Trusted Energy Interoperability Alliance

eBook

The true cost of vendor lock-in

Proprietary security systems limit device manufacturers' growth.

Executive summary

Device manufacturers face a critical strategic choice: continue investing heavily in proprietary security systems that limit market reach, or embrace open standards that expand opportunities.

Current proprietary security approaches create hidden costs that compound over time. According to industry research, device OEMs allocate significant engineering resources to cybersecurity—a capability outside their core competencies.[1] These proprietary systems then create customer friction when utilities and energy companies deploy multi-vendor ecosystems.

The result is a lose-lose situation: manufacturers spend more to build features that actually reduce their market appeal. Meanwhile, open standard alternatives like TEIA offer a path forward that reduces costs while expanding market opportunities.

By adopting TEIA's open, interoperable, security standards, device manufacturers can reduce development costs, eliminate customer friction, and position their products for the rapidly growing distributed energy ecosystem—projected to reach $111.41 billion by 2034.[2]

"In today's energy landscape, device OEMs spend significant resources on cybersecurity measures that are outside their core competencies."[3]

The vendor lock-in trap

Traditional device manufacturers operate under the assumption that proprietary systems create competitive advantages. In reality, they create strategic vulnerabilities that limit growth and increase costs.

Security approach problem

When utilities and energy companies evaluate devices, vendor lock-in is a primary concern. Proprietary security implementations signal future dependency, making procurement teams hesitant. The result: manufacturers lose deals not because their hardware is inferior, but because their security approach raises red flags.

"Procurement decisions increasingly hinge not just on device capabilities, but on whether those devices will integrate seamlessly into multi-vendor ecosystems.

Issues with ecosystem exclusion

The future of energy is multi-vendor coordination. Virtual power plants, demand response programs, and grid services all require devices from different manufacturers to work together seamlessly. Proprietary security architectures exclude manufacturers from these high-value opportunities.

Service providers buying devices with proprietary approaches must choose: build costly custom integrations for each ecosystem partner, or miss market opportunities entirely. Neither option delivers competitive advantage.

"Proprietary systems can result in vendor lock-in, making it more difficult to 'mix and match' components when optimizing and upgrading systems."[4]

True costs to device manufacturers

The real cost of proprietary systems extends far beyond initial development. These hidden expenses compound year after year, creating an increasingly competitive disadvantage.

Cost category	Business impact
Engineering resource misallocation	Significant engineering budgets diverted to cybersecurity capabilities outside manufacturer expertise
Market access limitations	Longer sales cycles, higher customer acquisition costs, lost ecosystem opportunities
Maintenance cost escalation	Decade-long product lifecycles require continuous security updates and compatibility maintenance

Engineering resource misallocation

Device manufacturers excel at hardware design, power management, and industrial engineering. Yet proprietary security forces them to become cybersecurity experts—diverting talented engineers from core competencies to defensive capabilities that don't differentiate products. This investment delivers negative ROI when customers resist the very features that consumed these resources.

Market access limitations

According to TEIA founding members representing millions of energy customers, utilities now actively screen for vendor lock-in during procurement. Every proprietary security decision shrinks the addressable market and creates friction with the ecosystem partnerships that drive growth.

"This investment delivers negative ROI when customers resist the very features that consume these resources."

TEIA's solution for device manufacturers

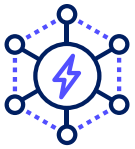
TEIA transforms device security economics by providing open, standardized security that lets manufacturers focus on building exceptional hardware.

Reduce development costs

Implement proven TEIA standards instead of building proprietary security stacks. Redirect engineering resources to actual product differentiation—power efficiency, reliability, cost optimization.

Expand market access

TEIA compliance becomes a selling point. Utilities and aggregators actively prefer TEIA-compatible devices for multi-vendor deployments without integration complexity.



Enable ecosystem participation

Virtual power plants, demand response programs, and grid services represent the highest-growth energy segments. TEIA compatibility is becoming table stakes.

Reduce support burden

Standardized security means standardized integration. Deployments become faster and less complex, reducing field support costs and accelerating revenue recognition.

Future-proof products

TEIA standards evolve through collaborative governance. Manufacturers gain input into standards development while ensuring products remain compatible with emerging requirements.

Simplify compliance

Built-in cryptographic audit trails and regulatory reporting meet evolving compliance requirements.

The way ahead

The energy industry stands at an inflection point. The distributed energy ecosystem—projected to reach $111.41 billion by 2034[2]—requires a fundamental shift from proprietary systems to open standards. Device manufacturers who recognize this reality early will capture disproportionate value.

The mathematics are straightforward: proprietary security diverts substantial engineering budgets to capabilities outside core competencies, creates customer friction that extends sales cycles, and excludes manufacturers from high-growth ecosystem opportunities. Each year this approach continues to compound the competitive disadvantage.

TEIA offers an alternative: redirect those engineering resources to actual product differentiation, convert security from a liability into a selling point, and position devices for participation in virtual power plants, demand response programs, and grid services where growth is concentrated.

The question facing device manufacturers isn't whether to adopt open standards—market forces will make this inevitable. The question is whether to lead this transition or follow it. Early movers gain strategic advantages: they help shape standards that favor their architectures, they build ecosystem relationships before markets consolidate, and they capture customer mindshare as the reference implementation.

"The TEIA standard will reduce time to market and create an open environment for cost-effective, standardized and secure energy solutions."[5]

Getting started

TEIA provides complete specifications for interoperable security. Technical white papers detail the standardized trust model. Membership in TEIA working groups allows manufacturers to influence standards development while connecting with implementation partners experienced in TEIA deployment.

The distributed energy future belongs to manufacturers who embrace interoperability. Transform your competitive position through TEIA's open standards.

Learn more at: www.trusted-energy.org

Contact us at: contact@trusted-energy.org

Endnotes

1. IANS Research & Artico Search, "*2022 Security Budget Benchmark Summary Report*", 2022. https://venturebeat.com/security/benchmarking-your-cybersecurity-budget-in-2023

2. Precedence Research, "*IoT in Energy Market Size, Share, and Trends 2024 to 2034*", 2024. https://www.precedenceresearch.com/iot-in-energy-market

3. TEIA, "Global Energy Leaders Announce Availability of First Secure IT/OT Standards for Digital Energy Systems", *Business Wire*, May 21, 2024. https://www.businesswire.com/news/home/20240521155931/en/

4. TEIA, "*Introducing TEIA: Securing IoT Data and Devices for Affordable and Clean Global Energy Systems*", June 26, 2023. https://www.trusted-energy.org/blog/introducing-teia/

5. Thomas Birr, Chief Strategy & Innovation Officer, E.ON SE, quoted in TEIA founding announcement, *Business Wire*, June 6, 2023. https://www.businesswire.com/news/

Trusted Energy Interoperability Alliance

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