intertrust®

WHITE PAPER

Building resilient and secure distributed energy ecosystems

Balancing DER flexibility with emerging security challenges

Building trust for a connected world.

Contents

Executive summary

The rapid evolution of distributed energy resources (DERs) is ushering in unprecedented energy resilience and flexibility.

The rapid evolution of distributed energy resources (DERs) is ushering in unprecedented energy resilience and flexibility. However, this decentralization introduces significant cybersecurity challenges as the footprint of devices grows and attack surfaces expand.

This white paper explores the delicate balance between the resilience advantages of distributed energy systems and their inherent security vulnerabilities, proposing comprehensive strategies for creating secure distributed energy ecosystems with a particular focus on zero-trust architectures and protocol-agnostic security solutions.

The evolution of distributed energy

Global energy systems are undergoing a significant shift. Traditional centralized power generation and distribution systems are giving way to more distributed, digitalized, and decentralized energy ecosystems.

This is driven by renewable energy growth, storage advancements, evolving regulations, and consumer demand for sustainability.

Distributed energy resources (DERs) include solar photovoltaics (PVs), wind turbines, battery storage systems, fuel cells, combined heat and power plants, and other generation and storage technologies deployed at or near points of consumption. The International Energy Agency reports that distributed solar PV capacity alone has grown at an average annual rate of over 40% in the past decade, with similar growth trajectories for other DER technologies (IEA, 2023).

This rapid expansion brings both opportunities and challenges. On one hand, DERs contribute to grid resilience by diversifying energy sources and reducing dependency on centralized infrastructure (NREL, 2022).

On the other hand, the proliferation of digitally connected energy assets creates new cybersecurity vulnerabilities that must be addressed to protect critical energy infrastructure (DOE, 2023).

The dual imperative of resilience and cybersecurity has never been more crucial. As energy systems become increasingly distributed and interconnected, they must be designed to withstand both physical disruptions and cyberthreats from sophisticated adversaries. The stakes are high: energy is the lifeblood of modern economies, and disruptions can have cascading effects on essential services, economic activities, and public safety (CISA, 2024).

As energy systems become increasingly distributed, they must withstand both physical disruptions and cyberthreats.

Resilience and reliability of distributed energy

Distributed energy systems offer inherent resilience advantages over traditional centralized models, fundamentally changing how we conceptualize energy security and reliability. By their very nature, distributed architectures provide strategic defense mechanisms against both physical and cyberthreats.

Strategically placed DERs can reduce outage frequencies by up to 15%.

Decentralization as a strategic defense mechanism

Unlike centralized systems where a single point of failure can cause widespread outages, distributed energy ecosystems distribute risk across multiple generation points and microgrids. This architectural resilience means that damage or compromise to individual components has limited impact on the overall system functionality. During extreme weather events or other disruptions, areas with distributed generation can maintain essential services even when disconnected from the main grid (Panteli & Mancarella, 2022).

Real-world evidence supports this resilience advantage. During Hurricane Sandy in 2012, while millions lost power from centralized grid failures, facilities with combined heat and power systems and microgrids maintained operations (Lacey, 2022). Similarly, during California's wildfire-induced power shutoffs, communities with solar+storage installations maintained critical services while surrounding areas experienced blackouts (Mullendore, 2023).

Reduced dependency on a single point of failure

Distributed energy systems reduce vulnerability by eliminating single failure points that can cascade throughout the system. Key reliability benefits include:

- **Geographic distribution.** Energy assets spread across different locations ensure that localized events cannot compromise the entire system
- **Technology diversity.** Multiple generation technologies create redundancy and reduce dependency on any single resource type
- **Operational autonomy.** Local control capabilities enable portions of the grid to operate independently during wider system disturbances
- **Rapid restoration.** Distributed resources can facilitate faster service restoration after outages

This reduced dependency translates to measurable reliability improvements. Studies by the National Renewable Energy Laboratory show that strategically placed DERs can reduce outage frequencies by up to 15% and outage durations by up to 20% at the distribution level (NREL, 2024).

Cybersecurity paradox—The dark side of distributed systems

The same architectural characteristics that make distributed energy systems resilient against physical threats create a cybersecurity paradox: increased complexity, diversity, and connectivity expand the attack surface, potentially introducing new vulnerabilities into the energy ecosystem (Leszczyna, 2023).

Attacks targeting distributed energy assets increased by 300%+ between 2019 and 2022.

Increased complexity creates new security vulnerabilities

Distributed energy systems incorporate diverse technologies, protocols, and control systems, creating a heterogeneous environment that is inherently more complex to secure than traditional centralized infrastructure. This complexity manifests through diverse technology stacks where distributed energy resources often utilize different hardware, software, firmware, and communication protocols, each with their own security profiles and vulnerabilities (NIST, 2023).

The supply chain complexity of components sourced from multiple vendors creates potential for compromises and inconsistent security standards (GAO, 2024). The sheer number of devices and their interactions make it difficult to maintain secure configurations across all system elements. Many DERs must integrate with legacy operational technology (OT) systems that were designed without modern security considerations.

Security research from Idaho National Laboratory indicates that over 40% of vulnerabilities in energy systems stem from complexity-induced misconfigurations rather than inherent software flaws, highlighting how complexity itself becomes a security liability (INL, 2023).

More connection points mean more attack vectors

The proliferation of connected devices dramatically increases the number of potential entry points for cyberattacks. Each connected DER effectively extends the network boundary, creating potential access points for attackers (SANS, 2024). Many modern DERs have direct or indirect internet connectivity for monitoring, management, and firmware updates.

Customer-facing applications and portals create potential attack pathways if not properly secured. Wireless communication technologies used in field deployments introduce attack vectors that didn’t exist in traditional energy infrastructure (EPRI, 2023).

The European Network for Cyber Security reports that attacks targeting distributed energy assets increased by over 300% between 2019 and 2022, with particular focus on inverters, battery management systems, and energy management platforms (ENCS, 2024).

Endpoint security imperatives

Securing distributed energy ecosystems requires a multi-layered approach with particular focus on endpoint security, as these represent the most numerous and vulnerable components of the system (Johnson & Smith, 2023).

Over 40% of vulnerabilities in energy systems stem from complexity-induced misconfigurations.

Here are four key methods to foster robust endpoint security for distributed energy systems that go beyond traditional hardware-based security protection.

1. **Strong authentication and authorization mechanisms**
   Robust identity and access management is essential for all system entities. Multi-factor authentication requiring multiple verification methods for human operators accessing critical systems provides a significant security enhancement. Device identity management through unique, cryptographically verifiable identities for all connected components ensures that only legitimate devices can participate in the ecosystem (NIST SP 800-63, 2023).
2. **Zero trust: Assume compromise, continual verification**
   The zero trust principle is particularly relevant for distributed energy systems. The fundamental approach of "never trust, always verify" treats all network traffic as potentially malicious regardless of source. Micro-segmentation divides networks into isolated zones to contain potential breaches, while continuous authentication provides ongoing verification of device identities and data generated throughout sessions (CISA, 2023).
3. **24x7x365 monitoring, detection and rapid response**
   Comprehensive visibility and incident response capabilities are critical for distributed energy security. Centralized monitoring of security events across the distributed ecosystem provides holistic awareness of potential threats. Specialized tools for identifying potential attacks on energy-specific protocols and systems are essential given the unique characteristics of operational technology (E-ISAC, 2024).
4. **IT/OT convergence and trust model integration**
   The historically separate worlds of information technology (IT) and operational technology (OT) must be brought together securely. Coordinated security policies spanning both IT and OT domains, alignment of previously disparate security approaches, and integrated visibility across IT and OT environments are essential elements of this convergence (Gartner, 2023).

Security research from Idaho National Laboratory indicates that over 40% of vulnerabilities in energy systems stem from complexity-induced misconfigurations rather than inherent software flaws, highlighting how complexity itself becomes a security liability (INL, 2023).

Enhancing security with Intertrust Connect

Intertrust Connect represents a comprehensive approach to securing distributed energy ecosystems, specifically designed to address the unique challenges of decentralized architectures while maintaining their resilience benefits (Intertrust, 2024).

A zero-trust architecture can reduce the mean time to detect incidents by up to 60%.

Zero-trust architecture

Intertrust Connect implements zero-trust principles throughout the distributed energy ecosystem. Every device, service, and user has a cryptographically verifiable identity that serves as the foundation for all authenticity and authentication. Access privileges are verified for every transaction, with no persistent trust relationships (Intertrust, 2023). A zero-trust architecture operating in this manner reduces the mean time to detect security incidents by up to 60% and limits the potential impact radius of any compromise (Cooper & Associates, 2024).

Protocol-agnostic security and interoperability

One of Intertrust Connect's key differentiators is its ability to provide consistent security across diverse protocols and technologies. An abstraction layer applies security controls regardless of underlying communication protocols.

The system can secure inherently insecure protocols without requiring infrastructure replacement, a critical capability for energy systems with substantial legacy components (GridWise Alliance, 2023). This approach enables organizations to secure both modern and legacy systems within a single security framework, addressing one of the most significant challenges in distributed energy security (Ramirez et al., 2024).

Uniform trust overlay

Intertrust Connect creates a consistent security layer across the fragmented distributed energy landscape. Unified security policies applied consistently across diverse technologies and distributed enforcement with security controls enforced locally at each endpoint while maintaining central governance provide comprehensive protection (Williams & Chen, 2023). A trust overlay approach can deliver up to 40% reduction in security management complexity while improving overall security posture in real-world deployments.

Real-time, direct OT access

Secure operational technology access is critical for distributed energy operations. Protected pathways for authorized access to field devices without exposing them to public networks reduce vulnerability. Temporary access rights granted only when needed for specific operational tasks minimize the window of opportunity for attackers (Sandia National Laboratories, 2023).

By implementing these capabilities zero-trust solutions such as Intertrust Connect can address core security challenges of distributed energy systems while preserving their structural resilience advantages (IEEE Power & Energy Society, 2024).

Conclusion: Future of secure distributed energy

Energy systems lie at the intersection of distributed architectures and robust security frameworks. As distributed energy resources continue their exponential growth, organizations must navigate the inherent tension between the resilience benefits of decentralization and the cybersecurity challenges of expanded attack surfaces (World Economic Forum, 2023).

Distributed energy systems offer unparalleled resilience against physical threats and infrastructure disruptions. Their ability to operate independently, recover quickly from disturbances, and maintain critical services during wider outages makes them essential for future energy security (EPRI, 2024).

However, these same distributed systems face significant cybersecurity challenges that cannot be overlooked. The increased complexity, expanded attack surface, and IT/OT convergence issues create vulnerabilities that sophisticated adversaries can exploit (MITRE, 2023).

The path forward requires an integrated approach that combines five key steps:

1. **Security by design**
   Building security into distributed energy systems from initial conception rather than as an afterthought (NIST, 2024)
2. **Zero-trust architectures**
   Implementing "never trust, always verify" principles throughout the energy ecosystem (CISA, 2023)
3. **Comprehensive endpoint security**
   Hardening all components with robust authentication, encryption, and monitoring (DOE, 2024)
4. **Uniform trust overlays**
   Creating consistent security frameworks that span diverse technologies and protocols (Forrester, 2023)
5. **Resilient architectures**
   Designing systems that can detect, resist, and recover from cyber attacks (IEA, 2024)

Energy ecosystem design must be both structurally resilient and cybersecure. By acknowledging the inherent security challenges of distributed systems and implementing comprehensive security strategies, organizations can build truly resilient and secure distributed energy ecosystems that power our future with confidence.

Contact us today to schedule a consultation or demo and learn how Intertrust Connect can accelerate your DER program.

Learn more at:
intertrust.com/intertrust-connect
Contact us at: energy@intertrust.com
+1 408 616 1600

References

1. CISA. (2023). Zero Trust Maturity Model. Cybersecurity and Infrastructure Security Agency.
2. CISA. (2024). Energy Sector Criticality Assessment Report. Cybersecurity and Infrastructure Security Agency.
3. Cooper & Associates. (2024). Benchmarking Security Response Times in Energy Management Systems. Journal of Energy Cybersecurity, 14(2), 78-92.
4. DOE. (2023). Cybersecurity Vulnerabilities in Distributed Energy Resources. Department of Energy.
5. DOE. (2024). Framework for Secure Energy System Design. Department of Energy.
6. E-ISAC. (2024). Distributed Energy Resources Threat Landscape Report. Electricity Information Sharing and Analysis Center.
7. ENCS. (2024). Attack Trends in Distributed Energy Systems 2019-2022. European Network for Cyber Security.
8. EnergyTech Review, 8(3), 42-51.
9. EPRI. (2023). Wireless Security Challenges in Energy Distribution Systems. Electric Power Research Institute.
10. EPRI. (2024). Resilience Metrics for Modern Energy Systems. Electric Power Research Institute.
11. Forrester. (2023). Trust Models for Next-Generation Energy Systems. Forrester Research.
12. GAO. (2024). Supply Chain Risks in Critical Energy Infrastructure. Government Accountability Office.
13. Gartner. (2023). IT/OT Convergence in Energy: Best Practices and Future Directions. Gartner Research.
14. GridWise Alliance. (2023). Protocol Security in Advanced Energy Systems. GridWise Alliance Report.
15. IEA. (2023). Distributed Energy Resources Growth Trends 2015-2023. International Energy Agency.
16. IEA. (2024). Resilient Energy Architecture: Global Perspectives. International Energy Agency.
17. IEEE Power & Energy Society. (2024). Security and Resilience in Modern Power Systems. IEEE.
18. INL. (2023). Vulnerability Analysis of Complex Energy Control Systems. Idaho National Laboratory.
19. Intertrust. (2023). Zero Trust Implementation in Critical Infrastructure. Intertrust Technologies Corporation.
20. Intertrust. (2024). Securing Distributed Energy Resources: Technical Approaches. Intertrust Technologies Corporation.
21. Johnson, A., & Smith, B. (2023). Endpoint Security Strategies for Distributed Energy Systems. Journal of Critical Infrastructure Protection, 18(3), 214-226.
22. Lacey, S. (2022). Microgrids During Superstorm Sandy: How Distributed Energy Fared. Greentech Media.
23. Leszczyna, R. (2023). The Cybersecurity Paradox in Energy Systems. Energy Policy Journal, 176, 113467.
24. MITRE. (2023). ATT&CK Framework for Industrial Control Systems in Energy. MITRE Corporation.
25. Mullendore, S. (2023). Solar+Storage During California Power Shutoffs: Impact Analysis. Clean Energy Group.
26. NIST. (2023). Managing Complexity in Energy Control Systems. National Institute of Standards and Technology Special Publication.
27. NIST. (2024). Security by Design Principles for Critical Infrastructure. National Institute of Standards and Technology.
28. NIST SP 800-63. (2023). Digital Identity Guidelines for Critical Infrastructure. National Institute of Standards and Technology Special Publication 800-63.
29. NREL. (2022). Distributed Energy Resources and Grid Resilience. National Renewable Energy Laboratory.
30. NREL. (2024). Reliability Impacts of Distributed Energy Resource Integration. National Renewable Energy Laboratory Technical Report.
31. Panteli, M., & Mancarella, P. (2022). Modeling and Evaluating the Resilience of Power Systems with Distributed Energy Resources. IEEE Transactions on Power Systems, 37(2), 784-796.
32. Ramirez, C., et al. (2024). Protocol Security Integration in Legacy Energy Systems. Energy Informatics, 7(1), 23-42.
33. Sandia National Laboratories. (2023). Secure Remote Access Methods for Operational Technology in Energy. Sandia National Laboratories.
34. SANS. (2024). Attack Surface Expansion in Distributed Energy Systems. SANS Institute.
35. Williams, J., & Chen, L. (2023). Unified Trust Models for Heterogeneous Energy Systems. IEEE Security & Privacy, 21(4), 47-59.
36. World Economic Forum. (2023). The Future of Energy Security: Balancing Resilience and Cybersecurity. World Economic Forum.

intertrust®

Building trust for a connected world.