APPLICATION SECURITY, INC. ®
Database Security, Risk and Compliance

FISMA and Application Security, Inc.

Title III of the E-Government Act of 2002, also known as The Federal Information Security Management Act (FISMA), provides a comprehensive framework for ensuring information security controls are enforced for all federal information and assets. Based on this framework, FISMA mandates that all agencies, contractors, and associated entities develop, document, and implement information security programs and annually report security status to the Office of Management and Budget (OMB).

This Act, which underscores the importance of information security, was developed with the sole purpose of strengthening federal systems. The compliance framework, developed by the National Institute of Standards and Technology (NIST), requires agencies to inventory information systems, categorize information for risk assessment and management, implement security controls and planning, and continuously monitor all systems for effectiveness.

Non-compliance with FISMA is published by Congress in public agency scorecards and may require explanations before Congress or result in monetary penalties.
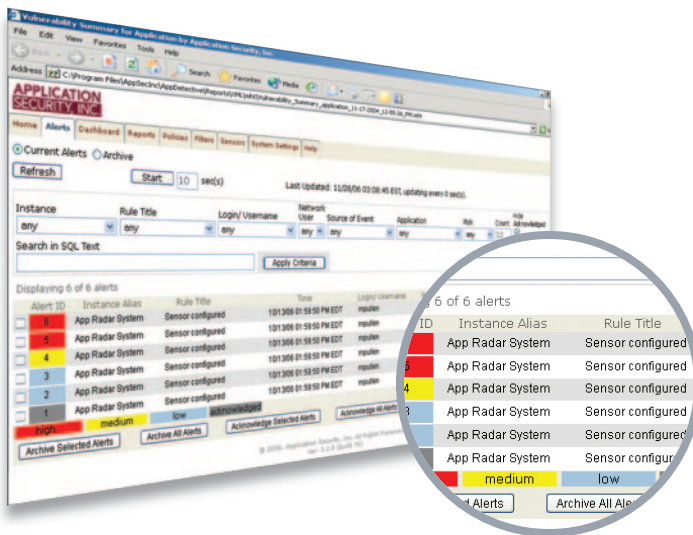

DbProtect acts as a continuous "data sentry" – monitoring and alerting on suspicious behavior and inappropriate access including the actions of insiders. Secure, tamper-proof and tamper evident repositories maintain the integrity of the forensic evidence in the event of a database breach or security-related incident.

THE SOLUTION:
APPLICATION SECURITY, INC.'S DbPROTECT

Application Security, Inc. solutions harden and secure database systems for over 200 unique federal, state, and local government clients and is the leading provider of database security, risk and compliance solutions for the enterprise. Commercial and federal agencies bolster FISMA compliance efforts by grounding compliance where the data lives – in the database. The company's DbProtect platform mitigates risk and automates compliance through integrated database asset management, vulnerability management, audit and threat management, policy management, and reporting and analytics.
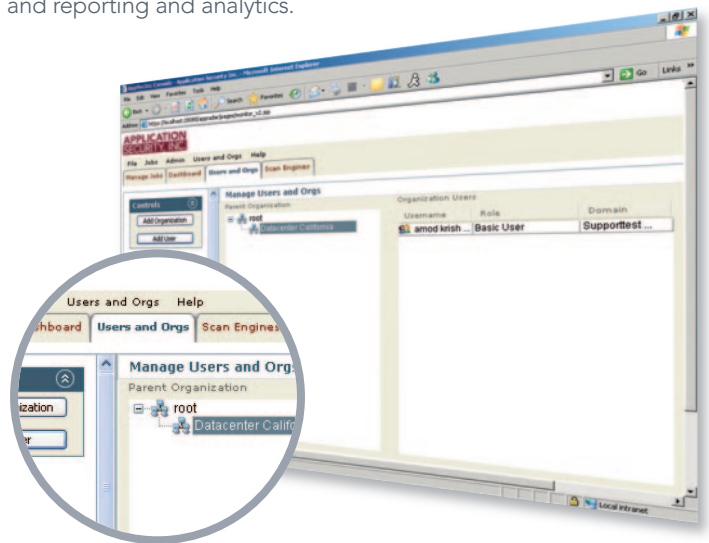
DbProtect gives users a "hacker's eye view" into system weaknesses, enabling IT professionals with a way to determine which security holes to address first.

DbProtect discovers databases within the infrastructure and assesses their security strength with its proven security methodology and extensive knowledge of database-level vulnerabilities.

Application Security, Inc. is aligned with NIST efforts to streamline standards under FISMA with comprehensive, automated capabilities to help agencies meet all compliance requirements.

Overview of Mandated FISMA Safeguards

Mandated by FISMA, government agencies must have adequate security in place to ensure the confidentiality, integrity and availability of government data and be held accountable for these measures by providing reports outlining the agencies' overall security position.

Section	Application Security, Inc. Solution
3451 – Purposes	FISMA specifically calls out for the adoption of security checklists from NIST. NIST 800-53 requires full risk and security assessment of all components that comprise the Federal system, including databases. DbProtect's Asset Management module discovers the databases within the network and adds detailed variables to help with database classification. DbProtect's Asset Management module audits databases and provides a complete inventory which agencies can use to classify for databases compliance.
3544 – Federal Agency Responsibility	DbProtect's Vulnerability Manager provides full database vulnerability and configuration assessment which map back to CA-2, RA-2, and RA-5 of the guidelines. DbProtect monitors the network and database user id's to verify only one person is using the account and tests, the password strength of all unique ID usernames and passwords, and identifying database vulnerabilities through detailed penetration tests and security audits. NIST 800-53 calls for the proper user identification and authentication in control number IA-2. DbProtect's Rights Management module facilitates proper access and control and separation of duties in the database. DbProtect can identify violations if excessive privileges are granted the user based on business function.
3545 – Annual Independent Evaluation	For comprehensive risk management, DbProtect tracks, monitors and reports on all relevant data on information access and system events. All information is captured and retained in a separate, secure data repository to maintain audit integrity.
3546 – Federal Information Security Incident Center	DbProtect's alerting capabilities capture not only log-in attempts but also the highly detailed information necessary to support audit logs. DbProtect provides a solution for regularly scheduled and ad hoc database system testing to ensure regulatory compliance.
3547 – National Security Systems	DbProtect provides a comprehensive analysis of which users have access to each system, which data and functionality they can access, and verification that the level of access that has been granted is appropriate based on the user's business function.

Over the past three years, 38% of enterprise respondents say that their organization has failed a security or compliance audit "one time" or "multiple times."

Finding based on a recent Enterprise Strategy Group survey

ABOUT

Db**Protect**™

Organizations use DbProtect to evaluate and improve the security posture of their databases. Backed by the industry's most comprehensive knowledge base, DbProtect helps agencies and companies improve their "threat intelligence" while adhering to compliance mandates. Based on a proactive security approach, and the Database Security, Risk and Compliance Lifecycle, DbProtect delivers the asset management, real-time data intrusion detection, and comprehensive auditing required for regulatory compliance. Actionable reports, quick start policy toolkits, and fix scripts as well as step-by-step remediation plans allow for easy communication of the database assessment across the organization and can be used to demonstrate due diligence efforts to auditors.

DATABASE SECURITY, RISK AND COMPLIANCE LIFECYCLE

A centrally-managed enterprise solution for comprehensive database security, risk and compliance, the DbProtect platform consists of five modules:

Asset Management

DbProtect's Asset Management module provides complete visibility of all databases on the corporate network. Leveraging an agentless, zero-knowledge network-based discovery scanner, DbProtect Asset Management finds and identifies every database on the network.

Policy Management

DbProtect's Policy Management module allows organizations to accelerate database security, risk and compliance initiatives with templates for scanning and monitoring databases in accordance with industry "best practices" and compliance standards, including NIST 800-53, DISA STIG, PCI-DSS, Sarbanes-Oxley, HIPAA, and GLBA.

Vulnerability Management

DbProtect's Vulnerability Management module is the foundation of Application Security, Inc.'s database security, risk and compliance platform. Offering unparalleled database assessment, DbProtect's agentless solution locates, examines, reports, and fixes security holes and misconfigurations in any database.

Audit and Threat Management

DbProtect's Audit and Threat Management module monitors privileged user activities, identifies unusual or suspicious behavior, and alerts on attacks and attempts to exploit database vulnerabilities.

Analytics and Reporting

The Analytics and Reporting module provides through interactive dashboards and reports a consolidated picture of vulnerabilities, threats, risk, and compliance efforts across the heterogeneous database environments found within today's enterprises.

DISCOVER · CLASSIFY · ASSESS · PRIORITIZE · FIX · MONITOR

DbProtect — Asset Management · Policy Management · Vulnerability Management · Audit & Threat Management · Analytics & Reporting

THE FISMA/DbPROTECT BENEFIT

FISMA attempts to mitigate risks by increasing information security requirements throughout Federal agencies. By becoming FISMA compliant, Federal agencies not only increase their data security posture and protect themselves against the penalties associated with non-compliance, but they also improve the national security and economic stability of the United States.

DbProtect safeguards organizations and ensures that data is protected, risks are minimized, and compliance mandates are met. For agencies seeking to optimize data protection, implementation of the standard should begin with the database.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

Application Security, Inc. is the leading provider of agentless database security, risk and compliance (SRC) solutions for the enterprise. Application Security, Inc.'s agentless approach - AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise - deliver the industry's most scalable database SRC solution and is in use around the world in the most demanding environments by over 1,600 customers. The company was named to Inc. Magazine's 2007 (Inc. 500) and 2008 list of America's Fastest Growing Private Companies, and was also named to the 2008 Deloitte Technology Fast 50.

For more information, please visit www.appsecinc.com.

APPLICATION SECURITY, INC.®

www.appsecinc.com