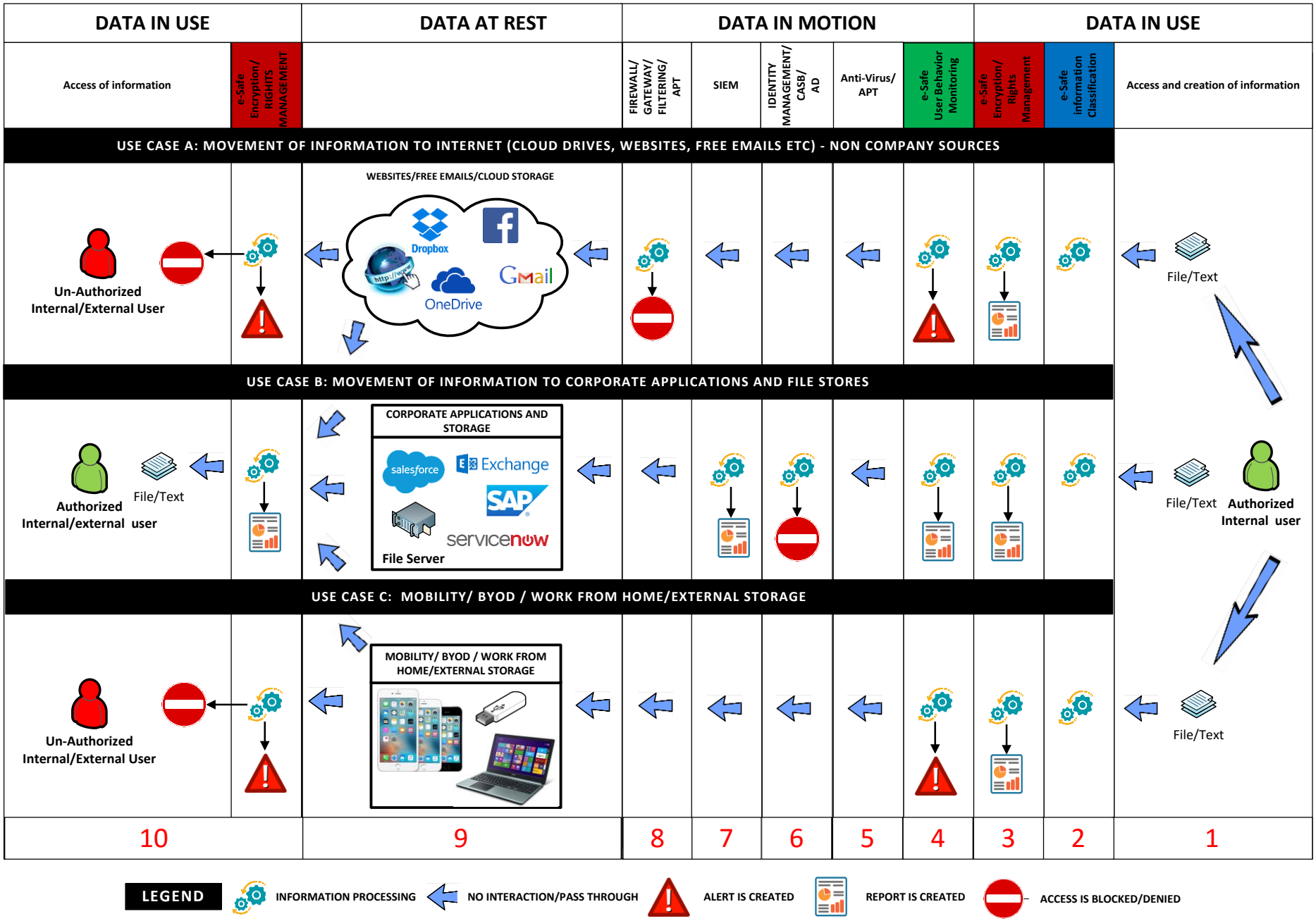
SECURITY GAPS COVERED BY E-SAFE COMPLIANCE NOT ADDRESSED BY OTHER SECURITY PRODUCTS


DATA IN USE
DATA AT REST
DATA IN MOTION
DATA IN USE
Access of information
e-Safe Encryption/ RIGHTS MANAGEMENT
FIREWALL/ GATEWAY/ FILTERING/ APT
SIEM
IDENTITY MANAGEMENT/ CASB/ AD
Anti-Virus/ APT
e-Safe User Behavior Monitoring
e-Safe Encryption/ Rights Management
e-Safe information Classification
Access and creation of information
USE CASE A: MOVEMENT OF INFORMATION TO INTERNET (CLOUD DRIVES, WEBSITES, FREE EMAILS ETC) - NON COMPANY SOURCES
WEBSITES/FREE EMAILS/CLOUD STORAGE
Dropbox
Gmail
OneDrive
Un-Authorized Internal/External User
File/Text
USE CASE B: MOVEMENT OF INFORMATION TO CORPORATE APPLICATIONS AND FILE STORES
CORPORATE APPLICATIONS AND STORAGE
salesforce
Exchange
SAP
servicenow
File Server
Authorized Internal/external user
File/Text
File/Text
Authorized Internal user
USE CASE C: MOBILITY/ BYOD / WORK FROM HOME/EXTERNAL STORAGE
MOBILITY/ BYOD / WORK FROM HOME/EXTERNAL STORAGE
Un-Authorized Internal/External User
File/Text
10
9
8
7
6
5
4
3
2
1
LEGEND
INFORMATION PROCESSING
NO INTERACTION/PASS THROUGH
ALERT IS CREATED
REPORT IS CREATED
ACCESS IS BLOCKED/DENIED

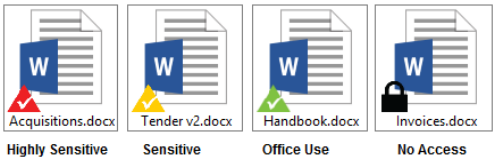
1 DIAGRAM EXPLANTION

The diagram explains the access and movement of information such as payroll, contracts, financials etc either file or text based by **Authorised staff or partner**. The following use cases have been showcased.

Note: The numbers in the above diagram refer to the sub points under each use case.

1.1. USE CASE A → MOVEMENT OF INFORMATION TO INTERNET (CLOUD DRIVES, WEBSITES, FREE EMAILS ETC) – NON COMPANY SOURCES

1. **Access and creation of information**→ An authorised user creates or accesses information (file or text based) and uses free internet sources to either store or transfer the information.
2. **e-Safe Compliance – Information Classification** → e-Safe Compliance classifies the information (file or text based) on access and in movement based on its sensitivity. Several methods of information classification are provided which include decentralized classification by information owners, automated classification based on location (shared folder), user, content etc. The advanced Information Classification mechanism allows e-Safe Compliance to trigger alerts (under user behaviour, encryption and rights management modules) based on the level of sensitivity of that information. This reduces detection time which is crucial in preventing insider leaks.
3. **e-Safe Compliance – Encryption and Rights Management** → Once information leaves the organization it is considered lost. e-Safe Compliance solves this problem by encrypting the sensitive documents. e-Safe applies the appropriate access rights (with AD integration) on the documents based on the defined classification. The encryption used is known as **UNIVERSAL ENCRYPTION** which is transparent (no need for users to provide keys, certificate etc) and persistent (information remains encrypted even for authorised users). Encrypted information is showcased with triangles based on the document's sensitivity levels. Complete tracking of sensitive documents is available in the form of forensic tracking reports.



4. **e-Safe Compliance – User behaviour Monitoring** → The User Behaviour Monitoring module monitors all forms of information movement, whether file based or text based and generates alerts based on the defined classifications. As the monitoring is done at the end-point e-Safe Compliance is able to monitor the device even if it is **offline,** or not connected to the corporate network (using 4g networks). Further it is not affected by encrypted content.

   The system is able to monitor files uploaded to any websites, cloud storage (Dropbox, Google Drive, etc), social media or free emails/webmails. The system is also able to monitor movement of all text based information via chat, in an email body or web post. Additionally it has keystroke monitoring as a backup feature, to be turned on for specific applications and highly sensitive areas. **e-Safe Compliance**

produces detailed user-centric reports with complete evidence of the event (visual evidence and contextual information) which can be produced in court.

5. **Anti-Virus/APTs**→ As the information being passed is of a corporate nature, and is being moved to websites which are generally considered safe (Gmail, Dropbox etc), the software lets this information pass through without creating any alerts.

6. **Identity Management Software/CASB/AD**→ Identity management software works to define access to information for corporate applications. CASB does the same for cloud based services such as Salesforce etc. However, as the applications/websites being accessed are not corporate in nature, these applications cannot control the information being uploaded to these non-authorised company applications and therefore let the information go through.

7. **SIEM**→ Gathers logs from company related applications. It doesn't connect to or process information being passed to non-standard websites and applications (online or offline). As such it doesn't produce or gather any logs for this use case and allows the information to pass through without any evidence.

8. **FIREWALL/GATEWAY FILTERING/APT PREVENTION** → They have been used traditionally to handle non-authorised internet applications and web-uploads. They are effective in blocking access to non-authorised internet websites and applications. However, where access is provided, they have been known to be inadequate in monitoring content. For example, they mostly fail to decipher encrypted traffic such as encrypted chats, attachments and their content in free emails etc. **Further, the reports produced are inadequate from a legal perspective as they cannot, with certainty, indicate that the particular user was involved in the incident.**

9. **Websites/Cloud Storage/Free emails**→ Information transferred to these media remains vulnerable as the security of this information lies with the user. Also the information stays there, even if the person leaves the organization. With e-Safe Compliance encryption, information remains protected and secure.

10. **Unauthorized internal or external users** → Unauthorised users, either internal or external to the organization, cannot gain access to the encrypted sensitive files. In case of internal users where the agent is installed, the system also generates alerts for this unauthorised interaction.

    a. **Authorized internal or external user** → Authorised internal or external users will be able to access encrypted files transparently (without the need to provide password or certificates etc). All key management is done automatically. Reports of this interaction are produced in the system.

1.2. USE CASE B → MOVEMENT OF INFORMATION TO CORPORATE APPLICATIONS AND FILE STORES (INTERNAL AND EXTERNAL CLOUD BASED APPLICATIONS)

1. **Access and creation of information**→ Authorised user creates or accesses information (file or text based) and transfers the information using corporate applications and file stores. These applications can either be internally hosted or based on cloud services.
2. **e-Safe Compliance – Information Classification → SAME AS PREVIOUS SECTION.**
3. **e-Safe Compliance – Encryption and Rights Management → SAME AS PREVIOUS SECTION**. Additionally, an exception can be set in the system to not encrypt files when being uploaded to corporate applications such as document management systems. This ensures easy integration with various corporate systems.
4. **e-Safe Compliance – User behaviour Monitoring → SAME AS PREVIOUS SECTION**. Corporate email is an important application that is monitored and reports are produced in the case of suspicious behaviour. Additionally, exceptions can be set in the system not to monitor interaction with corporate applications. This is to ensure false hits can be reduced. Another option is to lower the alert level and only to report on the various file and text based interactions.
5. **Anti-Virus/APTs**→ As the information being passed is of a corporate nature, and is being moved to websites which are generally considered safe, these software let this information pass through without creating any alerts.
6. **Identity Management Software/CASB/AD**→ Identity management software/CASB/AD ensure that only authorised users can access corporate systems. Further they also define the level of access for each user within the corporate system.
7. **SIEM**→ Gathers logs from company related applications and can be used in relation to the e-Safe User behaviour reports to give a consolidated picture.
8. **FIREWALL/GATEWAYS FILTERING/APT PREVENTION**→ These systems don't monitor the internal corporate applications as they are considered safe. Some specialized products monitor corporate emails and generate alerts in case sensitive information is being sent out.
9. **CORPORATE APPLICATIONS AND STORAGE** → Information is processed and stored in these applications and stores. Information stored in Cloud based corporate systems can be secured using e-Safe Compliance encryption as the files are maintained in an encrypted state. This protects information leakage in the event the authorised user tries to download the information by accessing it from outside of corporate network…such as from his home.
11. **Authorized internal or external user** → Authorised internal or external users will be able to access encrypted files transparently (without the need to provide password or certificates etc). All key management is done automatically. Reports of this interaction are produced in the system.
    a. **Unauthorized internal or external user** → unauthorised users, either internal or external to the organization, cannot gain access to the encrypted sensitive files. In case of internal users, where the agent is installed, the system also generates alerts for this unauthorised interaction.

1.3. USE CASE C → MOBILITY/ BYOD / WORK FROM HOME/EXTERNAL STORAGE

1. **Access and creation of information**→ An authorised user either creates or accesses information (file or text based) from home, using non-corporate networks, but using company laptops or using his own device such as a mobile phone and tablet. Further the information can be transferred by the user to external storage media such as USBs, mobile phones, SD cards etc.
2. **e-Safe Compliance – Information Classification → SAME AS PREVIOUS SECTION.**
3. **e-Safe Compliance – Encryption and Rights Management → SAME AS PREVIOUS SECTION**. As the files are encrypted it doesn't matter if the user transfers them to any external media (USB, mobile phone sync, SD card) as they remain encrypted and secured. Encryption ensures that it is future proof against new forms of storage mechanisms.

   Special BYOD features ensure that only company related information is encrypted and secured. Further special variants are available for people who wish to work from home and for long term partners. For mobile devices, APPs are available to ensure encrypted information can be accessed seamlessly and securely on these devices.

4. **e-Safe Compliance – User behaviour Monitoring → SAME AS PREVIOUS SECTION**. Alerts are produced in case information is transferred to external storage. In case of BYOD and personal devices, monitoring is limited to only corporate encrypted files and corporate emails.
5. **Anti-Virus/APTs**→ With respect to BYOD and personal devices, these software have no control over them. For corporate laptops, as the information being passed is of a genuine nature (non-virus /malware related) these software let this information pass through without creating any alerts. Further these software don't monitor information being moved to external storage.
6. **IDENTITY MANAGEMENT SOFTWARE/CASB/AD**→ They can't prevent the user from copying sensitive information to a USB device or other forms of external storage such as mobile phones**.** Their main focus is to ensure that only authorised users can access corporate systems even when logging on from their house or outside of the network.
7. **SIEM→ SAME AS PREVIOUS SECTION.** Produces no logs if/when information is transferred to USBs and mobile phones, or if information is being transferred to non-corporate file stores and applications.
8. **FIREWALL/GATEWAY FILTERING/APT PREVENTION** → No monitoring of offline file transfers to USB devices or other forms of external storage such as mobile phones.

   Further they are unable to monitor users when they don't connect via the corporate network, as in the case of mobility, such as laptops connecting to the internet from home.

9. **MOBILITY/ BYOD / WORK FROM HOME/EXTERNAL STORAGE** → Information is now accessed and stored in numerous devices, many of which don't belong to the company. Further, the locations (home, office etc) where the users access this information have also diversified. e-Safe Compliance, through its encryption and user behaviour monitoring features, offers control over these devices and information.

10. **Unauthorized internal or external user** → Unauthorised users (either internal or external to the organization) cannot gain access to the encrypted sensitive files. In the case of internal users where the agent is installed, the system also generates alerts for this unauthorised interaction.

    a. **Authorized internal or external user** → Authorised internal or external users will be able to access encrypted files transparently (without the need to provide password or certificates etc). All key management is done automatically. Reports of this interaction are produced in the system.