Info on Demand™ Cloud Security Features

Info on Demand™ is a cloud-based application, meaning the data is not stored on a local machine. There are numerous benefits to cloud computing including automated data backups, accessing data anywhere it is needed, and the mitigation of on-site equipment that needs to be constantly monitored for proper function.

The main concern customers have with cloud computing is security and having piece of mind that their data is safe and only accessible to them. To understand the measures that are put into Info on Demand™ to ensure your data is safe, we will breakdown security by the different hardware and software levels:

- Server: Where Info on Demand data is hosted and stored
- Account: Who has access to the data stored, and what data they have access to
- IoT Gateway: How our API controllers security transmit data to the IoD server
- Devices: The devices that are authenticated to access Info on Demand

Server Level Security

Info on Demand is deployed in a private cloud environment hosted through AWS. A private cloud deployment makes sure only you have access to your data and resources. Not only does a private cloud hosting environment increase security due to additional security flexibility, but the server hardware is always reserved for you, so nobody else can slow down your process and use the hardware resources you need.

Account Level Security

There are two account levels in IoD:

1. Admin Account – Admin accounts in IoD have access to the web admin portal for modifying configurations within the IoD platform
2. Employee Account – Employee accounts have access to use IoD by logging in with their accounts that were setup by Admins. Employees do not have access to modify any configurations or settings

Employee's need to have an account setup for them by an Admin. If the admin assigns an email address to the employee, the employee will receive an email to setup the employee account and define their own password.

If the employee is not assigned an email address, a temp password will be randomly assigned to the employee. The admin will need to supply this information to the employee for access.

IoT Gateway Level

IoD Digital Documents features an optional tool controller that allows automatic advancing through documentation without the input of end users.

The IoT Control Box uses platform APIs that are secured through HTTPS, keeping your data safe and preventing any Man-in-the-Middle (MITM) attacks.

Device Level

End devices need to have access to IoD. The devices access IoD through the web using HTTPS so all traffic is encrypted to prevent any data from being sent over the web in plain text.
There is no way to access your internal network by using a connection through IoD. Any device security not related directly to the web application Info on Demand ™ are the responsibility of the end user.