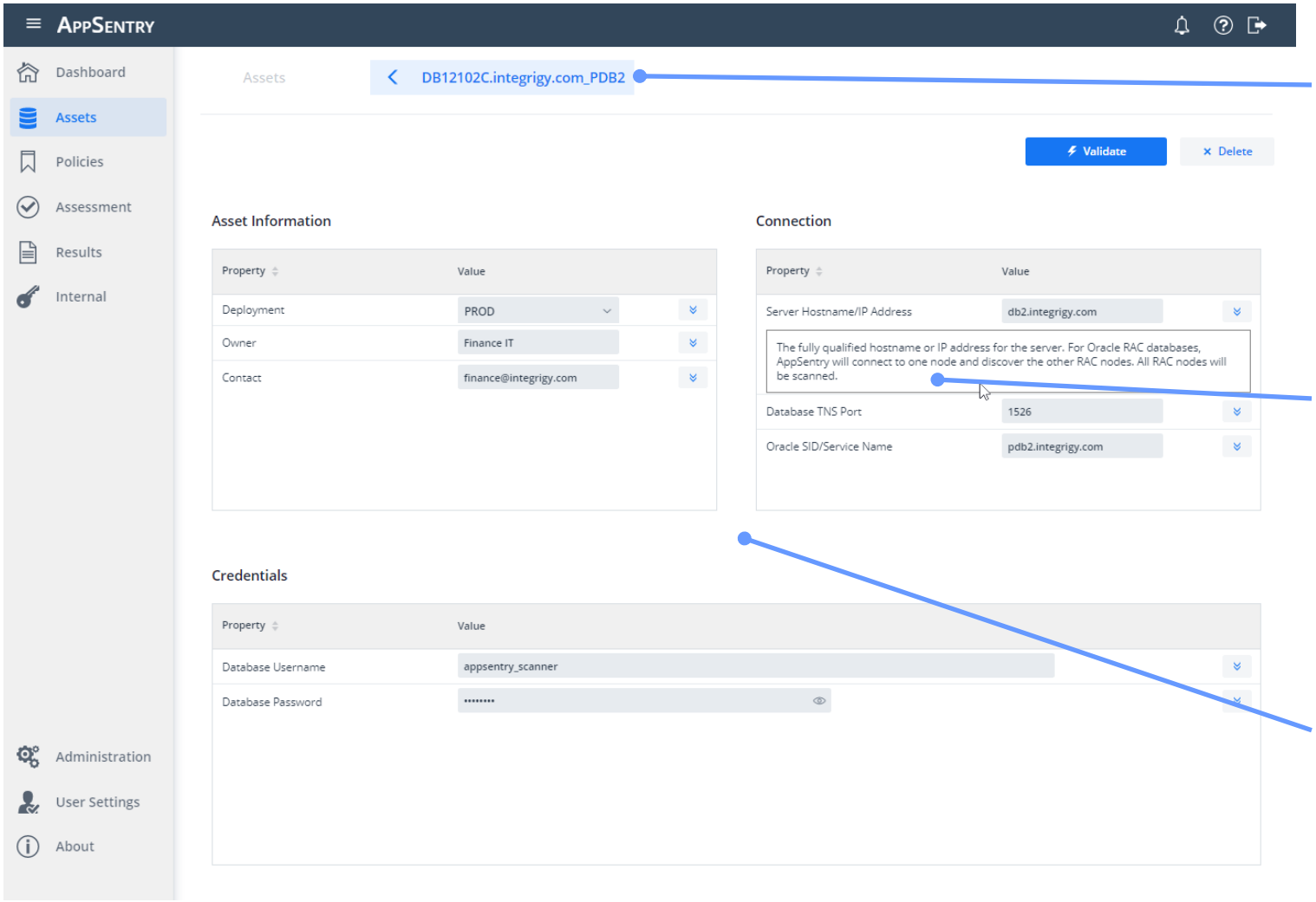
AppSentry – Policies



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

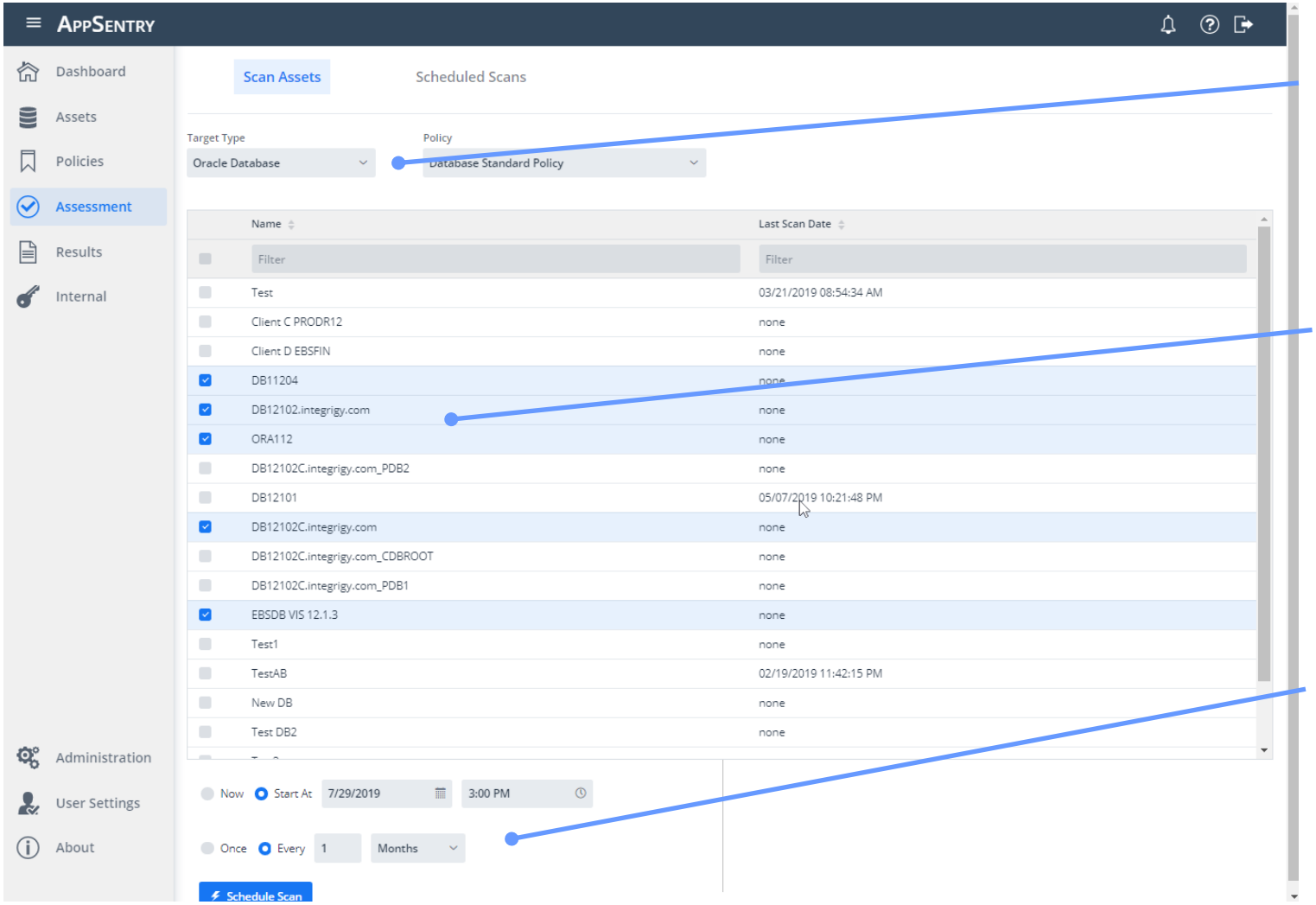


Configurations are defined for different environments including Oracle database, Oracle Application Server, and Oracle E-Business Suite

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

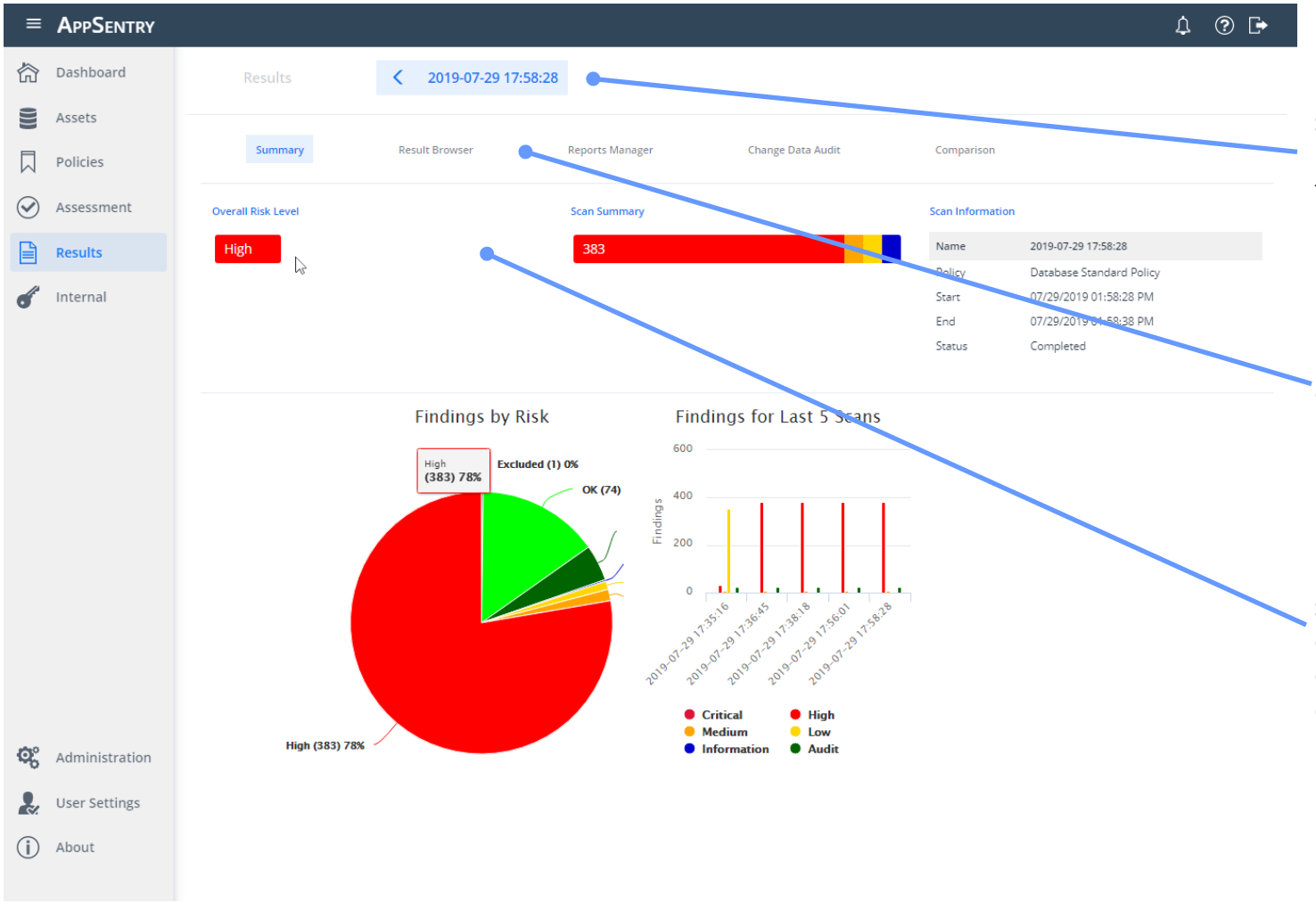


Running an assessment is as simple as choosing a configuration and policy and clicking start

Multiple assests may be included an assessement

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

AppSentry – Results

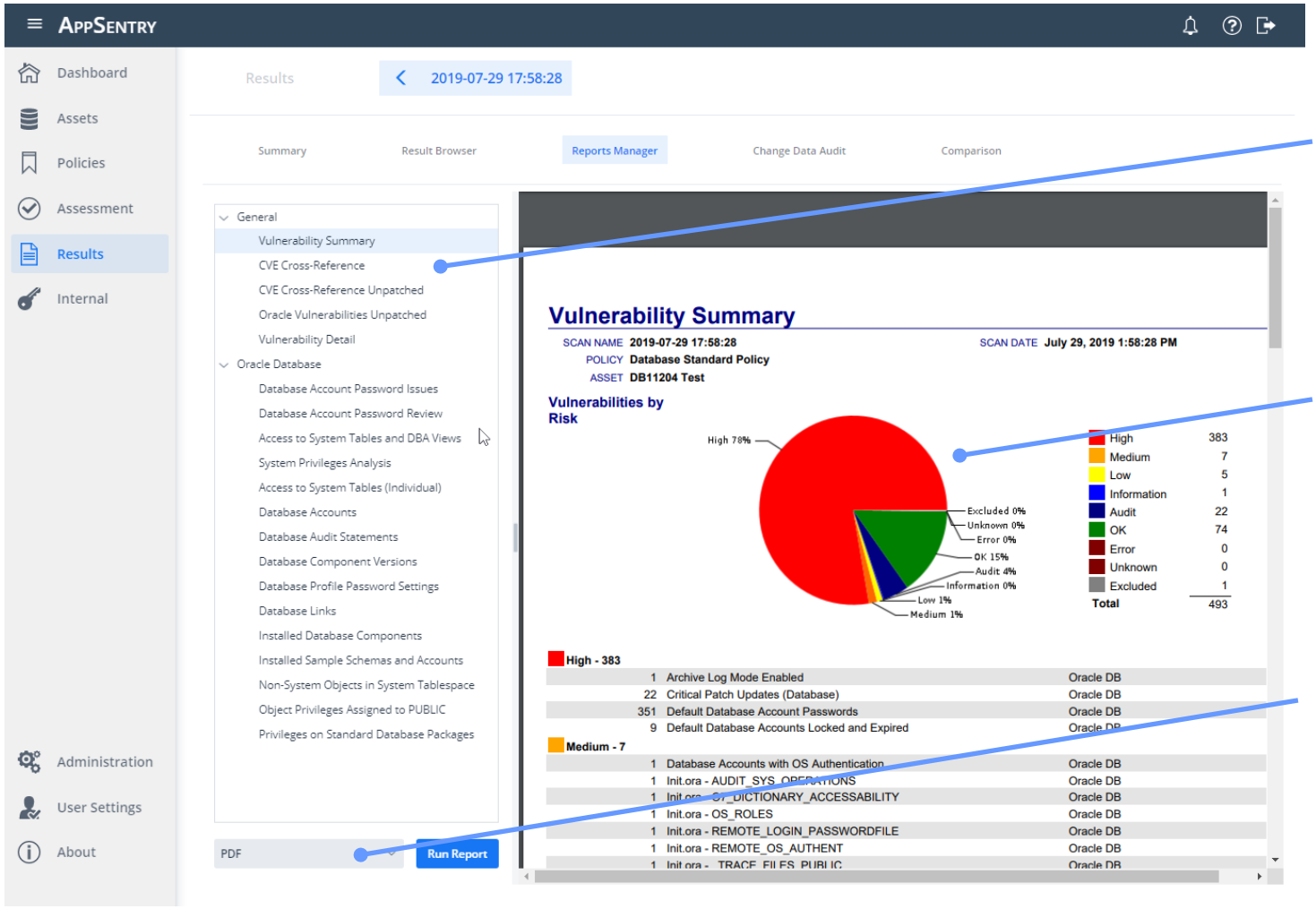


Results from all scans can be reviewed at any time.

Results can be browsed or reports run

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

AppSentry – Reporting

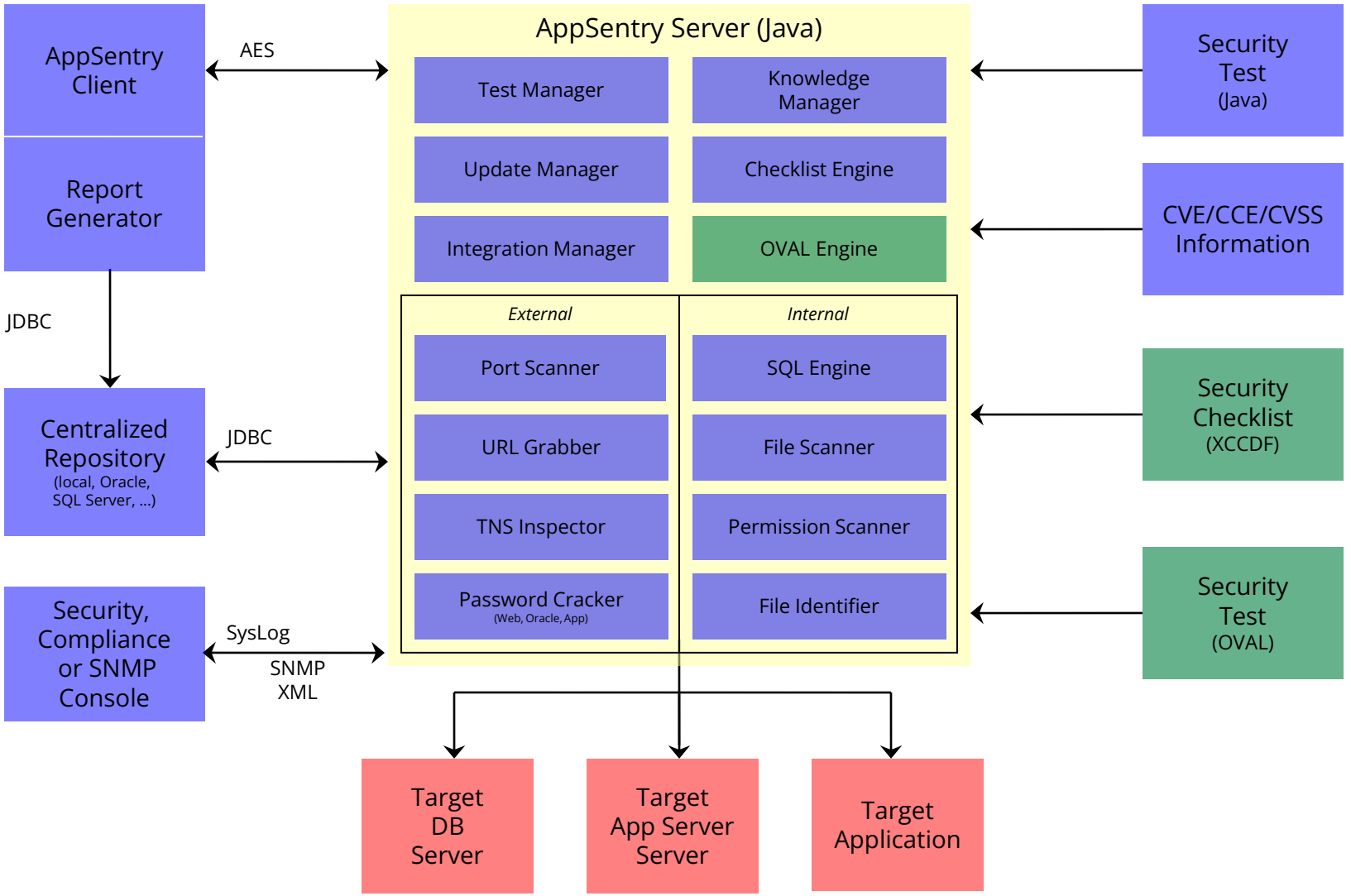


Reports are interactive and some allow drill-down into detailed information

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	23ai 21c 19c 12c (12.1, 12.2)	11g (11.1, 11.2) 10g (10.1, 10.2) 9i (9.0.1, 9.2.0) 8i (8.1.7)
Oracle E-Business Suite	R12 (12.2, 12.1, 12.0) 11i (11.5.1 – 11.5.10 CU2)	
Oracle PeopleSoft	9.1, 9.2 PeopleTools 8.53 – 8.61	
Microsoft SQL Server	2022 2019 2017 2016 2014	2012 2008, 2008 R2 2005 2000

AppSentry Modules

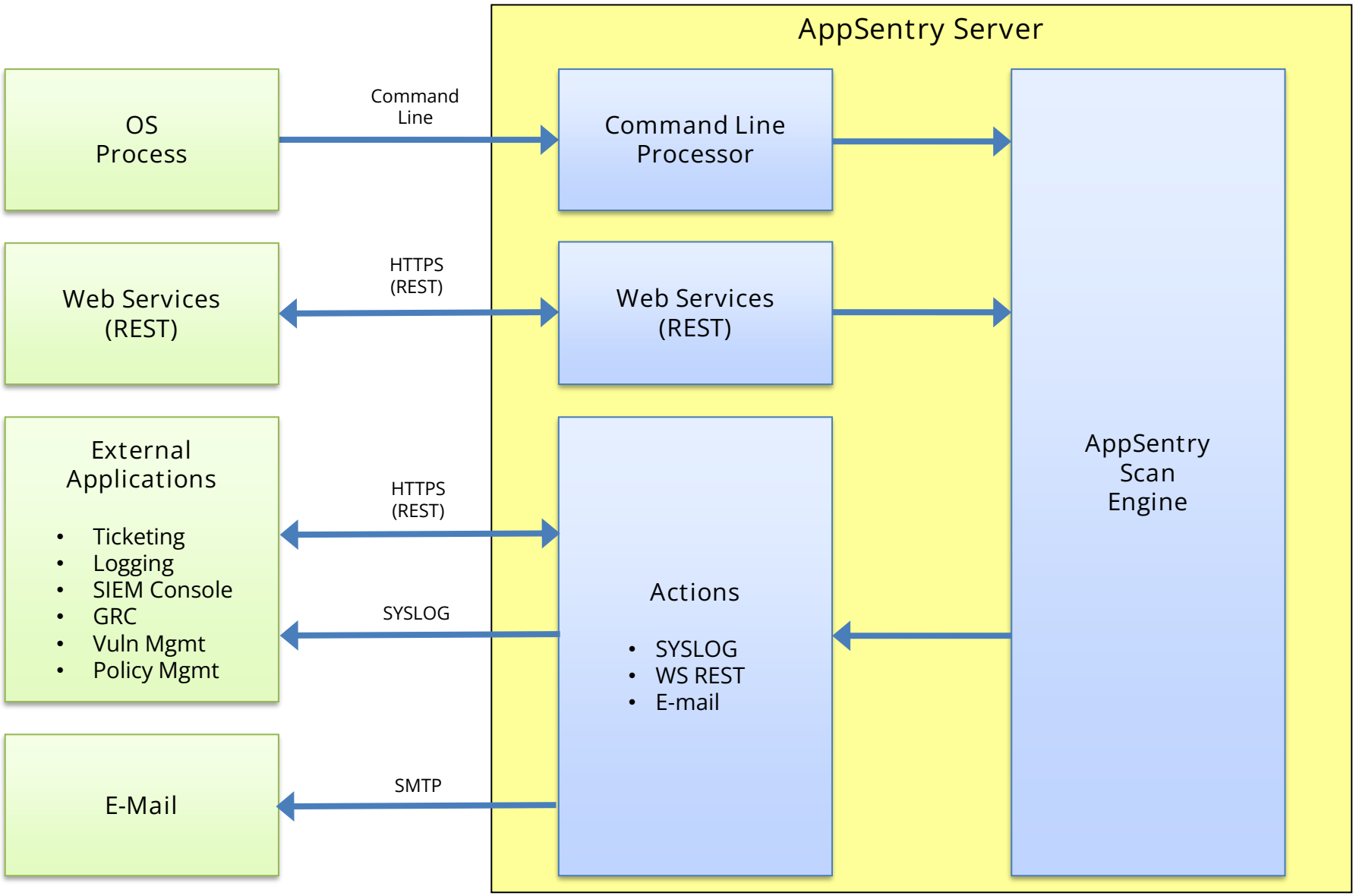
Databases	Cloud Databases	Applications and Application Servers
<u>Relational</u> Oracle RDBMS † Microsoft SQL Server † Oracle MySQL *† MariaDB * Sybase ASE IBM DB2 (LUW) *† PostgreSQL *† Teradata * Informix <u>No SQL</u> Cassandra * MongoDB *† Hadoop	<u>Relational</u> AWS RDS – Oracle *† AWS RDS – SQL Server *† AWS RDS – MySQL * AWS RDS – MariaDB * AWS RDS – PostgreSQL *† AWS Aurora ^ AWS Redshift ^ Azure SQL Database † Azure MySQL/PostgreSQL † <u>No SQL</u> 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

† DOD STIG policy available

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

AppSentry Insights

AppSentry Insights centralizes audit and log data for the Oracle E-Business Suite, Oracle Database, and application server. All audit data locations are automatically found and dynamically adjusts to changes in the application and database. Auditing configuration is continually verified, and recommendations are provided for any missing audits or gaps in auditing according to policy.

AppSentry Insights Features

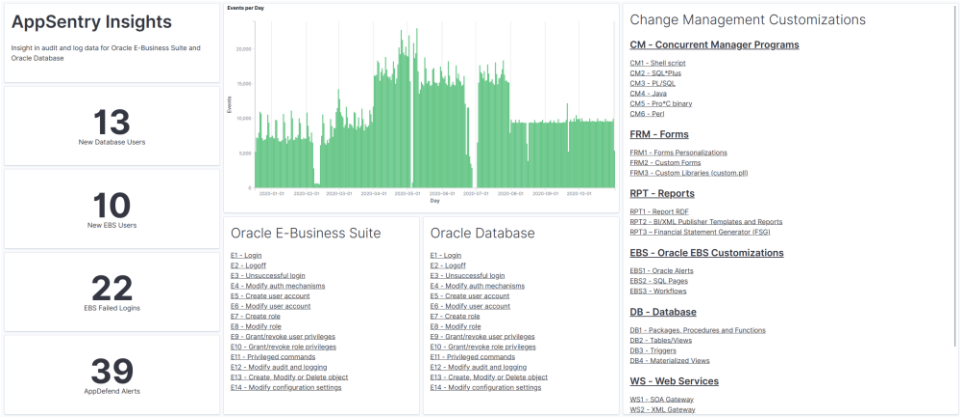
- One-step configuration – a database account
- Pre-configured dashboards, reports, and alerts optimized for Oracle EBS and Oracle Database
- Automatic discovery of Oracle EBS audit and log data locations
- Validation of organizational policy and best practice audit and log configuration

AppSentry Insights Benefits

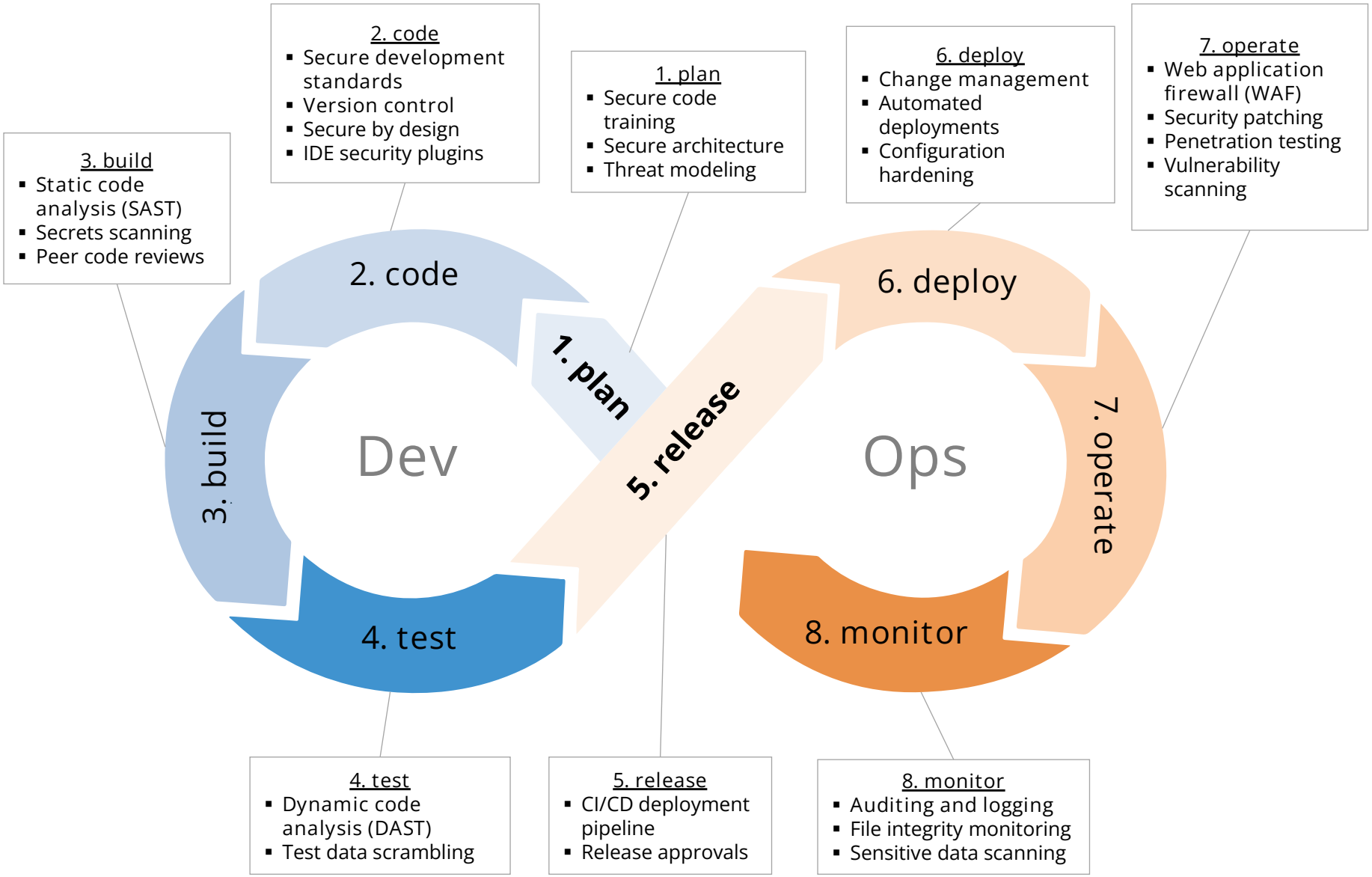
- Improved security and compliance visibility
- Protection, retention, reporting, and alerting of Oracle EBS and Oracle Database audit data
- Audit data analytics and ad-hoc analysis

AppSentry Insights Scope

- Oracle E-Business Suite
- Oracle Database
- Oracle WebLogic (with AppDefend)



Oracle E-Business Suite DevSecOps



Oracle EBS Customizations

Type	Customization	Language	Deployment	Secrets?	Key Issues
Concurrent Manager Programs	CM1 - Shell script	Shell	File (.prog)	Yes	echo APPS password, injection
	CM2 - SQL*Plus	SQL	File (.sql)		SQL injection
	CM3 - PL/SQL	PL/SQL	File (.pl*)	Yes	SQL injection
	CM4 - Java	Java	File (.java)	Yes	SQL injection
	CM5 - Pro*C binary	C	File (.c)		SQL injection, buffer overflow
	CM6 - Perl	Perl	File (.pl)	Yes	Injection
Forms	FRM1 - Forms Personalizations	PL/SQL	Database		SQL injection, authorization
	FRM2 - Custom Forms	PL/SQL	File (.fm*)		SQL injection, authorization
	FRM3 - Custom Libraries (custom.pll)	PL/SQL	File (.pl*)		SQL injection
Reports	RPT1 - Report RDF	SQL, JS	File (.rdf)		SQL injection
	RPT2 - BI/XML Publisher Templates and Reports	SQL	File (.xml)		SQL injection
	RPT3 - Financial Statement Generator (FSG)		Database		
EBS Customizations	EBS1 - Oracle Alerts	SQL	Database		unauthorized SQL
	EBS2 - SQL Pages	SQL	Database		unauthorized SQL
	EBS3 - Workflows	XML	File (.wft)		

Oracle EBS Customizations

Type	Customization	Language	Deployment	Secrets?	Key Issues
Web Pages	WEB1 - Java Server Pages (JSP)	JSP	File (.jsp)		SQL injection, authorization
	WEB2 - Servlets	Java	File (.java)	Yes	SQL injection, authorization
	WEB3 - OA Framework (OAF) Pages	Java	File (.java,.xml)		SQL injection
	WEB4 - OA Framework Personalizations	XML	Database File (.xml)		
	WEB5 - Modplsql	PL/SQL	Database		SQL injection
	WEB6 - Application Express (APEX)	SQL	Database File (.sql)		SQL injection
	WEB7 - ADF applications	Java	File (.java)	Yes	SQL injection
Database	DB1 - Packages, Procedures, and Functions	PL/SQL	Database File (.sql)	Yes	SQL injection, authorization
	DB2 - Tables/Views	SQL	Database File (.sql)		
	DB3 - Triggers	SQL	Database File (.sql)		authorization
	DB4 - Materialized Views	SQL	Database File (.sql)		
Web Services	WS1 - SOA Gateway	Multiple	Database	Yes	SQL injection, authorization
	WS2 - XML Gateway		Database		

3. Build

SAST (Static Code Analysis)	▪ All source code and custom database code (PL/SQL, APEX, etc.) must be periodically scanned for security vulnerabilities ▪ Problem with Oracle EBS customizations is that there are at least nine languages that may be used ▪ Use tools like PMD (Java, PL/SQL), FindSecBugs, SonarCube, Checkmarx to scan source code repository ▪ AppSentry Code uses open source and proprietary libraries to scan all Oracle EBS languages includes Oracle Forms/Reports and APEX
Secrets Scanning	▪ Eliminate hard-coded secrets including passwords, credentials, encryption keys, cloud keys, and certificates ▪ Use a tool such as AppSentry Code to scan source code and database for secrets – scan all deployment packages using both regex and entropy ▪ Wrapped PL/SQL code may contain DBMS_CRYPTO encryption keys

AppSentry Code

AppSentry Code brings DevSecOps to the Oracle E-Business Suite, Oracle Database, and Microsoft SQL Serer.

AppSentry Code Features

- All source code and database code is scanned using open source and proprietary scanners
- Secrets scanning for all source code files
- Scan code where your customizations reside be it in Git, the database, CI integration, or local file system

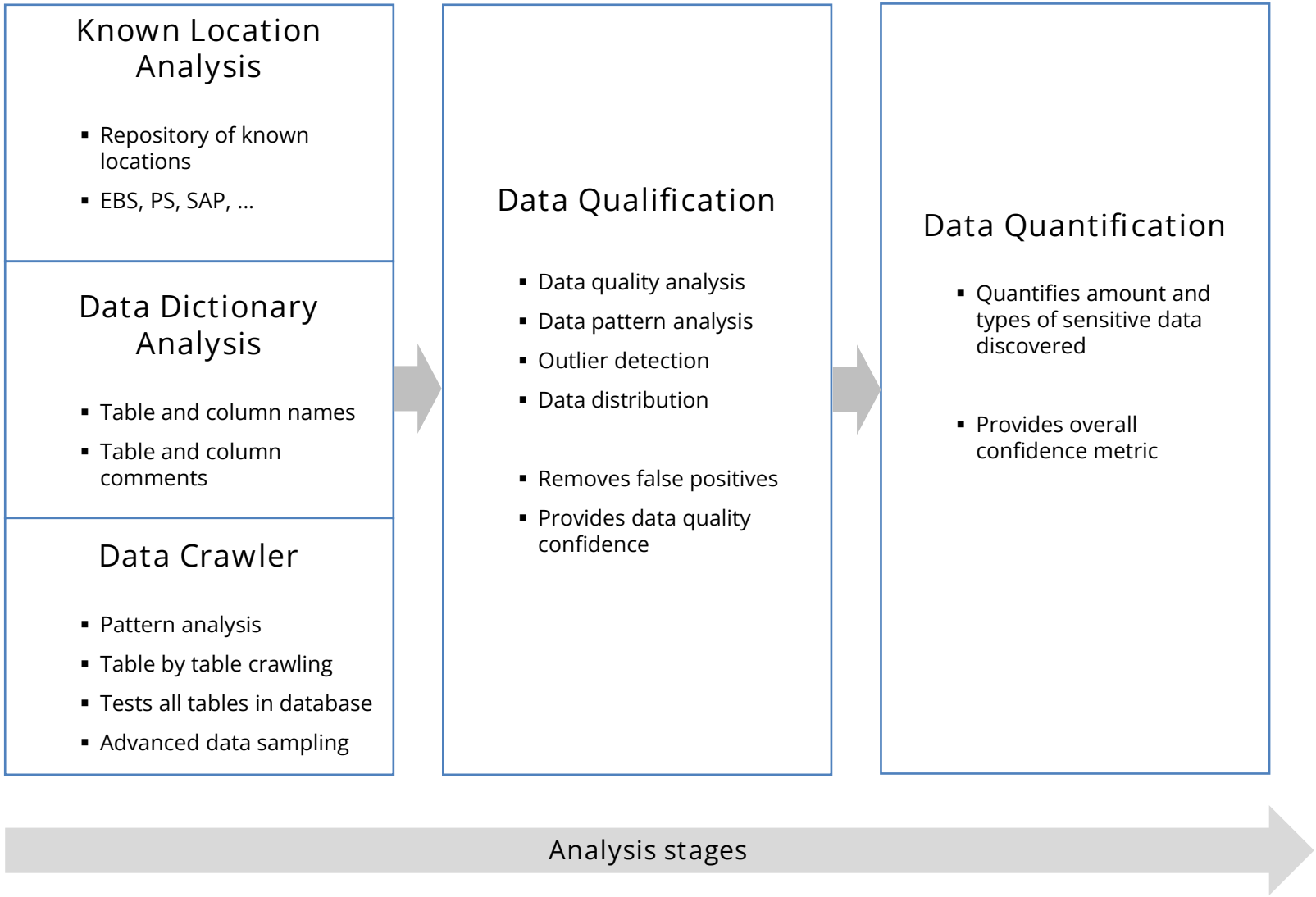
AppSentry Code Benefits

- Early Vulnerability Detection reducing remediation costs by up to 100x compared to post-deployment fixes
- Reduced Manual Code Review Burden by automating the analysis of custom code across multiple layers
- Supply Chain Risk Management by identifying security issues in customizations developed by third-party vendors or offshore development

AppSentry Code Scope

- Oracle E-Business Suite
  - Concurrent Manager programs
  - Custom PL/SQL and SQL objects
  - Web page customizations
  - Forms and Reports
  - Web Services
- Oracle Database
  - PL/SQL custom objects
  - Oracle Application Express (APEX)
- Microsoft SQL Server
  - T-SQL custom objects

AppSentry Sensitive Data Discovery (SDD)



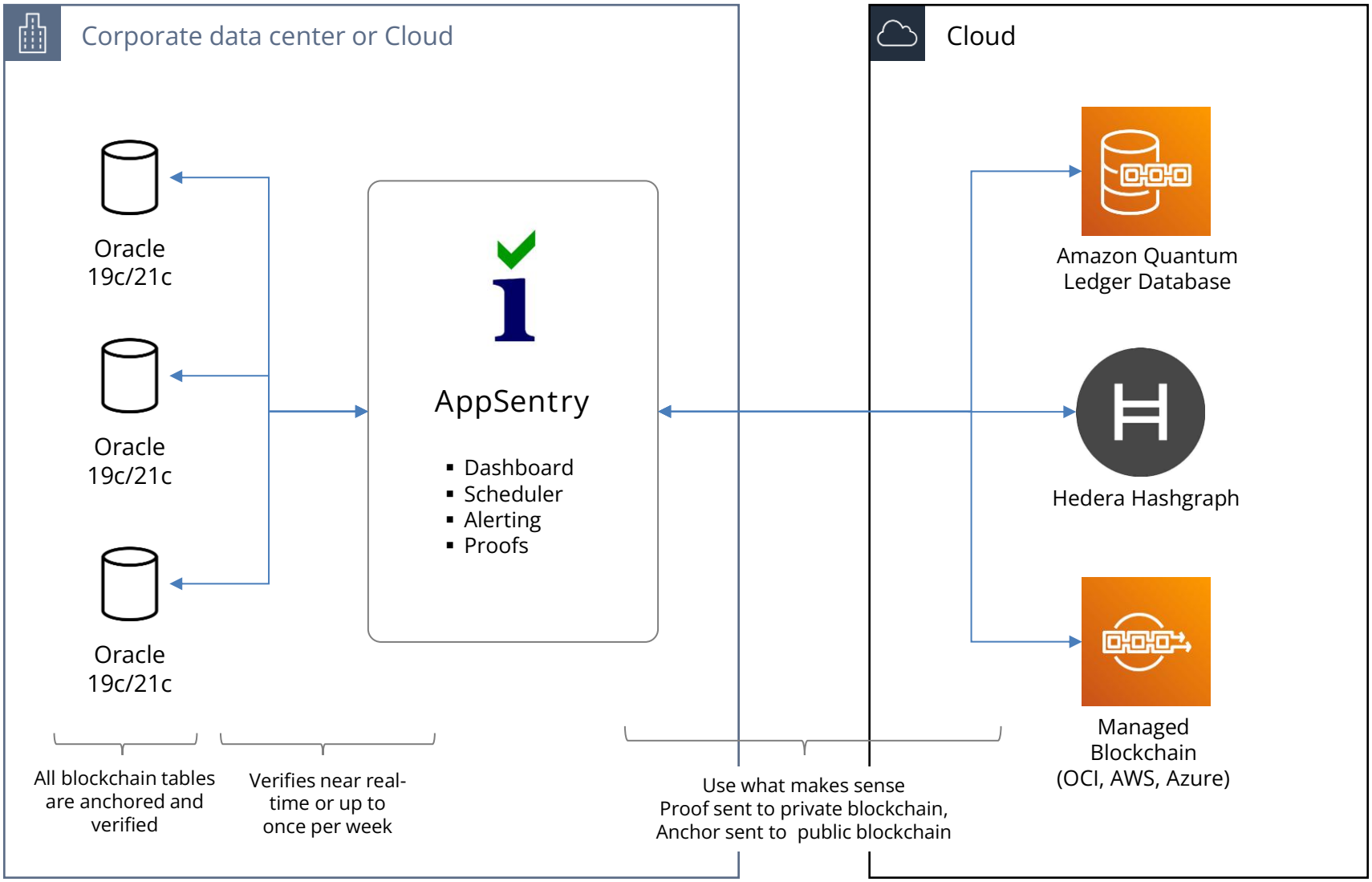
Blockchain Table Integrity

Oracle Database 21c Database Administrator's Guide

"An important aspect of maintaining the integrity of blockchain table data is to ensure that all rows are intact. Computing a signed digest provides a snapshot of the metadata and data about the last row in all chains at a particular time. You must store this information in [an external] repository. Signed digests generated at various times comprise the input to the DBMS_BLOCKCHAIN_TABLE.VERIFY_TABLE_BLOCKCHAIN procedure. Use this procedure to verify the integrity of rows created between two *specified times."*

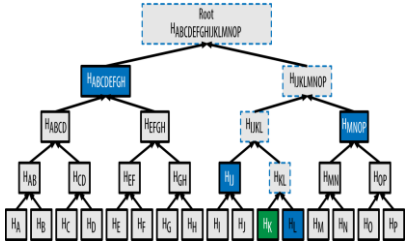
- Use Integrigy AppSentry to periodically retrieve, store, and verify the integrity of all blockchain tables – "anchor the blockchain"
  - Fingerprints the database to verify the database
  - Detects all blockchain tables
  - Fingerprints the table to verify the table
  - Generates a signed digest for each blockchain table
  - "Anchors" the signed digests for each blockchain table to AppSentry, AWS Quantum Ledger Database, or Hedera Hashgraph (future Ethereum and Oracle, Azure, and AWS blockchains)
  - Verifies since last signed digest to confirm the integrity of the blockchain table

AppSentry Blockchain – Blockchain Table Anchor

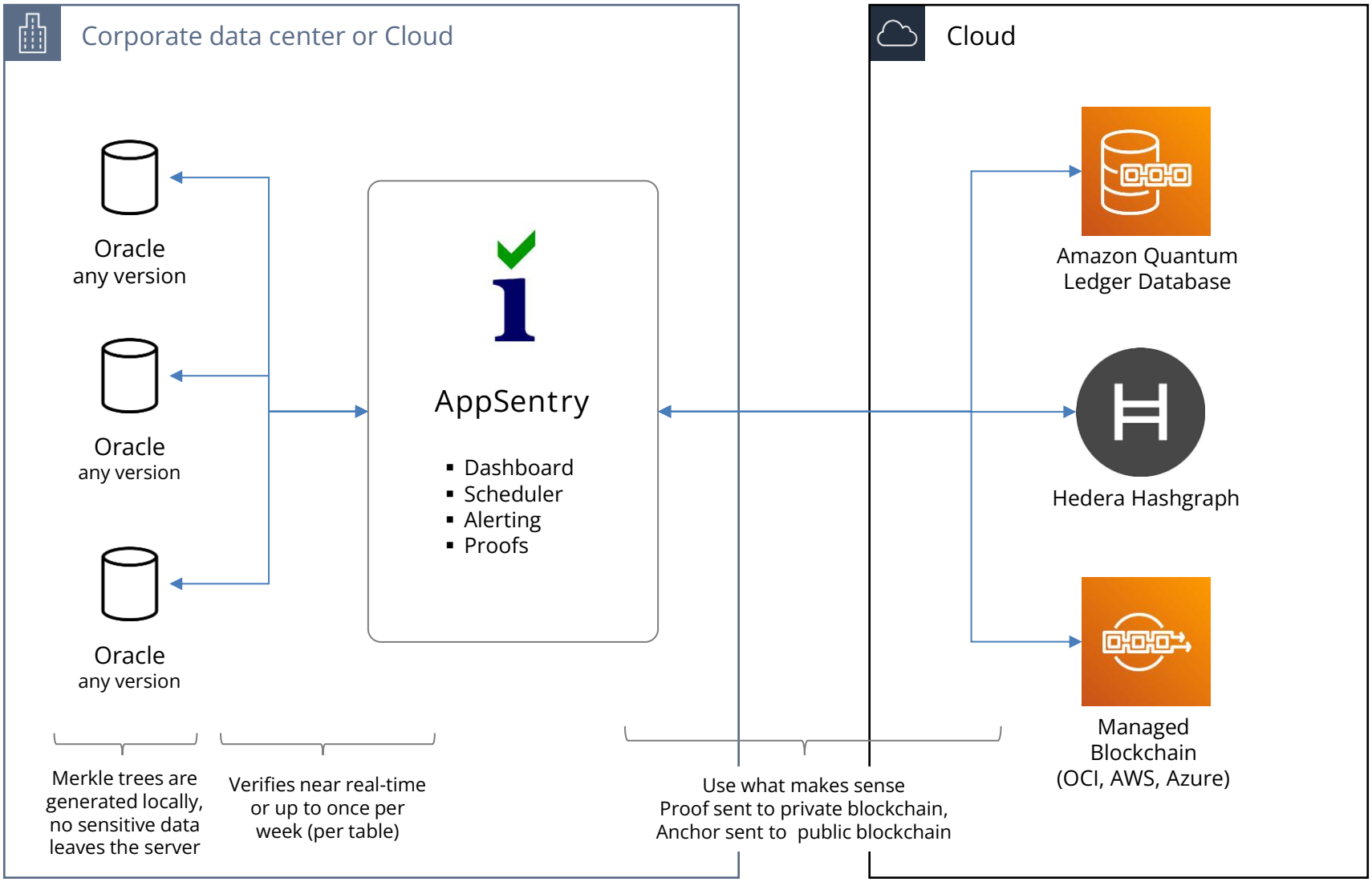


AppSentry Blockchain – Standard Table Anchor

- AppSentry Blockchain allows you to anchor any Oracle table when you can't use Blockchain or Immutable tables – create digital trust
  - Pre-19.10 databases
  - Package applications
- Generates Merkle trees for all new and changed rows
  - A Merkle tree is a tree of hashes that allow for efficient and secure verification of large structures of data
  - Triggers and Flashback may be used to enhance detection of table inserts and changes
  - Merkle trees are calculated in-database so no sensitive data is transferred outside of the database server



AppSentry Blockchain – Standard Table Anchor



Integrigy Contact Information

Integrigy Corporation

web – www.integrigy.com

e-mail – info@integrigy.com

blog – integrigy.com/oracle-security-blog

youtube – youtube.com/integrigy