Data Protector

GEOSPATIAL IMAGE DATA DURING TRANSPORT AND ARCHIVING

Large raw geospatial and LIDAR image data is processed for clients and transferred to cloud technology services (e.g. ESRI, AutoDesk / AutoCAD, etc.) or directly to the client. The current process uses an open FTP protocol leaving files vulnerable to theft.

Additionally, the original raw data along with its processed version is being archived with required restoration capabilities for future review or update. The current process prevents using external storage solutions (cloud-based, etc.) due to inherent security issues.

Note: For ease in the provided flow diagrams, the archived data is generically grouped and titled as one.

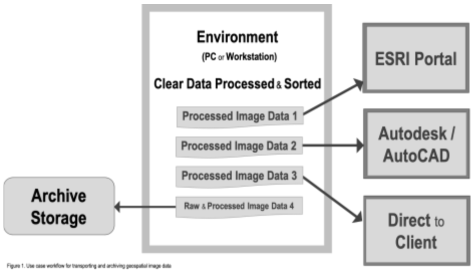

Figure 1. Use case workflow for transporting and archiving geospatial image data

This scenario represents two independent solutions using the Data Protector to address the transport and archiving security issues.

Transport

The Data Protector is implemented seamlessly at the data's source providing an automated protection process that secures the processed geospatial images at their origin (GIS or CAD processing applications). The images are auto-protected resulting in UXP Objects prior to FTP transport to a cloud service or directly to a client. Also at each Destination, the Data Protector is implemented. At the Destination, the Data Protector facilitates an automated Auto-Unprotect process. This process is a non-disruptive authentication and image extraction process when the UXP Object arrives at its respective location.

Archiving

Similar to the transport solution, the Data Protector auto-protects both raw geospatial and LIDAR images and their respective processed versions. The resulting UXP Objects are transported via FTP to the archive location. When the protected data is needed or has reached its end-of-useful life, the Data Protector facilitates the Auto-Unprotect process. This process authenticates and extracts the data (if necessary); one of four events below at a designated location occurs:

- Clear data is placed into a folder for further use.
- Clear data is shredded.
- UXP Object given an "open ended" status and remains protected in the archive until the client decides it is unneeded.
- Clear data is directed to initiate as the starting point for a new raw data collection for an ongoing project.

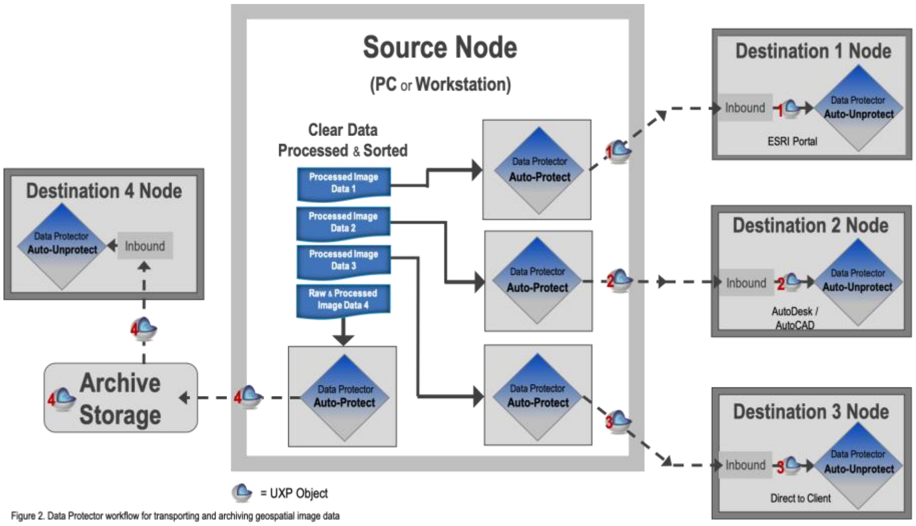
Source Node
(PC or Workstation)
Clear Data Processed & Sorted
Processed Image Data 1
Processed Image Data 2
Processed Image Data 3
Raw & Processed Image Data 4
Data Protector Auto-Protect
Data Protector Auto-Protect
Data Protector Auto-Protect
Data Protector Auto-Protect
Destination 1 Node
Inbound
1
Data Protector Auto-Unprotect
ESRI Portal
Destination 2 Node
Inbound
2
Data Protector Auto-Unprotect
AutoDesk / AutoCAD
Destination 3 Node
Inbound
3
Data Protector Auto-Unprotect
Direct to Client
Destination 4 Node
Data Protector Auto-Unprotect
Inbound
4
Archive Storage
= UXP Object

Figure 2. Data Protector workflow for transporting and archiving geospatial image data

Transport

IMPLEMENTATION REQUIREMENTS

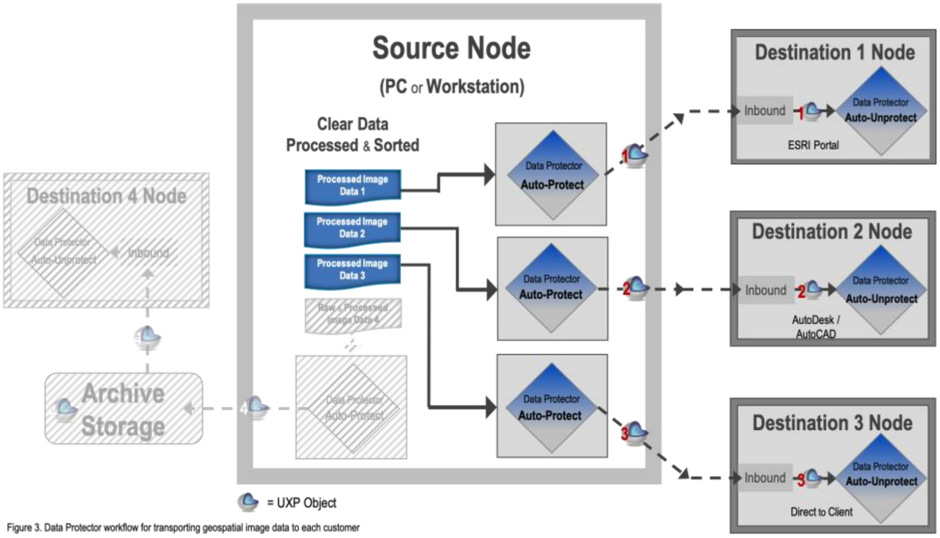

Figure 3. Data Protector workflow for transporting geospatial image data to each customer

- The Source Node (workstation) is owned by the Sertainty Customer.
- On the Source Node, each customer has a designated folder for their processed images. These are managed by the Sertainty Customer. Each folder corresponds to a single Data Protector Auto-Protect Task unique for each recipient.
- The Sertainty Customer creates and manages a transport / transfer process.
- The Sertainty Customer manages the corresponding inbound folders for each customer to receive their protected file(s) in UXP Object format. UXP Objects are received on a cloud service or a direct client Destination Node. Each inbound folder corresponds to a single Data Protector Auto-Unprotect Task on that Destination Node.
- The Sertainty Customer creates and manages the software-specific dashboard on the cloud service or direct client Destination Node that facilitates file viewing when needed.

DATA PROTECTOR SOLUTION

- The Data Protector is implemented on the 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 protected images. The images for each Destination will be protected on the Destintation's behalf using that machine's unique Identity. The protected images can only be authenticated by that machine at the Destination Node.
- On the workstation Source Node, processed geospatial or LIDAR images are placed in their respective folders that correspond to their intended destinations..
- The Data Protector executes the Auto-Protect process for image files in each folder using the UXP ID of the intended Destination and places the protected file in the Sertainty Customer defined and managed location for transport. Transport of the protected image files occurs as expected to their intended Destination Nodes.
- At arrival to the Destination Node, the protected file is placed in its corresponding inbound folder.
- The Data Protector executes the Auto-Unprotect process that includes authentication using the UXP ID associated with the Destination Node embedded in each respective protected file (UXP Object).
- The processed images are extracted and put into a folder where the prescribed access protocol allows the customers to view their specific images.

Archive

IMPLEMENTATION REQUIREMENTS

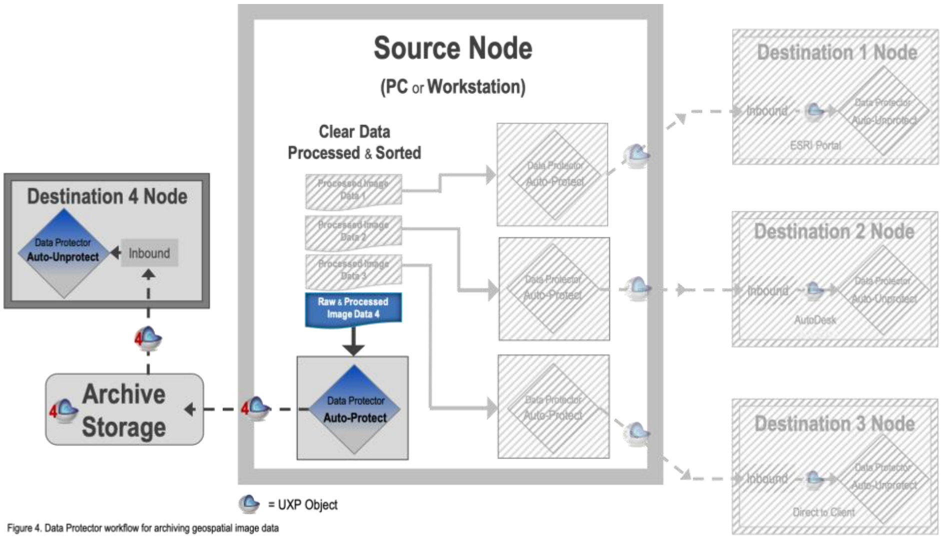

Figure 4. Data Protector workflow for archiving geospatial image data

Note: For ease in the provided flow diagram, the archived data is generically grouped and titled as one.

- The Source Node (workstation) is owned by the Sertainty Customer
- On the Source Node, each client recipient is assigned a folder for protected processed images in UXP Object format to be archived. These are managed by the Sertainty Customer. Each folder corresponds to a single Data Protector Auto-Protect Task unique for the archive workflow

  Note: These individual folders could be grouped into one folder for a more simple configuration using the Auto-Protect process
- The Sertainty Customer creates and manages a transport / transfer process to the archive
- The Sertainty Customer creates and manages an archive storage location either locally on the workstation or on a cloud service
- The Sertainty Customer creates and manages a Destination Node locally or on a cloud service for accessing archived files

DATA PROTECTOR SOLUTION

- The Data Protector is implemented on the Source Node and on a separate Destination Node associated only to the archive.
- At the Destination Node, a UXP Identity is generated unique to the machine for the archive that will be accessing the UXP Objects protecting the images. The images for archive will be protected using the separate Destination Node's unique Identity. The protected images in UXP Object format can only be authenticated by that machine at that Destination Node.
- On the workstation Source Node, processed images are placed in respective client folders for archive*.

  ***Note:** Depending on the workflow for the archiving process, this could be a single folder with sub-folders for each client. In this scenario, the single folder would be protected instead of the single client folders.
- The Data Protector executes the Auto-Protect process using the Identity specific to the Destination Node associated with the archive.
- The protected raw geospatial and LIDAR images in UXP Object format are moved to the archive storage location either local or cloud – not the Destination Node.
- When the archived UXP Object is ready for use again, the Object is moved to the Destination Node's inbound folder.
- The Data Protector executes the Auto-Unprotect process that includes authentication using the Identity associated with the Destination Node embedded in the UXP Object.

Email us today:
tech-support@sertainty.com