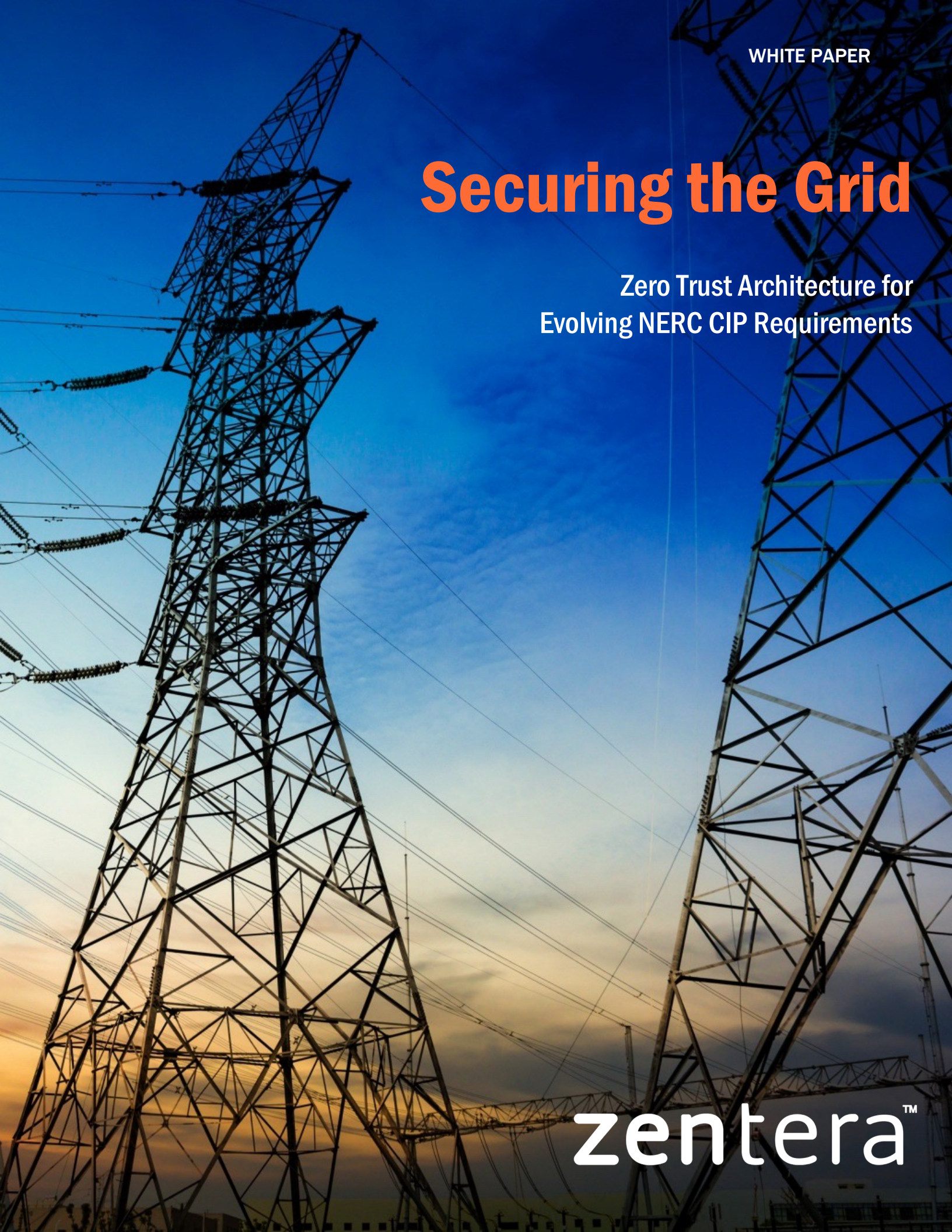


WHITE PAPER

Securing the Grid

Zero Trust Architecture for Evolving NERC CIP Requirements

zentera™

Executive Summary

As state-sponsored threat actors like Volt Typhoon actively target U.S. critical infrastructure with sophisticated "living off the land" techniques, and as NERC introduces more stringent requirements through CIP-015 (Internal Network Security Monitoring) and CIP-005-8 (Logical Isolation), electric utilities face an urgent dual challenge: defending against increasingly sophisticated attacks while adapting to rapidly evolving compliance mandates.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are evolving beyond traditional perimeter-based security toward comprehensive, identity-centric protection at every connection point. This shift requires utilities to reimagine their approach to cybersecurity without compromising the operational reliability that remains paramount to their mission.

Zentera's Zero Trust framework directly addresses this transition, providing a solution that not only meets current CIP requirements but anticipates and prepares for upcoming regulatory changes. Through non-disruptive deployment options that protect even legacy OT systems, granular policy enforcement, and centralized management, Zentera enables utilities to strengthen their security posture and streamline compliance efforts while preserving operational reliability across IT/OT environments.

This document demonstrates how Zentera's Zero Trust architecture and micro-segmentation capabilities align with core CIP technical requirements while providing a clear path to compliance with emerging standards – including CIP-005 (Electronic Security Perimeters), CIP-007 (Systems Security Management), CIP-011 (Information Protection), CIP-012 (Communications between Control Centers), and the forthcoming CIP-015 (Internal Network Security Monitoring).

The Evolving Landscape of NERC CIP Requirements

NERC CIP standards establish mandatory cybersecurity controls for electric utilities to protect critical assets tied to the Bulk Electric System. These standards continuously evolve to address emerging threats, with recent and upcoming changes signaling a clear shift toward defense-in-depth and zero trust principles.

Current Core Requirements

CIP-005 (Electronic Security Perimeters)
- Defines Electronic Security Perimeters (ESPs) around critical cyber assets
- Requires default-deny rules at perimeter access points
- Mandates secure, logged, and multi-factor authenticated interactive remote access

CIP-007 (Systems Security Management)
- Focuses on minimizing attack surface through disabling unnecessary ports/services
- Requires timely patching, malware protection, and detailed event logging
- Mandates strong access controls at the system level

CIP-011 (Information Protection)
- Enforces confidentiality of sensitive data, including encryption in transit
- Requires secure handling and disposal of sensitive information

CIP-012 (Communications between Control Centers)
- Requires securing real-time operational data in transit between control centers

CIP-013 (Supply Chain Risk Management)
- Addresses vendor-related risks, including remote access controls
- Requires notification processes for vendor product vulnerabilities

Critical Emerging Updates

CIP-015 (Internal Network Security Monitoring)
- Introduces requirements for monitoring traffic inside the ESP to detect malicious activity
- Timeline: 36 months for high-impact systems and 60 months for medium-impact systems after approval
- Driven by recognition that perimeter breaches can lead to undetected lateral movement

CIP-005-8 (Logical Isolation)
- Moves away from purely physical perimeter concepts toward logical isolation
- Provides flexibility to accommodate zero trust architectures
- Recognizes the reality of hybrid cloud / on-premises environments

The Regulatory Shift: From Perimeters to Zero Trust

The evolution of CIP standards reflects a fundamental shift in cybersecurity thinking from "trust everything inside the perimeter" to "never trust, always verify." This has been driven by:

1. Advanced Persistent Threats: State-sponsored actors like Volt Typhoon have demonstrated the ability to bypass traditional perimeters and move laterally within networks.

2. Hybrid IT/OT Environments: As utilities adopt cloud services and enable remote operations, the concept of a fixed perimeter becomes increasingly obsolete.

3. Supply Chain Vulnerabilities: Recent incidents have highlighted how trusted vendor connections can become attack vectors if not properly secured and monitored.

For utility cyber architects, this regulatory evolution demands a new approach that goes beyond traditional firewalls and VLANs while still satisfying the rigorous documentation and evidence requirements of NERC CIP compliance.

Zentera's Zero Trust Architecture: Built for Critical Infrastructure

Zentera's approach to Zero Trust involves application-level microsegmentation and identity-centric access enforcement specifically designed to address the challenges of securing critical infrastructure. The architecture recognizes the unique constraints of OT environments, including legacy systems, reliability requirements, and the need for non-disruptive implementation.

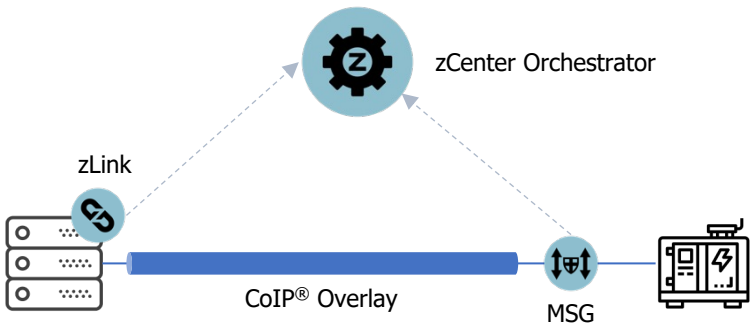
Core Components

Microsegmentation Gatekeeper (MSG)
- Hardware appliance that enforces per-workload segmentation and access control
- Deploys transparently inline with legacy OT devices without modifying them
- Hardware fail-open capability to ensure operational continuity in failure scenarios

zLink Agent
- Software-based policy enforcement point for bare metal servers, virtual machines, and cloud instances
- Application-aware segmentation and access control

zCenter Orchestrator
- Creates logical "secure bubbles" spanning on-premises, cloud, and hybrid networks
- Integrates with corporate identity management (AD/LDAP/SAML) and supports multi-factor authentication
- Defines who can access which resource under what conditions and logs access for compliance evidence
- Provides centralized visibility and control across distributed environments

CoIP® Overlay
- Overlay fabric that encrypts traffic, enforces identity-based policies, and brokers connections
- Routes remote sessions via an "intermediate system" consistent with CIP-005
- Overlays existing infrastructure without requiring network reconfiguration



Key Design Principles for Utilities

Non-Disruptive Deployment
Zentera's architecture can overlay existing utility networks without requiring reconfiguration of critical systems, preserving operational reliability while enhancing security.

Agentless Protection for Legacy OT
Many CIP-critical devices (PLCs, RTUs, relays) cannot be modified. Zentera's Gatekeeper can protect these systems without installing agents, closing a critical security gap.

Defense-in-Depth by Design
Rather than replacing existing security controls, Zentera adds a layer of identity-based microsegmentation that complements traditional perimeter defenses.

Centralized Policy, Distributed Enforcement
Security policies are defined centrally but enforced at each connection point, ensuring consistent protection across distributed environments.

Scalability Across Hybrid Environments
The architecture extends consistently from substations to control centers to cloud environments, providing uniform security across increasingly hybrid utility infrastructures.

Zentera's Alignment with NERC CIP Requirements

CIP-005: Electronic Security Perimeters

CIP-005 Requirement	Zentera's Implementation	Compliance Benefit
R1.1-R1.3: Electronic Security Perimeter	Microsegmentation creates logical isolation around protected assets	Creates "virtual ESPs" that can be documented as defined electronic boundaries
R1.3: Default Deny Posture	Zero Trust architecture enforces explicit allow policies; all other traffic is blocked	Exceeds requirement by enforcing default-deny at the workload level, not just at perimeter
R1.5 ("615"): Detect Malicious Communications	Connection logging, policy enforcement, and integration with security monitoring tools	Creates comprehensive detection capabilities for both inbound and outbound traffic
R2.1-R2.3: Interactive Remote Access	Provides secure methods of access to a jump host, including ssh and virtual desktops to satisfy the requirement for an "intermediate system"	Simplifies compliance by integrating remote access, MFA, and encryption in one solution

Beyond Compliance

While traditional approaches focus on perimeter firewalls, Zentera's microsegmentation extends protection to each asset, anticipating CIP-005-8's shift toward logical isolation and providing deeper protection against lateral movement.

Deep Dive: CIP-005-6 R1.5 Compliance

CIP-005-6 R1.5 specifically requires utilities to implement methods to detect known or suspected malicious communications for both inbound and outbound communications across the ESP boundary. This is a critical requirement focused on identifying potential attacks and data exfiltration attempts.

Zentera's Zero Trust architecture addresses this requirement through multiple mechanisms:

Microsegmentation as a Detection Framework

- By enforcing a default-deny posture, any unauthorized connection attempt is automatically logged and can be flagged as suspicious
- Connection attempts outside of defined policies are immediately detected, providing early warning of potential malicious activity
- Both inbound threats (attacks) and outbound communications (potential data exfiltration or command-and-control traffic) are captured

Identity-Based Anomaly Detection

- Zentera's identity-centric policies can identify when a legitimate system attempts to communicate in ways inconsistent with its defined role
- Even if attackers compromise valid credentials, they remain limited to authorized actions; attempts outside these boundaries trigger alerts
- This approach effectively detects "suspicious" behavior, not just known threat signatures

Enhanced Monitoring Through Traffic Reduction

- By limiting traffic to only authorized flows, Zentera dramatically reduces "noise" that might hide malicious activity
- Integration with SIEM platforms and security analytics tools creates a powerful detection ecosystem
- Denial logs provide critical insights for security teams to identify patterns of potentially malicious behavior

Comprehensive Outbound Protection

- Zentera controls outbound connections, preventing compromised devices from freely connecting to external command-and-control servers
- Unauthorized outbound connection attempts are logged and can trigger alerts, satisfying the outbound monitoring requirement of R1.5
- This capability is especially valuable for detecting lateral movement and exfiltration attempts

Traditional compliance approaches for CIP-005-6 R1.5 often rely solely on perimeter IDS and network monitoring solutions. Zentera's approach provides more granular detection capabilities by enforcing policies at each protected endpoint or segment, creating multiple detection points throughout the environment.

CIP-007: Systems Security Management

CIP-007 Requirement	Zentera's Implementation	Compliance Benefit
R1: Ports and Services	Gatekeeper or zLink agent effectively closes unused ports by blocking unauthorized traffic	Addresses requirement to disable unnecessary logical ports without modifying legacy devices
R2: Security Patch Management	While not handling patching directly, microsegmentation limits exploit scope for unpatched systems	Provides compensating control while formal patch programs are executed
R4: Security Event Monitoring	Logs policy changes, connection events, and suspicious attempts	Generates required security events for monitoring and analysis
R5: System Access Controls	Enforces identity-based access to systems based on roles	Supplements system-level access controls with network-level enforcement

Beyond Compliance

Traditional approaches require modifying each system to disable ports or implement controls. Zentera offers not only agent-based approaches for modern systems, but also agentless hardware to protect systems that cannot be modified, addressing a critical gap in many utility environments.

CIP-011 & CIP-012: Information and Communications Protection

CIP Requirement	Zentera's Implementation	Compliance Benefit
CIP-011-2: Information Protection	CoIP overlay encrypts sensitive data in transit	Ensures protection of BES Cyber System Information during transit
CIP-012-1: Control Center Communications	Encrypted tunnels between control centers	Secures data in transit with encryption and integrity checking

Beyond Compliance

Rather than point-to-point encryption solutions, Zentera provides consistent, policy-driven protection for all sensitive communications, simplifying compliance across multiple types of data flows.

CIP-013: Supply Chain Risk Management

CIP-013 Requirement	Zentera's Implementation	Compliance Benefit
R1.2.6: Vendor Remote Access	Time-limited, authorized-only vendor access with MFA	Restricts vendor access to only specified devices for specific durations
R1.2.6: Vendor Access Monitoring	Complete audit trails of all vendor activities	Provides documented evidence of third-party access

Beyond Compliance

Traditional vendor access management often relies on VPNs with broad network access. Zentera's approach restricts vendors to only the specific systems they need to access, significantly reducing supply chain risk.

Preparing for Emerging Requirements

Emerging Requirement	Zentera's Implementation	Strategic Benefit
CIP-015: Internal Network Monitoring	Granular logging of connection attempts provides visibility into network activity	Forms foundation for comprehensive internal monitoring strategy
CIP-005-8: Logical Isolation	Identity-based overlays create logical isolation without physical separation	Already aligned with the direction of CIP evolution toward logical controls

Strategic Advantage

By implementing Zentera now, utilities gain compliance with current requirements while building the foundation for emerging standards, avoiding costly retrofits as regulations evolve.

Comparative Analysis: Zero Trust Architecture vs. Traditional Approaches

When evaluating security architectures for NERC CIP compliance, utilities must consider how different technological approaches align with both current requirements and emerging standards:

Traditional Perimeter-Focused Security

Approach
- Network-centric defense relying primarily on firewalls at ESP boundaries
- VLAN segmentation for network separation
- VPNs and jump servers for remote access

CIP Alignment
- Strong for traditional ESP boundaries (CIP-005 R1)
- Requires extensive firewall rule management
- Typically requires separate solutions for remote access, monitoring, and encryption

Operational Considerations
- Often requires network redesign and reconfiguration
- Can be difficult to extend to legacy OT systems
- Creates potential single points of failure at perimeter

Future-Readiness
- Limited ability to address CIP-015's internal monitoring requirements
- May require significant updates to align with CIP-005-8 logical isolation concepts
- Struggle to adapt to increasing hybrid cloud/on-premises environments

Zero Trust Architecture

Approach
- Identity-centric defense enforcing access based on who, not where
- Microsegmentation creating virtual chambers around individual assets
- Universal ZTNA integrating access control, encryption, and monitoring

CIP Alignment
- Addresses CIP-005 through logical isolation and default-deny
- Supports CIP-007 by limiting attack surface without modifying systems
- Inherently aligns with CIP-011/012 through encrypted overlay
- Facilitates CIP-013 through granular vendor access control

Operational Considerations
- Overlay approach minimizes disruption to existing infrastructure
- Agentless options protect legacy systems without modification
- Can be deployed incrementally, starting with most critical assets

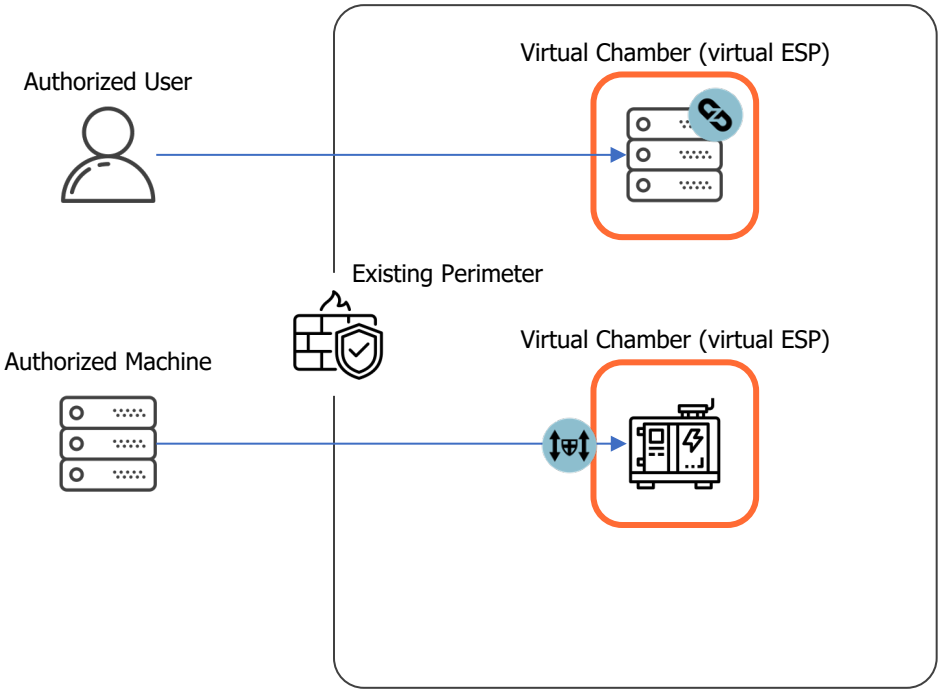
Future-Readiness
- Already embodies the "logical isolation" principles in CIP-005-8
- Provides foundation for CIP-015 internal monitoring
- Adapts readily to hybrid environments

Defense-in-Depth: The Optimal Approach

Traditional security tools continue to have value, but to meet the challenges of modern threat actors, utilities must find ways to scale up security. With traditional network security models already at the breaking point, the most effective strategy for utilities to scale is to combine existing perimeter defenses with Zero Trust principles in a defense-in-depth architecture:

1. Maintain perimeter controls for broad threat protection and compliance with current interpretations of CIP-005
2. Place critical assets in virtual chambers with microsegmentation to protect against lateral movement and prepare for CIP-005-8
3. Add Universal ZTNA to tie all accesses to user-, machine-, and software-identities
4. Deploy agentless protection for legacy systems that cannot be modified

This layered approach satisfies current compliance requirements while building the foundation for emerging standards, all while minimizing operational disruption.



New security controls overlay existing ones, adding a new layer of protection against malicious actors and insider threats

Mounting Urgency: Threats and Regulatory Timelines

The Evolving Threat Landscape

The urgency for utilities to move beyond perimeter-focused security has never been greater. Recent developments highlight the inadequacy of traditional approaches:

State-Sponsored Threats Targeting Critical Infrastructure

- Volt Typhoon: This Chinese state-sponsored actor has been actively targeting U.S. critical infrastructure since at least mid-2021. Unlike previous threats, Volt Typhoon specifically focuses on infrastructure that would enable high-impact operations during a conflict.
- Living Off the Land Techniques: Modern attackers use legitimate tools and credentials to bypass traditional defenses, making lateral movement detection critical.
- Supply Chain Compromises: Recent incidents have shown how trusted vendor connections can become attack vectors if not properly secured and monitored.

Lessons from Recent Incidents

- Attackers are increasingly targeting operational technology after gaining initial access through IT networks
- Lateral movement often goes undetected for extended periods
- Traditional perimeter defenses struggle against sophisticated threats using legitimate credentials

The CIP-005-6 R1.5 Challenge

- The requirement to detect malicious communications (both inbound and outbound) is increasingly difficult to satisfy with traditional monitoring approaches
- Advanced threats like Volt Typhoon are designed to evade signature-based detection systems
- The volume of traffic crossing ESP boundaries continues to grow, creating "noise" that can hide malicious activity
- Outbound communication from compromised systems is particularly challenging to detect without identity-based controls
- Modern attack techniques often use legitimate channels and credentials, requiring more sophisticated detection capabilities

Regulatory Timeline and Compliance Pressure

NERC CIP standards continue to evolve, with several critical deadlines approaching:

CIP-015 (Internal Network Security Monitoring)

- Filed with FERC in 2024
- Implementation timeline after approval:
- High-impact BES Cyber Systems: 36 months
- Medium-impact BES Cyber Systems: 60 months
- Utilities should begin planning now to meet these requirements

CIP-005-8 (Logical Isolation)

- Draft development underway
- Shifts focus from physical perimeters to logical isolation
- Will require documentation of logical isolation mechanisms

Enforcement and Penalties
- NERC CIP violations can result in penalties up to $1 million per violation per day
- Recent enforcement actions demonstrate increased scrutiny of network security controls
- Self-reported issues receive more favorable treatment than those discovered during audits

The combination of escalating threats and evolving regulations creates clear urgency for utilities to modernize their approach to cybersecurity while maintaining rigorous compliance documentation.

Implementation Roadmap: From Traditional Security to Zero Trust

Implementing Zentera's Zero Trust architecture can follow a phased approach that minimizes disruption while progressively enhancing both security and compliance posture:

Phase 1: Assessment and Planning (Months 1-2)

Key Activities
- Map current environment and communications patterns
- Document existing CIP compliance controls and potential gaps
- Develop phased implementation plan starting with critical assets
- Create detailed compliance mapping between Zentera capabilities and CIP requirements

Compliance Focus
- Baseline documentation of existing ESP configurations
- Identify areas where additional controls are needed for emerging requirements

Phase 2: Controlled Pilot (Months 2-3)

Key Activities
- Deploy Zentera in a controlled environment (test lab or isolated substation)
- Validate functionality against CIP controls
- Test remote access, monitoring, and policy enforcement
- Document procedures and gather compliance evidence

Compliance Focus
- Validate that Zentera logs provide necessary evidence for CIP-005 and CIP-007
- Develop compliance documentation templates
- Test integration with existing security monitoring

Phase 3: Critical System Protection (Months 3-6)

Key Activities:
- Deploy Zentera to protect high-impact BES Cyber Systems
- Implement agentless protection for legacy OT systems
- Configure secure remote access for operations and vendors
- Integrate with existing security monitoring and SIEM

Compliance Focus
- Update ESP documentation to incorporate Zentera controls
- Develop evidence collection procedures for audits
- Classify Zentera components as Electronic Access Control and Monitoring Systems (EACMS)

Phase 4: Enterprise-Wide Deployment (Months 6-12)

Key Activities
- Extend protection to medium-impact and low-impact systems
- Implement additional use cases (cloud connectivity, vendor access)
- Optimize policies based on operational experience
- Train staff on operations and maintenance

Compliance Focus
- Comprehensive documentation update across CIP-005, CIP-007, CIP-011, CIP-013
- Prepare for CIP-015 by enhancing monitoring capabilities
- Develop procedures for change management (CIP-010)

Phase 5: Continuous Improvement (Ongoing)

Key Activities:
- Regular policy reviews and updates
- Integration with new systems and environments
- Monitoring and response to emerging threats
- Preparation for evolving CIP standards

Compliance Focus:
- Keep compliance documentation current with system changes
- Periodic testing and assessment
- Alignment with updated standards and requirements

This phased approach allows utilities to implement Zero Trust principles at a pace that aligns with operational constraints while methodically enhancing compliance posture.

A 9 Step Program: Actionable Recommendations for Utility Cybersecurity Architects

1. Map Zentera Capabilities to CIP Requirements

Create a compliance matrix showing exactly how each CIP requirement is addressed by specific Zentera capabilities. This documentation will be invaluable during audits to demonstrate a cohesive compliance strategy. For example:

1. CIP-005 R1.3 (Default Deny): Zentera policies enforce explicit allow-only rules
2. CIP-005 R1.5 ("615" - Malicious Communications Detection): Zentera logs and blocks unauthorized connection attempts
3. CIP-005 R2.1 (Intermediate System): Zentera-enabled jumphosts serve as the intermediate systems
4. CIP-007 R1 (Ports and Services): Zentera blocks unauthorized access to ports without modifying devices

2. Integrate with Existing Security Architecture

Design Zentera deployment to complement rather than replace existing security controls:

1. Maintain perimeter firewalls as outer defense layer
2. Feed Zentera logs to SIEM for correlation with other security events
3. Align Zentera's user authentication with corporate identity management
4. Consider how Zentera will interact with existing jump servers, VPNs, and access control systems

3. Prioritize Protection for Legacy OT Systems

Identify critical OT systems that cannot be modified with traditional security controls:

- Deploy agentless MSG appliances to protect legacy PLCs, RTUs, and relays
- Create virtual chambers around control system components
- Implement strict access controls for vendor connections to these systems
- Document how Zentera addresses the security gaps in legacy systems

4. Create Policies Defining Expected Traffic Flows

Leverage Zentera to strengthen your implementation of CIP-005-6 R1.5 requirements:

- Leverage Zentera to observe existing inbound and outbound traffic flows
- Use Learn capabilities to implement comprehensive inbound and outbound traffic policies
- Configure alerts for denied connection attempts, which represent potential malicious communication
- Document how Zentera's logs provide evidence of malicious communication detection
- Integrate Zentera logs with SIEM or security analytics platforms to identify patterns of suspicious activity

5. Design for High Availability

Ensure Zentera deployment maintains the reliability requirements of critical infrastructure:

- Deploy Gatekeepers in redundant pairs where appropriate
- Document failover procedures for CIP-009 recovery plans
- If using hardware bypass options, document when and how they operate
- Test and validate high-availability configurations before full deployment

6. Develop Audit-Ready Evidence Collection

Establish processes to gather and maintain compliance evidence from Zentera:

- Create regular reports of access attempts and policy changes
- Document quarterly reviews of access permissions
- Maintain historical logs for the required retention periods
- Prepare demonstrated procedures for audit day

7. Train Operations and Security Teams

Ensure all relevant personnel understand the new architecture:

- Train operators on secure access procedures
- Educate security teams on monitoring and incident response
- Provide compliance teams with documentation for audit preparation
- Create quick reference guides for common tasks

8. Establish Governance Processes

Develop clear governance around the Zero Trust implementation:

- Define roles and responsibilities for policy management
- Establish change control procedures aligned with CIP-010
- Create review cycles for access policies
- Document exception handling processes

9. Plan for Future Evolution

Design implementation with flexibility for evolving requirements:

- Document how Zentera positions the utility for CIP-005-8 compliance
- Establish roadmap for enhancing internal monitoring capabilities
- Consider how emerging threats might influence future configurations
- Maintain awareness of regulatory developments and adjust strategy accordingly

By following these recommendations, utilities can implement a Zero Trust architecture that enhances security, streamlines compliance, and prepares for evolving requirements while maintaining the operational reliability essential to the grid.

Conclusion: The Path Forward

The electric utility sector stands at a critical juncture where traditional security approaches are increasingly inadequate against sophisticated threats, while regulatory requirements continue to evolve toward more comprehensive protection models. The combination of active state-sponsored threats targeting critical infrastructure and the development of new standards like CIP-015 and CIP-005-8 creates clear urgency for utilities to modernize their cybersecurity architecture.

Zentera's Zero Trust approach directly addresses this dual challenge by providing:

Enhanced Security Posture
Microsegmentation and identity-based access control limit lateral movement and reduce attack surface, even for legacy systems that cannot be modified.

Streamlined Compliance
Alignment with current CIP requirements while building the foundation for emerging standards, reducing future retrofit costs.

Operational Continuity
Non-disruptive deployment options and high-availability features ensure that security enhancements don't compromise reliability.

Future-Readiness
An architecture that already embodies the "logical isolation" principles that CIP standards are evolving toward, positioning utilities ahead of regulatory changes.

By implementing Zentera's Zero Trust architecture, utilities can move beyond the limitations of perimeter-focused security while maintaining rigorous compliance with NERC CIP requirements. The result is a more resilient grid, better protected against emerging threats and prepared for the evolving regulatory landscape.

The time to act is now. With Volt Typhoon and similar threats actively targeting U.S. critical infrastructure, and with CIP-015 implementation deadlines approaching, utilities that proactively implement Zero Trust principles will be better positioned both to defend against attacks and to demonstrate compliance during audits.

Zentera provides a clear path forward, allowing utilities to enhance security incrementally without disrupting the reliable operations that remain their primary mission.

References

NERC CIP-005, CIP-007, CIP-011, CIP-013 – Official Reliability Standards
NERC White Paper: "Zero Trust Security for Electric Operational Technology"
CISA Advisory on Volt Typhoon – Alert AA23-144A
DOE Office of Cybersecurity, Energy Security, & Emergency Response – CESER Website
CISA Cybersecurity Performance Goals – CISA CPGs

About Zentera

Zentera Systems is the leader in Zero Trust Security solutions for the digitally-transformed enterprise. Founded by experts in networking, security, and remote access, we offer award winning Zero Trust networking, security, and multi-cloud connectivity that overlays any fragmented infrastructure and deploys rapidly on premises or as a service.

Our global enterprise customers and network of partners use our products to secure employee and third-party access, protect against data leaks, and instantly defend applications in complex hybrid and IT/OT environments. Based in Silicon Valley, we have received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.

zentera™

www.zentera.net

sales@zentera.net

+1 (408) 436-4811

Copyright© 2025 Zentera Systems, Inc. All rights reserved. Zentera®, Zentera CoIP®, CoIP®, and certain other marks are registered trademarks of Zentera Systems, Inc., in the U.S. and other jurisdictions, and other Zentera names herein may also be registered and/or common law trademarks of Zentera. All other product or company names may be trademarks of their respective owners.