

AppSentry

Assess and validate the security and compliance of mission critical

AppSentry™ is a new generation of security auditing tool and vulnerability assessment scanner. Unlike other security scanners, AppSentry knows the application and database it is validating – its technology and data model. The security audits and checks are written specifically for the application or database being tested. Hackers and mischievous employees often exploit security issues at different layers of the technology stack, thus only a complete and comprehensive security validation will uncover all risks in a multi-tiered environment.

The advantage of AppSentry is now you don't have to have separate tools for the application, database, web server, and application server. AppSentry is a single tool that can validate and audit the security of the entire application technology stack from operating system to application layer.

Application and Database Security Validation

Application and Database Security Validation uses two techniques to identify security risks –

- ◆ Vulnerability testing to externally discover risks
- ◆ Auditing to internally discover risks

AppSentry uses advanced penetration testing techniques to externally discover security risks in the operating system, web servers, application servers, databases, and application. Tests for known exploits and configuration errors are performed externally to the application in an attempt to break-in. Common and well-known network ports, web server directories, and database accounts are probed to identify vulnerabilities in the configuration. The password module will brute-force operating system, web server, database, and application authentication using either default passwords, dictionary attacks, or a password list.

AppSentry Highlights

Target Applications and Databases

- ◆ Oracle E-Business Suite
- ◆ Oracle PeopleSoft
- ◆ Oracle Database
- ◆ Microsoft SQL Server

Easy to Deploy and Use Regularly

- ◆ Runs on server, cloud, laptop, or USB
- ◆ No database drivers or other special software required
- ◆ No agents or other software need to be installed on the target

Pre-defined Compliance Policies

- ◆ Sarbanes-Oxley (SOX)
- ◆ European Union GDPR
- ◆ Payment Card Industry Data Security Standard (PCI-DSS)
- ◆ DOD 8500.1—DISA STIG
- ◆ FISMA—NIST 800-53
- ◆ HIPAA

Simple GUI and Friendly Reporting for Use By

- ◆ Internal and external auditors
- ◆ Database administrators
- ◆ System administrators
- ◆ IT Security professionals

AppSentry

AppSentry Audits and Checks

AppSentry performs over 1,450 security audits and checks against the target. All technology components – database, web server, application server, and operating system – are analyzed as well as the application. The audits and checks are internal and external; some are performed through penetration testing while others are performed by accessing the file-system, database, and application.

AppSentry can be deployed in the cloud, on virtual servers, to auditor's laptops, and even to a USB key. AppSentry seamlessly integrates with your existing security eco-system through web services, syslog, and xml.

Sample AppSentry Audits and Checks

Oracle E-Business Suite

- Application accounts
- Users with Sysadmin responsibility
- Application security patches
- Application auditing
- Security related system profile options

Oracle PeopleSoft

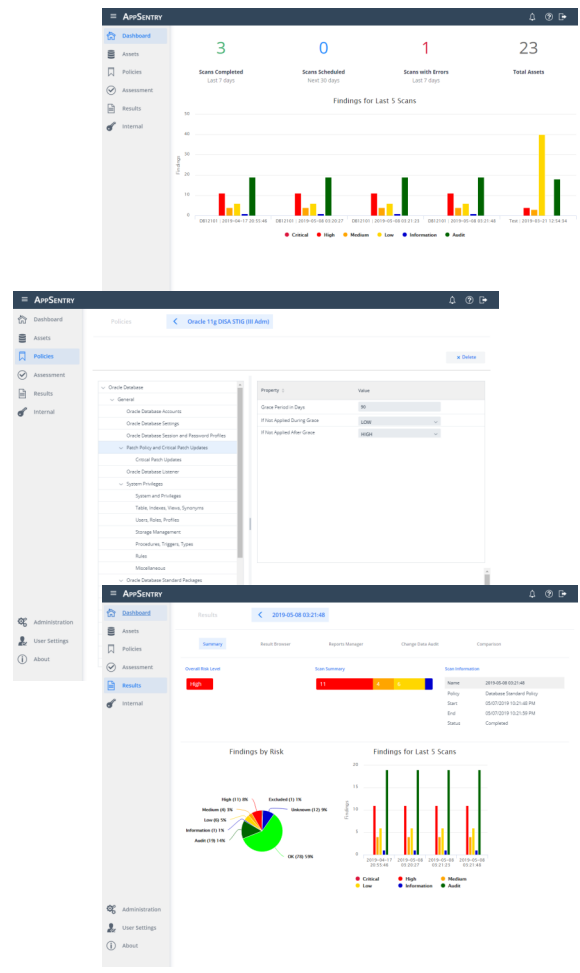
- Application accounts
- User profiles
- Roles and permission lists
- Application security patches
- Application auditing
- Query security

Oracle Database

- Database accounts
- Listener exploits
- Database auditing (SYS.AUD\$)
- Database security patches
- APPS permissions
- APPLSYSUB permissions
- Database links

Oracle Web Server/WebLogic

- Apache configuration (http.conf)
- Apache logging (http.log)
- Apache virtual directories
- Web server security patches
- SSL configuration



AppSentry Target Requirements

Oracle E-Business Suite	12.2 12.1 12.0 11.5.10 CU2	All supported operating systems
Oracle PeopleSoft	9.1, 9.2 8.50 - 8.60	All supported operating systems
Oracle Database	23c (23.x), 21c (21.x), 19c (19.x), 18c (18.x) 12c (12.1, 12.2) 11g (11.1, 11.2) 10g (10.1, 10.2) 9i (9.0.1, 9.2) 8i (8.1.7)	Sun Solaris (SPARC and Intel) HP (HP/UX and Tru64) IBM (AIX) Linux (all supported vendors) Windows Server
Microsoft SQL Server	2022, 2019, 2017, 2016, 2014, 2012, 2008, 2008 R2, 2005, 2000	All supported operating systems including Linux

AppSentry Platform Requirements

Operating System	All Java supported operating systems (Oracle Java, OpenJDK, Amazon Corretto, Azul Zulu)
Browser	Chrome, Firefox, Safari, Edge
Processor, RAM, Disk	Intel Pentium or AMD CPU 1 GB RAM 2 GB Free Disk Space
Database Drivers	AppSentry requires no database drivers or other software to be installed on either the server or target

MySQL, Sybase, DB2 LUW, Teradata, and PostgreSQL available as part of a consulting engagement.