SERTAINTY PROTECTED DATA CARRIES ITS OWN SECURITY AND DOES NOT DEPEND ON THE INFRASTRUCTURE OR COMMUNICATION NETWORK SECURITY.

Through policies one can control the behavior of the protected data. For example, the protected data can Call Home, Lock Down and/or Self Destruct:

- **If an attempt is made to compromise it,**
- **If it is accessed outside the permitted environment or time-period**
- **If it is accessed by an unauthorized party or unauthorized device**

WHAT IT MEANS TO HAVE SECURITY WITH SERTAINTY™

Security with Sertainty combines data with a nano-intelligence module, access control logic, trusted access identities and AES 256 encryption and additional proprietary components that form self-protecting files or messages. Security with Sertainty files and messages are unique, passive in appearance, and actively empowered to defend themselves. They are capable of deception, misdirection, and other active protection measures.

As the complexity of sensitive information grows within organizations, so does their vulnerability.

The security net put into place grows weaker as it's stretched further, while patchwork repairs from overworked IT teams open holes that ever-watchful hackers sit waiting to exploit.

MOST DATA IS VULNERABLE DATA

Think your data is secure when it's protected by security measures that surround it from the outside? There are a few hard realities to consider:

- Encryption does not equal security.
- Threat Intelligence, Firewalls, Intrusion Detection and Cyber Analytics do not prevent intrusions.
- Network security and encrypted communications do not prevent data loss.
- Trusted security does not prevent identity theft.
- Passwords offer little security, are often simple to guess and easily stolen.

Static data will inevitably find its way outside of your security perimeter, or someone will find their way in to retrieve it. But living data has the intelligence to defend itself from unauthorized access no matter where it finds itself or the nature of the threat it's facing.

HOW IT WORKS

STEP 1 Unique Identities for people, devices, applications, or roles are created with Sertainty technology; built from multi-factor components, device metadata or sensor data, such as biometrics or location.

STEP 2 Whether using the Sertainty Data Protector Utility or the Software Development Kit for a customized solution along with the Identity, self-protecting data packages are created through an API-enabled method.

STEP 3 Store and transport data with assured security without network security dependencies or SSL/TLS. All data is immutably secured, no matter if it is sitting at one location or on the move.

CONTACT US TODAY TO LEARN MORE. 615.846.5500 • SALES@SERTAINTY.COM

sertainty

SERTAINTY MAKES DATA COME ALIVE

Living data is data transformed by Sertainty into a self-aware, self-reliant and self-protecting digital asset that protects itself at all times and in all places.

Sertainty Protected Data (SPD) self-manages access according to your pre-defined security and governance parameters. By embedding actionable intelligence directly within the data file, it's protected from both external attacks and internal security lapses. The result is a nearly zero-trust model where security is literally one with the informational assets it is designed to protect.
By embedding protection in the data, not just the device or the network, you can mitigate the consequences of human error, software failures and security misconfigurations. Your most sensitive data can be better protected using Sertainty at a fraction of the cost of legacy security measures.

WHAT IT MEANS TO BE LIVING DATA

When data is "alive," it has the ability for self-preservation, just like any living organism. With Sertainty Technology, it can actively defend itself without dependency or assistance from network services or encrypted communications channels. Otherwise the data appears as an inert entity. When data is out in the wild, data is never exposed regardless of where it is in the world.

ULTIMATELY THE DATA IS **PERPETUALLY AND ACTIVELY SELF-DEFENDING** WHILE PROVIDING **SEAMLESS ACCESS TO AUTHORIZED CONSUMERS.**

JUST THE RIGHT AMOUNT OF ACCESS

While the security method we use is not homomorphic, we say it is homomorphic-like. For example, applications with Sertainty-embedded security can be designed to decrypt only the data the application needs while the rest of the data remains encrypted.

PUTTING IT ALL TOGETHER

The protection algorithms including encryption, the digital identities of devices and users, UXP Metadata along with the data, are blended. Simultaneously being mixed into the data is the nano-intelligence module and access control logic as part of the protocol.
The elegance and simplicity of this patented data protection method is self-evident. The data and all the necessary security apparatuses are locked in a secure multi-dimensional data object. Brute force attacks simply cannot reverse this process.
And yet the entire data package is seamlessly accessible, typically in milliseconds, for authorized processes. And the data has no reliance on external security mechanisms. Sertainty changes the paradigm for data security to one where every piece of information becomes inherently secure.

Let Sertainty demonstrate just how powerful this approach can be. Security with Sertainty™ delivers the peace of mind, knowing your data is secure at any moment, anywhere in the world.

BRING YOUR OWN DATA TO LIFE

sertainty

615.846.5500 • SALES@SERTAINTY.COM