sertainty™

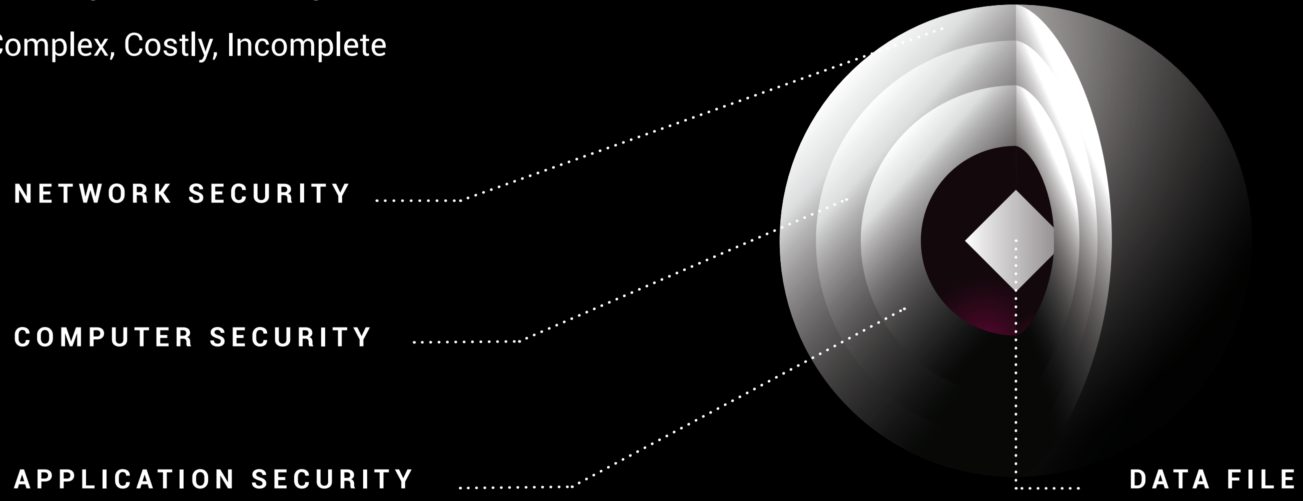
data: empowered

Unstructured data is a passive, defenseless participant in systems that are inherently vulnerable ...*until now.*

Sertainty technology enables developers to mix intelligence into data files, giving data an ability to act and react to its environment. Sertainty shifts data control and risk mitigation from an indirect/re-active paradigm to a direct/active paradigm by driving governance, provenance and protection **INTO YOUR DATA** and technology solutions.

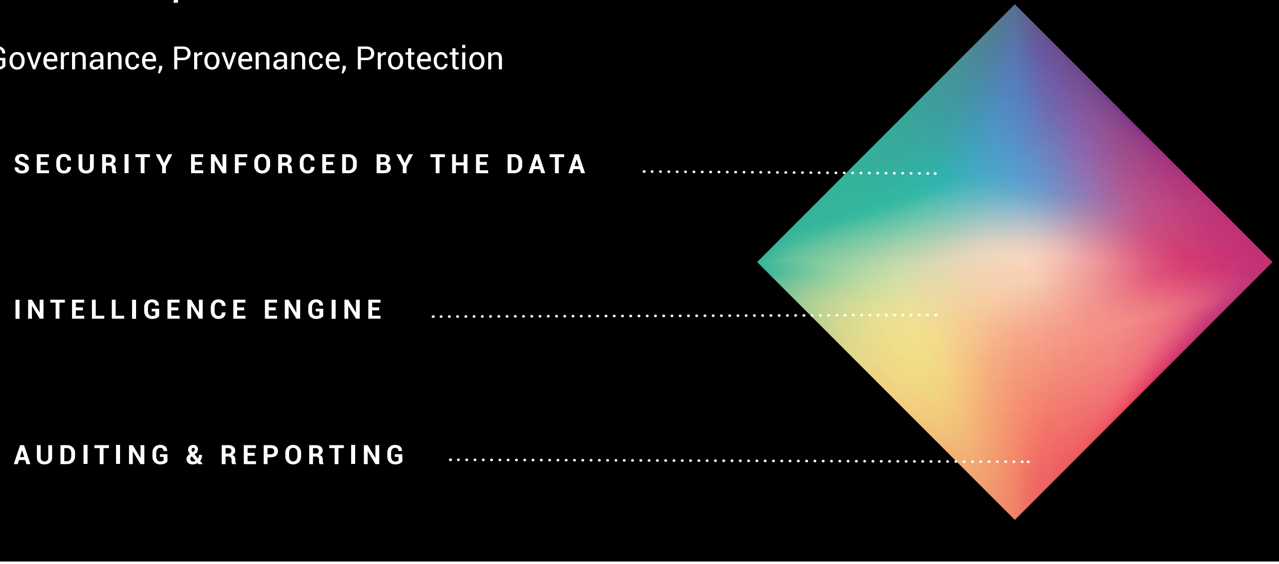
Today's Security Fabric

Complex, Costly, Incomplete



Data: *empowered*

Governance, Provenance, Protection



Data: *empowered*

The Sertainty technology imbues data with self-governance, provenance and protection capabilities. In its activated state, we refer to this data as “Data: *empowered*.” For the first time, data can actively participate, as if an endpoint itself. With Sertainty, the data-owner-user relationship is monitored and governed by Data: *empowered* and assured for the life of that relationship, whether at rest, in transit or under process. The owner's intentions are manifested within and enforced by the data.

No longer is there a perimeter or extraneous control of data exerted by an application like a firewall or other system; the data controls, protects and governs itself.

GOVERNANCE

Data: *empowered* solutions ensure the data is in control even when it is threatened. The **EMBEDDED INTELLIGENCE ENGINE ENFORCES POLICIES** without deviation. For example, unauthorized access, including super-users, is prohibited. When an entity attempts access to important information the data first determines its environment (physical device, location, time, etc.). If an anomaly is detected the self-governing data takes action.

Some actions to mitigate risk include providing access only to a subset of the information, denying access, alerting the owner, requesting access permission from an external authority, presenting an alternate view to the user or process, and self-destructing.

PROVENANCE

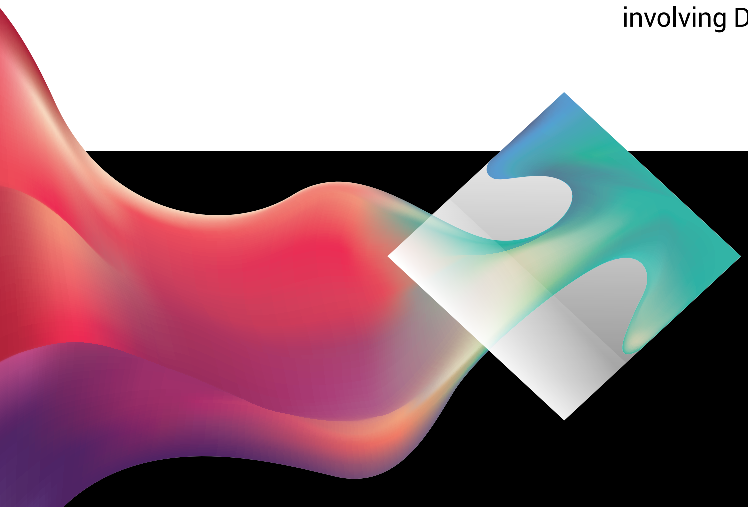
Provenance (a record of ownership) is enforced by Data: *empowered*. However, this record of ownership is of more value than just who owns the data. Not only is the owner established as a legitimate entity that the user can trust, Data: *empowered* employs anti-tampering technology that assures the integrity of the data.

The record of ownership can also include environment(s), access attempts and event occurrences. These **EVENT LOGS ARE IRREFUTABLE** and are likewise protected with Sertainty technology. This invaluable and trustworthy resource is essential for data monetization. Business owners and legal entities are now equipped with independent monitoring, collecting, and reporting of all activity involving Data: *empowered*.

PROTECTION

Sertainty technology provides security and controls within the data file, **REDUCING THE DEPENDENCY ON INFRASTRUCTURE** (hardware, firewalls, endpoints, etc.) for protection and governance. With these security controls mixed-in, your data now has the ability to reside in multiple trusted and untrusted environments at the same time. It maintains protection and control mitigating additional risk.

Data: *empowered* is self-managing. Encryption keys are never exposed. Instead, your data manages the keys internally, removing the vulnerability of shared/stolen keys. As a result, key management overhead is eliminated.



Get in touch to find out how you can empower your data with Sertainty.

☎ 615-846-5500

✉ sales@sertainty.com