

# AppRadar™

## KEY FEATURES

- Monitor all user activity and system changes
- Real-time database threat monitoring
- Best practice policies and reports for rapid regulatory compliance (HIPAA, SOX, PCI, GLBA, FISMA, etc.)
- Extensive up-to-the-minute knowledgebase of database security threats
- Network-based and host-based sensors for easy deployment
- Scalable high-performance architecture and centralized management and reporting
- Support for Oracle, Microsoft SQL Server, Sybase and IBM DB2

## Real-time database activity monitoring

AppRadar™ is a real-time database activity monitoring solution that combines enterprise-class database security with intelligent, real-time monitoring and auditing. Unlike generic network or operating system solutions, and much more than just a generic logging system, AppRadar delivers database-specific auditing and threat monitoring. As a result, AppRadar not only alerts on security events in real-time, but also flags audit events defined by user activity. In doing so, AppRadar enables a layered defense and augments corporate privacy and regulatory compliance initiatives.

### Real-Time Database Security Solution

AppRadar offers network and host-based versions of its security solution based on the industry's most complete knowledgebase of database threats. AppSecInc's network-based sensors are able to monitor many databases, and types of databases with a single sensor while an AppRadar Sensor on the host will detect local activity on the database. AppRadar monitors and detects all database events and attacks in real-time. Through its sophisticated notification system, it sends alerts to either your existing monitoring infrastructure, or to the AppSecInc Console.

### Non-Intrusive Security Monitoring and Database Auditing

Existing monitoring solutions focus on network-level issues or web traffic; furthermore, these solutions tend to be targeted at the perimeter and thus do not inspect and audit internal traffic, partner/VPN traffic, or encrypted traffic. Finally, these solutions do not understand the complex protocols used by databases and database applications—a severe handicap when trying to detect threats to the database.

AppRadar, on the other hand, protects database applications directly. AppRadar inspects all traffic—from outside or inside an enterprise—and applies the industry's most comprehensive knowledgebase of database application threats. Thus, even if the attack is deeply embedded in a

SQL command and is executed by an employee with privileges on the database, AppRadar detects it. In addition, AppRadar has a flexible auditing system that allows organizations to log and/or alert on specified users and queries. Our filter wizard allows you to customize exactly which audit and security events you need to monitor. AppRadar also includes best-practice policies based on auditor recommendations for rapid compliance with industry standard regulations including Sarbanes Oxley, HIPAA, FISMA and PCI, to name a few.

### Scalable Enterprise Architecture

Through a distributed architecture with local AppRadar Sensors and the central AppSecInc Console, AppRadar's database activity monitoring and security audit is built for the enterprise. Role-based access control to the AppSecInc Console helps operationalize enterprise deployments by allowing privileges to be segmented according to responsibility.

### Intuitive to use and easy to deploy

The host-based version of AppRadar was painstakingly designed to have little to no impact on your database performance. Similarly, the network-based version of AppRadar adds no delay and does not use database-installed programs. AppRadar Sensors are centrally monitored and configured through the web-based AppSecInc Console.



**APPLICATION  
SECURITY, INC.**

# AppRadars™

## Complementary and Compatible Security Solution

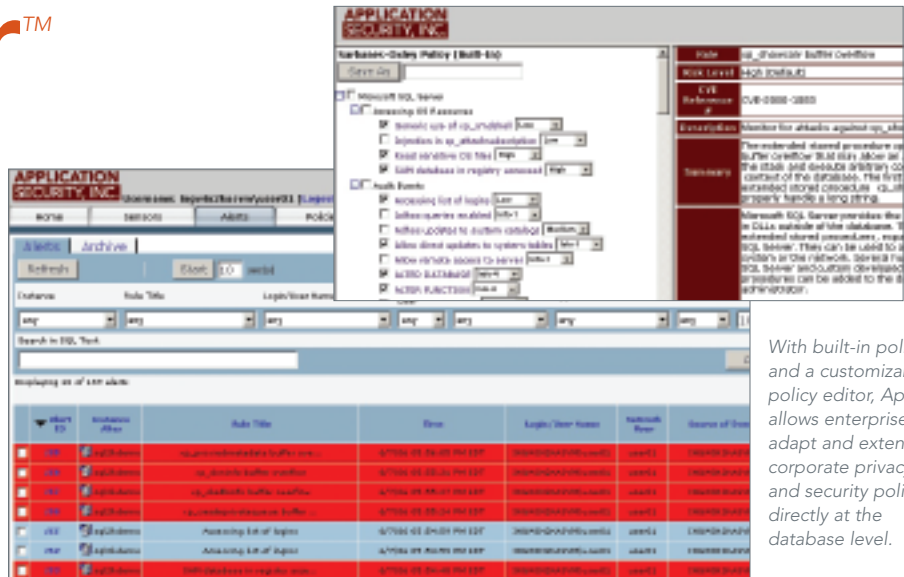
AppRadars picks up where existing network and operating system security solutions leave off by extending real-time monitoring and protection directly to the database. This approach tightens your enterprise security architecture by directly securing sensitive assets. It also enhances corporate privacy and regulatory compliance initiatives, since most customer data and transactions reside in a database.

## Industry-Leading Database Security Knowledgebase

AppRadars is built upon the industry's most comprehensive catalog of database-specific threats, many discovered by our own research and development team (SHATTER). AppSecInc's ASAP Update™ mechanism ensures protection remains up to date. This allows us to immediately identify and detect worms, buffer overflows and privilege escalation attacks while also explaining the details of the event for a useful response.

## AppRadars Event/Attack Categories and Rules

- Accessing OS Resources
- Audit Events
- Buffer Overflow Attacks
- Password Attacks
- Privilege Escalation Attempts
- Security Tools in Use
- System Events
- Web Application Attacks
- User-Created Signatures and Rules



With built-in policies and a customizable policy editor, AppRadars allows enterprises to adapt and extend corporate privacy and security policies directly at the database level.

### MINIMUM SYSTEM REQUIREMENTS

#### Network-based AppRadars Sensor

**Operating Systems:** Microsoft Windows Server 2003, Microsoft Windows 2000 Server

**Hard Drive:** 150 MB

**Supported Databases:** Oracle 7.x; Oracle 8, 8i, 9i, 10g; Sybase 11.x-15; IBM DB2 UDB version 8

#### Host-based AppRadars Sensor

*Monitoring Microsoft SQL Server*

**Operating Systems:** Microsoft Windows Server 2003, Microsoft Windows 2000 Server

**Hard Drive:** 150 MB

**Supported Versions:** Microsoft SQL Server 2005 (all editions), Microsoft SQL Server 2000 (all editions)

*Monitoring Oracle Database*

**Operating Systems:** Solaris 8, 9, 10; Red Hat Enterprise Linux 3 and 4

**Hard Drive:** 50 MB minimum

**Supported Versions:** Oracle 9i, 10g

**RAC support:** Yes

*Monitoring Sybase ASE and IBM DB2 UDB-Coming soon.*

#### AppSecInc Console for AppRadars

**Operating Systems:** Microsoft Windows Server 2003, Microsoft Windows 2000 Server, 64-bit supported

**Browser:** Internet Explorer 6.0

**Processor:** Intel Pentium 1 GHz

**RAM:** 1 GB

**Hard Drive:** 150 MB for program files, 3 GB minimum for data repository

**Network Connectivity:** Must exist between AppSecInc Console and AppRadars Sensor

**A 30-day evaluation copy of AppRadars is available for download at:**  
[www.appsecinc.com/products/appradars/](http://www.appsecinc.com/products/appradars/)

## ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is the leading provider of database security solutions. The company's products - the industry's only complete vulnerability management solution for the application tier - proactively secure enterprise applications at more than 600 organizations worldwide. By securing data at its source, AppSecInc enables organizations to more confidently extend their business with customers, partners and suppliers while meeting regulatory compliance requirements. Our security experts, combined with our strong support team, deliver up-to-date application safeguards that minimize risk and eliminate its impact on business. Please contact us at 1-866-927-7732 to learn more, or visit us on the web at [www.appsecinc.com](http://www.appsecinc.com).

**APPLICATION SECURITY, INC.**

[www.appsecinc.com](http://www.appsecinc.com)