

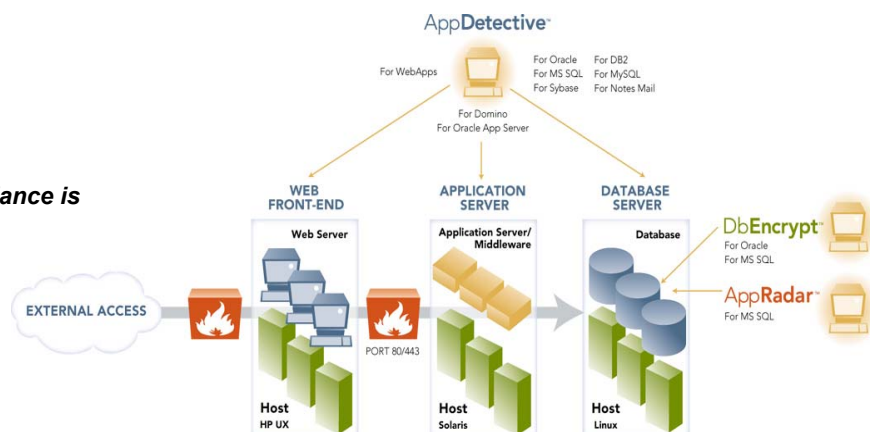
Sarbanes-Oxley and Application Security

The Sarbanes-Oxley Act (SOX) radically redesigned federal regulation of public company corporate governance and reporting obligations by demanding executives, auditors, securities analysts and legal counsel be accountable for the integrity of financial reporting

With the integrity of financial data at stake, compliance efforts must include securing data at its source – the database.

The single common threat to SOX compliance is

**UNAUTHORIZED
DATA DELETION,
MODIFICATION, OR ACCESS**



Application Security Inc's (AppSecInc) line of database application security solutions, in use by more than 200 organizations around the world, can bolster SOX compliance efforts by extending them to include the database – arguably the crown jewels at any organization.

VULNERABILITY ASSESSMENT

AppDetective, a network-based vulnerability assessment scanner, secures against unauthorized deletion, modification, and access to data by discovering database applications within your infrastructure and assessing their security strength based on the industry's most extensive knowledge of database application-level vulnerabilities. AppDetective empowers you to help address SOX compliance needs related to access control:

- **Discovery** – Accurately inventory all database applications on your network, identifying and documenting which store critical financial data.
- **Pen Test and Audit** – Assess the security of your database applications both from the outside and the inside by checking for denial of service and password attacks, misconfigurations, vulnerabilities, identification/password and access control issues, and application and operating system integrity weaknesses.
- **Reports** – Generate both detailed and high-level reports to serve the needs of all levels of your organization.

INTRUSION DETECTION AND AUDITING

AppRadar is a real-time database intrusion detection and auditing solution that provides purpose-built protection for enterprise databases. Unlike generic network or operating system solutions, AppRadar delivers database-specific, active protection, monitoring, and auditing. By complimenting existing perimeter-focused defenses, AppRadar enables you to track all access to data by unique ID providing you with:

- Centralize auditing/tracking across all SQL transactions on your databases
- Gain real-time notification of all system events and attacks such as; OS resource attacks, buffer overflow and password attacks, privilege escalation, and web application attacks

COLUMN-LEVEL DATABASE ENCRYPTION

DbEncrypt secures sensitive data at the specific column level on your production databases. Far more than an encryption toolkit, DbEncrypt includes a robust user and key management system, templates to ease deployment, and support for a variety of strong encryption algorithms - all from a point-and-click interface. DbEncrypt empowers you to address SOX compliance, serving as the "last line of defense" controlling access to view, modify or otherwise corrupt your most sensitive financial data.

Although not specifically stated in SOX, the importance of IT security is implied to ensure, confidentiality, integrity, and availability of financial data within the following sections:

STATUTE	SUMMARY	CONTROL FRAMEWORK	APPSECINC COVERS
Section 103 – Auditing, Quality Control, And Independence Standards and Rules	Requires maintenance of all audit-related records (including electronic) for 7 years.	<u>Monitoring</u> – Determine adequate controls for flow of information <u>Control Activities</u> – Set policies and procedures for risk management	The database is sometimes overlooked in a SOX review; but it is the most important infrastructure component at an enterprise and must be identified as a critical component to be assessed for SOX compliance.
Section 302 – Corporate Responsibility for Financial Reports	Requires CEO and CFO to certify the accuracy of corporate financial reports.	<u>Control Environment</u> – Set tone and policy for internal controls from the top	AppSecInc solutions help management ensure the accuracy of corporate financial reports by applying proven vulnerability assessment, intrusion detection and auditing, and encryption methodologies to the database.
Section 404 – Management Assessment Of Internal Controls	Requires CEO, CFO, and auditors to confirm the effectiveness of internal controls for financial reporting.	<u>Monitoring</u> – Determine adequate controls for flow of information <u>Risk Assessment</u> – Evaluate risk from internal and external views <u>Control Activities</u> – Set policies and procedures for risk management	AppDetective offers an essential piece to overall SOX compliance. In a SOX review, it is critical to blueprint and identify all applications related to financial reporting transactions. AppDetective allows enterprises to intelligently discover their database applications. Having identified the critical databases, through external penetration tests and internal audits AppDetective helps enterprises proactively minimize the likelihood of an attack by identifying all the security holes and providing detailed remediation information. Canned reports are provided for all levels within the enterprise from high-level management reports to detailed remediation reports. Beyond an initial SOX review, AppDetective enables enterprise IT security personnel to continuously track and manage database vulnerabilities.
Section 409 – Real Time Disclosure	Requires any significant changes in financial state of issuer “on a rapid and current basis.”	<u>Monitoring</u> – Determine adequate controls for flow of information <u>Control Activities</u> – Set policies and procedures for risk management <u>Information & Communication</u> – Ensure information is identified and communicated	AppRadar provides real-time monitoring of all access to financial data by unique ID. Built on the industry’s most extensive knowledge-base of database vulnerabilities, AppRadar alerting captures detailed information, including the SQL statement transmitted to the database and the user and the application used to execute it for each user and system event occurrence -- information that is essential for a proper audit trail. By retaining audit logs and providing a mechanism to manage them, AppRadar helps enterprise IT personnel integrate this information with existing management systems via several notification methods, including, email, SNMP traps, and log files.
Section 802 – Criminal Penalties For Altering Documents	Requires retention and protection of audit and related documents, including electronic records.	<u>Control Environment</u> – Set tone and policy for internal controls from the top <u>Information & Communication</u> – Ensure information is identified and communicated	
Section 906 – Corporate Responsibility For Financial Reports	Requires CEO and CFO to certify the accuracy of corporate financial reports.	<u>Control Environment</u> – Set tone and policy for internal controls from the top	If for any reason the database is compromised, DbEncrypt protects your critical information from unauthorized modification, deletion, or access. DbEncrypt has won product reviews based on its ease of deployment and application transparency. In contrast to bulk encryption, column-level protection provides precise security with minimal performance impact.

AppSecInc and AppDetective, AppRadar, and DbEncrypt are trademarks of Application Security, Inc. All other company and product names are trademarks of their respective companies.