Data Protector

INTELLECTUAL PROPERTY IN FLIGHT

Product designs are maintained simultaneously within the corporate network as well as from external locations. These proprietary design files (*.svg, *.stl, *.dwg, etc.) are saved on workstations, laptops and the server on the network. The file sharing or sending process utilizes a system that provides syncing or uploading / downloading capabilities that allows the design files to be forwarded to the appropriate manufacturer. These files require secure transfer, and the current process uses an open transfer protocol leaving files vulnerable to theft.

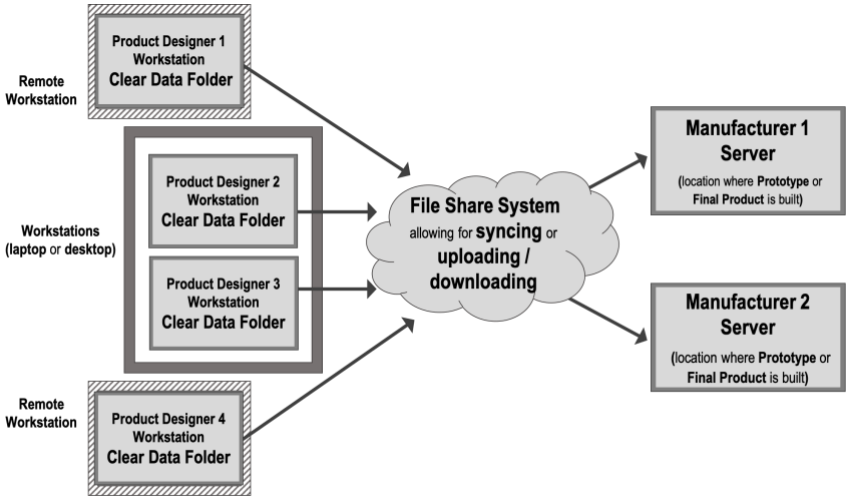

Figure 1. Use case for intellectual property in flight

The Sertainty Data Protector is implemented seamlessly providing an automated protection process that secures files (*.svg, *.stl, *.dwg, etc.) before the files leave the workstations. The protected design files in UXP Object format are transported as expected using the current file sharing or sending process. Upon arrival at the manufacturer, the Data Protector facilitates an automated Auto-Unprotec process. This process provides non-disruptive authentication and extraction of the product designs for the manufacturers to view.

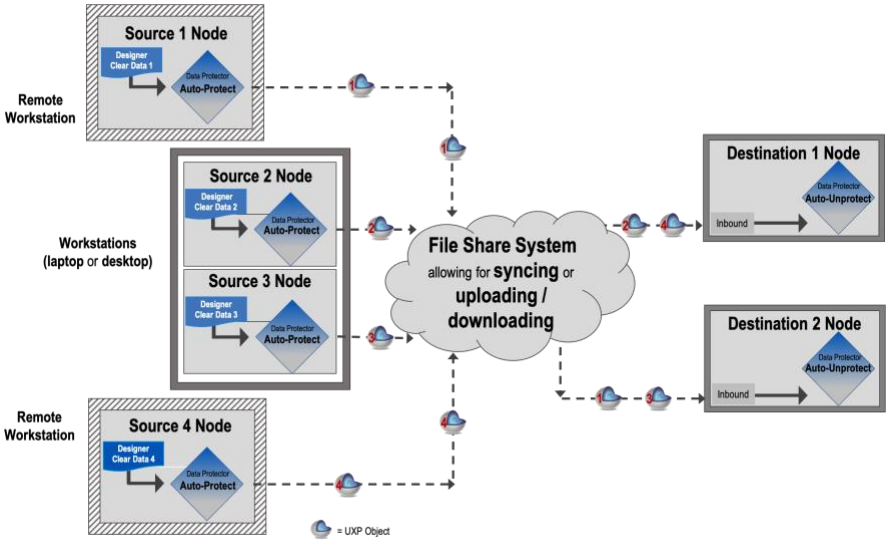

Figure 2. Data Protector workflow for intellectual property in flight

IMPLEMENTATION REQUIREMENTS

- The Source Nodes (workstations) are owned by the Sertainty Customer.
- Each workstation has a designated folder(s) associated with the specific manufacturer corresponding to this Source Node for implementing a specific automated protection process that is managed by the Sertainty Customer. Each folder corresponds to a single Data Protector Auto-Protect Task unique for each recipient.
- Each Destination Node is owned by the respective manufacturer.
- The Sertainty Customer creates and manages corresponding folders for each manufacturer to receive the protected file(s) at each Destination Node.
- The Sertainty Customer creates and manages a transport / transfer process.

DATA PROTECTOR SOLUTION

- The Data Protector is implemented on each Source Node and on each of the Destination Nodes.
- At each Destination Node, a UXP Identity is generated unique to the machine that will be accessing the product design files. The design files for each Destination will be protected on the Destination's behalf using its unique Identity. The protected product design files in UXP Object format can only be authenticated by that machine at the Destination Node.
- On the workstation Source Node, completed prototype / design files are placed in the corresponding manufacturer's folder (who is to receive them).
    - This is a configuration during the installation process.
    - The manufacturer location may be within the organization or an external.
- The Data Protector facilitates the Auto-Protect process for the files in each folder using the UXP Identity of the intended Destination Node (manufacturer).
    - Each Destination Node has a unique Identity.
- The protected protoype / design files in UXP Object format are placed in a folder for syncing or for a transport process using the expected file sharing system (cloud services).
- Within the file sharing system, designated locations / folders for each manufacturer exist for receiving the UXP Objects.
- At the Destination Node, the manufacturer (via syncing or downloading) moves the UXP Objects to the specific Data Protector folder to initiate authentication.
- The Data Protector facilitates the Auto-Unprotect process that includes non-disruptive authentication using that Destination Node's UXP Identity embedded in each respective UXP Object.
    - UXP Object can only be opened using the intended Destination Node's UXP Identity.
- The prototypes / designs are extracted and placed in a folder to continue the typical access protocols for that manufacturer.

Email us today:
tech-support@sertainty.com