AppSentry

Assess and validate the security and compliance of mission critical databases and applications with precision and confidence

AppSentry is a new generation of security auditing tool and vulnerability assessment scanner. Unlike other security scanners, AppSentry knows the application 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.

Using auditing to internally pinpointing security weaknesses configuration issues, AppSentry can spot risks missed by traditional vulnerability testing. AppSentry knows the application it is validating – its technology and data model. By pinpointing weaknesses by internally auditing and alerting to suspicious activity, AppSentry can spot risks in the installation, configuration, and operation of the database and application missed by traditional vulnerability testing.

AppSentry Highlights

Target Applications, Databases, and Web Servers -

- Oracle E-Business Suite
- Oracle Database
- Microsoft SQL Server
- Oracle Application Server

Easy to Deploy and Use Regularly -

- Runs on any Microsoft Windows PC
- No database drivers or other special software required on the PC
- No agents or other software need to be installed on the target

Pre-defined Compliance Policies -

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

Simple GUI and Friendly Reporting for Use By -

- Internal auditors
- Database administrators
- System administrators
- IT Security professionals

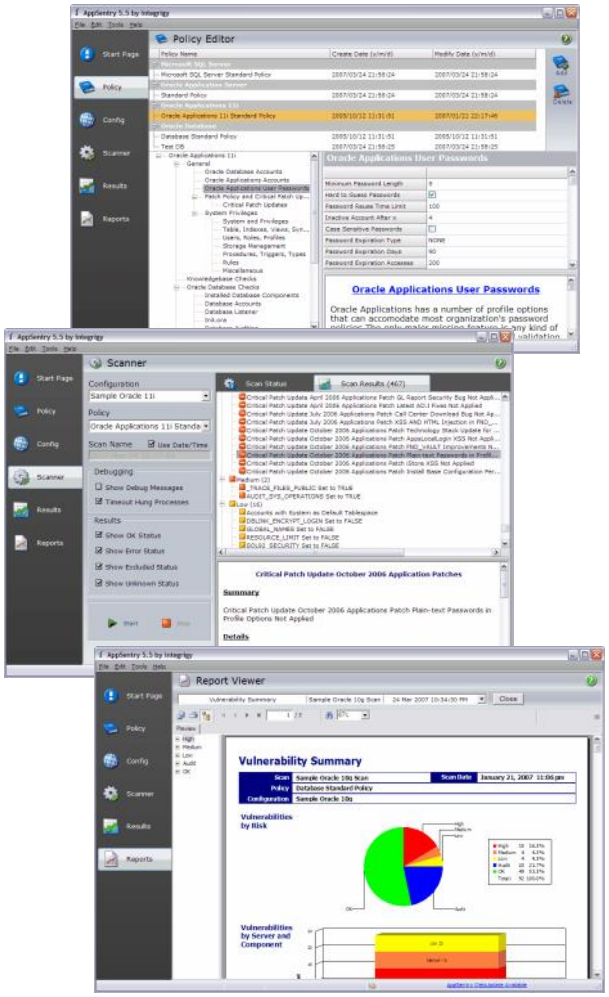
Integration with Third-party Systems -

- XML Import/Export
- Security Event Managers (SIEM)
- SYSLOG

AppSentry

AppSentry Audits and Checks

AppSentry performs over 300 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.



Sample AppSentry Audits and Checks

Oracle E-Business Suite
Application accounts
Users with Sysadmin responsibility
Application security patches
Application auditing
Security related profile options

Oracle Database
Database accounts
Listener exploits
Database auditing (SYS.AUD$)
Database security patches
APPS permissions
APPLSYSPUB permissions
Database links

Oracle Web Server
Apache configuration (http.conf)
Apache logging (http.log)
Apache virtual directories
Web server security patches
SSL configuration
Oracle support cgi-bin scripts
PLSQL Cartridge exploits

Oracle Application Server
Forms and reports security patches
SSL configuration

AppSentry Target Requirements		
Oracle E-Business Suite	11.5.7 - 11.5.10 CU2 12.0 12.1 12.2	Sun Solaris (SPARC) HP (HP/UX) IBM (AIX) Linux (all supported vendors) Windows Server
Oracle Database	8i (8.1.7) 9i (9.0.1, 9.2) 10g (10.1, 10.2) 11g (11.1, 11.2) 12c (12.1)	Sun Solaris (SPARC and Intel) HP (HP/UX and Tru64) IBM (AIX) Linux (all supported vendors) Windows Server
Oracle Application Server	9iAS (1.0.2, 9.0.x) 10g (9.0.4, 10.1) 11g (11.1)	Sun Solaris (SPARC and Intel) HP (HP/UX and Tru64) IBM (AIX) Linux (all supported vendors) Windows Server
Microsoft SQL Server	2000 2005 2008 2008 R2 2012 2014	Windows Server 2003 Windows Server 2008 Windows Server 2012

AppSentry Platform Requirements	
Operating System	Microsoft Windows 2000 SP4 Microsoft Windows XP SP1 Microsoft Windows Vista Windows 7 Windows 8 Windows 10 Windows Server (2003, 2008, 2012, 2012 R2)
Other Software	Adobe Acrobat 4.0 or later Web Browser (IE, Firefox, Chrome, Edge)
Processor, RAM, Disk	Intel Pentium or AMD CPU 1 GB RAM 500 MB Free Disk Space
Windows Privileges	AppSentry does not require administrator privileges to install or run
Database Drivers	AppSentry requires no database drivers or other software to be installed