

DbProtect's Database Activity Monitoring Facilitates PCI DSS Compliance

INTRODUCTION

PCI DSS, formed in 2004 from policies developed by American Express, Visa, Mastercard, Discover, and JCB, is a comprehensive world-wide information security standard aimed at any organization that stores credit card data. PCI includes requirements for security management, data protection, policies, procedures, network management, and other critical protective measures that were developed to proactively secure cardholder data and transaction information for consumer privacy.

The standard was developed by the payment card agencies to outline best practices for securing and protecting credit card numbers and transaction data at the retail level. Over time, the standard has expanded its requirements to include banks and third-party processors.

Non-compliance with the standard can result in hefty fines from each of the payment card compliance programs – from increased transaction processing fees, financial fines in the hundreds of thousands of dollars, to suspension of credit card transaction. In addition, many credit card providers offer financial incentives, such as reduced transaction rates, for organizations meeting PCI DSS compliance.

Despite this mandatory governing standard, the industry has experienced a record number of data breaches where customer names, addresses, social security numbers, bank accounts and credit card numbers have been stolen or compromised.

What is the reason for this?

1. The potential gains for a successful breach are very lucrative. A recent breach of a large credit card issuer netted the attackers over \$24 million.

2. Attackers are more sophisticated in their techniques, better organized, and well funded by criminal and foreign state organizations.
3. The focus of PCI DSS implementation has been on network-centric defense strategies. While important, periphery defense has proven to be insufficient in protecting customer personal identity information (PII).
4. Compliance is not security. In addition to compliance auditing, security best practices must be employed to ensure the protection of sensitive data.

What is the answer?

In order to more effectively meet PCI DSS compliance and increase the level of protection customers expect, organizations must look to adding a data-centric approach to their PCI DSS strategies. Specifically, they need to protect their critical and sensitive data where it lives - in the database.

THE DATABASE IS DEFINED IN THE PCI STANDARD

"Any network component, server or applications that is included in or connected to the cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to: firewalls, switches, routers, wireless access points, network appliances and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP) and domain server name (DNS)."

---PCI DSS Standard

ADDRESSING PCI DSS WITH DBPROTECT PRECISION DATABASE MONITORING

PCI DSS defines twelve requirements that address a wide range of security considerations including data protection, security management, policies and procedures, network architecture, and other related concerns. PCI DSS requires the implementation of proper database security process controls. DbProtect's Precision Database Activity Monitoring (DAM) enables organizations to implement proper database security process controls, and allows organizations to streamline and control the database security processes that impacts customer account 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 databases and meet PCI DSS compliance, 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 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 DAM

DbProtect CARE helps organizations to understand database ecosystems, focus on suspicious and unauthorized database activity, and streamline database security operations. This unique approach is **Precision Monitoring**.

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

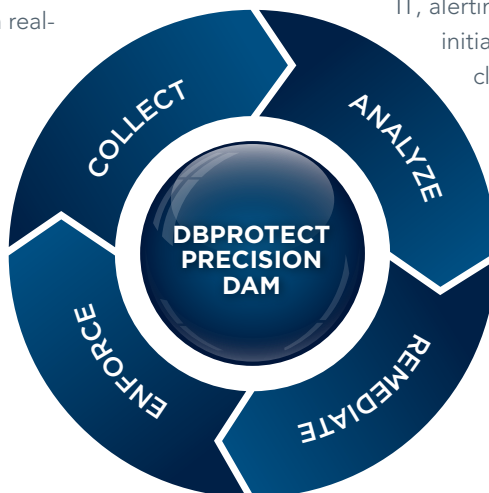
- Eliminate avenues of attack
- Improve overall risk profile
- Reduce the scope of database activity monitoring

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 the database.

FIVE STEPS TO COST-EFFECTIVE PCI DSS COMPLIANCE

Step 1: Isolate Sensitive Databases

The first step to effective PCI DSS implementation is to maintain an accurate inventory of all databases deployed across the enterprise and identify all card holder data residing on those databases. Over time, enterprises become populated with unauthorized databases. These "rogue" databases typically fall outside of IT control and may not be properly configured or secured. As a result, they create a security risk by enabling backdoor access to other databases containing sensitive data. Vulnerability Management's Database Discovery solves this problem by providing a complete inventory of all databases on your corporate network, including:

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

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

DbProtect's **Sensitive Data Discovery** (optional) locates and identifies card holder data stored across these databases. Sensitive Data Discovery quickly categorizes data according to confidentiality and risk impact and it can identify sensitive data down to the column level. This helps organizations develop more granular and precise policies to restrict access to sensitive data, prioritize remediation plans, and focus on monitoring operations. Together DbProtect's Database Discovery and Sensitive Data Discovery help organization to isolate their card holder data.

Step 2: Eliminate Vulnerabilities

The second step to effective PCI DSS implementation is continually identifying and fixing vulnerabilities that expose databases. Default and weak passwords, database misconfigurations, missing security patches, SQL injections, and social engineering provide avenues of attack to sensitive data. Vulnerability Management's penetration testing and security and configuration auditing provide

unparalleled database vulnerability assessment. Vulnerability Management collects, analyzes, and remediates vulnerabilities in any database.

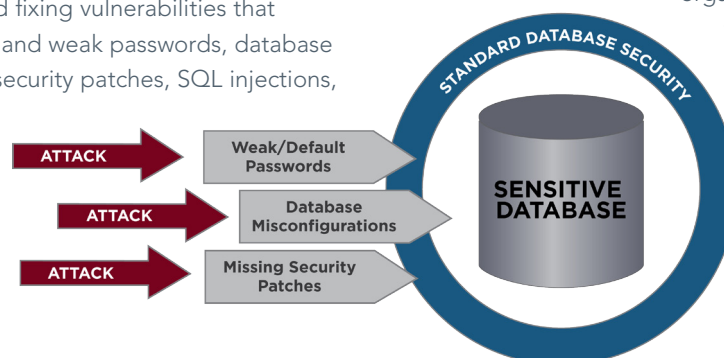
DbProtect's Vulnerability Management is driven by a powerful policy development engine that enables Precision DAM. It helps organizations develop effective and fine-tuned policies customized to their database ecosystem. DbProtect's Policy Management features an easy-to-use wizard that guides users through a simple three step process.

DbProtect begins the policy development process with a proven PCI DSS template based on a validated library of rules. 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 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.

Policy Management is facilitated by DbProtect's **SHATTER** vulnerability knowledgebase. SHATTER is the most comprehensive vulnerability and threat knowledgebase in the market. It is supported by TeamSHATTER, the largest and most experienced database vulnerability research organization. The SHATTER knowledgebase is updated monthly with the latest database vulnerabilities, including the most advanced SQL injection and social engineering-based attacks. DbProtect's ASAP Update feature ensures that database protection remains current.

The SHATTER knowledgebase is developed with vulnerability remediation in mind. 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.

DbProtect's **Risk Analysis** (optional) helps organizations prioritize vulnerability remediation plans to ensure 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, enabling organizations to prioritize their remediation efforts.



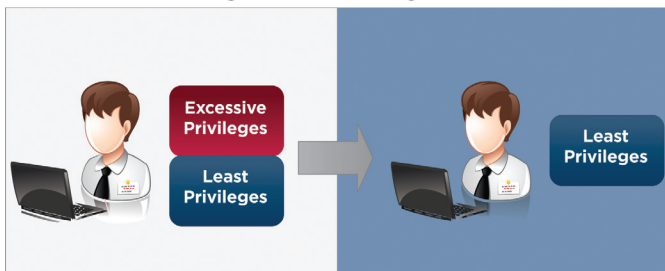
Step 3. Enforce Least Privileges

DbProtect's **Rights Management** module provides a detailed view of an organization's data ownership, access controls, and rights to sensitive information. It allows organizations to establish and document PCI DSS compliance with the required segregation of duties controls.

Over time, user rights can escalate and violate the principle of least privilege. Promotions, transfers, acquisition and mergers, and inheritances can result in users accumulating far more privileges than needed. Inappropriate access to card holder data can lead to fraudulent changes or a data breach.

To manage these access control challenges, audit firms recommend implementing the Principle of Least Privilege, which suggests that employees be entitled only to as much database access as is required to perform their job. Rights Management enables organizations to proactively identify users and their privileges down to specific data in specific tables in specific databases. This allows organizations to restrict database access on a business need-to-know basis and mitigate shared accounts. In addition, DbProtect Rights Management provides an auditable record of how privileges were granted, to help prevent inappropriate privilege escalation.

Rights Management



With Rights Management, organizations can more effectively:

- Identify users with inappropriate and undesired access to card holder data
- Identify valid privileged users requiring ongoing monitoring
- Provide an accurate audit trail of how a user's rights were assigned

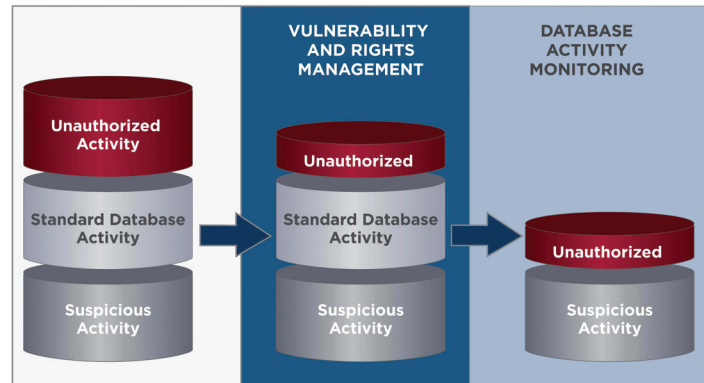
In this way, organizations can meet PCI DSS to restrict user access, secure their databases against inappropriate access, and save time and money associated with the database entitlements mining process.

Step 4. Monitor for Deviations

DbProtect's **Database Activity Monitoring** monitors privileged user activities, identifies and blocks unusual or

suspicious behavior, and alerts on attacks and attempts to exploit database vulnerabilities. Backed by the same SHATTER knowledgebase that drives DbProtect's Vulnerability Management module, DbProtect's Precision Monitoring with Active Response reduces risk and offers best-in-class data protection and compliance reporting.

Precision DAM



DbProtect's Database Activity Monitoring software allows 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

Step 5: Respond to Suspicious Behavior

Active Response is an important feature of DbProtect's Precision Monitoring module. It provides an added layer of security around your sensitive data by allowing organizations to define a set of automatic actions based on policy and the risk level to respond to suspicious behavior that may threaten card holder data. With Active Response:

- Alerts can be sent to IT
- Trouble tickets can be opened to track incidents
- Alerts can be sent to SIEM systems to correlate suspicious database activity with web application logs
- Malware scans can be initiated
- Suspicious activity can be blocked.

In addition, Active Response allows organizations to create custom responses that strengthen the incident response process, and offers flexibility to fit the needs of each and every unique environment.

Active Response's blocking feature (aka virtual patching and Intrusion Prevention System) stops unauthorized access to card holder data. Blocking can be configured to automatically terminate a user session or lock out a user account.

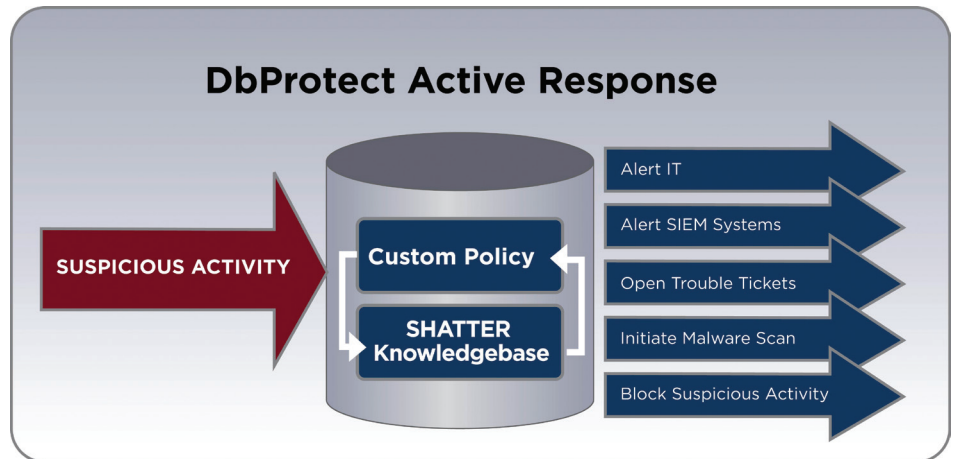
Active Response is driven by DbProtect's powerful policy engine that allows organizations to define the appropriate response by specific activity, by specific users, by specific data, in specific databases. By providing this fine level of granularity, organizations can avoid the risk of mistakenly blocking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

SIMPLIFIED IMPLEMENTATION

AppSecInc's DbProtect is based on a low traffic network architecture. Host-based agents communicate directly to a management console and storage devices without intermediate collectors. As a result, installation and deployment require no network reconfiguration or maintenance, freeing up networking resources for other projects. AppSecInc's DbProtect employs "intelligent" host agents to filter database events. This significantly reduces the volume of data sent over the network and eliminates not only the risk of losing PCI relevant data due to capacity limitations, but also the risk of introducing latency to business systems sharing networking resources with DbProtect.

DbProtect is a software-only solution that:

- Provides more flexible deployment. As an organization's database ecosystem changes they can simply reconfigure the software versus deploying more appliances.
- Allows organizations to deploy and fine-tune a solution to more closely adhere to operational models.
- Provides greater and more cost-effective scalability as Db ecosystems grow. Simply add more licenses versus adding additional expensive appliances.



DbProtect provides a lower total cost of ownership for PCI control:

- Lower deployment and ongoing maintenance costs
- Lower technology refresh costs.
- Flexible licensing for cost containment and protection
- Lower cost policy development
- Lower monitoring operation costs

SUMMARY

AppSec's DbProtect is a simple and effective DAM solution that allows organizations to manage and meet PCI compliance requirements.

(See following page for a Summary of PCI DSS Requirements)

Summary Of PCI DSS Requirements

<p>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</p>	<p>Through vulnerability management, AppSecInc examines all database account passwords and configuration. All findings of default and weak passwords and configuration settings are flagged as a vulnerability and specific guidance is given on how to remediate these issues.</p>
<p>Requirement 3: Protect stored cardholder data</p>	<p>Though specific encryption requirements are defined by the standard, PCI DSS understands the complexity of encryption and accepts the use of compensating controls. Through vulnerability assessment, user rights review, and activity monitoring at the database, AppSecInc solutions offer a strong comprehensive compensating control approach to data-at-rest encryption. AppSecInc solutions proactively scan the database for vulnerabilities and configuration issues. AppSecInc solutions provide a deep analysis of all access granted to specific tables and columns in the database and it can actively, and in real time, monitor all activity at these levels.</p>
<p>Requirement 6: Develop and maintain secure systems and applications</p>	<p>It is critical to develop and maintain secure applications from front-end web application, to middleware web server, and backend database. AppSecInc solutions provide a powerful assessment through vulnerability and configuration assessment and user rights review essential for baselining the backend database of the application. Database scanning can be adopted as part of the SDLC and will identify test and custom database accounts used for development. Once in production the same scans can be performed to ensure proper compliance and track any deviations to the baseline.</p>
<p>Requirement 7: Restrict access to cardholder data by business need-to-know</p>	<p>Comprehensive examination of restrictive access to cardholder data can be achieved by AppSecInc solutions. Through vulnerability and configuration assessment, AppSecInc will identify all users that have access to high profile database functions that grant, by default, the ability to escalate privileges, thus minimizing the possibility of attack. Through user rights review, AppSecInc will identify all effective privileges, users, and roles within a given database. AppSecInc solutions also report exact grant path by which privileges were granted. This feature is key to restricting access of users and roles.</p>
<p>Requirement 8: Assign a unique ID to each person with computer access</p>	<p>Shared accounts remain common in many organizations despite the risk involved. Through vulnerability assessment and user rights review, AppSecInc solutions help mitigate shared account usage and allow for the review of each users' access rights to the database and specific tables in the database.</p>
<p>Requirement 10: Track and monitor all access to network resources and cardholder data</p>	<p>AppSecInc solutions monitor all activity at the database. Access directly at the database by privileged users is tracked and defined. Alerts are fired when malicious activity, such as bulk selects on credit card data occur.</p>
<p>Requirement 11: Regularly test security systems and processes</p>	<p>Merchants and Service Providers must regularly test all system components. AppSecInc solutions facilitate scheduling of scans for vulnerability and configuration assessment and user rights review. AppSecInc solutions give you the ability to manage your database assets. This database discovery allows you to group assets and set different risk ratings based on an understanding of most effective policies.</p>
<p>Requirement 12: Maintain a policy that addresses information security</p>	<p>PCI DSS is all about a comprehensive approach to protecting the cardholder data environment. Driving an information security policy is critical for its success. AppSec solutions fit into existing security and risk-based methodologies and frameworks.</p>

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)

**APPLICATION
SECURITY, INC.**[®]
www.appsecinc.com