Domo Data Security & Encryption

Decision makers recognize the value of insights gained from their business data. The ability to quickly review relevant data provides better understanding of business operations and accelerates better decisions. To continually improve business processes, companies are looking for new data sources, improved data modeling and easier, direct access to data warehouses. With the exponential growth of data, companies have increasing concerns around data security. How can you keep data secure, with whom should you partner for IT projects and applications and how should you share data internally as well as externally?

Increased exposure to data breaches and other nefarious data security issues are concerns that now reside on the desk of the CEO, not just the CTO or CIO. It's simple to find examples of data compromise and the negative impact it has on organizations[1]. All company departments need to be concerned about inadvertently sharing their protected data with individuals and partners who do not need to see that data while still enabling others in their ecosystem to use the data to complete their critical tasks. Protecting all data has to become a primary concern when selecting employees, vetting partners, and selecting vendors. You need a partner that can help you help you ensure that your business data are being handled correctly.

All data is not created equal

Your organization generates and consumes different types of business data. Some of your business data are publically available and can be used and accessed by multiple users without strict control measures. Other data are sensitive to specific business processes like salaries or revenue. And finally, there are data protected by law such as employee medical information. In each case you have the responsibility to ensure that different operational requirements and processes for handling the data are secure.

As a company, you are obligated to ensure that the PII and PHI data used is secure and/or is properly obfuscated to safeguard the identity of the individual from anyone not directly providing service to the individual. This includes a charge to control data used in 3rd party vendor applications.

Domo delivers greater control of your business data. Workbench (Domo's on-premise data acquisition tool) provides you options on how to de-identify your data, manage who can see it, and track and log when it is accessed.

Data Security is a consumption problem

As decision makers are constantly moving between meetings, locations, and critical decisions, the mobile experience demands access to information from anywhere, at anytime, and on any mobile

device. Questions around data security and mobility become complex and difficult to answer. Companies are no longer able to simply keep their data locked away in data centers and control access through their intranet. The successful decision maker requires access on their mobile device to critical business information.

There exist many data security concerns regarding who can see the data, who has access to the data, and how data is being handled and processed. Therefore, the question is not only how secure is your data architecture but also how secure is the data architecture of your partners and vendors. Laws stipulate that you need to know who had access to the data, when they had access to the data, and what they did with that data.[2]

Domo Data Security

Domo has made security its number one priority. This is completed in two ways; first it is the integrity of the system, which is to protect the data at rest and/or in-transport from compromise and inadvertent exposure. Second, the administrative control provided to users of the Domo Business Management Platform.

In order to maintain a high standard of system integrity and security, Domo undergoes several measures to be in compliance with regulatory and industry security standards. In addition, Domo provides periodic risk assessments designed to identify and manage risks to Domo and Domo's customers' hosted data. Various methodologies are associated in the risk identification process, including: technical assessments, threat assessments, vulnerability assessments, and attack and penetration exercises.

For customers of Domo, various security-related functions within the platform are available for administrators. Only those users with a Security Profile of "Administrator" can control the invitation of new users, removing of users, assigning security profiles to users, creating user groups, etc. Domo provides integrations to single sign-on, directory services so your IT organization can mirror your policies and compliance rules of your organization into your Domo instance.

Domo Data Encryption

Domo keeps you in control of your data and your data security. Our cloud-based service provides data consumers the access they need while your organization's IT administrators have the confidence knowing the data are secure. Domo provides tools to confidently manage your data before it leaves your data center and know it is secure while at rest until your designated users request it.

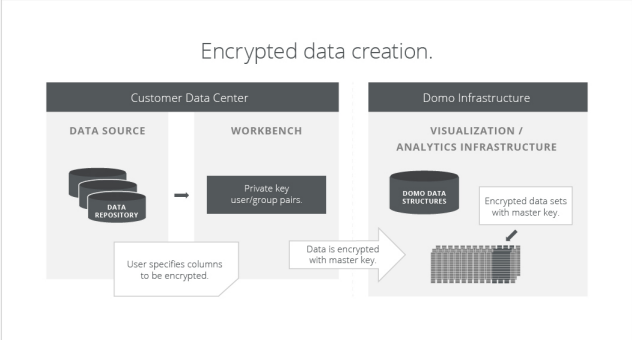
Data in Motion

Domo's Workbench application provides you the ability to connect into your on-premise data sources and encrypt specific columns that contain sensitive data while it is in your data center. Before a single byte is transferred from your secure data center you will have encrypted sensitive information and granted access on a per user basis. This gives you granular access to both the individual columns of protected data as well as a by user access list, to ensure that you are in full control of both data and access.

When you transfer data from your data center your data remain encrypted using AES 256 encryption. The decryption is accomplished only in your user's secure browser session when they provide their unique secure passcode.

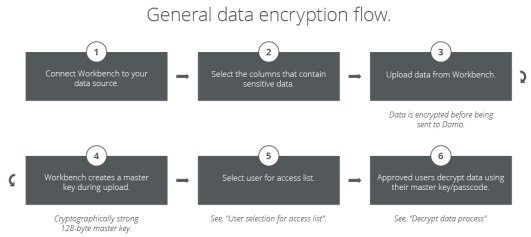
Data at rest

While your business data reside on Domo servers, the data remain encrypted, completely unusable and unidentifiable. There is only a single instance in which your encrypted business data can be decrypted. This instance is in the secure browser at the request of the user you designate on the access control list managed on Workbench. At no time does anyone, inside or outside of your organization, have access to read or use your encrypted data, unless they have been granted access by you.



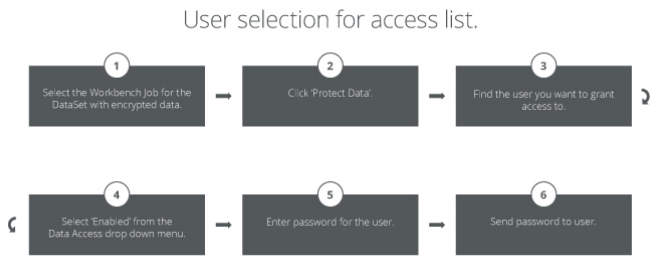
The Domo Encryption Solution

Domo Workbench provides encryption and decryption capabilities. In this section, we will describe how you are able to maintain secure handling of data deemed sensitive, while outside of your data center. There are two primary actions needed to encrypt your data in Workbench: the creation process and the consumption process.



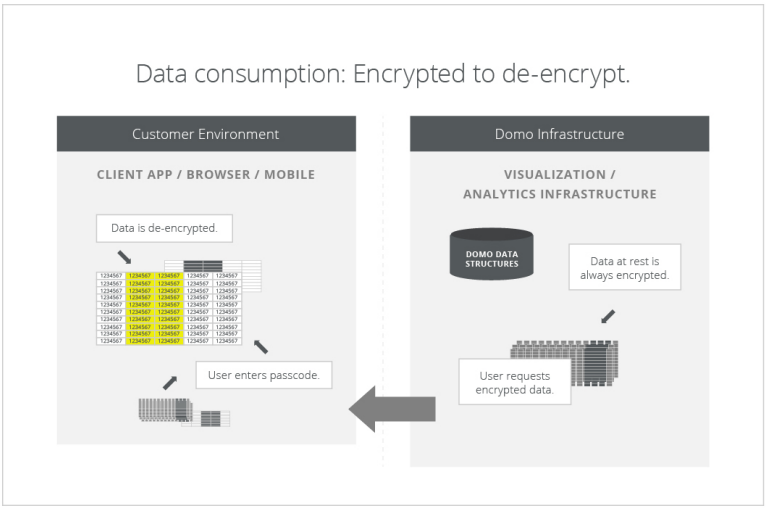
The creation of your encrypted data starts with the connection of Workbench with your data source. Once your data schema has been loaded, you will select the columns that you want to encrypt.

Workbench will then create a cryptographically strong 128-byte master key. Your data will then



then be encrypted through the master key using AES 256. Each time your job runs, the previously selected data columns are encrypted at the source with the master prior to being sent to Domo.

The administrator can then select which users will have access to decrypted data in the visualization stage. The administrator will provide a passcode that will be shared with the selected user. The passcode is used to create the user key, which is the master key that has been encrypted using the passcode and AES 256. This capability and process of selecting employees with access is done within the Workbench platform.



The consumption of encrypted data is only available to the users pre-selected in Workbench. When you selected a user and granted access they received a passcode that will be used to decrypt the user key. The authorized user can now request visualization using the encrypted data. The visualization is presented with a lock icon where the encrypted data would normally be used. The authorized user clicks on the 'lock' icon and is prompted for the user passcode set when the data was encrypted. Upon successful input of the passcode, the encrypted data is revealed in the visualization.

In this process, the level of encryption and security of sensitive data remains in the administrator's control. At no point is the data decrypted on the Domo server and at no time does Domo maintain the information to decrypt the keys or data; all decryption takes place within the browser, all encryption and key management takes place in Workbench prior to upload within your data center.

Conclusion

Data security is the responsibility of the company that creates and captures data. The Domo Business Management Platform and its features provide you the ability to share your data with the decision makers that drive your business while continuing to maintain control of your business data.

[1] "Target says over 70 Million..."; http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html
"Sony Pictures: The Data Breach..."; http://www.forbes.com/sites/davelewis/2014/12/17/sony-pictures-how-the-criminal-hackers-won/
"Evernote says security has been breached"; http://www.bbc.com/news/technology-21644317
"Home Depot hackers used vendor log-on.."; http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/

[2] "Table 1. Principles used by experts in the determination of the identifiability of health information." http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html