Trusted Energy Interoperability Alliance

eBook

From zero trust to explicit trust

Why energy infrastructure needs cryptographic data-level security

Executive summary

Traditional zero-trust approaches create compounding costs that extend far beyond network segmentation budgets. The global zero-trust security market reached an estimated $42.28 billion in 2025 and is projected to grow at a compound annual rate of about 14.8 percent.[1]

Without data-level trust verification, organizations face a compounding dilemma. Each new smart sensor, each vendor cloud connection, and each cross-border energy transaction introduces trust relationships that network segmentation cannot govern.

By adopting explicit trust through cryptographic data verification, organizations can maintain essential connectivity while achieving genuine security assurance. The IoT-in-energy market is projected to grow at a double-digit compound annual rate, with total value expected to exceed $50 billion around 2030.[2]

The Trusted Energy Interoperability Alliance (TEIA) provides the standard for securing this growth, turning trust from a network property into a data property.

The global zero-trust security market reached an estimated $42.28 billion in 2025.[1]

Smart devices bypass network controls

Today's energy infrastructure is populated by intelligent sensors and actuators that communicate directly with vendor cloud platforms via cellular networks. A smart meter sending data to its manufacturer for predictive maintenance, or a solar inverter transmitting performance telemetry for firmware optimization, creates trust relationships entirely outside the network perimeter.

These devices feature added computing and storage capabilities, autonomous self-diagnostics, and direct cloud communication channels that deliver tremendous operational value.

Organizations cannot afford to sever these connections, yet they represent exactly the kind of implicit trust that zero-trust principles seek to eliminate.

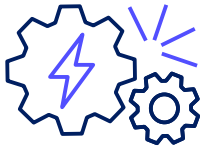
The energy sector as the fourth most targeted industry globally.[3]

Network trust cannot cross boundaries

Cost categories

Security blind spots

Smart devices communicating via cellular or satellite networks bypass segmentation entirely.



Integration friction

Multi-vendor, multi-protocol energy environments require continuous custom integration to maintain trust across system boundaries.

Compliance exposure

Regulators increasingly demand verifiable audit trails for energy transactions and grid services.

As energy systems become more distributed, transactions and data flows increasingly span multiple protocols, organizations, and jurisdictions. A virtual power plant aggregating demand response across building controllers, or a cross-border energy trade requiring proof of origin, involves trust chains that no single network can govern.

Network-based zero trust was designed for environments with a definable perimeter. Distributed energy has no such perimeter.

TEIA's founders recognized that the trust model itself, not the network architecture around it, needed to change. The paradox disappears entirely with explicit trust. What remains are only questions of implementation quality.

The actual cost of relying solely on network-based security extends far beyond firewall and segmentation budgets. Organizations face three interconnected cost categories that compound as distributed energy systems grow more complex.

The compounding cost of blind spots

When a charging point operator deploys OCPP-connected chargers across multiple sites, each unit may also communicate with its manufacturer for diagnostics and firmware updates. Network segmentation secures the OCPP channel but has no visibility into the vendor connection.

Multiply this pattern across hundreds of devices and multiple vendors, and the proportion of data flows operating outside security governance grows with every deployment. Organizations invest more in network controls while the trust gap widens.

Global spending on cybersecurity is projected to approach a quarter of a trillion dollars in 2026.[4] Much of that investment reinforces perimeter models that govern a shrinking share of actual energy data traffic.

Energy service providers working across virtual power plant aggregation, demand response, and grid balancing must maintain trust across multiple protocols and organizational boundaries. Each integration point requires custom security mapping that must be rebuilt whenever a protocol changes or a new partner joins.

Global spending on cybersecurity is projected to approach a quarter of a trillion dollars in 2026.[4]

Explicit trust for energy systems

TEIA's explicit trust model delivers six strategic advantages by moving trust verification from the network layer to the data layer. Rather than adding security tooling, TEIA changes where trust lives, embedding cryptographic verification directly into every interaction.

Reduced security blind spots

Every message and endpoint is cryptographically verified regardless of communication path. Smart devices communicating via cellular, satellite, or any network carry their trust credentials with the data itself.

Protocol-agnostic security

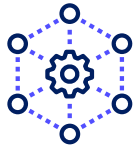
TEIA works across OCPP, OpenADR, IEEE 2030.5, and other standards without custom security mapping for each protocol. Trust attestation survives protocol translation and network boundary crossings.

Verifiable audit trails

Cryptographic proof of every energy transaction, dispatch decision, and grid service interaction provides the immutable records that regulators increasingly demand.

Seamless multi-party trust

TEIA excels in multi-party scenarios, enabling trust chains that extend from grid operator to individual device without custom integration at each boundary.



Non-disruptive deployment

TEIA's integration libraries enhance current systems without full replacement. Organizations protect existing investments in protocols and infrastructure while gaining data-level trust assurance.

AI-ready verification

As AI-enabled optimization grows across energy systems, TEIA provides verifiable decision audit trails. Every action can be cryptographically traced.

Where energy is going and beyond

Each new smart device, each new vendor integration, and each new cross-border connection adds trust relationships that network-based controls cannot govern.

As the number of connected energy devices grows by double digits annually, the gap between network-based trust and actual operational trust widens. Incremental improvements to perimeter security cannot close a structural gap.

Adopting explicit trust is a reallocation of resources, shifting investment from complex network segmentation toward cryptographic verification that travels with the data.

The result is security that scales with connectivity rather than against it, and integration costs that decrease as the trust model standardizes rather than compounds with each new connection.

The U.S. Cyber Incident Reporting for Critical Infrastructure Act takes full effect in May 2026, and energy-specific cybersecurity legislation continues to advance globally. Organizations that build explicit trust into their architecture now position themselves to lead the next phase of energy digitalization.

As the number of connected energy devices grows by double digits annually, the gap between network-based trust and actual operational trust widens.

Taking the next step

Organizations looking to adopt explicit trust for their energy infrastructure have access to comprehensive resources through TEIA. The alliance provides open specifications, technical documentation, implementation guides, and integration libraries designed to enhance existing systems without disruption.

Working groups bring together charging point operators, energy service providers, grid operators, and technology vendors to develop and refine the standard collaboratively. Reference architectures demonstrate how explicit trust integrates with OCPP, OpenADR, IEEE 2030.5, and other established protocols. Partner organizations offer implementation support and training to accelerate adoption and reduce deployment risk.

The future of energy depends on systems that can maintain trust across increasingly complex, distributed networks. Explicit trust provides that foundation: verified data, verified identity, any network. The question is not whether this transformation will occur, but whether your organization will lead it.

Sources

1. Fortune Business Insights, “Zero Trust Security Market Size, Share & Forecast 2025–2034,” accessed April 2026. Global market valued at $42.28 billion in 2025, projected CAGR of 14.76%.
2. The Business Research Company, “Internet of Things (IoT) in Energy – Global Market Report,” 2026. Market growing at a double-digit CAGR, projected to exceed $50 billion by 2030.
3. IBM Security, “X-Force Threat Intelligence Index 2025,” as summarized in CyberScoop, “Attackers stick with effective intrusion points, valid credentials and phishing,” April 2025. Energy sector ranked as the fourth most targeted industry, accounting for around 10% of attacks.
4. Elisity, “Cybersecurity Budget 2026: Benchmarks & Spending Trends,” November 2025. Summarizes Gartner and Cybersecurity Dive projections of approximately $240–262 billion in global cybersecurity and security and risk management spending in 2026.

Trusted Energy Interoperability Alliance

Join the TEIA community to access specifications and implementation resources.

Learn more at: trusted-energy.org
Contact us at: contact@trusted-energy.org
+1 408 616 1600