

DbProtect™

PRECISION DATABASE ACTIVITY MONITORING (DAM) WITH ACTIVE RESPONSE

Ensure Your Sensitive Data is Secure and Your Compliance Requirements Are Achieved

Are your databases secure? How do you know? A recent survey by the Enterprise Strategy Group found that while 84% of enterprises believe their data is secure, 57% have been breached in the last 12 months. High profile database breaches are increasing, and identity theft has become a \$388+ billion per year industry. Social security numbers, credit card information, and other personally identifiable information (PII) residing in an organization's database is a financially lucrative target for today's cyber-criminals. In order to protect data, organizations must secure the database.

Protecting sensitive data requires proper database security process controls. Basic vulnerabilities including unauthorized databases, improper or escalated user privileges, weak, default, or missing passwords, misconfigurations, and outdated or missing security patches provide easy avenues of attack to today's hackers.

Malware designed to exploit database vulnerabilities is readily available on the web, dramatically reducing the skill set required to compromise databases and significantly increasing the threat. In response, organizations must proactively implement appropriate technology and process controls to minimize data security risk. Defining, implementing, and controlling proper database security processes is a challenge for today's organizations. Dynamic database ecosystems where new databases, applications, software revisions, and users are

frequently added, changed, or deleted become too complex for organizations to maintain and control.

DBPROTECT SOLUTION OVERVIEW

DbProtect is a database security and compliance solution designed to meet the needs of heterogeneous database environments. DbProtect enables organizations to streamline and control the database security processes that impact sensitive data. In a dynamic database ecosystem, new applications, databases, users and software updates are frequently added, making it increasingly difficult for IT to maintain control. IT organizations require a new set of tools to automate and simplify this process.

In order to effectively secure their databases, organizations must address five critical requirements:

1. **Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.

"96% of breaches were avoidable through simple controls."

Verizon 2010 Data Breach Report

- 2. Eliminate Vulnerabilities:** Continually assess, identify and remediate vulnerabilities that expose the database.
- 3. Enforce Least Privileges:** Identify user entitlements and enforce user access controls and privileges to limit access to only the minimum data required for employees to do their jobs.
- 4. Monitor for Deviations:** Implement appropriate policies and monitor any vulnerabilities that cannot be remediated for any and all activity that deviates from authorized activity.
- 5. Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.

DBPROTECT ENABLES DATABASE SECURITY PROCESS CONTROL – COLLECT, ANALYZE, REMEDIATE, ENFORCE (CARE)

DbProtect enables a proven process control methodology to meet the aforementioned critical requirements.

DbProtect's complete solution **collects** data detailing an organization's database ecosystem through an automated discovery process. DbProtect then **analyzes** the data to highlight areas where risks reside and where database security process improvements are needed. Based on this analysis, DbProtect provides tools and detailed **remediation**



instructions to eliminate database vulnerabilities. And finally, DbProtect **enforces** database security processes by monitoring and responding to deviations from authorized behavior.

DBPROTECT PRECISION DATABASE ACTIVITY MONITORING

DbProtect's database security process control helps organizations understand database ecosystems, focus on suspicious and unauthorized database activities, and streamline database security operations. This unique approach is **Precision Monitoring**.

DbProtect's Vulnerability Management, Rights Management, and Risk Analysis, supported by the SHATTER knowledgebase, locates, examines, reports on, and fixes security holes and misconfigurations present in the database. This automated process allows an organization to:

- Eliminate avenues of attack
- Improve overall risk profile
- Reduce the scope of database activity monitoring

DbProtect's **Precision Database Activity Monitoring (DAM)** provides efficient and effective fine-grained monitoring based on user-defined policy and unique characteristics of the database resulting in:

- An additional reduction in the scope of database activity monitoring
- Reduced risk of data loss
- Minimized impact on the availability and response time of critical business systems

DbProtect's **Active Response** allows organizations to define automatic responses to specific types of suspicious and unauthorized behavior. Types of responses include: alerting IT, alerting SIEM systems, opening trouble tickets, initiating malware scans, and blocking activity or closing sessions. The benefits of DbProtect's Active Response include:

- Stopping suspicious activity in real time
- Initiating forensic analysis and database security process improvements.

- Providing an additional protective layer to secure sensitive data.

DbProtect Precision DAM reduces the complexity, resource requirements, and costs associated with properly securing databases.

DBPROTECT SOFTWARE

DbProtect is a software-only solution designed to scale from small to medium sized business to large enterprises . A modular architecture and flexible pricing allow organizations to cost effectively deploy and grow DbProtect to meet an organization’s needs today and in the future.

VULNERABILITY MANAGEMENT

Vulnerability Management is the foundation of AppSec’s DbProtect, offering unparalleled database assessment. DbProtect’s agentless solution locates, examines, reports on, and fixes security holes and misconfigurations in any database.

Vulnerability Management is backed by the SHATTER knowledgebase, the most extensive set of database vulnerability and misconfiguration checks and rules on the market. AppSec’s ASAP Update mechanism ensures protection remains current. As new vulnerabilities and exploits are identified and database patches are released, DbProtect is systematically updated to ensure the latest protection for critical database assets. Vulnerability Management consists of:

- Database Discovery
- Penetration Testing
- Security and Configuration Auditing
- Reporting and Analytics
- Policy Development
- SHATTER Knowledgebase

Database Discovery

The first step to effective database security process control is to maintain an accurate inventory of all databases deployed

Compliance vs. Security

Regulatory mandates – SOX, PCI, NIST800, HIPAA, DISA STIG and others speak to database process control. Many require the isolation of sensitive data, to the implementation of least privileges, the elimination of vulnerabilities, and monitoring and response to unauthorized activity. While these regulatory mandates provide a good foundation, they do not guarantee security. To properly secure databases and the sensitive data they hold, organizations must:

- Protect the data where it lives – In the database.
- Look beyond the limitations of regulatory mandates.
- Take a proactive and preventative approach to ensure that proper database security process controls are implemented

across the enterprise. Over time, enterprises can lose track of their database inventory and become populated with forgotten and unauthorized databases. These “rogue” databases typically fall outside of IT control and are rarely configured or secured properly. As a result, they create a security risk by giving attackers an easy target to gain a foothold on the network and find access to other databases containing sensitive

data. DbProtect solves this problem by maintaining a complete inventory of all databases on the corporate network, including:

- Production databases
- Test databases
- Authorized temporary databases
- Unauthorized databases

DbProtect identifies every database by IP address, database type, platform and version.

Sensitive Data Discovery

DbProtect’s Sensitive Data Discovery (optional) takes database inventory to the next level by locating and identifying sensitive data stored in each database.

Discovery quickly analyzes data and classifies the sensitive information it finds according to regulatory and risk impact. It reports sensitive data location down to the column level. This

KEY BENEFITS:

Vulnerability Management

- Support for all major database platforms
- Database penetration testing (non-credentialed, outside in scans, i.e. hacker’s view)
- Security audit (credentialed scans)
- Database vulnerability remediation scripts
- Industry leading vulnerability knowledgebase
- Assessment baselines that meet and exceed industry leading security checklists and security benchmarks.
- Automated scans for large environments

helps organizations develop more granular and precise policies to restrict access to sensitive data, prioritize remediation plans and focus monitoring operations. DbProtect Sensitive Data Discovery combined with Database Discovery allows any organization to easily and automatically isolate sensitive databases.

Penetration Testing and Security & Configuration Auditing

The second step to effective database security process control is to identify and fix vulnerabilities and misconfigurations that expose databases continually. Default and weak passwords, missing security patches, disabled security features, and improper access controls provide avenues of attack to sensitive data.

DbProtect provides unparalleled database vulnerability assessment allowing organizations to eliminate vulnerabilities and fix misconfigurations that put their sensitive data at risk. Vulnerability Management collects, analyzes and remediates vulnerabilities in any database. DbProtect's ASAP Update feature ensures that database protection remains current.

Policy Development

Vulnerability Management is driven by DbProtect's powerful policy development engine. It allows organizations to develop effective and fine-tuned policies customized to their database ecosystem. DbProtect's policy development is facilitated by an easy-to-use wizard which guides users through a simple three step process which allows organizations to define any privileged activities that need to be monitored, any access to sensitive data that must be audited, and any suspicious activities that may require an Active Response.

DbProtect begins the policy development process with proven templates based on a validated library of rules. Templates include SOX, PCI-DSS, NIST 800.53, DISA STIG, HIPAA and many others. To facilitate the creation of filters and business rules, the policy wizard presents a catalog of all database objects. It allows organizations to identify specific tables and columns of interest and to assign risk. This approach allows organizations to look for all modifications to specific objects down to the column level, providing a more granular policy and eliminating any false positives and negatives.

SHATTER Knowledgebase

DbProtect's SHATTER knowledgebase sets the industry standard for comprehensive vulnerability and threat detection. It is supported by TeamSHATTER, the world's largest and most experienced database vulnerability research organization. DbProtect's ASAP Update feature ensures the SHATTER knowledgebase is updated monthly with the latest database vulnerabilities and threat signatures, keeping coverage current with the most advanced SQL injection and advanced persistent threat based attacks.

The SHATTER knowledgebase is developed to provide rapid vulnerability mitigation and remediation. Each check provides detailed and easy to understand information that enables a common understanding between DBAs, IT Security, and other organizations. In addition, each check provides clear and detailed remediation instructions.

Risk Analysis

DbProtect Risk Analysis (optional) helps organizations to prioritize vulnerability remediation plans to ensure that the most immediate threats are addressed quickly. Risk Analysis provides a "risk score" for database vulnerabilities based on exploitability, susceptibility and business impact. In this way database vulnerabilities can be mapped to IT risks helping organizations to properly prioritize their remediation efforts.

Reporting and Analytics

DbProtect Reporting and Analytics provides a consolidated picture of vulnerabilities, threats, and compliance efforts across heterogeneous database environments found in today's enterprises. An easy-to-use interface composed of interactive dashboards and reports summarize data gathered by the system and offer extensive filtering, sorting and drill through capabilities for a dynamic reporting experience. This feature allows executives to quickly ascertain where and how resources should be applied to most effectively reduce risk and implement compliance requirements around the database. Drill downs and detail reports offer a complete picture of each individual database or group of databases. DBAs and IT Security Analysts are provided with the level of detail they require, without burdening managers and executives with unnecessary details.

KEY BENEFITS:

Reporting and Analytics

- **High-level data visualization via Security, Compliance, and Operations Dashboards**
- **Dozens of built-in reports including Executive Level roll-ups, Director Level summaries, and IT level detailed reports**
- **Compliance reports, Risk reports, Inventory reports, Policy Reports and User Activity reporting**
- **Reports can be scheduled and automatically emailed to the appropriate personnel as required**

DbProtect Reporting and Analytics offers built-in and customizable compliance reports, risk reports, inventory reports, policy reports and user activity reporting. Reports can be scheduled and automatically emailed to the appropriate personnel as required.

by the same SHATTER knowledgebase that drives DbProtect Vulnerability Management, DbProtect's DAM reduces risk and offers best-in-class data protection and compliance reporting.

DbProtect's policy development engine allows organizations to focus only on the specific database events that require attention. Monitoring policies can be defined to focus on specific activities, performed by specific users, accessing specific data, in specific databases. This approach analyzes all access down to the column level and provides fine grained monitoring policies that serve to eliminate any false positives or negatives. DbProtect's built-in monitoring templates for SOX, PCI-DSS, NIST 800.53, DISA STIG, HIPAA and many others help organizations quickly implement their compliance monitoring initiatives.

Active Response

Active Response is an important feature of DbProtect Database Activity Monitoring. It provides an added layer of security around sensitive data by allowing organizations to define a set of automated reactions to policy violations in respond to suspicious behavior. Active responses can be customized to an organization's database ecosystem, and can include:

- Sending Alerts to IT staff to prompt further investigation
- Sending alerts to SIEM systems to correlate suspicious database activity with web application logs for forensic

Rights Management

DbProtect Rights Management provides a detailed view of an organization's data ownership, access controls, and rights to sensitive information. Over time, user rights can escalate and run out of control. Promotions, transfers, acquisition and mergers, and inheritances can result in users accumulating far more privileges than they need to do their jobs. This can lead to a toxic combination of privileges that enable an insider to make fraudulent changes or steal data. An important step to effective database security process control is to enforce least privileges. Simply put, only grant users the privileges they need to do their jobs.

Managing user privileges and monitoring for segregation of duties violations are considered so important that they are defined in almost all regulatory mandates, including: Sarbanes-Oxley (SOX), PCI-DSS, NIST-800, DISA STIG, HIPAA and others.

Database Activity Monitoring

DbProtect's Database Activity Monitoring (DAM) tracks privileged users, identifies and alerts on unusual or suspicious behavior, and blocks attacks and attempts to exploit database vulnerabilities. Backed

KEY BENEFITS:

Rights Management

- **Identify inappropriate access that can lead to fraudulent changes or data breach**
- **Meet standards and regulations to restrict access**
- **Identify the privileged users**
- **Enables information security analysts, DBAs, and business managers to assess database entitlements**
- **Save time and resources by automating the entitlements mining process for databases across the network**
- **Accurately unravel complex databases**

analysis

- Opening trouble tickets to track incidents
- Initiating malware scans
- Blocking suspicious and unauthorized activity

Active Response's blocking feature (aka virtual patching or Intrusion Prevention System) stops attacks and unauthorized access to sensitive data. Blocking can be configured to automatically terminate suspicious user sessions or lock out the accounts of repeat policy violators.

Active Response is driven by DbProtect's powerful policy engine that allows

Network Centric vs. Data Centric

Many organizations attempt to protect their sensitive data through network centric strategies. Organizations rely on network firewalls, network scanners and web application firewalls to lock out attacks at the periphery. The growing number of successful breaches demonstrates that network centric strategies, by themselves, do not sufficiently protect sensitive data.

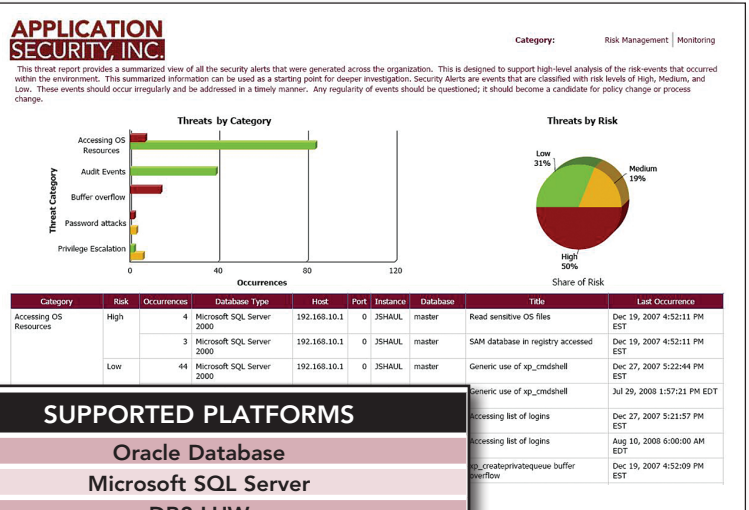
Today's attackers are sophisticated, well-organized, and well-funded. Perimeter defenses are regularly breached and provide no protection from insider attacks. In order to adequately secure their sensitive data, organizations must look to data centric strategies and protect the data where it lives – in the database.

organizations to define an appropriate response to specific activity, by specific users, accessing specific data, in specific databases. By providing this fine level of granularity, organizations can avoid the risk of mistakenly responding to authorized activity.

SUMMARY

DbProtect helps organizations to more effectively control their database security processes, enabling organizations to achieve database security, minimize risk, and achieve regulatory compliance.

DASHBOARD



- ### SUPPORTED PLATFORMS
- Oracle Database
 - Microsoft SQL Server
 - DB2 LUW
 - DB2 z/OS
 - Sybase ASE
 - MySQL Enterprise
 - Lotus Notes/Domino

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: www.appsecinc.com/downloads/appdetectivepro

Follow us on Twitter: www.twitter.com/appsecinc | www.twitter.com/teamshatter

APPLICATION SECURITY, INC.
www.appsecinc.com