goldilock

ENERGY SECTOR

Use Case 09

Protecting networks, lives and livelihoods at

Goldilock FireBreak™ for Energy Infrastructure: Keeping the Lights On, Even Under Attack

Securing The Whole Of The Energy

Exploring the evolving threat landscape, regulatory imperatives and breakthrough new resilience technologies now shaping the future of cybersecurity across the five domains of the global energy ecosystem; fossil fuels, nuclear, renewables, grid infrastructure, and smart energy services.

Since the energy sector is unique in its position spanning the underpinnings of all social, commercial, domestic and sustainable society functions, securing the world's most critical infrastructure from every threat model remains paramount, even as those threats expand, transform and gain energy.

Even a brief summary of the nature of the sector highlights the sheer scale of the technology landscape, the variability and complexity of systems deployed. In addition, there is an inevitable and widening gap between legacy systems that remain on long productive lifecycles and modern energy architecture.

Encompassing fossil fuels, nuclear power, renewables, grid infrastructure, and emerging smart energy services, not only does it represent one of the most vital and interdependent systems supporting global stability, economic growth, and societal well-being, but it is managed across a massive array of disparate systems, sub-systems and networks.

It is that network function and resilience this document explores. Representing an estimated $7–8 trillion global market and projected to attract over $35 trillion in investment by 2050, the energy sector is undergoing a profound transformation. Yet also attracts a rising and increasingly energetic cyber threat.

As countries pursue cleaner, smarter, and more efficient energy systems, they are converging physical and digital domains, from upstream extraction and generation to cloud-integrated grid distribution and storage operations. The reshaping how energy is produced, delivered, and consumed worldwide must now consider how this complexity is protected, fully.

The Challenge: Critical Threats to Energy Infrastructure

The technology shifts across the energy sector have created one of the largest and most complex attack surfaces of any industry. Energy systems rely on an intricate web of Operational Technology (OT) (e.g., control systems, SCADA, PLCs), Information Technology (IT) (enterprise systems, business networks), and millions of Internet of Things (IoT/IIoT) devices, from smart meters to remote sensors, bringing them together. Analysts estimate that over 41 billion IoT devices will be connected globally by 2025, significantly expanding potential entry points. Some recent threat studies show more than 145,000 ICS/OT systems exposed online across 175 + countries, many of which are energy-critical.

The result is a hyperconnected environment where a single compromised endpoint, misconfigured sensor, or exploited control interface can cascade across networks, disrupting generation, transmission, or supply. Unlike other sectors, disruptions in energy systems translate directly into physical impact, affecting heat, light, transport, and national infrastructure. Strengthening cybersecurity across this interconnected ecosystem is therefore not only a technical imperative but a strategic necessity, to secure the world's transition toward a cleaner, smarter, and more resilient energy future.

The Nature of Threats

Ransomware and operational disruption:
Energy utilities, oil and gas producers, and renewable operators are prime targets for ransomware attacks that can paralyze industrial control systems (ICS) and supervisory control and data acquisition (SCADA) networks. Threat actors exploit remote access points, VPNs, and maintenance interfaces to halt production, encrypt systems, or extort critical service providers, causing cascading blackouts, fuel shortages, or costly downtime.

State-sponsored espionage and sabotage:
Nation-state actors view energy infrastructure as a strategic target for both cyber warfare and political leverage. Attacks on grid operators, refineries, or nuclear facilities aim to disrupt national power supplies, compromise safety systems, or steal proprietary technology tied to next-generation energy innovation. These campaigns often blend cyber intrusion with physical or insider coordination.

Insider threats (intentional or accidental):
Employees, contractors, or third-party technicians with privileged OT or IT access can unintentionally introduce malware, misconfigure systems, or, in rare cases, deliberately sabotage operations. Given the distributed nature of energy assets and reliance on outsourced maintenance, insider risk remains a persistent and often underreported threat vector.

Supply chain and third-party vulnerabilities:
Energy organizations depend heavily on external suppliers for hardware, software, field services, and maintenance. Attackers increasingly compromise trusted partners or firmware updates to infiltrate energy environments undetected. Supply chain attacks can embed persistent backdoors into critical components such as turbine controllers, substation relays, or grid management systems.

Energy Sector — Use Case

Distributed energy and grid decentralization threats:
As renewable generation and microgrids expand, the grid's topology is becoming more decentralized. This increases the number of access points and reduces centralized control visibility. Threat actors can target distributed assets, such as solar farms or EV charging networks, to trigger instability or coordinated grid imbalances.

IT/OT/IoT convergence risks:
The integration of digital IT systems with legacy OT and a rapidly expanding layer of IoT and IIoT devices, smart meters, sensors, predictive maintenance platforms, creates a vast and fragmented attack surface. Insecure protocols, outdated firmware, and poor network segmentation allow adversaries to move laterally from digital management systems into physical operations, making compromise potentially kinetic in nature.

Physical and cyber-physical security breaches:
Unauthorized access to substations, control rooms, or pipeline monitoring facilities, whether via social engineering, credential theft, or physical intrusion, can result in sabotage or data theft. The blending of cyber and physical attack methods magnifies risk in an industry where real-world impact is immediate.

Legacy infrastructure vulnerabilities:
Much of the global energy infrastructure still relies on decades-old control systems that lack modern authentication, encryption, or patching capabilities. These legacy assets cannot easily be replaced and often operate in isolation, or worse, are hastily connected to digital networks without sufficient segmentation.

AI and digital automation risks:
As energy companies deploy AI for predictive maintenance, load balancing, and automated grid optimization, attackers are turning to AI manipulation. Adversarial data poisoning, model theft, or tampering with automated decision systems can cause incorrect operational responses, service interruptions, or false alerts across critical energy systems.

Regulatory pressure and public accountability:
With energy systems now formally recognized as part of Critical National Infrastructure (CNI) in the UK and covered by frameworks such as the EU's NIS2 Directive and the US Department of Energy's Cyber-Informed Engineering Strategy, operators face mounting obligations for demonstrable resilience, transparent reporting, and continuous risk assessment. The energy sector operates under intense regulatory and public scrutiny, where a single breach can trigger market instability and national-level repercussions.

Physical Segmentation with Goldilock FireBreak

Goldilock FireBreak represents a breakthrough in how critical infrastructure can achieve true cyber resilience without sacrificing operational efficiency. Unlike conventional network segmentation or purely software-defined isolation, FireBreak delivers patented, hardware-enforced physical disconnection of digital assets, creating a controllable, verifiable air gap between operational systems and external networks. This approach transforms the concept of resilience from reactive recovery to proactive protection.

For energy operators, FireBreak provides the capability to physically isolate and reconnect control systems, data networks, and backup infrastructure instantly and remotely, without relying on software commands or human presence on site. Whether protecting a grid substation, refinery control network, or renewable energy farm, FireBreak ensures that critical assets remain inaccessible to remote attackers, even if IT or OT environments are compromised.

By integrating FireBreak into CNI-grade architectures, operators can meet regulatory requirements under frameworks such as NIS2, the UK's CNI mandates, and the U.S. Department of Energy's Cyber-Informed Engineering (CIE) principles. It aligns perfectly with the industry's transition toward Zero Trust architectures, offering a layer of "Zero Connectivity Assurance"—where the absence of connection, rather than the strength of encryption, defines the highest form of security.

As the energy ecosystem becomes more digital, distributed, and dependent on automation, Goldilock FireBreak provides the missing control: a deterministic, physically enforced way to deny cyber access when it matters most. In an industry where uptime, safety, and trust are non-negotiable, FireBreak redefines what it means to be truly secure.

Real-World FireBreak Deployment Scenarios

Fossil Fuel Networks (Oil, Gas, and Petrochemical)

Challenge: Protecting refinery control systems, pipeline monitoring, and drilling platforms from ransomware, insider threats, and remote exploitation.

FireBreak Solution: Deploy FireBreak between core OT systems (e.g., SCADA, PLCs) and enterprise or cloud networks to enable instant, verifiable disconnection during cyber incidents or maintenance. Integrate with SOC/SIEM platforms for automated isolation if anomalous data flows or unauthorized commands are detected, preventing attacks from spreading between corporate IT and operational networks.

Nuclear Energy Facilities

Challenge: Ensuring the highest possible assurance for reactor control, safety, and monitoring systems while meeting strict CNI and regulatory requirements.

FireBreak Solution: Use FireBreak to physically segment safety-critical systems from administrative and external networks. Enable remote, policy-based connection windows for authorized maintenance or data transfer, with immutable audit logs and hardware-enforced disconnection to guarantee regulatory compliance and operational integrity.

Renewable Energy Generation (Wind, Solar, Hydro, Geothermal)

Challenge: Securing distributed, often remote, generation assets and IoT-heavy monitoring environments that are vulnerable to lateral movement and supply chain compromise.

FireBreak Solution: Deploy FireBreak at turbine or inverter control nodes, substations, and regional aggregation points. Automate isolation based on sensor telemetry or intrusion alerts to prevent the spread of threats across distributed assets. Enable secure, time-bound access for maintenance crews and third-party technicians without persistent exposure.

Grid Operations and Distribution Networks

Challenge: Protecting grid control centres, substations, and transmission infrastructure from state-sponsored attacks and remote command manipulation.

FireBreak Solution: Integrate FireBreak between real-time grid management systems and external communication channels, allowing operators to physically disconnect vulnerable nodes while maintaining control via redundant, segmented pathways. Use event-driven triggers from SIEM or intrusion detection systems to activate disconnection within milliseconds, preserving grid stability and preventing cascading failures.

Smart Energy and Digital Services

Challenge: Managing the explosion of connected devices; smart meters, EV charging networks, and IoT-based demand-response platforms, without exposing control systems to cyber intrusion.

FireBreak Solution: Deploy FireBreak between IoT aggregation layers and backend control or billing systems. Automate disconnection of compromised devices or service clusters while maintaining availability for unaffected systems. Provide utilities and service providers with audit-ready, deterministic control over connectivity, enabling "Zero Connectivity Assurance" in highly distributed smart environments.

Disaster Recovery and Backup Infrastructure (Cross-Domain)

Challenge: Ensuring that critical backup and failover systems remain uncompromised and clean until required for emergency use.

FireBreak Solution: Position FireBreak between live and backup environments across all energy domains. Automate connection only during backup windows or disaster declarations, guaranteeing isolated, verified data restoration and uninterrupted recovery in the event of an attack or outage.

Why Energy Operators Choose Goldilock FireBreak

Absolute Invisibility = Zero Attack Surface

When critical energy systems such as grid control networks, SCADA platforms, turbine controllers, pipeline telemetry, and backup infrastructure, are physically isolated by FireBreak, they become completely unreachable, even to the most advanced cyber adversaries. No IP address. No digital footprint. No remote access. FireBreak ensures that when a system is disconnected, it is truly offline, immune to ransomware, insider threats, and state-sponsored intrusions.

FireBreak is engineered to integrate seamlessly across the entire energy ecosystem:

- Fossil Fuels: Secures refinery control systems and pipeline monitoring.
- Nuclear Energy: Isolates reactor command modules and safety subsystems.
- Electric Power Generation & Distribution: Protects grid operations and substations.
- Renewable Energy: Shields solar, wind, and hydrogen systems from cloud-native threats.
- Energy Services & Efficiency: Defends smart meters, IoT platforms, and digital control systems.

Whether safeguarding legacy infrastructure or modern AI-driven environments, FireBreak delivers uncompromising protection, without costly redesigns or operational disruption.

Rapid, Non-Disruptive Deployment

FireBreak is designed for fast, flexible implementation using secure SMS commands, physical key switches, or API integration. Its system-agnostic architecture supports both legacy and next-gen environments, enabling operators to enhance resilience across plants, substations, control centres, and remote sites, without interrupting service delivery.

True Zero Trust, Enforced by Hardware

FireBreak brings Zero Trust principles into the physical realm. It enforces just-in-time, role-based access to critical systems, allowing connections only when necessary and only for the required duration. Whether isolating an oil pipeline control network, a nuclear safety subsystem, or a distributed renewable array, FireBreak ensures security rooted in physical control, not just digital policy.

Proven Protection for Critical National Infrastructure

Trusted across defense, finance, government, and energy sectors, FireBreak is battle-tested in environments where uptime and security are non-negotiable. It delivers robust protection against ransomware, insider threats, supply chain compromise, and nation-state attacks, ensuring continuous availability and regulatory compliance.

Peace of Mind in a Volatile Threat Landscape

Knowing your most critical systems are physically unreachable when not in use provides unmatched assurance. FireBreak dramatically reduces the attack surface across the entire energy value chain, supporting compliance with global frameworks such as:

- NIS2
- UK CNI mandates
- ISO 27001
- US DOE Cyber-Informed Engineering

It demonstrates to regulators, investors, and the public a tangible commitment to resilience, protecting not just data, but the energy that powers the modern world.

Summary

Goldilock FireBreak offers a pioneering cybersecurity solution tailored for the entire energy sector, including fossil fuels, nuclear power, renewables, grid operations, and smart energy services. It ensures hardware-enforced physical isolation of critical assets such as turbine controllers, SCADA networks, pipeline monitoring, and backup systems, making them completely invisible and inaccessible to any remote cyber threats. This approach delivers true offline security when systems are disconnected, providing immunity against ransomware, insider attacks, and state-sponsored intrusions by physically disconnecting at Layer 1—a capability no software-based firewall can match.

FireBreak supports seamless integration across legacy and next-generation environments, promoting rapid, non-disruptive deployment. It allows remote, authenticated control using SMS, physical keys, or APIs, enabling instant physical disconnection or reconnection of systems with millisecond speed and zero network performance impact. This capability enables just-in-time, role-based physical access control, enforcing strict Zero Trust segmentation principles to minimize exposure and reduce risk.

Trusted and deployed by NATO and numerous critical national infrastructure operators, FireBreak helps energy companies maintain continuous uptime and comply with regulations such as NIS2 and ISO 27001. Its robust defence against evolving cyber threats supports resilience in today's complex and digitized energy ecosystem, from traditional plants to renewable infrastructure, making it an indispensable part of cybersecurity strategies for energy operators.

In summary, Goldilock FireBreak stands out by providing verifiable, physical-layer network disconnection with instant remote control, high throughput without latency, and seamless automation integration—offering energy providers unparalleled control and protection over their critical systems in an increasingly hostile cyber threat environment.