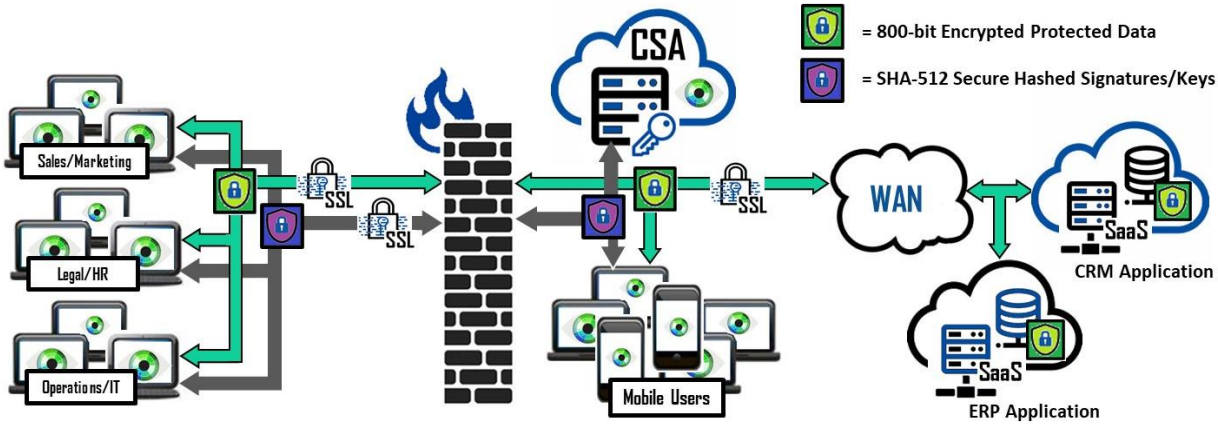
Securing 3rd Party SaaS Applications

Software as a Service (SaaS) is an immensely popular alternative to the traditional model of installing application software in a company's managed business environment. SaaS' success is driven by the ease of deployment, cost efficiency, scalability, mobility, reduced software implementation and maintenance costs. The only drawback is that customers must rely on the SaaS provider to ensure privacy and data security. SaaS offerings such as customer relationship management, enterprise resource planning, supply chain management, human resource management, business process management are database driven. Therefore, when it concerns data security, SaaS solutions have the same risks as traditional database deployments but also introduces new forms of data loss vulnerability.

In May of 2019, CRM cloud giant, Salesforce.com, Inc. (SFDC) service was disrupted when as posted by them, "A maintenance-related single-purpose database script launched at 01:45 UTC on May 17, 2019 mistakenly gave elevated data access permissions to users within an organization." It was purported by customers and the press; the script gave past and current users of the company's Pardot B2B marketing automation system full read and write access to all data. In other words, an Enterprise's data was openly available to other companies to examine and query. This unfortunate event is analogous to an insider attack, albeit an accidental one. Nevertheless, whether the SaaS or the cloud host for the SaaS adds another form of vulnerability. Today, a SaaS offers the industry standard data-in-transit and data-at-rest protection technologies, access controls and some optionally offer proprietary onsite security gateway appliances requiring one of these boxes at each customer location. Question is how can customers independently secure their data in a SaaS application without modification and available to remote employees, partners and even clients?



The solution starts with protecting data at the source, the database. Bonafeyed's data define security approach allows database backed SaaS applications to use encrypted data transparently, without changes and maintains data protection across domains down to an end-point device. It starts with the web application for the SaaS solution. It is here where the browser plugin intercepts individual data fields to determine if the data is encrypted or needs protection. The Cy4Secure Arbiter is contacted to authorize key request then upon reception data or records are decrypted. This approach allows broader sharing of secured data and ensures in the event of a data breach or theft by a bad actor, data remains protected, unavailable, and demonetized.

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