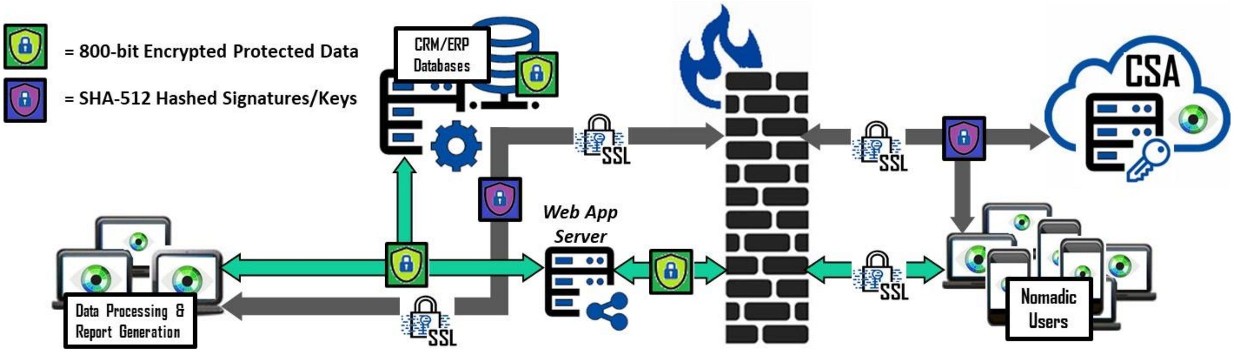
bonafeyed
privacy in plain sight

Securing Databases/DataApps/SaaS

Strategic and operational databases are the foundation for running business applications and financial transactions and have become the engine for today's ecommerce. Databases store and retrieve data very quickly and are used to track or hold customer, business activity, inventory, employee, and accounting information. In the era of cloud computing, these databases are the backend workhorse for many Software as a Service systems, health services, financial institutions, online retailers, and website applications. Unfortunately, they are also high-value targets for cybercriminals worldwide. ZDNet reported on December 10th, 2020 that "More than 85,000 MySQL databases are currently on sale on a dark web portal for a price of only $550/database". Protecting an enterprise's database typically involves setting up security using some of the most advanced technologies covering detection, prevention, and transportation. However, as evident in the weekly news regarding corporate data breaches, cybercriminals persistence continues to prevail at finding a digital path into a company's security domain and ultimately gain access to those databases that, when queried, sensitive data is ripe for exploitation or monetization.

Bonafeyed's Data-Defined security approach – safeguards database entries rather than applying an "at-rest" encryption of the entire database or the storage where it resides. This means first encrypting data and then submitting to the database application. By leveraging this approach, the ***Cy4Secure*** data security solution is capable of individually encrypting each field or row or column of data. The benefits of protecting the records or individual fields allow not only the highest level of data protection but access control as well as preserving the value of the data.



= 800-bit Encrypted Protected Data
= SHA-512 Hashed Signatures/Keys
CRM/ERP Databases
SSL
CSA
Web App Server
SSL
SSL
Data Processing & Report Generation
SSL
Nomadic Users

The question that instantly comes to mind is, how can the database work with encrypted data? The answer is remarkably simple. Database systems do not know the difference between data that is encrypted with ***Cy4Secure*** or data that is human readable. Its only concern is that the data meets the entry field's attributes. If it looks like data, databases can perform their operations such as whole searches and partial searches or sorts. When making queries, the operations are performed using ***Cy4Secure*** encrypted versions of the data and the database just searches for the encrypted equivalent version of the data. For instances where arithmetic operations are required on numerical entries, order preserving encryption can be used on numerical fields. Conversely, each PII numeric data entries such as a social security numbers, can be individually encrypted and obfuscated because they are not used in mathematical or sorting operations.

Therefore, individual data fields, records and columns can be encrypted to control access from unauthorized users. This allows broader sharing of its data or records and ensures in the event of a data breach or theft by a bad actor, data remains protected, unavailable, and demonetized.

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