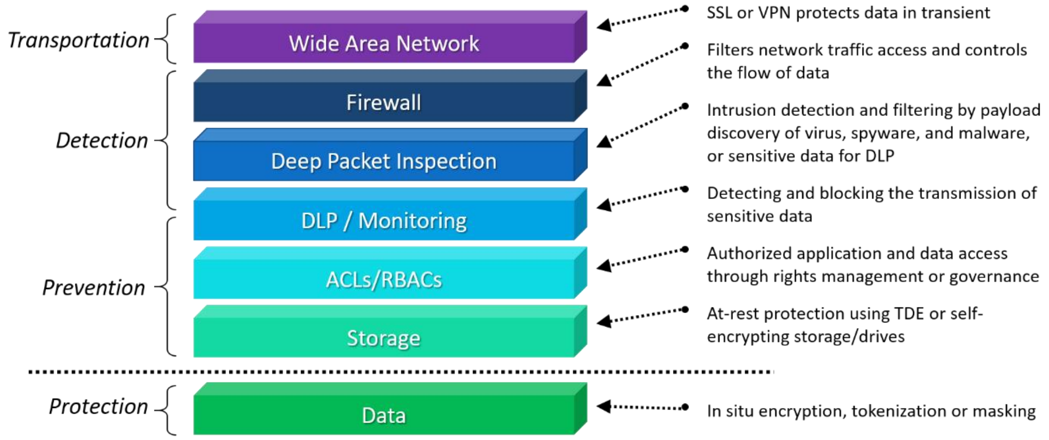
Stop Data Leakage

Believe it or not, a data breach is not the only cause of a data leak. Poor data security practices, inadvertent actions can lead to a leaky database. To prevent data loss entails integrating robust security techniques. The challenge however is protecting these corporate data assets while simultaneously allowing access to grow and support business activity. Sensitive data can reside in classic ERP, CRM, and HRM databases and can be shared between departments, partners, or customers. Highly prized by cybercriminals is Personally Identifiable Information (PII), known in the healthcare space as Protected Health Information (PHI), contained in these databases. To prevent data loss or unauthorized access, various industry techniques are utilized by enterprises:

- Good ole fashion access management that controls the rights to retrieve data records or submit queries to a database application.
- Encrypting data while en route to and from a database system.
- Encrypting data before the database management system sends it to storage and again decrypting once read from storage.
- Obfuscating data in database records.

Each of these techniques represents a well understood security layer that attempts to work in concert to accomplish database privacy. The downside is that security responsibility ends as data leaves an adjacent layer before entering another. Each layer protects the data while transiting that layer. The handoff between layers requires the data to be unprotected.


Transportation
Detection
Prevention
Protection
Wide Area Network
Firewall
Deep Packet Inspection
DLP / Monitoring
ACLs/RBACs
Storage
Data
SSL or VPN protects data in transient
Filters network traffic access and controls the flow of data
Intrusion detection and filtering by payload discovery of virus, spyware, and malware, or sensitive data for DLP
Detecting and blocking the transmission of sensitive data
Authorized application and data access through rights management or governance
At-rest protection using TDE or self-encrypting storage/drives
In situ encryption, tokenization or masking

The human factor is the single weakest link that often neutralizes security measures utilized to protect databases. Meaning, when data is inadvertently delivered in human readable form (plaintext) to the unauthorized. Let us look deeper in how each layer plays a role and why Bonafeyed's data defined security approach of individually encrypting data elements ensures that after a breach, no data is accessible to an unauthorized entity.

Access Control

Controlling user access to systems, applications or data comes in two forms: RBAC, role-based access control and ACL, access control levels. In both cases, data records or fields are not specifically encrypted, rather, this security scheme limits the availability of data. RBAC controls access to systems or applications based on a user's status within a domain or an enterprise's business hierarchy. ACL differs by explicitly limiting access to data either in the form of a file (as with Microsoft's active directory) or a data field such as Row Level Security (RLS) in a DBMS. If RBAC or ACLs are compromised as is common with phishing attacks, the outcome is the same – the data is freely available in the clear. Data is guarded, not encrypted.

Payload Protection

Whether in motion or at rest, data is treated as an intermediate payload and once delivered is stripped of its protection. Data saved to storage by the database is encrypted by built-in or 3rd party functions known as Transparent Data Encryption (TDE) and is in turn decrypted when pulled from the storage before it is delivered to the database management system. This means data in the DBMS is always in the clear. Now consider when data is sent over networks using TLS/SSL transport protocols. The data is encrypted just before it leaves the machine and stays encrypted while in transit and is immediately decrypted once it arrives at its destination. Again, in both cases, data, whether stored or transported, is delivered in the clear or as plaintext after it exits these security layers.

Data Security

First it should be mentioned, obfuscation techniques such as data masking and tokenization is effective, but ultimately just removes information from a database and places it in a data vault, which is typically managed by a 3rd party, for later retrieval. Naturally, you trust that 3rd Party implicitly to keep your data safe. Unfortunately, this approach hinders the ability to perform relational queries and analytics on a database, an important if not critical function to gain insight on data. Conversely, data considered "non-sensitive" in the same database remains in the "clear" such as zip code, race, gender, and date of birth which can be leveraged to distinguish an individual and violating all data privacy regulations.

Masking sensitive data in a database record – partially searchable

Acct ID	Login ID	Password	Last Name	First Name	SSN	Drivers License	Gender	State	Birthdate	Phone Number	Email Address	Home Address	Zip Code
clear	masked	masked	clear	clear	masked	masked	clear	clear	masked	clear	masked	masked	clear

Tokenizing sensitive data in a database record – limited searchability

Acct ID	Login ID	Password	Last Name	First Name	SSN	Drivers License	Gender	State	Birthdate	Phone Number	Email Address	Home Address	Zip Code
clear	token	token	clear	clear	token	token	clear	clear	token	clear	token	token	clear

To truly protect data, it should be encrypted and remain encrypted, whether at-rest, in-motion, or in-use. Cy4Secure's Data Defined Security encrypts all data no matter the size or type and more importantly the data remains encrypted even while in-use by a database. This technology separately encrypts data fields within a database record yet still allows complete searchability without any changes to the database management system.

Encrypting all data in a database record – fully searchable

Acct ID	Login ID	Password	Last Name	First Name	SSN	Drivers License	Gender	State	Birthdate	Phone Number	Email Address	Home Address	Zip Code
RLE	FLE	FLE	CLE	CLE	FLE	RLE	CLE	CLE	RLE	RLE	CLE	RLE	RLE

For example, applying column level encryption (CLE) to protect searchable data fields, field level encryption (FLE) for unsearchable, and row level encryption (RLE) to protect all remaining fields within a record, translates into dozens of cryptographic keys to decrypt a single record and 100% data protection coverage. In situ data security is now possible with Cy4Secure ensuring that breached databases or data leakage of illicitly queried records remain secured and protected.

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.