illumio

INDUSTRY GUIDE

Zero Trust Segmentation for Energy Providers

Energy organizations are turning to Zero Trust Segmentation to stay resilient against ransomware and other cyberattacks that can halt operations

Modern Challenges for Today's Energy Sector

The single biggest issue facing the long-term evolution of the world's population is how we meet the huge growth in demand for energy while not destroying the planet.

Equally, the world is so reliant on a predictable energy supply that any break can have serious consequences. The race to nuclear, renewables, and hydrogen is significant not just for climate change but also for energy security.

Globally, we see the major impact of current challenges in energy supply, including:

- Increased prices creating energy poverty, even in G7 countries
- The weaponization of energy in global physical and cyber conflicts
- The "tsunami" of demand caused by the shift to electricity-powered transport
- Climate change forcing a rethink on how energy is generated, and the automation and computerization of processes

The increased reliance on energy in every aspect of life makes the energy sector critical to society and, as such, a growing target for threat actors, criminal groups, terrorists and other nations. As the electricity, gas, and oil grids implement smart technology, they become more vulnerable to cyberattacks, particularly where connected industrial control systems support operations on the grid. The adoption of wireless smart devices and the global positioning system to synchronize operations create new vulnerabilities as they use many technologies that cyber criminals can exploit.

> "The global fossil fuel crisis must be a game changer. So let us not take the 'highway to hell' but let's earn the clean ticket to heaven."
>
> **Ursula von der Leyen,**
> **President of the European Commission**

The growth of what is becoming known as the electricity grid edge is also adding to security challenges. The adoption of smart meters, the interconnection of building power distribution systems with the grid, and the proliferation of home generation all create potential new attack vectors. If you then add into the mix distributed energy resources like private wind farms and micronuclear stations, it's clear that a significant shift in the power landscape is taking place.

Although cybersecurity incidents have not yet resulted in major power outages in North America, attacks on industrial control systems have disrupted grid operations in other countries. Recent assessments as detailed in the April 2022 report on the GridEx VI exercise run by NERC and E-ISAC show that a cyberattack could cause widespread power outages, the scale of which is still indeterminate due to the nature of the exercise.

Energy providers around the world are trying to digest a barrage of new regulations, directives and guidance to secure their infrastructure. Many energy organizations are regulated by multiple authorities, including federal, state, and sector bodies. The U.S. Government Accountability Office (GAO) has highlighted this as a challenge due to the time it will take to fully protect the national infrastructure. This makes it imperative that any new cybersecurity infrastructure is as simple as possible.

In this guide, we further explore the energy sector's unique cybersecurity challenges and examine how Zero Trust Segmentation builds cyber resilience, enables operational continuity during and after an attack, and helps providers achieve regulatory compliance.

> "The character of cyberthreats has changed. Respondents now believe that cyberattackers are more likely to focus on business disruption and reputational damage."
>
> **World Economic Forum 2023 Global Cybersecurity Outlook Report**

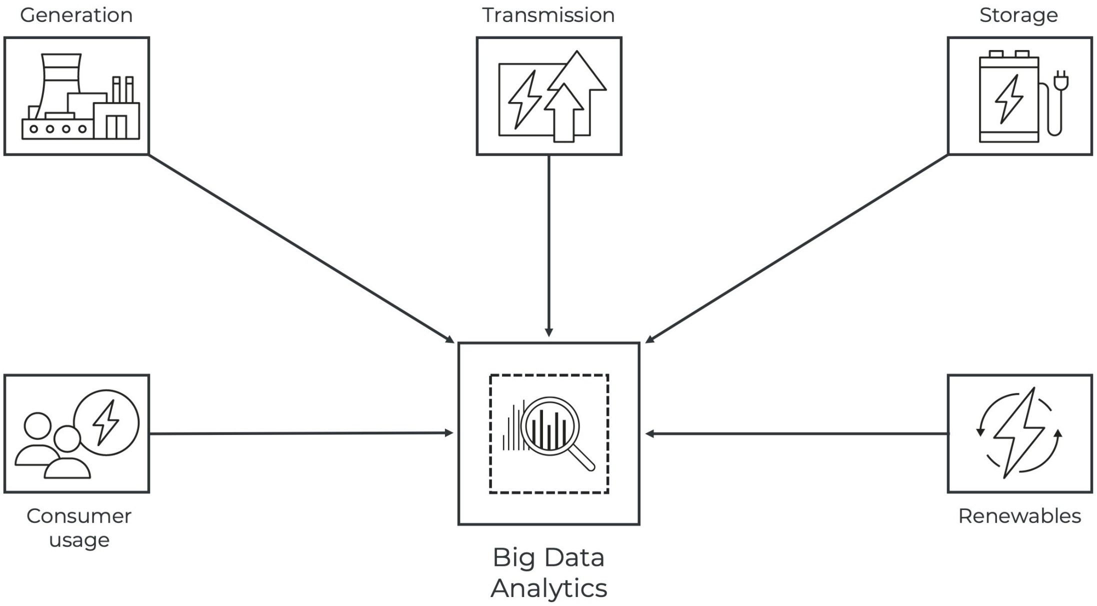
Keeping the Lights On

With the cost of energy becoming unpredictable and the consistency of the energy supply so critical, the energy industry needs to adapt. However, digital transformation within the energy sector is not like other sectors. The industry works on two models:

- Big physical entities like refineries, pipelines, and power stations, which all take a long time to build or transform
- A large scale on which updating the sheer number of systems is daunting

Energy providers must be able to react to fluctuations in both the supply and distribution side of the business, requiring constant small, regular adjustments that can make a huge difference. To understand the required changes, they must analyze vast amounts of data.

Big data analytics offers the granular detail needed to optimize energy flow across the network. As the data processing and grid become ever more intrinsically linked, a failure on the IT side can have a major impact on energy delivery.



However, the energy infrastructure must be updated to smart systems that generate big data. This upgrade requires a considerable investment that will be paid back over the years. But it also creates potential cyber risks.

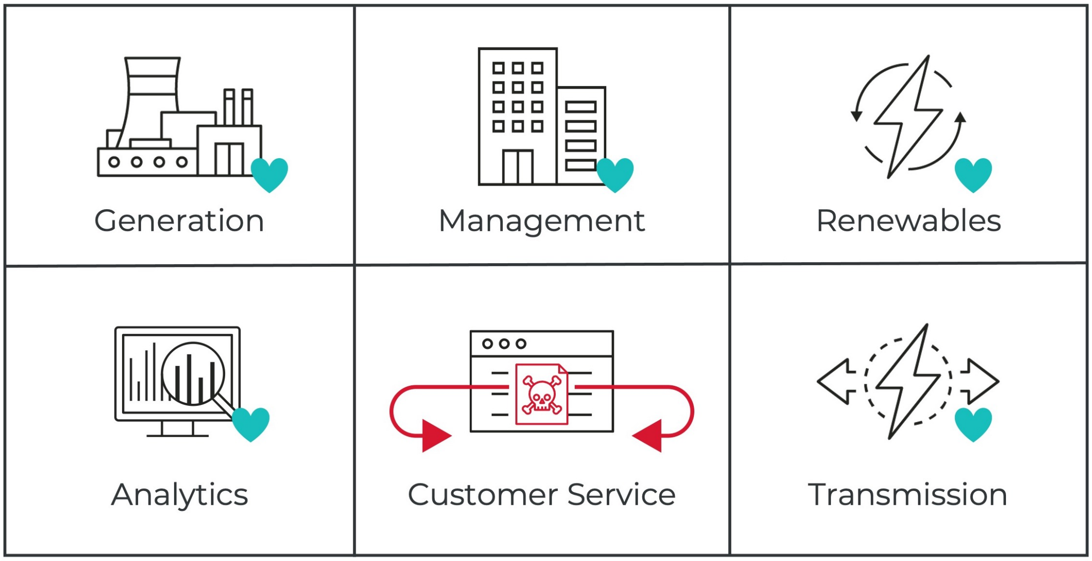
Because most new smart systems are remotely located, it is not possible to use traditional network-based security to protect them. Each asset needs to be individually protected to limit what it is connected to and how it communicates.

> Because most of these new smart systems are remotely located, it is not possible to use traditional network-based security to protect them.

In March 2022, the SEC issued a proposed rule, Cybersecurity Risk Management, Strategy Governance and Incident Disclosure, which includes the intention to require public companies to disclose if their boards have cybersecurity expertise. The rule is principally aimed at driving boards to define who is responsible for risk and to include risk as part of their business strategy. It mirrors the World Economic Forum's Cyber Resilience Pledge, which encourages CEOs to sign a pledge to make their organizations more resilient to attack.

These steps are especially important for the energy market, where maintenance of service is the fundamental objective.

The key to building a robust cyber resilience model is to adopt an "assume breach" mindset. If organizations assume they have already been breached, they will take a more proactive security posture to contain breaches and search for potential lateral movement within the network.



> “When implementing cybersecurity requirements, grid and DER planners should build cyber defenses with the goal of surviving an attack while maintaining critical functionality.”
>
> **Department of Energy, Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid Report**

During recent cyberattacks, operators have tried to contain the attack by disconnecting their organization’s IT and OT, causing breaks in supply. This approach is becoming less viable as IT and OT converge.

IT/OT Convergence Increases the Attack Surface

The worlds of IT and OT are relentlessly converging and creating new security issues. Digital transformation, if pursued without security transformation, can create a security debt that needs resolving. Boosting cyber resilience must start with improving communication between cyber and business leaders.

To optimize the delivery of energy, operators must process huge amounts of data to be able to adjust the network’s parameters. This data needs to be gathered from as many components of the network as possible on both the supply and delivery side, making it a key driver in the convergence of OT and IT in the energy industry.

Historically, the ICS (Industrial Control System) and OT environments have been kept separate from the IT world. By implementing the Purdue Model for ICS Security, energy operators could protect cyber-physical devices by separating them from the IT side. This model worked well when the systems were largely “dumb” and static.

Another approach was to airgap systems so that they were physically separate. This idea has lost credibility because there may always be a connection in modern systems, especially due to the nature of wireless attacks.

An increasing number of devices are “smart” and connected via VPNs, wireless and other methods, increasing an organization’s attack surface. It’s likely that devices are not connected to your network, so the network security model no longer applies. This means traditional security models need to evolve.

The challenge becomes ensuring that an attack on either the IT or OT side of the operation does not proliferate to the other. This means restricting who and how individual devices communicate.

Illumio Zero Trust Segmentation for the Energy Sector

Unlike prevention and detection technologies, Zero Trust Segmentation (ZTS) contains the spread of breaches and ransomware across the hybrid attack surface.

With Illumio ZTS, you can:

- **See risk:** Continually visualize how workloads and devices are communicating
- **Set policy:** Create granular policies that only allow wanted and necessary communication
- **Stop the spread:** Automatically isolate breaches by restricting lateral movement proactively or during an active attack

ZTS is a foundational and strategic pillar of any Zero Trust architecture.

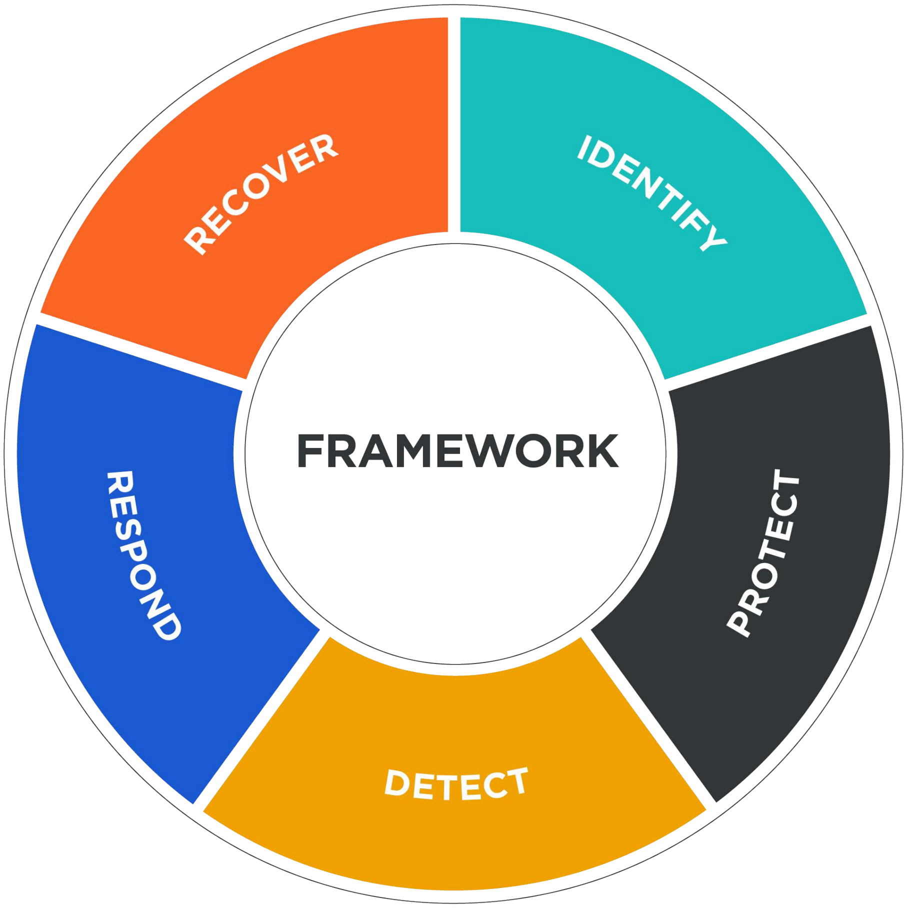
Illumio's ZTS technology enhances traditional perimeter and firewall defenses to embed security at a far more granular level into the interior of networks and data centers. Instead of a single firewall protecting hundreds of applications and devices, security is applied at each asset individually.

Aligning With the NIST Cybersecurity Framework for Energy

Many energy directives have been created worldwide to help all types of businesses address cybersecurity risks and build cyber resilience. They all share a common basis in the NIST Cybersecurity Framework (NIST CSF).

The U.S. Electricity Subsector Coordinating Council (ESCC) explicitly recommends the five steps of the NIST framework in their Ransomware Preparedness document.

Illumio supports the NIST framework and its five pillars of Identity, Protect, Detect, Respond, and Recover. Illumio's platform and technology partners provide additional security capabilities and functionality specific to energy providers.



How Illumio Maps to the NIST CSF

Addressing cyber risks and building cyber resilience is not contingent on full implementation. There are five simple steps based on the NIST framework that can improve cyber resilience during implementation.

Illumio provides the technology to use this model to build resilience in the energy system.

1. Identify

Identifying what to protect and in which order can sometimes become the most complex part of any cybersecurity strategy. Budget and resource restrictions often remove the ability to protect everything to the same level and at the same time. When regulation and security directives are added to this mix, there is a potential for delay.

The first step is a simple audit to identify which systems have the biggest impact on maintaining services. In other words, what are the minimum resources required to keep the energy flowing?

Most national cybersecurity directives require operators to map the interdependencies of all systems.

With Illumio, you can:

- Generate an application dependency map to see all devices and their communication flows to applications, servers, databases, the internet, or even smart devices
- Gather metadata from IT devices, OT and IoT security platforms like Armis, or configuration management databases (CMDBs) like ServiceNow

2. Protect

Once you know what needs to be protected, the next step is to enforce that protection with a solution like Zero Trust Segmentation (ZTS) from Illumio.

It is important to allow only communication between necessary devices using the minimum verified protocols to prevent malware from spreading between IT and OT environments. This “principle of least privilege” should be applied across all communication.

With least-privilege security controls consistently deployed across a hybrid network, organizations can stop a breach at its first point of entry — preventing any further movement across the network.

With Illumio ZTS, you can block specific traffic routes and ports that ransomware typically uses to spread. Or you can block all traffic on a given pathway while allowing only traffic from specific sources.

Many energy sector OT systems run on older, sometimes unsupported versions of software and operating systems. These systems cannot be patched to the latest levels, requiring some mitigation to protect these vulnerable devices. However, patching limitation can be managed by limiting systems that can communicate and which protocols they use.

Illumio ZTS helps ensure that an organization can continue to deliver services even while undergoing a cyberattack.

3. Detect

Detecting an attack is key to neutralizing the threat — and the quicker, the better.

Detection covers a number of technologies. Tools like EDR/XDR (Extended Endpoint Detection and Response) and NGAV (Next-generation Antivirus) monitor your computing systems looking for indicators of compromise (IoCs). IoCs raise the suspicion that a piece of code could be malware. Other security tools like NDR (Network Detection and Response) and UEBA (User and Entity Behavior Analytics) monitor for activities on the network that fall outside of normal baselines.

The final piece of the puzzle is detecting any connections that should not be allowed (e.g., a sensor communicating with the internet).

Illumio ZTS improves the performance of EDR technologies by restricting the spread of an attack and thereby reducing the area required for detection.

4. Respond

Once an attack is detected, you must respond instantly — it must be stopped as soon as it starts.

Illumio ZTS supports this essential security capability. Illumio's incident response segmentation can be built as a manual or automated response within various incident response security systems, including SOAR (security orchestration, automation and response) and SOC (security operation center) tools.

With Illumio ZTS, you can effectively lock down ransomware and breaches to maintain services while the malware is removed from your computing systems.

Your response process and configurations should be planned and tested for efficacy; any attack could be devastating with unknown consequences. Establishing a cyber resilience plan and practicing the response can be the difference between maintaining or disrupting services.

5. Restore

The last action is to restore services. If the attack is still underway, any premature repair work could create new risks.

With Illumio ZTS, security and IT teams can set up protection around individual departments and systems, so they can resume operations while being shielded from the attack.

And with knowledge gained during the unsuccessful attack, you can tune your policies to further tighten access and boost your organization's cyber resilience.

The Illumio Approach

Illumio has a five-step approach to building a consistent least-privilege security model across OT and IT environments. This includes an asset-centric way of understanding the properties, risks, and state of each device or system to apply the appropriate level of protection.

Step 1

Collect connectivity data from IT and OT devices to map interdependencies. This allows you to identify exactly what is communicating and with which system and help identify any high-risk protocols that an attacker could use to propagate through the network.

Step 2

Enrich OT metadata with asset and vulnerability scanning data. When creating security rules, it is vital to understand exactly what the OT devices are and what vulnerabilities exist. This understanding will allow you to mitigate any risks created by unpatched systems.

Step 3

Apply easily understandable labels based on function and risk. By identifying high-risk and high-value assets, it becomes easier to apply the appropriate rules.

Step 4

Enforce policy based on least privilege and risk using the native firewall on IT and supported OT devices. Many modern systems run on standard builds of Linux or Windows. Illumio leverages the native firewalls of these operating systems to enforce security rules.

Step 5

For legacy systems that do not have their own native firewalls enforcement will need to be provided by the network using Access Control Lists in network switches. Rules can be created using Illumio and pushed to each of the switches.

Learn More About Illumio for Energy Providers

The transformation in the energy sector is driven by a global necessity to secure energy delivery systems and infrastructure. With the increasing reliance on energy, any failure can have a significant impact — criminal and nation-state actors could target the power supply of regions and countries.

Energy providers are turning to Zero Trust Segmentation to maximize their cyber resilience and contain breaches to ensure continuous operations.

To learn more about how Illumio can strengthen the security and resilience of your energy operation:

- Explore our products.
- Schedule a demo and consultation with one of our energy security experts.
- Sign up for a virtual hands-on lab session.

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.