FACT SHEET

Protegrity DPS – Database Protector

The high-performance, enterprise-class software solution that secures sensitive data in databases through encryption, monitoring, masking, and tokens.

In a world where sensitive information is stored on almost every computer system, it is our number one priority to protect data. Protegrity's Data Protection System (DPS) is a comprehensive solution that secures data at the application, file and database levels, all driven from one central security policy.

Protegrity's DPS Database Protector provides a comprehensive database security solution for all major databases utilized in the market today. It enables column level data protection in databases, storage and backup systems by employing strict encryption, masking, and monitoring methods and by applying strong access and usage constraints.

KEY FEATURES

Column level encryption

Data Monitoring

Dynamic Masking

Token solution

Central security policy

Central reporting, auditing and alerting

Central key management

High performance, scalable solution

Separation of duties

Cross platform support

Part of Protegrity Security Suite, protecting databases, applications and files

Encryption

To achieve maximum protection of data and maintain the best system performance, Protegrity offers a patented system that allows implementation of encryption down to the column level within the database.

- **Strong encryption** - is provided with support for 3DES, AES-128 and AES-256 algorithms, and with the use of CBC, IV (Initialization Vector), and CRC (Cyclic Redundancy Check) of the encrypted data.
- **Format Controlling Encryption (FCE)** – is an alternative algorithm that is based on AES, but delivers output that maintains the format and length of the original data. This option maintains storage requirements and improves transparency.

Data Monitoring

The DPS Database Protector enables the Security Officer to audit, report and alert on any data activity, on any column of data. Policy-driven monitoring can be used for audit, reporting and alerting of any suspicious activity. This policy can further be defined to go the next step by blocking access to data in the case of a breach.

Dynamic Masking

Whether the underlying data is encrypted or in the clear, even authorized users of the data can be restricted from seeing full sensitive information. Dynamic masking enables the Security Officer to define how much of the clear data the user is authorized to see. Access to credit card numbers, for example, could be limited to just the last 4 digits.

Tokens (replacement values)

The DPS Database Protector delivers the option to utilize Tokens, or replacement values, for data as part of our Token Solution. Using the API an application can replace sensitive information in a system with same length and type "tokens".

Performance and Scalability

The DPS Database Protector takes full advantage of the processing power offered by the database server and keeps machine cycles to a minimum, thus optimizing performance. As sensitive data typically resides on multiple databases, this design allows for great scalability where each added database receives the full processing power of its accompanying server.

Cross Platform Support

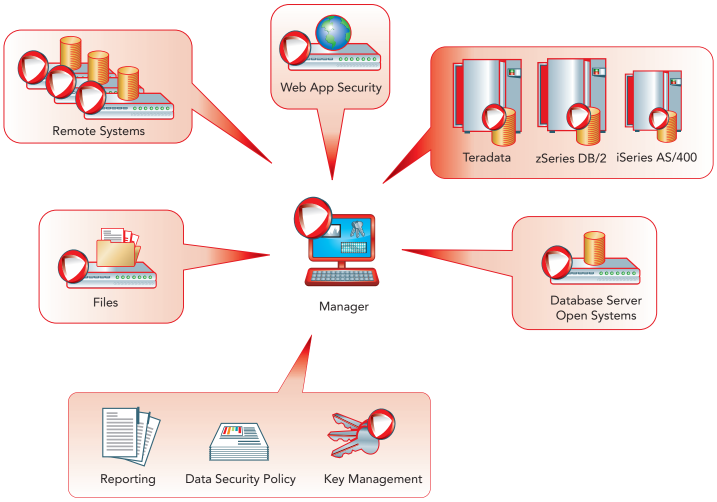
The DPS Database Protector is designed to protect sensitive data regardless of database and operating system type or version. It runs on any industry standard Linux, UNIX or Windows environment, as well as IBM iSeries and zSeries environments, in conjunction with all major relational databases.

Transparency

The DPS Database Protector is implemented with minimal changes to the database schema or to supporting applications.

Key Management

The DPS Database Protector utilizes Protegrity's central Key Manager which manages the key life cycle for all its protection points, across platforms, enterprise-wide. Protegrity has a patented key management and rotation process minimizes down-time by processing in the background.



Data Security Management

Protegrity's Enterprise Security Administrator (ESA) enables security officers to centrally define, distribute, and enforce security policies independently from database administration with a full range of secure audit reports that show complete accountability of access to secure data. ESA enables security officers to monitor database activity including database security, user authorization, data selection, creation, change or deletion.

Protegrity's ESA provides a real-time dashboard view of system status, policy deployment status, policy audits and internal audits. All authorized and unauthorized attempts to access protected data as well as any changes to security policies are monitored and logged by the system.

Management and compliance reports come standard, and a powerful rules engine allows for alerting when a potential security violation occurs.

protegrity

Protegrity delivers centralized data security management solutions that protect sensitive information from acquisition to deletion across the enterprise. Protegrity solutions protect data, safeguard web applications, and manage and report on security policy. Maximize security with minimal business impact with Protegrity's Security Suite, the high performance, transparent solution optimized for the dynamic enterprise. To learn more, visit **www.protegrity.com** or call 1.**203.326.7200**.