

How DbProtect's Precision Database Activity Monitoring (DAM) with Active Response Improves Your Database Defenses

DBPROTECT OVERVIEW

DbProtect is a database security and compliance solution designed to meet the needs of heterogeneous database environments. DbProtect streamlines and controls the database security processes within organizations and protects sensitive data in the database. In dynamic database ecosystems, new applications, databases, users, and software updates are frequently added - making it increasingly difficult for IT to maintain a high standard of security control.

DbProtect's **Database Activity Monitoring** 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

Precision Monitoring

DbProtect's Precision Monitoring software allows

5 Key Steps to Ensuring Database Security

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.
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's Complete Enterprise Solution

COLLECT

DbProtect collects data detailing an organization's database ecosystem through an automated discovery process.

ANALYZE

DbProtect analyzes the data to highlight areas where risks and vulnerabilities reside and where database security process improvements are needed.

REMEDiate

Based on this analysis, DbProtect provides tools and detailed remediation instructions to eliminate database vulnerabilities.

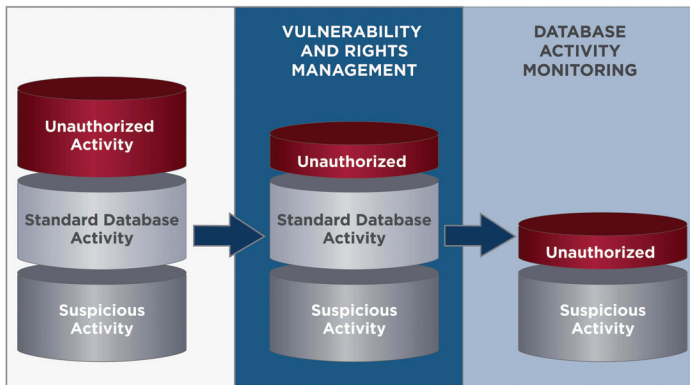
ENFORCE

DbProtect enforces database security processes by monitoring and responding to deviations from authorized behavior.

organizations to monitor for deviations from normal authorized activity. Precision Monitoring is driven by DbProtect's powerful Policy Management engine which helps organizations focus monitoring operations and:

- Validate remediated vulnerabilities
- Monitor unremediated vulnerabilities to ensure they are not being exploited
- Monitor privileged user activities
- Monitor for any new avenues of attack

Precision DAM

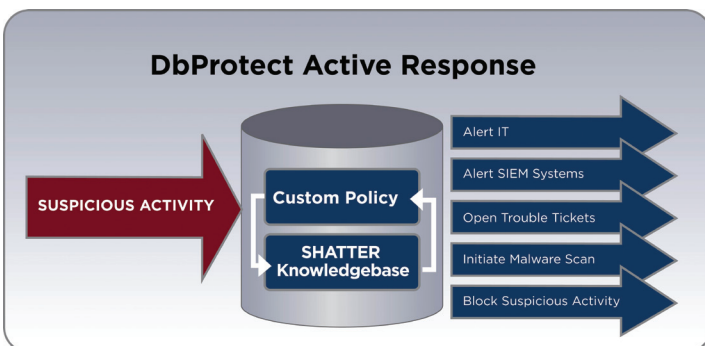


Active Response

DbProtect's Active Response provides an added layer of security around sensitive data by allowing organizations to define a set of automatic actions based on policies, risk level and business impact of an activity. Active Response 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 analysis
- Opening trouble tickets to track incidents
- Initiating malware scans
- Blocking suspicious and unauthorized activity

In addition, Active Response allows organizations to create custom responses that strengthen the incident response



process, while offering the flexibility to suit the needs of each and every unique environment.

Active Response's blocking feature (aka virtual patching and Intrusion prevention system) stops unauthorized access to sensitive data assets. Blocking can be configured to automatically terminate a user session or lock a user account.

Active Response is driven by DbProtect's powerful policy engine that allows organizations to define an appropriate response by specific activities and by specific users. By providing this fine level of granularity, organizations can avoid the risk of mistakenly blocking authorized activity by authorized users.

EXAMPLE USE CASES

Isolate Sensitive Databases

It is important for organizations to account for all databases and the sensitive data that resides in those databases. This involves maintaining an accurate inventory of all databases on the network and tracking the movement of sensitive data across those databases. DbProtect can be configured to initiate an Active Response whenever a new database is added to the network and whenever sensitive data are moved.

Activity: *Sensitive data moved to an unauthorized database*
 Risk Level: *Moderate*
 Active Response: *Send alert to IT Security*

When sensitive data are moved to an unauthorized database, Active Response can be configured to send an alert to IT Security to initiate an investigation. If they find there is a valid reason to relocate the sensitive data, IT Security can then initiate a vulnerability scan to identify any default or weak passwords, ensure all database security features are enabled, and the latest security patches are installed.

Enforce Least Privileges

The principle of least privileges states that users should only be given the minimal privileges needed for job performance. This principle should govern the assignment of rights in every organization. However, in every organization there are a number of users – DBAs, Application Developers, System Admins – who need to be highly privileged to do their jobs. If not carefully monitored, this can lead to a Segregation of Duties (SoD) violation. DbProtect can be configured to initiate an Active Response when a SoD violation occurs and whenever a user's privileges have changed unexpectedly.

Activity: A highly privileged user is issuing delete commands into a database containing financial data

Risk Level: High

Active Response: Send an alert to IT Security, Terminate Session and Lock out User

Tampering with sensitive data is a violation of the Sarbanes-Oxley (SOX) act. Active Response can be configured to react to a specific set of activities performed on specific tables in specific databases. When a privileged user changes, modifies or deletes sensitive data, Active Response can be programmed to immediately terminate the session, lock out the user from further access and then notify IT Security for further investigation. DbProtect's Active Response supports similar requirements for PCI, NIST-800, DISA STIG, HIPAA and other regulator mandates.

Eliminate Vulnerabilities

Advanced attacks like SQL Injections and social engineering-based attacks are designed to penetrate network centric defenses (firewalls, WAFs, network scanning tools). Once in, they are designed to take advantage of basic database vulnerabilities such as default and weak passwords, database misconfigurations, and missing security patches. DbProtect's Active Response can be configured to send an alert whenever one of these vulnerabilities is identified.

DbProtect provides early intervention and protection from advanced attacks. DbProtect Precision Monitoring is supported by the SHATTER Knowledgebase. TeamSHATTER is the most comprehensive knowledgebase of database vulnerabilities and attack vectors in the industry. With the SHATTER Knowledgebase, DbProtect's Precision Monitoring will identify a SQL injection signature as an attack on the database. Active Response can also be configured to take appropriate action.

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](https://twitter.com/appsecinc) | [www.twitter.com/teamshatter](https://twitter.com/teamshatter)

Activity: DbProtect Precision Monitoring detects a SQL injection signature

Risk Level: Very High

Active Response: Alert IT, Send Request to SIEM, Initiate Malware Scan, Terminate Session

SQL injections pose a serious risk to databases and the sensitive data they contain. When DbProtect Precision Monitoring detects an SQL injection attack, Active Response can be configured to take multiple immediate and preventative actions. First, it will alert IT Security of the attempted attack. Second, it can initiate forensic analysis by sending an alert to a SIEM system to correlate database activity with web application logs so that current attack vectors can be identified, and future preventative measures can be implemented. Third, Active Response can initiate a malware scan on the database to remove unauthorized software. Fourth, it can immediately terminate the session to prevent data loss.

These are just a few examples of how DbProtect's Active Response can provide an additional layer of protection around an organization's database environment.

SUMMARY

DbProtect's Active Response is a powerful tool that self-polices database security processes. It allows organizations to create custom policies that initiate automated responses when suspicious or unauthorized activity is detected.

KEY BENEFITS:

Active Response

- Stops suspicious activity in real time
- Initiates forensic analysis and additional process improvements
- Provides an additional protective layer around sensitive data