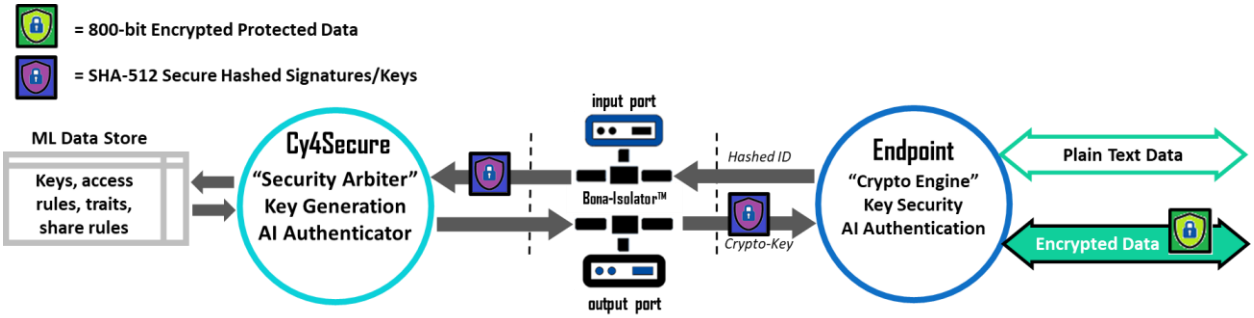
Cy4Secure is **Bonafeyed's** answer to the increasing threat of data breaches. ***Cy4Secure***'s architecture accomplishes this feat by only encrypting/decrypting data at authorized user endpoints. Our Data-Defined Security approach continuously safeguards data as it moves across different security domains, when it lands on an application server, after delivery from a cloud-based application, and finally, when the data rests on a recipient's endpoint device. ***Cy4Secure*** uses the following security methods:

- Bonafeyed never sees or touches any customer data
- All encrypt/decrypt operations are performed on the user's secure endpoint device (SED)
- All authentication data is hashed using SHA-512
- Shared data is encrypted before it leaves the user's SED
- Encryption secrets are disassociated from the protected data's location
- Data and corresponding encryption secrets only unite on an authorized user's SED
- Agnostic Data-Defined Architecture with all transport, network, or other security protocols
- "Airgap" technology ensures keys and credential information are inaccessible to hackers
- Minimum of 800-bit size keys are utilized for strong crypto operations
- Five 9's Availability for authentication, and crypto management services reliability and uptime



At the center of ***Bonafeyed's*** data security is the **Cy4Secure Arbiter (CSA)** which is responsible for managing all crypto functions. They include maintaining crypto secrets and credentials relationship, authorizing crypto information, supporting RESTful API, enforcing encryption key lifecycles, monitoring access habits, trends, frequency to proactively detect attacks, and theft or misuse of user credentials. It stores cryptography secrets and credentials, operates in a highly reliable and available clustered and distributed configuration. The CSA is deployable within the cloud as a service or on premise using a software-defined deployment model.

The Bona-Isolator™ provides an industry leading security air gap between public facing servers and the CSA. It ensures that no direct access to the **ML Data Store** or the CSA is possible

The **Cy4Secure SDK** allows easy cryptography integration into browsers, 3rd party SaaS, and Enterprise applications for automatic deployment to endpoint devices. The SDK provides prebuilt functions to perform cryptographic operations and to interact with the CSA. It also provides an optional conversion function to make encrypted data transportable across 8-bit transport mechanisms. The SDK supports multiple languages: JavaScript, Java, C, Python, C#, and Swift.

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