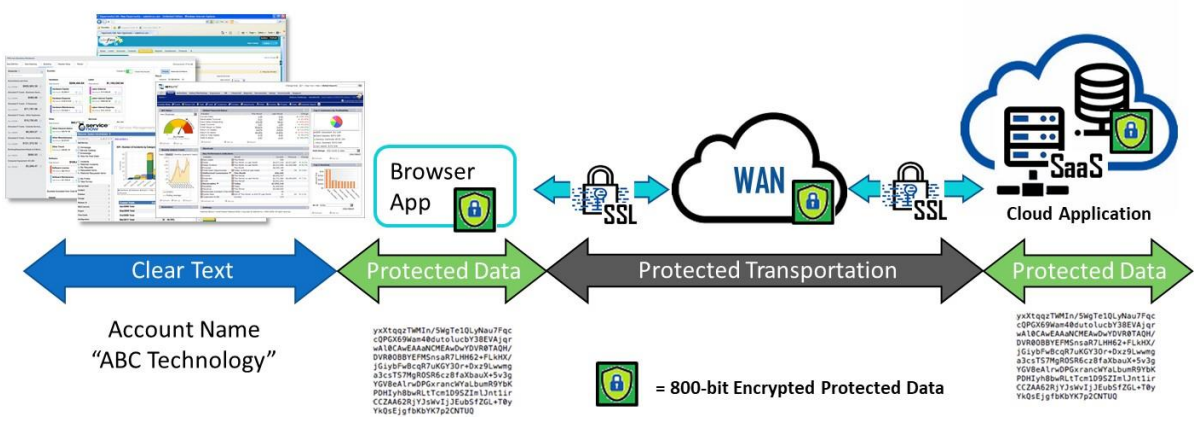
Worldwide, enterprises are experiencing a massive number of data breaches. RiskBased Security published in their 2020 Q3 report, nearly 3000 publically reported breaches occurred in the first nine months of 2020 exposing over 36 billion records. Data continues to be Enterprise's valuable asset and now is a liability given the likelihood of reoccurring breaches and the penalties driven by data protection regulations. Traditional data-at-rest and data-in-transist protection schemes are already deployed with marginal success. IT and DevOps are faced with the difficult task of finding an acceptable solution that goes beyond basic data protection such as Data Loss Prevention, discrete file encryption and application file passwording without changing workflows or replacing applications. The remaining holy grail is to safeguard "data in use" by an application, by users or between systems. Bonafeyed's data-defined protection approach enables data applications and 3rd party SaaS backed by databases to operate on encrypted data without ever accessing the data in the clear and preventing breached data to be monetized by criminals.

Bonafeyed's approach eliminates the tedious task of cryptography, key management and access control. It is completely transparent to users and applications with the goal of protecting all data, data types and data sizes no matter where it is shared or how it is utilized. Bonafeyed's ***Cy4Secure*** data defined security works behind the scenes such that all data is encrypted using 800-bit or 256-bit encryption just before sending to a database management system, database backed websites, SaaS or cloud applications. These applications simply use the protected data without knowing its encrypted. This is because it still appears as real data that can be searched, sorted, queried and referenced by databases. Why? Databases do not know or care if the data is English, German, French, or Italian. ***Cy4Secure*** encrypted data appears as just another language.



Cy4Secure data defined security works behind the scenes such that all data is encrypted using 800-bit or 256-bit keys just before sending to a database backed website, SaaS or cloud applications. In turn, when recipients receive Bonafeyed encrypted data and they are authorized, it is unencrypted without additional steps or separate passwords to gain access to the data. The "clear" data is also available for the user's local application or web browser.

Eliminating the arduous task of data encryption now ensures the security of all data in-use by applications, or shared with others, remains in the control of the sender or data owner. When Bonafeyed protected data is lost, stolen, abandoned, or forgotten, it remains secure and becomes permanently inaccessible once access is removed or retired ensuring cybercriminals or non-authorized users only obtain unintelligible, demonetized data.

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