GeoFit™ SECURITY

GeofitSecurity_WHP_ALL_20181008_REV00

Revision History

Documents are reviewed annually to ensure relevance to the systems and process that they define.

Rev	Date	Originator/Reviser	Dept	Reason for Change
0.0	10 - 2018	Dryer, J.		
0.0				

Table of Contents

Data Security

Security of data is a major focus in the Oil and Gas industry, principally due the the value attached to the data. For many Operators, this focus has been sharpened by the interest in ISO 26700 https://en.wikipedia.org/wiki/ISO/IEC_27000 standards. There are two aspects of data security that are of concern: loss of data and misappropriation. Data loss is the total removal of access to data, such as that caused by hardware failure, accidental or purposeful deletion or data corruption. Misappropriation is the theft of data, possibly without the knowledge of the data owner. Both are appropriate concerns.

Loss of data

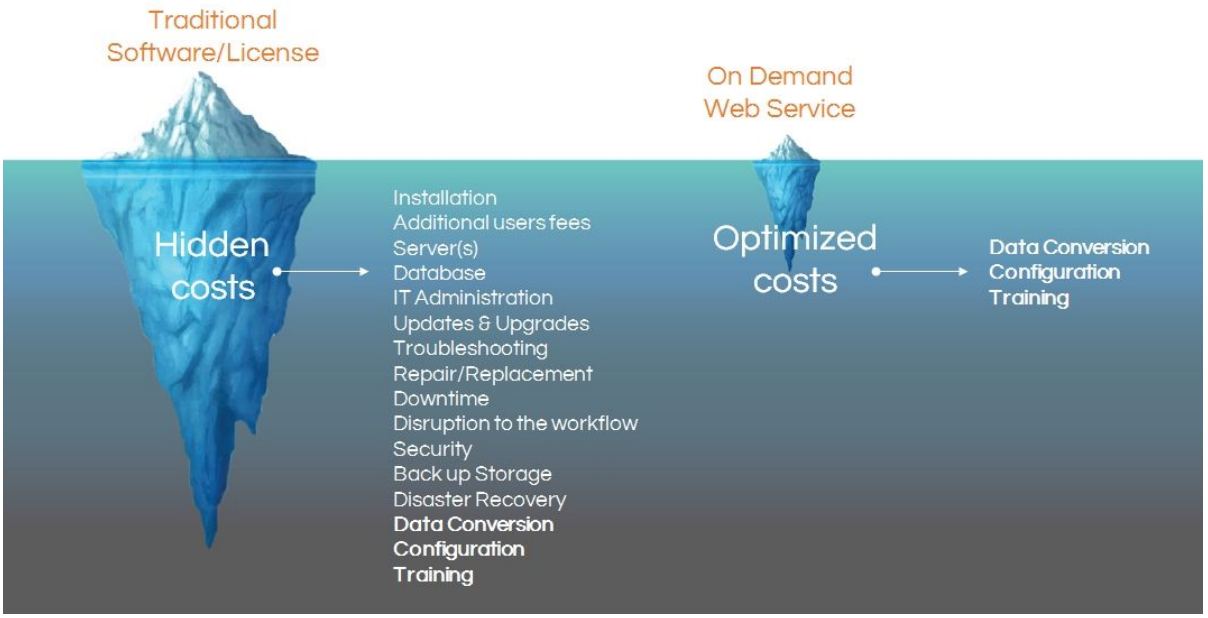
Backup

Traditional data management on company-owned servers and computers are exposed to data loss. The traditional protection against this is backup of the data and restrictions on those who have access. Backups, when actually done, have often not been tested, hence prove worthless and have issues of storage integrity. The cloud now offers an order of magnitude improvement on this process otherwise unavailable to even the largest companies.

Our cloud data storage is 99.999999999% durable with objects stored redundantly across multiple physically separated locations. The multiple copies are continually checksum verified and restored if the checksum is incorrect. The verification is designed to allow recovery if any two of the copies fail. This allows the durability figure, which corresponds to .12 files lost per petabyte (PB) (1015 bytes of data, 1,000 terabytes (TB) or 1,000,000 gigabytes (GB)) per year[1]. This can be compared with normal disk drives which have been found to have a 1.2% failure rate per year, with the loss of all data on the drive[2]. An additional factor is the many aspects of physical and programmatic security that can reduce disk reliability and represent additional expense but are routinely provided by cloud providers as shown in the following illustration.

[1] https://wasabi.com/blog/11-nines-durability/?utm_referrer=https%3A%2F%2Fwww.google.com%2F

[2] https://www.backblaze.com/blog/hard-drive-stats-for-q1-2018/



An ongoing issue is the vulnerability of data to third party attacks, such as ransomware or computer viruses. The typical scenario is malicious software gets installed on a server or on a user's computer. The malicious software examines all files that are write accessible to the server or computer, and corrupts or encrypts any such files, reducing their availability or usefulness. We do not install user software in our GeoFit instance and all data manipulation is conducted within our instance. A user has a defined interface to exchange information, with no direct view or access to the data storage.

Normal malware has no path to disrupt the data storage. A user with authorization and a valid password could delete data, but objects inadvertently deleted can be recovered if saved during the backup period. GeoFit provides incremental backup periodically over a number of days so that recovery of the data can be accomplished at any point over these period of days.

Data Misappropriation

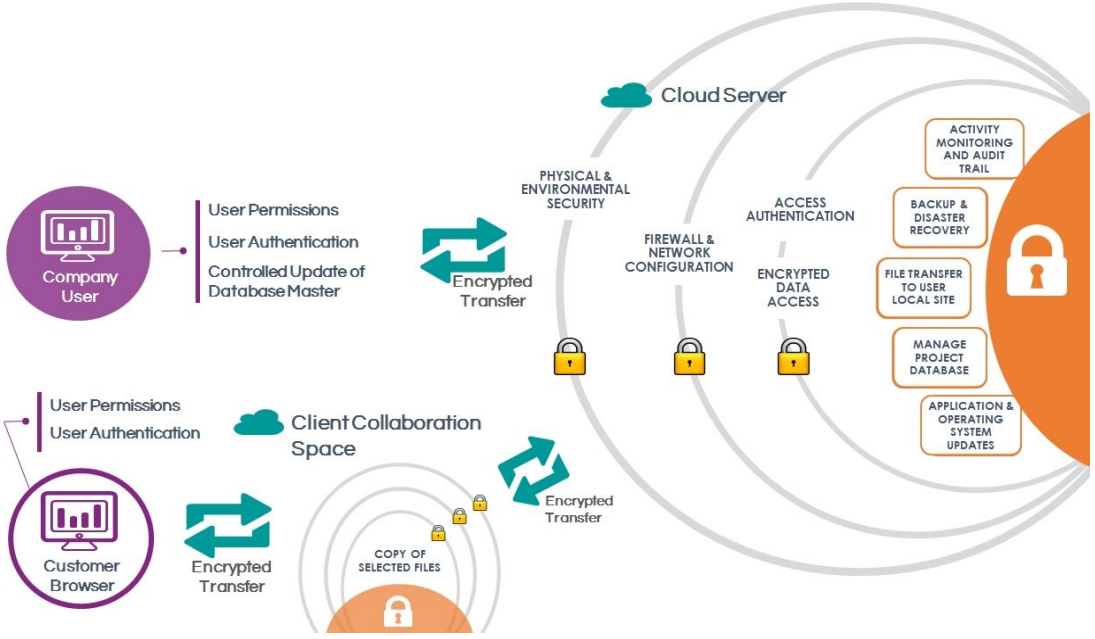
It is important that data be secured from unauthorized disclosure to third parties. These third parties may also wish to hide any indication that they have access or have accessed the data. Hacking of data servers and computers is a serious and growing problem [3] including particular attention in Oil and Gas [4]. Not only is the misappropriation of data a potential loss to a company's bottom line, but generally a company has agreed they will protect third-party shared data with "no less than reasonable care," opening the possibility of liability if data is not protected.

Data security is enhanced by a centralized database where all efforts can be concentrated on secure transmission, storage and access. These tasks are made difficult when the data is in

[3] http://ecis2018.eu/wp-content/uploads/2018/05/Industrial-espionage-and-information-security.pdf
[4] https://www.manufacturing.net/article/2018/01/10-cybersecurity-threats-facing-oil-and-gas-industry
https://www.spe.org/en/jpt/jpt-article-detail/?art=3748

many independent locations. We install no software on the customer's machine outside the computer's browser. While everyone has their favorite browser, all common browsers have expended great effort to make their product secure and very difficult for software loaded with javascript-type interfaces, as we do, to infect host computers outside the browser "sandbox" where such code is downloaded and run (e.g. see the discussion for Chrome [5]). This creates at least an order-of-magnitude improvement over natively-installed code and allows the safe use of upgrades. As the following drawing illustrates, all communications over the Internet uses secure encryption such as SSH. Such technology is used by banks and brokerages to protect your financial transactions. There are a number of security enhancements in the cloud instance, such as authentication of each user and verification of their access permissions, monitoring of Internet traffic to detect anomalous activity, firewall protection, etc.

The next generation of GeoFit will include the ability to add a collaboration instance which will provide the ability to have an independent location outside a company's main database to securely share selected information with third parties using an additional GeoFit to allow the third parties to view, upload and download files without the possibility of exposing any unselected data on the main database.



For those jurisdictions around the world where there are legal restrictions in data leaving the jurisdiction, talk with us on our options for addressing this issue. Installation on local servers or in our portable servers are a possibility.

[5] https://cloud.google.com/chrome-enterprise/browser/security/