OptimalCipher Encryption Suite
Value Proposition and Use Cases

OptimalCipher

Data Security/Analytics Problem

The impact of security breaches continues to increase:

- Number of records compromised due to breaches rose from 169.1 million in 2015 to 15.1 *billion* in 2019.
- The global average total cost of a breach has risen from $3.50 million in 2014 to $3.92 million in 2019.

Sources: Statista: Annual number of data breaches and exposed records in the United States from 2005 to 2019; The Definitive Cyber Security Statistics Guide for 2020; DataInsider: What's the Cost of a Data Breach in 2019?

Data Security/Analytics Problem

Reason for many security breaches:

- Data is typically not collected for its own sake; organizations need to *analyze* their collected information.
- To support analytics, data must be in a decrypted state.
- But in plaintext form, data can be stolen by hackers or viruses (theft of files, memory attacks, etc).

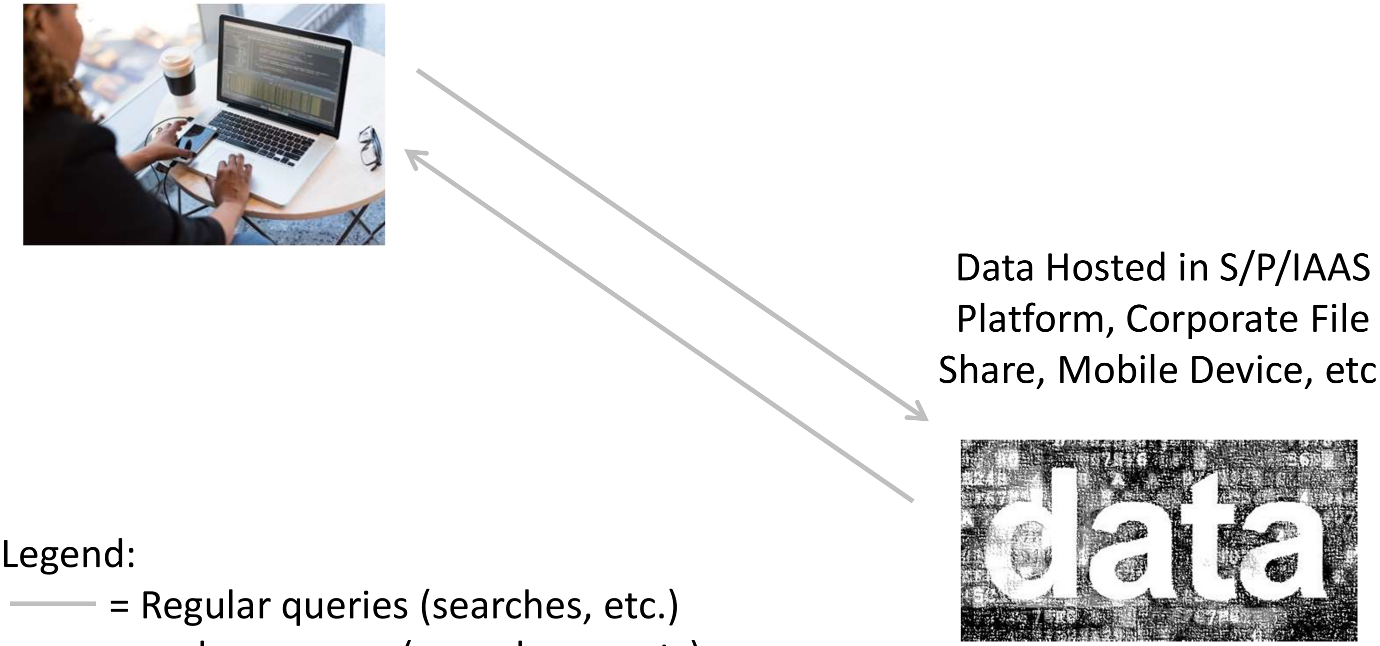
To support today's increasing data-driven processes, a system is needed which strongly, continually protects information, while permitting data analysis.

OptimalCipher Encryption Suite (OES) Value Proposition

First patented system that provides comprehensive analysis of data while the data are entirely encrypted. The OES:

- Fully encrypts data, yet allows applications to search, sort, and perform mathematics and statistics on the encrypted data.
- Protects data in numerous hosting environments, e.g. in cloud, data center, mobile devices, etc.
- Frequently requires no code changes to, and has minimal performance/latency impact on the underlying applications.
- Fully encrypts all rather than just some of the data--thereby preventing possibilities of data ‘re-identification’. This also significantly simplifies data classification activities, which prescribe different security controls for different data categories. All data is considered confidential and is encrypted.
- May provide a lower Total Cost of Ownership for enterprise encryption--as a single administrative console, instead of different point encryption solutions, is used to control multiple encrypted domains.
- Protects the data--not the systems the data lives on. No matter where the data travels to, it remains secure. Only authorized users with the appropriate decryption key can decrypt the data.

Typical Data Request



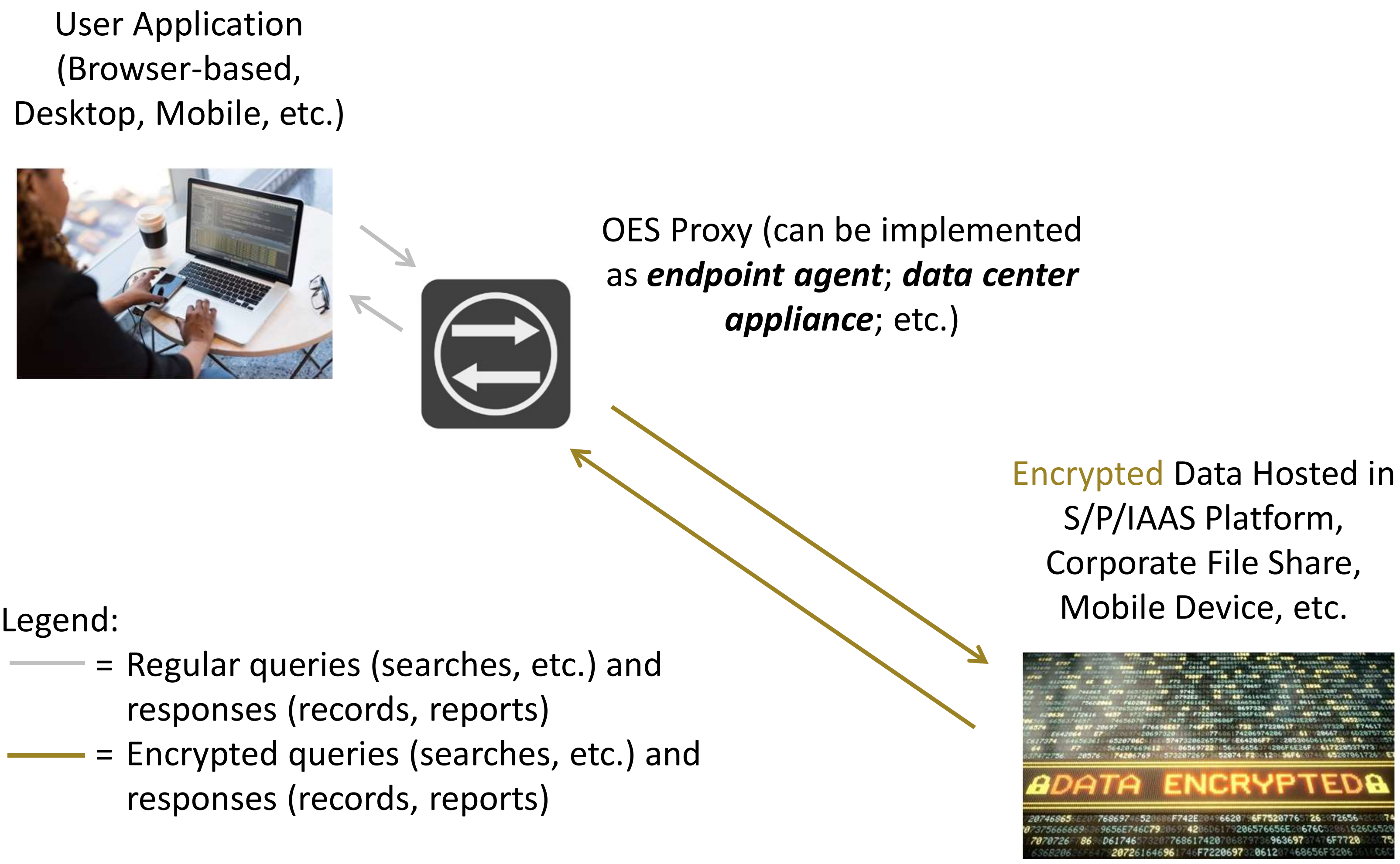
User Application
(Browser-based,
Desktop, Mobile, etc.)

Data Hosted in S/P/IAAS
Platform, Corporate File
Share, Mobile Device, etc.

Legend:

— = Regular queries (searches, etc.)
and responses (records, reports)

OES-Encrypted Data Request



User Application (Browser-based, Desktop, Mobile, etc.)

OES Proxy (can be implemented as ***endpoint agent***; ***data center appliance***; etc.)

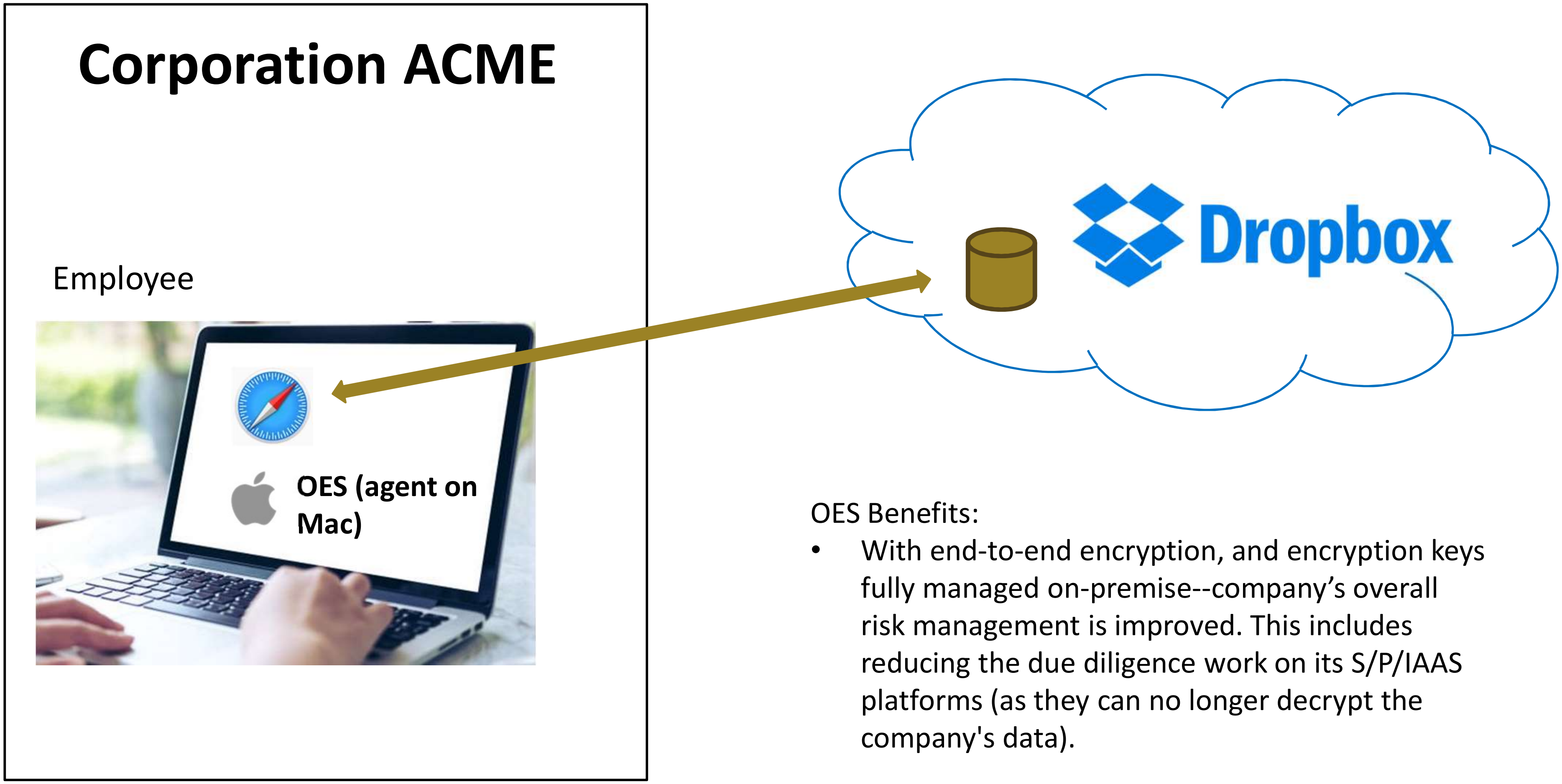
Encrypted Data Hosted in S/P/IAAS Platform, Corporate File Share, Mobile Device, etc.

Legend:

─ = Regular queries (searches, etc.) and responses (records, reports)

─ = Encrypted queries (searches, etc.) and responses (records, reports)

Use Case 1: End-To-End Encryption

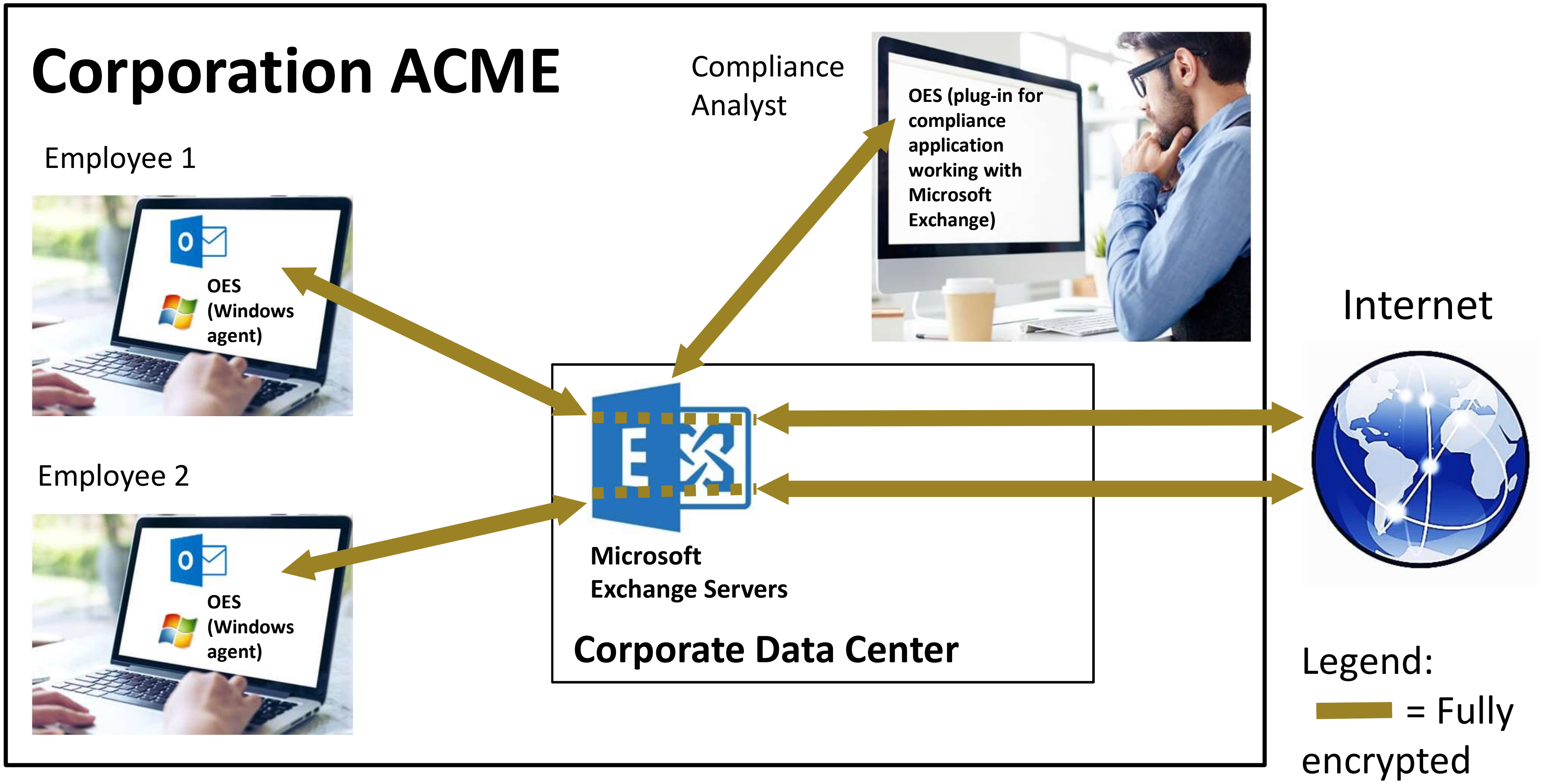


OES Benefits:

- With end-to-end encryption, and encryption keys fully managed on-premise--company's overall risk management is improved. This includes reducing the due diligence work on its S/P/IAAS platforms (as they can no longer decrypt the company's data).

Legend: ▬ = Fully encrypted data/traffic

Use Case 2: Encrypted Data Analysis



Legend:
▬ = Fully encrypted data/traffic

OES Benefits:

- Analysis of encrypted emails for compliance purposes before emails leave company (e.g. privacy-preserving policy enforcement).

Use Case 3: Obviating Data Classification

Typical Data Classification

Employee Last Name	Employee First Name	Employee Age	Employee Email
Smith	Bob	55	bob@acme.com
Kline	Susan	43	susan@acme.com
Jones	Philip	63	philip@acme.com

Does GDPR require protecting Employee Email?
Does HIPAA require protecting Employee Age?
Is my company's policy clear on protecting Employee Last Name?
Etc.

Data Classification Under OES

Employee Last Name	Employee First Name	Employee Age	Employee Email
8*(@31	**Hj+=;]**	**11**	**KS2%_+**
\}~d$#	**Nx^^%@**	**88**	**64G:?2Z**
pdW,{+	**D05=!z**	**24**	**%0^` | =8f<**

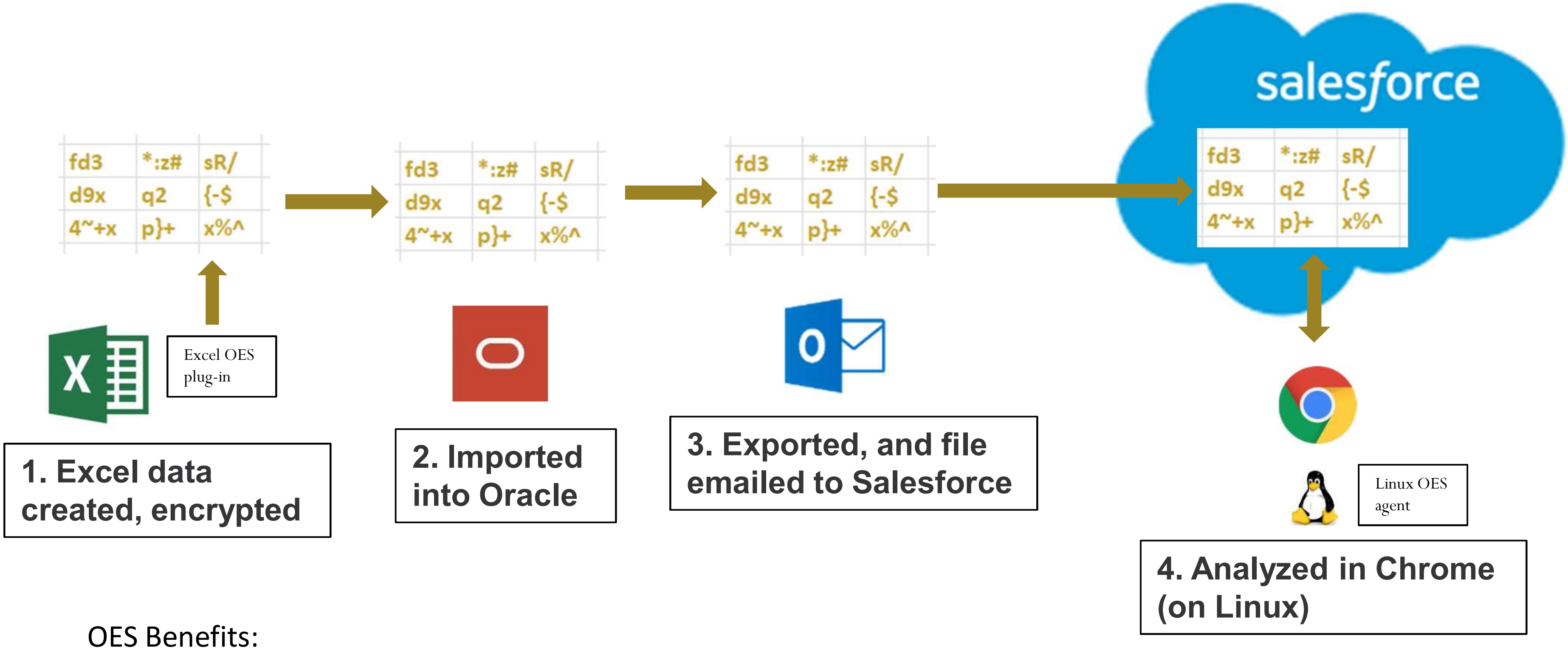
No substantial need for Data Classification, since within an IT system, virtually all data is encrypted. Effectively--no "sensitive data" remains.

Legend:
▬ = Fully encrypted data

OES Benefits:

- Substantially less time required for Data Classification activities--since OES considers all data to be at the highest sensitivity level, and applies one of the best security controls to data: encryption.

Use Case 4: Simplification of the Encryption Ecosystem



1. Excel data created, encrypted

2. Imported into Oracle

3. Exported, and file emailed to Salesforce

4. Analyzed in Chrome (on Linux)

OES Benefits:

- Encryption ecosystem Total Cost of Ownership can be reduced since only one encryption system—OES--is utilized (instead of using Excel’s **password-protected encryption**; Oracle’s **Transparent Data Encryption (TDE)**; etc).
- Relying on a single system also obviates the need to decrypt and re-encrypt data moving between platforms (e.g., removing Excel’s password protection to import data into and TDE re-encrypt it within Oracle). This reduces security breach risk as data is never in a decrypted state; and also speeds data throughput.

Legend:
▬ = Fully encrypted data/traffic

info@optimalcipher.com

OptimalCipher