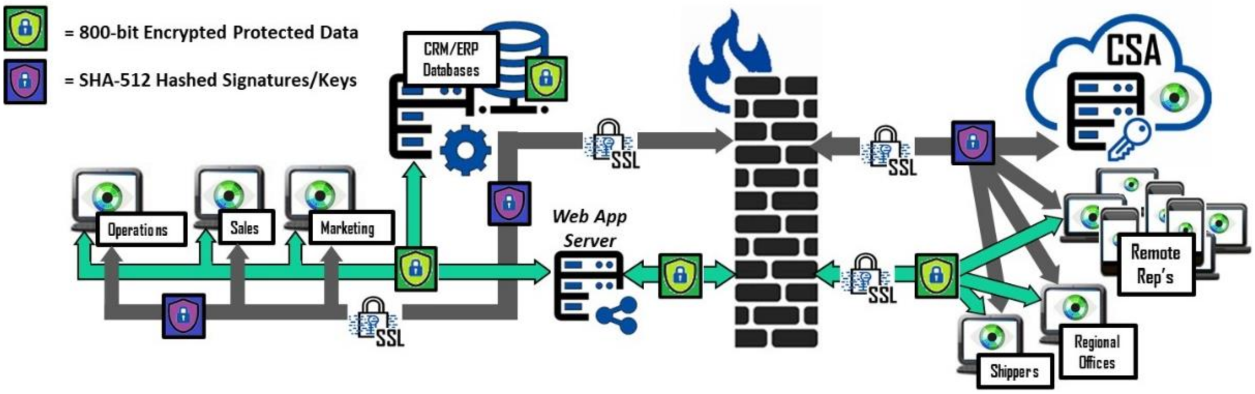
Retail CRM Databases

Use Case: Demonetizing exposed Customer Data

In an instant, the Covid-19 Pandemic forced society to change our way of life. After state and local governments shut down businesses and enforced stay-at-home orders, we were forced to basically socialize, conduct business and ecommerce activity from home. Sounds very convenient, but is the information exchanged during mobile commerce, electronic banking, supply chain management, inventory management, Internet marketing, online transaction processing, and electronic data interchange protected? Placing online orders with websites with "https" URLs should give confidence the transaction is secure. Then, why is this Personal Identifiable Information (PII) continually hacked and sold to the highest bidder on the dark web?

Take the recent Avon breach for example. As one of the largest and oldest company in the beauty industry, $5.5 billion in annual worldwide sales and 6.4 million representatives, suffered multiple cybersecurity incidents in 2020. The first, a malware attack, impacted operations and the other reported a 7GB database leaking **19 million records** went undetected for nine days on June 12. The unprotected PII data of customers and potentially employees, included full names, phone numbers, dates of birth, emails, and more. Adding insult to injury, it is alleged that a Microsoft Azure cloud server was inadvertently left open to the public with no password or encryption, allowing a vulnerable their Elasticsearch database to be effortlessly breached. Without a doubt, a leaky database is no "happy little accident". A recent Gartner report cited that, "99% of cloud security failures will be the customer's fault through 2025, and consequently, misconfigurations will continue to be a leading cause of data leakage across all organizations."



To prevent exploitation and monetization of customer breached data, an organization can leverage **Cy4Secure** to mitigate their risk and protect its brand. Encrypting data at the source (when users or systems enter data into database driven applications) and keeping it encrypted until it is accessed or read by an authorized user is data defined security. Individual data fields, records, and columns can be encrypted to control access from unauthorized users and manage risk. In Avon's situation, corporate marketing and sales, regional offices, sales representatives, regional offices, and supply-chain partners can search the protected databases with appropriate authorization. Bonafeyed's data defined security ensures cybercriminals cannot take advantage of leaky databases or open systems. The most they can obtain is unintelligible/encrypted data that has no value on the dark web. "Human Error" is a variable in the technology world and one we must anticipate. Protecting data at the source is the last stand against a data breach.

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