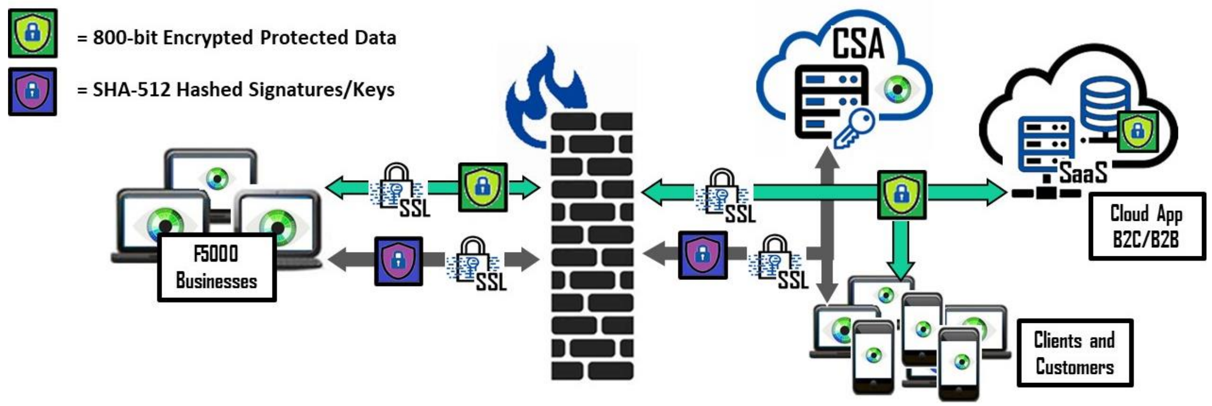
bonafeyed
privacy in plain sight

Data-Defined Security and Protection

Security and the protection of shared data is the core focus of the ***Cy4Secure*** product line. ***Bonafeyed*** spent many man years developing technology to protect all data while “in-use” not just “in-flight” or “at-rest”. To make this possible, ***Bonafeyed*** created an approach for encryption and management that interoperates with existing databases, applications, and network security technologies, and is compatible with endpoint devices or cloud applications. ***Cy4Secure*** utilizes encryption technology designed to protect data through the next decades, operates on the simplest devices, and eliminates the arduous task of managing encryption keys.

At the heart of ***Cy4Secure’s*** data protection is an 800-bit stream cipher algorithm. It is based on the industry hardened Mersenne Twister (MT) algorithm for its keystream. MT is commonly found and used in applications such as Microsoft’s Excel, Mathworks’ MatLab, Wolfram Research’s Mathematica, and development languages such as C++, GNU, PHP and Python. The National Security Agency (NSA) has used stream ciphers since the 1950s and it has many advantages. It can achieve a high security level with much less computational effort than the more common block ciphers. Stream cipher protected data is more difficult to attack because of the changing states and it is extremely fast**.** Another benefit is the detection of data corruption with encryption. ***Cy4Secure***, when decrypting, constantly checks the integrity of the data and can flag when data has rotted. ***In other words, protected data is more secure and durable.***



The next challenge in securing data is managing all the encryption keys used to protect data. Today, whether it is a simple password or a complex 800-bit key, users are forced to individually manage these keys to access data. ***Cy4Secure*** simplifies management by associating keys with the email address, common access control lists or active directories with whom protected data is shared. This can be a group of people, a distribution list, or a single individual. There are many benefits to this approach. Access to protected data is akin to already deployed access control list for the IT organization which is as simple as selecting recipients from a user’s contact list.

Once data is securely protected, key management is fully automated and transparent. Access can be easily controlled by the owner/sender, IT, or DevOps for shared data located on other servers, in the cloud, or on recipients’ computers. Availability of the decryption keys can be defined in many ways: When data can be first accessed, “Time to Birth”; How long it can be accessed, “Time to Live”; Or where it can be geographically accessed. Access permission can be revoked at any time. In the case when ***Cy4Secure*** 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 data.

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