Data Loss Prevention & Encryption

Introduction

The method selected for the data loss prevention and encryption strategy depends on the approach which has been requested by the client. Below we outline the 3 choices

Web Based

Utilizing the V5 Traceability web-based approach, cloud security is managed by the service provider (e.g., Amazon AWS, Microsoft Azure). Access is managed in terms of opening ports to target IP addresses. The database server only provides access to the application server which runs on the same provider. No external access to the database is possible unless explicitly defined. Only specified IP/Ports will be granted access to the application server.

The database is mirrored, and failovers are in place to the extend per the request of the client. The chosen provider will deploy across multiple different server locations to guard against downtime due to physical failure in one of these server clusters. The frequency of backups can be specified by the client.

Data exchanged over the network is encrypted as to prevent wire hacking of data. Authorization must be achieved for the web-servlet to service requests.

On Premises

For an on-site deployment of the V5 system, the responsibility of backing up data, virus scanning and securing the database and application servers rests with the client's IT security team/networking team. As we do not provide the server or network infrastructure in this case, this is the most prudent method of securing the system.

RDP Approach

For an RDP style approach, all data is transacted on the secure web server and only visual elements are returned to the client-side. In this instance, simply opening an RDP port to the virtual server is required, the database can either exist on the virtual machine or in a separate instance hosted by the same provider with explicit access as described above.