sertainty

TRANSFORM DATA INTO A SELF-AWARE DIGITAL ASSET, PROTECTING ITSELF NO MATTER WHERE IT GOES

As technology evolves, a company's digital security ecosystem will continue to grow in complexity and sheer volume of data. This adds additional management challenges to a complex security environment and an already overworked team and increases the vulnerability of the company's most important asset – their data. However, the problem is that data is a passive, defenseless participant in systems that are inherently vulnerable. Your systems were not designed to control data, but to protect it.

Ultimately, the safety and integrity of our data is wholly dependent on trusting the insider, and ITs ability to "control" users and infrastructure. Data loss and theft of valuable information is just a symptom of the problem. The problem is data is neither self-protecting nor self-aware. You need a solution that transforms your data into a self-reliant, self-aware, self-protecting asset.

HAVE SECURITY **WITH SERTAINTY**

By embedding a Sertainty Intelligence Module into the data-file, the data now has an ability to act and react to events happening to it. Ultimately, the safety and integrity of data will be less dependent on the trusted insider and systems hardware. This reduces the dependency on resources (human and cash capital) to operate and enables the data-owner to share valuable information without increasing risk.

Sertainty data-files self-manage access to relevant information according to the security and governance needs of the organization. Sertainty technology prevents external attacks on the company data and stops internal missteps from exposing data. With Sertainty, you can strengthen your infrastructure and reduce the friction of enforcing security procedures by embedding actionable intelligence within the data-files themselves.

ACTIONABLE INTELLIGENCE

Sertainty Technology introduces a new paradigm in data protection. By embedding actionable intelligence into the data, Sertainty files are created with an ability to execute their own security protocols – enabling them to now recognize and react to their environment. This "intelligence" is not sitting on a network server thousands of miles away – it's in the data-file. We call this self-protecting data.

- The embedded Intelligence Module enables the data-file to act and react to its environment
- Any file type of any size, sitting outside of the database can be protected
- Whether in transport or at rest, files protected by Sertainty Technology, are safe regardless of the infrastructure or network security settings
- Persistent protection travels with the data

POLICY ENFORCEMENT AT THE DATA LAYER

Sertainty further guarantees – and streamlines – the enforcement of policies, mitigating risk in real-time. With Sertainty, the data decides its access rights. If an authorized user attempts an illegitimate act, the data can react and if desired, take actions up to and including self-destruction.

- Policies are based upon device, location, time, identity, etc.
- The data owner retains control of the data, even after it leaves the network
- A Sertainty file monitors, detects anomalies and initiates mitigating action in real-time
- System is designed to defeat a malicious super user

ANOMALY DETECTION AND ACTIVE DEFENSE

When a Sertainty file detects an anomaly, say an unsuccessful access attempt from an unrecognized location, network or device, the Sertainty file can take any number of mitigating actions. The data owner sets the following at the time of creation, and the Intelligence Module enforces them throughout the life of the Sertainty file.

- The file can simply deny access and/or suspend the session
- The file can alert the owner
- The file can enforce other authentication routines and/or approvals
- The file can shred itself

BURDEN OF KEY MANAGEMENT ELIMINATED

Security protocols are embedded in the file, including the encryption keys. The embedded Intelligence Module manages its own symmetric encryption keys. The encryption keys are created using a NIST approved algorithm and are never exposed or shared. No person or external process has access to, nor has need to access any keys.

- Sertainty files are not based on a shared-key or PKI encryption model
- The burden and related attack surfaces associated with externally or centrally created/managed keys is eliminated

SELECTIVE DECRYPTION

Sertainty Technology is NOT about "access control" to files, i.e., not an IAM or DRM solution. It is about access control to information IN the files. The embedded Intelligence Module authenticates users (human and machine) and decrypts only the portions of a file that are associated with that user according to the governance rules of your organization, without exposing any other information in that file.

- Files containing PII, IP or other regulatory information can only be accessed by legitimate users
- Sertainty files provide practical sharing of valuable information while reducing risk
- You can now ensure the integrity of data from its creation to the end of its useful life

IRREFUTABLE AUDIT TRAIL

A Sertainty file maintains an irrefutable log of ownership, access attempts by whom, and other events. This invaluable and trustworthy resource is essential for data monetization. This equips data owners with a real time, independent monitoring, collecting and reporting of all activity involving their data.

- The data records access attempts, including who, what, when and where
- The data reports and/or alerts all activity to the data owner, providing complete visibility of all file activity
- The event logs are retained within the data-file and/or distributed as a Sertainty file