Illumio for NERC CIP Compliance

Illumio's Zero Trust Segmentation makes it easy for critical infrastructure operators to comply with NERC cybersecurity requirements for establishing electronic security perimeters (ESP) and preventing unauthorized network access.

Strict Security Requirements for Critical Infrastructure

As part of its mission to ensure the reliability of the North American bulk power system, the nonprofit regulatory agency North American Electric Reliability Corporation (NERC) established the Critical Infrastructure Protection (CIP) plan.

Critical infrastructure organizations need to comply with all 9 sections of NERC CIP, including requirements for:

- **CIP-005: Electronic Security Perimeters**
  All critical cyber assets must reside within an electronic security perimeter (ESP). CI organizations should tightly control access to these assets. Organizations should block unauthorized access and detect malicious communications, whether inbound or outbound. They should also provide secure intermediate systems for remote access.
- **CIP-007: Cyber Security — Systems Security Management Requirements**
  Where feasible, only required network ports should be enabled. CI organizations should mitigate malicious code and log network events for at least 90 days.

Zero Trust Segmentation for Protecting CI Assets

Illumio Zero Trust Segmentation makes it easy for critical infrastructure organizations to implement the cybersecurity controls in sections 5 and 7 of the CIP plan.

Using Illumio, organizations can quickly generate an application dependency map showing all the communications taking place on their network and which communication pathways are required for legitimate business. They can then use Illumio's Policy Compute Engine (PCE) to define high-level policies, such as limiting access to critical assets to authorized users. The PCE generates detailed firewall rules enforcing these policies and pushes these rules out to the host-based firewalls built into the systems already deployed.

The result: fast, effective Zero Trust Segmentation that blocks all communications that aren't explicitly allowed, and the elimination of pathways that ransomware and other attacks rely on.

Fast, Effective Zero Trust Segmentation for NERC CIP Compliance

Illumio provides the visibility and control that organizations need for implementing CIP-compliant cybersecurity.

Visibility Into All Communications

Illumio shows which network traffic is required for operations. It also shows which ports and protocols to shut down to prevent malware attacks.

Automated Rule Creation and Enforcement

Once traffic is understood, it's easy to define policies allowing only legitimate traffic. Illumio converts these policies to firewall rules and distributes them for enforcement.

Instant Control for Mitigating Attacks

Should an attack manage to get through, operators can use Illumio to shut down traffic around compromised endpoints, containing the attack.

How Illumio Helps With CIP Compliance

CIP-005 Regulations	Illumio Capabilities
1.1 All applicable networked cyber assets shall reside in a defined ESP.	Illumio Core makes it easy to define ESPs and enforce firewall rules for including or excluding assets.
1.2 All external routable connectivity should pass through an identified Electronic Access Point (EAP).	Through Illumio policies, IT administrators can configure an endpoint as an EAP and route all external traffic through it.
1.3 The ESP requires inbound and outbound access permissions. Access should only be granted with reason. By default, all other access should be denied.	Illumio's Zero Trust model denies access by default and grants access based on the principle of least privilege.
1.5 ESPs should be about to detect known or suspected malicious traffic, whether inbound or outbound.	By analyzing metadata, Illumio detects anomalous traffic and raises alerts, which can be forwarded to a SIEM or other logging system.
2.1 For all interactive remote access, use an intermediate system so that the remote system does not have direct access to assets within the ESP.	With Illumio, all external communication can be routed to a proxy or jump host, preventing direct access to assets.

CIP-007 Regulations	Illumio Capabilities
1.1 Where feasible, support only logical ports required by assets.	Illumio maps traffic so IT teams can identify required ports. Policies can restrict traffic to just those ports.
1.2 Mitigate the threat of detected malicious code.	Illumio quickly contains malicious code by isolating affected hosts and blocking all communication methods the code would use to propagate.
4.1 Log events for identifying and investigating cybersecurity incidents.	Illumio raises alerts for a wide range of events, including failed or blocked communications and attempts at tampering with rules.
4.2 Where feasible, retain event logs for at least 90 days except under exceptional circumstances.	Illumio can save event logs for 90 days or longer.

Protect Critical Infrastructure From Ransomware and Other Cyberattacks

Learn more about how you can build your defenses against cyberattacks in a matter of days.

Speak with our Zero Trust security experts and visit www.illumio.com

About Illumio

Illumio is the leader of Zero Trust segmentation. See your risks, isolate attacks and secure your data to stop breaches from becoming cyber disasters.