Sertainty Transforms Geospatial Information Files for An Aerial Data Acquisition and Analysis Company Into Self-Protecting Assets

In the Unmanned Aerial System (UAS) mapping world, it is critical for geospatial analytics companies to securely acquire and retain sensitive information, keeping the integrity of the data accurate and intact.

"We know that for our clients, data security isn't just a want — it's a requirement. The ability to provide a high level of security assurance is something that separates us from our competition in the industry. We can provide this to our clients for the entire lifetime of their project."

USE CASE HIGHLIGHTS

- Protect the data even beyond the Company's network
- Ensure the data is not at risk, retaining its privacy and integrity
- Enable the company to review how and where the data is used throughout its lifecycle

INTRODUCTION

A geospatial aerial data consultation business ("the Company") utilizes UAS aircraft to provide spatial analytics data services for their customers. They are challenged with protecting this information from the time it is collected, through sharing with their customers, to archive. Headquartered in Chattanooga, TN, they serve a wide range of customers from the energy, utility, infrastructure, and environmental sectors. Whether during presentation of the data to the customer or maintaining the data in a secure archive for legal validation, their clients expect absolute security. And yet the Company requires the ability to audit the data at every step of the process.

The Company has three distinct phases for every project — acquire, analyze, and inform. The first step taken is to obtain the data through aerially-collected survey and mapping technology. From there, the data is analyzed for accuracy and presentability. The finalized dataset is then provided to the client for use. These file sets can be quite large, ranging from a couple Mb to multiple Gb of data, and are touched and inspected at multiple points throughout the process, causing security to be a burdensome task. The method of data presentation to the customer can occur over insecure channels, such as posting the final data to a cloud drive via an insecure transfer protocol. Prior to utilizing Sertainty, the Company had to balance secure files or efficiency.

This use case summarizes two scenarios in which the Company uses Sertainty to empower their information to assure the safety, integrity and confidentiality of their customers' sensitive information without compromising performance.

USE CASE #1: **PRESERVING DATA INTEGRITY**

The Company collects and processes large raw geospatial image data and archives both the original raw data, as well as its processed version. If the original survey data is needed for validation, it is critical for the Company to have taken steps to assure the safety and integrity of this data. Current processes presented security risks that the Company felt did not guarantee the data was free from the risk of compromise or inadvertent modification.

Sertainty embeds intelligence into the Company - created data-files, giving the data the ability to control its fate while mitigating risks. These files are no longer dependent on the Company's security infrastructure for its protection. The data-file retains its own policies for authentication, governance, and provenance, and enforces them on itself. If an illegitimate user attempts access, the data-file reacts by performing actions up to and including refusal to open, alerting the owner, or even self-destruction. The data-file is aware of every activity attempted on the file and creates a record of these events. This enables the Company to review where and when the data is accessed throughout its lifecycle. These capabilities ensure the data is never at risk, retaining its privacy, authenticity and reliability.

Use Case #2: **CLOUD DATA SECURITY**

Once the survey data is processed, the Company needs to transport the files to the cloud while retaining data security for customer delivery. Prior to Sertainty, the Company used standard file transfer protocols which were often insecure, leaving the files vulnerable to theft during transit, or post-transfer.

Now that the data possesses intelligence, it remains protected no matter where it travels or resides. The embedded intelligence module manages multiple, dynamically-created, AES-256 encryption keys. These keys are never exposed outside of the data. Because the keys are managed internally by the intelligence module, the burden of key management is eliminated. Self-protecting files are safely and securely shared beyond the Company's network. This transformed the Company's approach to security and gave them the ability to assure their customers' sensitive information from compromise. Through the use of Sertainty Technology, the Company is the only provider of aerial mapping data that currently offers this comprehensive approach to data privacy and intends to elevate its status to an ARGUS Platinum Rating.

WHAT IS PROVABLE DATA PRIVACY

A new paradigm in data privacy: Sertainty makes data privacy certain, provable and manageable, so customers and businesses can feel confident data is accessed, stored and monetized responsibly. Sertainty Data Privacy Platform solves the problem of data privacy at the data level, empowering data to protect, govern and track itself. Sertainty. Data privacy made certain.

WHY IT WORKS

- Embedded intelligence in the data enables the data-file to act and react
- Data remains protected wherever it resides
- Encryption keys are kept internal to the file and never exposed, eliminating external key management
- The data mitigates risk in real time by enforcing policies set by the data owner

Why **SERTAINTY**

Sertainty solves the challenge of data privacy by enabling data to defend, govern and track itself, putting data in charge of its destiny. We make data self-protecting, so it can mitigate risks posed to it. We make data end-to-end self-governing, so rules can be set within the data itself. We make data self-tracking, so data provenance and every action is recorded. And we make data self-authenticating to enable Zero Trust and ensure only the right users access your data.

With Sertainty, you can create a competitive differentiator with customers and regulators who want more than promises about data privacy. You can establish and retain customer trust with data privacy you can prove. It's data privacy you can promise and data privacy you can prove.

sertainty

sertainty.com
sales@sertainty.com