illumio

INDUSTRY BRIEF

Maintaining Energy Security

How Zero Trust Segmentation can deliver cyber resilience in the energy market

Digital transformation and new cyber threats

Energy, and especially electricity, is the foundation unpinning all activities in today's world. There is an ever-growing list of challenges to energy security in many countries, including:

- Climate change forcing a rethink on how energy is generated
- Increased prices creating energy poverty
- The weaponization of energy in global physical and cyber conflicts
- The "tsunami" of demand caused by electric transport and the cloud

By digitally transforming many parts of the business, the demand and supply can be optimized to make sure that consumers' needs can be met. Energy operators can make small adjustments using both big data analytics and, in the future, AI to keep the flow consistent.

This could include the redirection of a gas supply or engagement of a pump storage hydroelectric system at peak times. A much smarter infrastructure is required to collect enough data to perform these analyses, and so we see the deployment of new systems with either built-in data collecting capabilities or the addition of such functions.

All of these steps potentially increases the attack surface available for bad actors to infiltrate the system and cause major disruption. It's now the top responsibility for security teams to reduce this risk and survive any attack that may come.

Resilience and the cyber-physical threat

"The character of cyberthreats has changed. Respondents now believe that cyber-attackers are more likely to focus on business disruption and reputational damage."

World Economic Forum 2023 Global Cyber Security Outlook

"When implementing cybersecurity requirements, grid and DER planners should build cyber defences with the goal of surviving an attack while maintaining critical functionality."

US Department of Energy

Attacks on energy companies fall into three distinct groups:

- Data theft of customer or business-critical information
- Generic ransomware that can be either directed or viral to attack information systems or operational technology
- A targeted cyber-physical attack on a specific system to cause maximum disruption

A large majority of these attacks will begin as phishing attacks and quickly propagate to their intended target. Reducing this movement can reduce the impact of an attack.

Challenges

High-profile cybersecurity requirements for essential services operators include:

- Identifying legacy and unknown IT and OT devices
- Mapping communications between applications, systems, and IT and OT devices
- Containing ransomware attacks
- Mitigating the risk of known and unknown vulnerabilities

The key to surviving any attack is to reduce the impact and to make sure that it doesn't reach the most critical parts of the network.

After some recent attacks, national regulators around the world are issuing new guidelines and directives for all areas of the energy market. This includes the AESCSF in Australia and the TSA directive on pipelines in the U.S.

Many regulators are recommending following the steps of the NIST Cybersecurity Framework:

1. **Identify**
   Illumio generates a simple map to show all devices and the flow of their communications to external computing resources, such as applications, servers, databases, the Internet, or even smart devices. With this knowledge, generating the required security policies is a much simpler process.

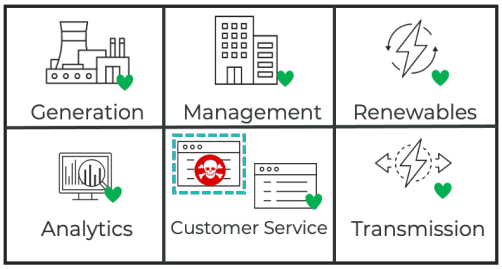
2. **Protect**
   To prevent the cross contamination of malware from IT to OT environments and vice versa, it is important to only allow communication between the necessary devices. With Illumio, you can block specific ports that cyberattackers and ransomware typically use.

   Any patching limitations can be managed by limiting the systems that can communicate and which protocols they use.

3. **Detect**
   Detecting an attack is key to neutralizing the threat — and the quicker the better. Segmenting the network is shown to improve the performance of endpoint detection and response (EDR) systems by restricting the spread of an attack, thereby reducing the area required for detection.

4. **Respond**
   Once an attack is detected, you must respond instantly. As soon as an attack starts, it needs to be stopped. With Zero Trust Segmentation (ZTS), you can effectively lock down attacks to help maintain services while the malware is removed.

5. **Restore**
   Security and IT teams can set up protection around individual departments and systems so they can resume operations while being shielded from the attack. With knowledge gained during the unsuccessful attack, you can tune your policies to further tighten access and boost your organization's cyber resilience.



Stop the spread of breaches

Secure your energy operation with ZTS

Go to: illumio.com/products

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.