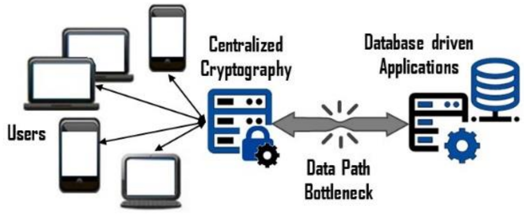
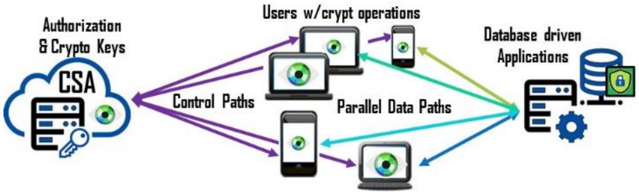
Split-Path Scalability

In the computing and networking world, separating data traffic and control operations is difficult to architect but yields scalability and performance. In other words, when data and control paths are centralized (usually for design convenience), all the traffic and operations are bottlenecked through one instance or appliance. Distributed architectures split these two paths to parallelize access and process capacity. In the security world, separating the data path from cryptography function has several distinct advantages: scalability, performance, and system security.

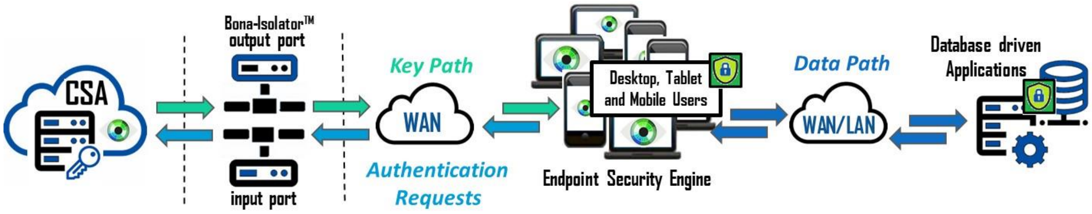


Scalability – In a large-scale data protection solution, many companies will design a solution such that all users must connect to a centralized function that is a proxy for the application it is protecting. Unfortunately, this also means the appliance, servlet or instance is responsible of encrypting and decrypting the requests, managing cryptographic keys, and providing authorization for 100's to 1000's of users along with funneling petabytes of data to and from the protected application. Bonafeyed's approach splits the data path from the other functions so that each user connects to the database driven application separately and performs the cryptographic operation on the user's endpoint device. With this, there are no data path bottlenecks and the massive amount of computing resources in the hands of the user is effectively utilized. This means an already deployed system can continue to support that same number of simultaneous users on the protected database back application.



Performance – User experience is key to deploying a data security solution. Slower response from a database or application sluggishness due to the overhead of data protection will frustrate users and impact businesses. Cryptographic operations can be computationally intensive, thus slowing application response. Natively turning on Columnar Level Encryption (CLE) on a database, for example, can impact query performance from 20-30% for a single column of data. Bonafeyed performs the encryption/decryption operations on the endpoint devices such as smartphones, laptops, tablets, and terminals which have the capacity to decrypt data in real time and on-demand. Bonafeyed offers AES-256 and an extremely fast 800-bit stream cipher that is about 10 times faster and about double the encryption strength. This translates into little to no impact on an application or user experience when data is being encrypted or decrypted.

Data Security – The strongest data security approach is to never bring encryption keys together with data until it is authorized and on the end user's machine. Bonafeyed uses millions of keys to protect a database but only retrieves those keys needed to decrypt a user's data on their end-point device. Keys are protected behind the Cy4Secure's air-gap technology, and only recently used keys are present on end-point devices limiting exposure in order to protect the data.



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