bonafeyed
privacy in plain sight

Cy4Secure Product Sheet

Bonafeyed*'s Cy4Secure** is a data protection solution that safeguards an unlimited number of data fields, records and tables contained within databases, whether deployed on premise, in the cloud or utilized by SaaS applications. It is fully interoperable with today's security technologies covering detection, prevention, and transportation, and ***protects data even after a security data breach. Our Data-Defined Security approach natively secures data, allows full database analytic operations, and keeps queried data protected when delivered to another enterprise or security domain, placed in backups or archives, or after received on endpoint devices. **Cy4Secure** supports an advanced 800-bit streaming cipher, AES-256 block cipher encryption, multi-factor authentication and password-less data cryptography without impacting user workflows. When compared to other approaches, **Cy4Secure** goes beyond traditional data "in-flight" or "at-rest" security technologies by protecting data "in-use" within a database or database driven SaaS CRM, ERP, Retail, Health Services, Finance, Telecom or Services applications.

The underlying problem with data protection is a general lack of awareness and understanding of how to protect the data itself, not just guard the systems holding it. Data protection regulations do not specify how to safeguard data, only that "somewhere" encryption be utilized. Transit protection only secures data "in-flight". Data "at-rest" protection only secures where data is physically stored. Traditional security solutions try to detect and prevent unauthorized access at the edge of an enterprise, but once a cybercriminal penetrates the security perimeter, data is freely available by querying the databases. When protected by **Cy4Secure**, unauthorized users can only receive or pilfer encrypted data. Data remains safe even while IT applies patches and updates to fix regularly discovered exploits to the perimeter security. In the event **Cy4Secure** protected data is lost, stolen, abandoned, or forgotten, it remains secure and is demonetized and permanently inaccessible once the crypto keys protecting it are disabled or retired, ensuring cybercriminals or non-authorized users only obtain unintelligible encrypted data.

Feature	Cy4Secure	Tokenization/Masking	Appliance/Driver
Encryption Strength	800-bit or 256-bit	N/A	256-bit or 128-bit
Stream & Block Cipher Support	Either or Both	Block Only	Block Only
Encrypted Queries/Searches	Yes	No	Partial or Exact-match only
Format Preserving	Yes	Yes	Yes
Order Preserving	Yes	No	No
Contains Search	Yes	No	No
Database Vendor Agnostic	Yes	Yes	Mostly Vendor Specific
SaaS Data Protection	Yes	Yes, Vendor Specific	Yes, Vendor Specific
Deployment Agnostic	Yes	No, requires data vault or appliance	No, requires appliance or DBMS upgrade
Domain-less Protection	Yes	No or requires field deployed appliance	No or requires field deployed appliance
Single Data Copy	Yes	No (Data vault)	Yes, Some Vendors
Zero-day detection	Yes	N/A	No

Cy4Secure Data Security can be seamlessly and rapidly deployed in existing environments. All modern database systems can be protected without impacting user workflows, changing existing infrastructure, and with no perceivable impact to performance. Users or external customer/clients perform password-less or multi-factor authentication to validate credentials which allow access to protected data. More importantly, each data element or field can be independently encrypted/protected. No two data elements are required to share the same key or authorization requirements. Bonafeyed delivers privacy in plain sight!

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