Trusted Energy
Interoperability Alliance

Is your Zero-Trust model truly protecting data?

Make data self-verifying at the source layer.

The challenge

Traditional Zero Trust validates network paths but not data itself, leaving organizations vulnerable to insider threats and impersonation attacks.

The solution

Explicit data trust binds identity directly to data with cryptographic proof, creating self-verifying information independent of network position.

4 key steps to explicit data trust

1. Bind identity to data

Embed cryptographic proof of origin into datasets, making them self-verifying regardless of location or movement.

2. Separate trust from networks

Validate trust at data layer, not network position, to prevent internal impersonation and lateral attacks.

3. Require continuous attestation

Verify system, code, and device integrity in real time to detect compromises before damage occurs.

4. Authenticate every interaction

Demand mutual cryptographic verification for all API calls, data exchanges, and automated build processes.

Discover how TEIA standards strengthen data trust across connected energy systems.

Learn more ›