OptimalCipher

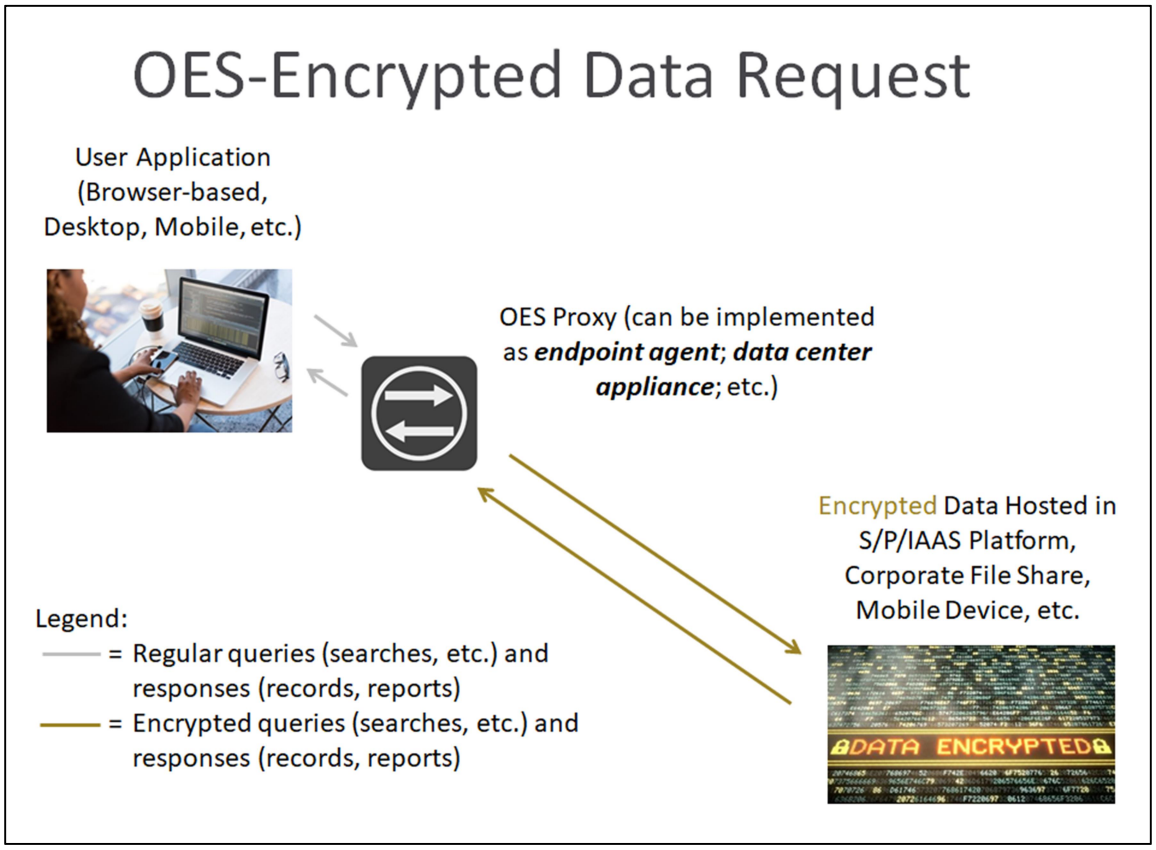
Overview of the OptimalCipher Encryption Suite

Security breaches continue to befall organizations large and small. The number of records compromised due to breaches has increased from 169.1 million in 2015 to 27 *billion* in just the first half of 2020. And the estimated average cost of a breach has increased from $3.50 million in 2014 to $3.85 million in 2020.

The reason for these increases is that current information security approaches used by almost all organizations still mostly protect their data's perimeter. But--as the growing volume of compromised data illustrates, perimeter controls--firewalls, intrusion detection systems, access controls, audit logs, etc.--are insufficient. External hackers and insiders keep finding novel ways to break through perimeter defense systems, and access organizations' sensitive data.

OptimalCipher has developed a groundbreaking technology to protect the data itself—the common target of these breaches--without impacting the applications that use the data. The OptimalCipher Encryption Suite (OES)--developed by PhD mathematicians--is the first patented system that can perform extensive analysis of data while the data are fully encrypted, across numerous platforms.

The OES is implemented by encrypting the data sources, placing a proxy between the applications and data sources, and mediating encryption/decryption as data travels between applications and the data repositories.



The OES provides the following key benefits:

- Fully encrypts data, yet allows applications to perform a comprehensive analysis of the encrypted information, including searching, sorting, and mathematics and statistics of encrypted numbers.
- Frequently requires no code changes to, and has minimal performance/latency impact on the underlying applications.
- Fully encrypts all data, rather than just some data, as most competitors do--obviating the need to perform costly data classification activities, and removing worries about potential data "re-identification". All data is considered confidential, and is encrypted.
- Can simultaneously aggregate and enrich information from numerous different data sources--e.g., emails, databases, IoT devices, etc.--in a privacy-protective fashion (if the same encryption key is used), to improve decision-making in a regulatory compliant manner.
- Can provide a lower Total Cost of Ownership--as a single administrative console can be used to control multiple encryption domains within an organization--instead of using point (and often siloed) encryption solutions.
- Protects the data--not the systems that the data lives on. So no matter where the data travels to, it remains secure. Only authorized users with the appropriate decryption key can decrypt the data.

info@optimalcipher.com
OptimalCipher