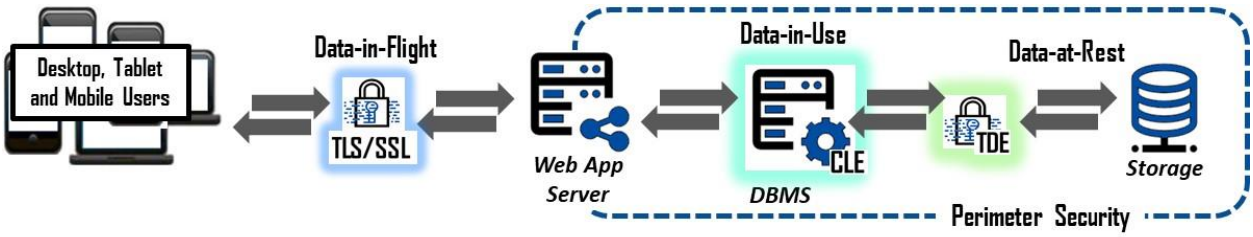
Stolen corporate data is a lucrative business driven by cyber criminals and monetized through ransomware demands or by data breach brokers on the dark web. In fact, loss of data is a cost of doing business. Tragically, Capital One confirmed on July 2019 that they were the target of a major data breach. An enterprising hacker exploited a vulnerability in the cloud infrastructure used by Capital One to hold sensitive data on more than 100 million customers and credit applicants. Capital One claimed the loss would approximately be $100 to $150 million in 2019, that is largely for customer notifications, credit monitoring, technology costs, and legal support. Globally, there are on average four data breaches per day losing approximately 6 million personal records. After all the billions of stolen Personally Identifiable Information (PII), why is this still happening? The truth is that once an attacker gets past the perimeter security, the data is freely available, stolen and then sold to the highest bidder on unscrupulous trading and auction sites.

It has been revealed by the Capital One hacker suspect and the Department of Justice, entrance was possible by exploiting a misconfigured web application firewall that enabled the attacker to run commands and exfiltrate data. What is more interesting is that once past the firewall, nothing stopped access to the data. The suspect claimed to have launched an instance within Capital One's cloud environment and after attaching the correct security profile, dumped the contents of their MySQL database to a 32TB storage before encrypting it and pulling it out over an OpenVPN session. This means that once past the perimeter security, the data is available in the clear for the taking. But how is this possible given the many database security measures touted by the Database ISVs?

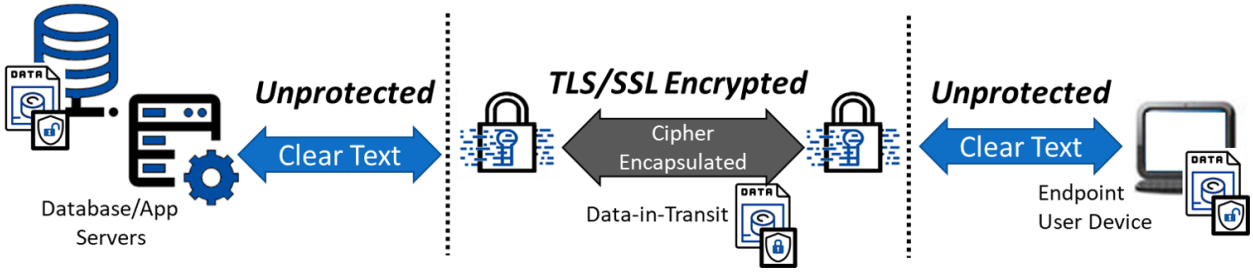
Let us take a closer look at what is available to protect data in most databases. Transparent Data Encryption, or TDE, is designed to protect data-at-rest. In other words, TDE encrypts and decrypts data as it is written or read from the storage connected to the database. Generally speaking, TDE really only protects from physical attacks on the actual storage. Otherwise, if someone steals the drives holding the data or somehow gets access to the file system managing the storage without TDE, then yes, one can get the data files lock, stock, and barrel. But given the data is in the cloud or in secured datacenters, this is unlikely and rarely if ever occurs these days.



Next is Column or Cell Level Encryption, CLE. CLE has been around for some time and allows the ability to encrypt a full column of data within a database. However, its use is limited due to the

impact on the database's performance. Most databases see a performance loss of 20% to 30% when encrypting a single column of data. Encrypting multiple columns is not recommended as a best practice because it is exponentially worse, therefore almost never deployed.

Finally, we have SSL/TLS. If you have ever seen that little gold lock icon in your web browser, then you have experienced the automated use of SSL to protect data-in-flight between the website and your browser. Unfortunately, SSL/TLS is routinely over inflated as having the ability to holistically protect data. Once data arrives in the cloud or on an end-user's system (laptop, smartphone, or tablet), SSL's job is done, and the data is decrypted. Continued data protection requires another system or solution to secure it. Therefore, if someone gets past the perimeter security and obtains permission to perform queries on the database, the data will be delivered to the intruder in the clear.



So, what is the solution? Adopt a data-defined approach to cybersecurity which enables demonetization of breached data. The best way to accomplish this, and dare we say to stop large- or small-scale data breaches such as the Capital One event, is to encrypt the data at the source (when users or systems enter data into the front-end application) and keep it encrypted until it's needed by an authorized user. At that time, data can be decrypted for the authorized user. What this means for database driven applications is to encrypt data before it is sent to the database application where it remains encrypted. When done correctly, the database management system has no idea it is operating on encrypted data allowing all the features of searching for records to remain the same. When a breach occurs, the best a cybercriminal can obtain is unintelligible/encrypted data from the database that has no value in the black market.

"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.