intertrust®

WHITE PAPER

Defending critical energy infrastructure

How cyberattacks are driving the shift to zero trust and open standards in global energy.

Building trust for a connected world.

Contents

Executive summary

A decade of escalating cyberattacks on energy infrastructure proves that perimeter-based security cannot protect multi-vendor OT environments.

Geopolitically motivated cyberattacks against energy infrastructure have grown sharply in both frequency and sophistication. From the 2015 BlackEnergy 3 attack on Ukraine's power grid to the 2025 DynoWiper assault on Poland's energy system, adversaries have demonstrated a consistent ability to breach perimeter defenses and cause physical destruction.

This paper examines the common failure patterns across five major infrastructure attacks and explains why a transition to zero trust architectures, implemented through open standards and alliances like TEIA, offers a transparent, scalable path forward for securing global energy systems.

The rise of hybrid cyber warfare

Nation-state and hacktivist attacks on critical infrastructure doubled in 2025. Geopolitics is now the defining feature of cybersecurity strategy.

Cyberattacks as instruments of state power

Modern cyberattacks against energy infrastructure are increasingly instruments of geopolitical strategy rather than criminal enterprise. The World Economic Forum's Global Cybersecurity Outlook 2026 reports that 64 percent of organizations now factor geopolitically motivated cyberattacks into their risk planning.[1] The Waterfall Threat Report 2026 confirms this trajectory: nation-state and hacktivist attacks doubled in 2025, with the majority targeting critical infrastructure.[2]

Russia's intelligence services have been at the forefront of this shift. Beginning with the GRU-linked Sandworm group's 2015 attack on Ukraine's power grid, a pattern of progressively sophisticated operations has targeted energy systems across Eastern Europe, each one refining the techniques of its predecessor.

From espionage to physical destruction

What distinguishes these campaigns is their intent. Unlike conventional cybercrime, the goal is not financial gain but physical disruption: blackouts during sub-zero temperatures, bricked communications equipment on the morning of a military invasion, and permanently destroyed industrial control hardware. The 2017 NotPetya attack alone caused an estimated $10 billion in global economic damage.[3]

64% of organizations now account for geopolitically motivated cyberattacks in risk planning.

Why perimeter defenses fail

Every major attack on energy infrastructure in the past decade followed the same pattern: breach the perimeter once, then move freely through implicitly trusted internal systems.

Cyberattacks as instruments of state power

Boundary-based security models assume that systems inside the perimeter are trustworthy. In practice, this means a single compromised VPN credential or phishing payload grants attackers lateral access to operational technology networks. In the BlackEnergy 3 attack, stolen VPN credentials provided direct passage from the business network to SCADA systems.

In the AcidRain attack, a misconfigured FortiGate VPN opened a path to satellite management servers. VPN vulnerabilities have grown 82.5 percent in recent years, and 56 percent of organizations reported a VPN-exploited breach in the past year.[4]

Multi-vendor complexity obscures risk

Energy infrastructure combines hardware and software from dozens of vendors, each with distinct authentication methods, communication protocols, and firmware update cycles. The DynoWiper attack exploited this directly: Hitachi RTU560 devices retained default account credentials, Hitachi Relion 650 protection relays exposed default FTP services, and Mikronika HMI systems ran with default accounts on unpatched Windows 10.

No single vendor owned end-to-end security, and no common standard enforced uniform protections. Claroty's survey of 1,100 critical infrastructure professionals found that 45 percent reported financial impacts exceeding $500,000 from attacks on cyber-physical systems.[5]

56% of organizations reported a VPN-exploited breach in the past year.

Imperatives for infrastructure security

The recurring failure patterns across a decade of attacks point to four requirements that any effective security framework for energy infrastructure must address.

Addressing the vulnerabilities exposed by BlackEnergy 3, Industroyer, NotPetya, AcidRain, and DynoWiper requires moving beyond incremental patching of perimeter defenses. Four imperatives emerge from the evidence.

1. Eliminate implicit trust.
No device, user, or system receives trust based on network location. Every connection is authenticated and authorized independently, closing the lateral-movement pathways that every attack in this paper exploited.

2. Establish direct, secure communication.
Success depends on creating closed, authenticated data paths directly between two endpoints without relying on the security of intermediary systems such as VPNs, firewalls, or gateways.

3. Replace obscurity with transparency.
Security specifications must be public, peer-reviewed, and uniformly implemented. Vendor-specific, opaque security mechanisms create the fragmented trust environment that attackers consistently exploit.

4. Enable rapid credential revocation.
Independent certificate authorities must be able to revoke compromised credentials across all vendors in real time. The zero trust security market reached $34.5 billion in 2024 and is projected to reach $84 billion by 2030, reflecting widespread industry recognition that these imperatives are urgent.[6]

The zero trust market is projected to grow from $34.5 billion to $84 billion by 2030.

Zero trust through open standards

TEIA provides the framework to define, implement, and operate zero-trust authentication infrastructure across multi-vendor energy environments at global scale.

The TEIA approach

The Trusted Energy Interoperability Alliance (TEIA) is a global initiative led by major energy companies, including E.ON, JERA, Origin Energy, GS Energy, and Intertrust Technologies. TEIA translates zero trust principles and open standards into a practical, deployable framework for multi-vendor energy infrastructure.

Zero-trust authentication
Every device, service, and operator receives a cryptographically verifiable identity. Access privileges are verified for every transaction with no persistent trust relationships.

Open security specifications
All security mechanisms follow public, peer-reviewed standards. Contractual obligations ensure uniform implementation across vendors, eliminating the fragmented trust model that current systems rely on.

Independent certificate management
Common, independent certificate authorities enable rapid revocation of compromised credentials across the entire ecosystem, regardless of hardware vendor.

The path forward

TEIA is already operational. In Texas, the Rhythm Project uses the TEIA framework to securely connect distributed energy resources at scale, replacing expensive one-off integrations with standardized, authenticated connections.

E.ON is deploying TEIA in Germany to connect and manage previously undigitized substations through secure cloud infrastructure. As 96 percent of organizations now favor a zero trust approach.[4] TEIA provides the standards-based foundation to make that transition practical for the energy sector.

Sources

[1] World Economic Forum. *Global Cybersecurity Outlook 2026*. January 2026.
[2] Waterfall Security Solutions. *Waterfall Threat Report 2026*. March 2026.
[3] Estimates based on U.S. government attribution statements and industry financial disclosures, 2017–2018.
[4] Zscaler ThreatLabz. *2025 VPN Risk Report*. April 2025.
[5 Claroty. *The Global State of CPS Security 2024: Business Impact of Disruptions*. 2024.
[6] Grand View Research. *Zero Trust Architecture Market Size, Share & Trends Analysis Report, 2030*. 2024.

96% of organizations now favor a zero trust security approach.

To explore how TEIA and Intertrust Technologies can help secure your energy infrastructure, contact us for a consultation

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

intertrust®

Building trust for a connected world.