# ACHIEVING NERC CIP COMPLIANCE THROUGH ZERO TRUST NETWORK ACCESS

## Introduction

Electric utilities and other operators of Bulk Electric Systems (BES) are under increasing pressure to protect their operational technology (OT) infrastructure against sophisticated cyber threats. The stakes are high—cyber events targeting industrial control systems can have serious consequences for grid reliability, safety, and critical services across North America.

As digital transformation increases connectivity across control centers, substations, and distributed energy resources, so does the risk surface. The North American Electric Reliability Corporation (NERC), under FERC authority, mandates that BES operators follow Critical Infrastructure Protection (CIP) standards to reduce cyber risks and uphold grid integrity.

Appgate Zero Trust Network Access (ZTNA) offers a modern, identity-centric solution that is purpose-built to secure remote and third-party access to sensitive OT systems—ensuring both compliance with NERC CIP standards and protection against real-world threats. Unlike traditional perimeter-based security or network anomaly detection platforms, Appgate directly enforces policy at the access layer, cloaking the underlying OT network resources and allowing only authorized users and devices to connect—under strict, context-aware conditions.

## Evolving Standards Demand Modern Access Controls

New and revised NERC CIP standards increasingly emphasize secure access, internal segmentation, and risk-based management of both high- and low-impact BES Cyber Systems:

**CIP-003-9 (Remote Access for Low Impact Systems):** Requires utilities to implement secure remote access controls for dispersed and diverse low-impact assets.

**Proposed Network Monitoring Standards:** Extend visibility and control expectations beyond the Electronic Security Perimeter (ESP) to internal zones, including systems with external routable connectivity.

**DER Integration:** As distributed energy resources (DERs) proliferate, regulators stress the need for strong authentication, access control, and segmentation tailored to modern, distributed power systems.

Appgate's ZTNA solution helps utilities meet these evolving requirements by enforcing least-privilege access, dynamically adapting to user, device, and contextual risk, and delivering granular visibility into who is accessing what, when, and why—without relying on traditional network inspection models.

## How Appgate Aligns with Key NERC CIP Standards

| NERC CIP Standard | Objective | Appgate ZTNA Capabilities | Support Level |
|---|---|---|---|
| **CIP-003-9:** Security Management for Low Impact Systems | Implement security controls for remote access to low-impact BES Cyber Systems | Enforces secure, policy-driven access to low-impact assets with MFA, device posture checks, and just-in-time provisioning | Complete |
| **CIP-005-7:** Electronic Security Perimeter | Control inbound/outbound access to ESPs | Establishes encrypted access only after trust is established via identity, device posture, time/location, and risk context | Complete |
| **CIP-007-6:** System Security Management | Protect BES Cyber Assets within the ESP | Segments access down to individual systems or ports, blocking unauthorized traffic by default | Complete |
| **CIP-010-4:** Configuration & Vulnerability Management | Monitor for unauthorized changes and vulnerabilities | Enhances security posture by minimizing attack surface and enforcing secure access methods that prevent unauthorized changes | Partial (focuses on prevention over detection) |
| **CIP-011:** Information Protection | Protect the confidentiality and integrity of sensitive information related to the BES | Protects sensitive information by using Appgate ZTNA's claims-based access controls to ensure that only authorized users can access sensitive data | Complete |
| **CIP-013-2:** Supply Chain Risk Management | Ensure vendors and third-party systems don't introduce cyber risk | Enables time-bound, fully cloaked access for approved vendors only under predefined conditions, with full session logging | Complete |

## Why Traditional Monitoring Tools Are Not Enough

While visibility and anomaly detection remain important, compliance with CIP-003 and CIP-005 standards increasingly requires proactive controls—not just passive observability. Monitoring-based platforms are designed to detect threats after network traffic has reached sensitive assets. Appgate takes a fundamentally different approach:

- **No Network-Level Visibility:** Appgate ZTNA cloaks all protected systems until access is explicitly granted based on identity and context.
- **Access Enforcement at the Edge:** Rather than inspecting traffic post-connection, Appgate ZTNA enforces policy before a session is ever established.
- **Granular Policy Engine:** Appgate's policies are identity-, device-, and time-aware, enforcing access by role, shift schedule, geolocation, or operational state.

With Appgate ZTNA, electric utilities and other operators gain a powerful tool to actively reduce their cyber risk footprint—and demonstrate enforceable compliance with CIP access control requirements.

### CRITICAL DIFFERENTIATOR

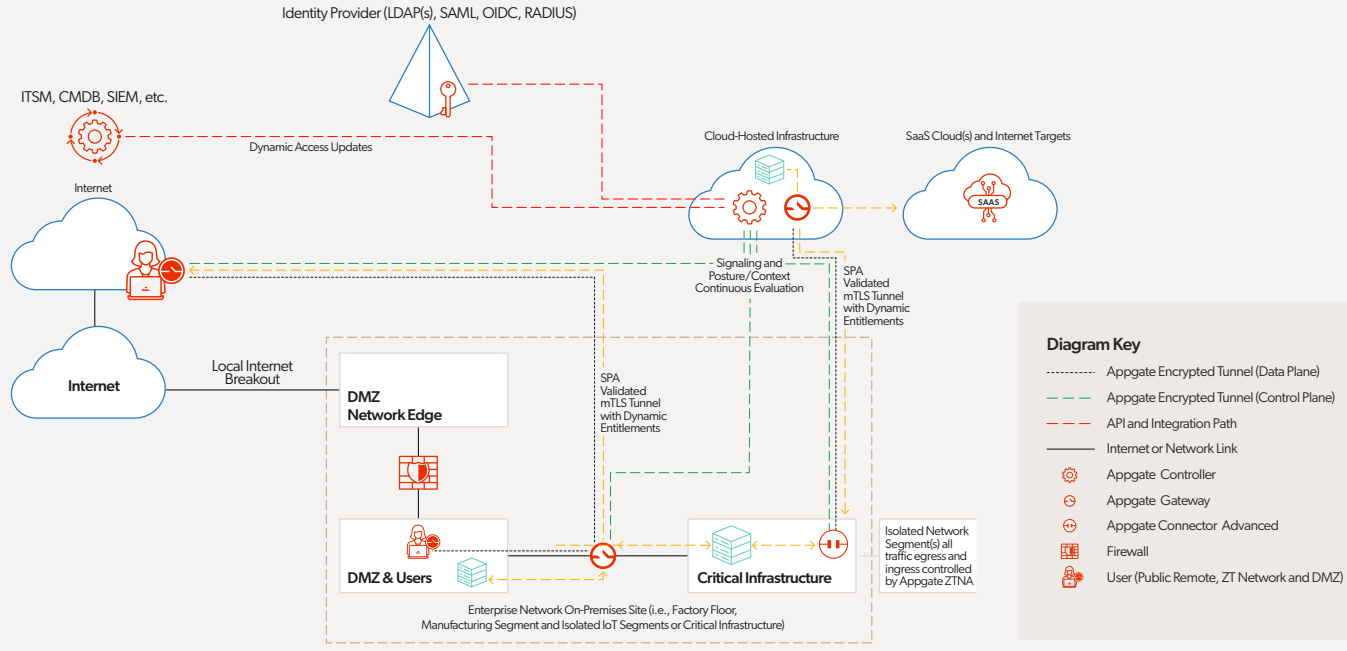
Appgate ZTNA doesn't just monitor your network for anomalies—it ensures untrusted users, devices, and systems can't even see what they're not allowed to access by leveraging Single Packet Authorization and cloaking technologies.

## Secure Remote Access for OT Environments

Whether supporting field technicians, substation contractors, or vendor support teams, Appgate ZTNA provides secure, direct-routed remote access to OT assets—without backhauling traffic through a central inspection point or requiring full network exposure.

**Key capabilities include:**

- **Single Packet Authorization (SPA):** Prevents unauthorized network probing by cloaking infrastructure until a valid request is received.
- **Identity-Centric Access:** Authenticates users via SSO, MFA, and device posture before authorizing access—eliminating static credentials or IP-based rules.
- **Just-in-Time Access Provisioning:** Dynamically creates access entitlements for specific timeframes and roles, then automatically expires them.
- **Session Logging and Auditing:** Captures detailed access session data to satisfy audit requirements and aid in forensic investigation.




Appgate's architecture for energy utilities delivers secure, identity-driven access with a direct-routed approach, minimizing attack surfaces while ensuring performance and reliability.

## Operationalizing Compliance: Best Practices

To effectively operationalize NERC CIP compliance in modern OT environments, utilities should adopt a series of targeted Zero Trust best practices. Begin by prioritizing protections for low-impact assets, such as DERs and substations, which are subject to stricter classifications under the 2025 NERC CIP revisions. Appgate ZTNA's adaptive access policies make it easy to apply granular controls to these systems without introducing unnecessary complexity. Bridging the IT and OT security divide is also essential—Appgate ZTNA enables secure, identity-based access across segmented environments, air-gapping critical assets while maintaining operational continuity. Automation plays a vital role in reducing audit fatigue: with built-in session logging and real-time dashboards, Appgate streamlines evidence collection and response during Compliance Monitoring and Enforcement Program (CMEP) audits. Lastly, organizations should modernize third-party access strategies by replacing legacy VPNs with policy-based Zero Trust controls that enforce device health, identity verification, and geolocation requirements before access is granted.

### OT-READY ACCESS ARCHITECTURE

Appgate ZTNA integrates seamlessly with jump servers, engineering workstations, and segmented SCADA zones—without requiring network redesign or inline appliances.

## Conclusion

NERC CIP compliance requires more than passive monitoring—it demands real-time, enforceable controls that align with Zero Trust principles. As standards evolve to account for increasingly distributed and dynamic operational environments, traditional detection-focused tools are no longer sufficient.

Appgate ZTNA is purpose-built to meet these demands with a secure, scalable, and highly performant approach to access control. It empowers utilities to:

- Securely enable remote and third-party access
- Reduce the OT attack surface through cloaking and segmentation
- Comply with evolving NERC CIP access control standards
- Increase operational flexibility without sacrificing security

By adopting Appgate ZTNA as part of a Zero Trust OT security strategy, critical infrastructure operators can confidently modernize their security posture—while ensuring uninterrupted, compliant operations.

### ABOUT APPGATE

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

appgate