appgate

APPGATE ZTNA: SECURING THE ENERGY SECTOR WITH ZERO TRUST

The energy sector faces escalating cybersecurity threats that jeopardize critical infrastructure and reliable energy delivery. Appgate ZTNA offers a transformative Zero Trust approach to mitigate these risks by providing identity-centric access and granular access controls to ensure users can connect to business-critical applications without negatively impacting the business.

Overview

The energy sector is undergoing a profound digital transformation, integrating smart grids, IoT devices, and cloud computing to enhance efficiency and responsiveness. However, this evolution introduces new vulnerabilities that legacy security models cannot adequately address. Appgate ZTNA is a Zero Trust Network Access solution that brings a transformative approach to cybersecurity, securing critical assets, minimizing the attack surface, and enabling business continuity. This solution brief provides an overview of how Appgate ZTNA can help energy organizations modernize their security posture and protect against sophisticated cyber threats.

Navigating the Complex Cybersecurity Landscape

Appgate ZTNA enables organizations to achieve true Zero Trust by providing:

- **Critical Infrastructure Protection:** Energy systems are vital to public safety, healthcare, and the economy, making them prime targets for cyberattacks.
- **IT/OT Convergence:** Integration of IT and operational technology (OT) networks creates new attack vectors, potentially exposing critical operational systems to cybercriminals.
- **Remote Access Requirements:** The need for remote monitoring and management increases vulnerability points if access is not properly secured.
- **Expanding Attack Surface:** The proliferation of smart grid technologies and IoT devices introduces new points of vulnerability.
- **Legacy Systems:** Many energy companies rely on outdated systems, increasing vulnerability. Upgrading or securing these systems without disrupting operations presents a challenge.

Building a Resilient Energy Cybersecurity Defense

To effectively address these multifaceted cybersecurity threats impacting the protection of power generation, transmission, smart grids, and reliable energy delivery, the energy sector is prioritizing several strategic pillars:

1. **Defense-in-Depth:** Implement multi-layered security measures, including strong authentication, endpoint detection and response (EDR), and security information and event management (SIEM).
2. **Least Privilege Access:** Ensure users and systems have only the minimum permissions necessary, conducting regular access reviews.
3. **Continuous Monitoring and Threat Intelligence:** Employ real-time monitoring and integrate threat intelligence feeds for prompt threat identification and response.
4. **Compliance with Industry Standards:** Adhere to standards like NERC CIP and ISA/IEC 62443.

KEY BENEFITS

By implementing Appgate ZTNA, energy companies can achieve:

ENHANCED SECURITY POSTURE
Renders the underlying infrastructure invisible to unauthorized users via single packet authorization.

IMPROVED OPERATIONAL RESILIENCE
Ensures service continuity during disruptions.

SIMPLIFIED ACCESS MANAGEMENT
Streamlines access control across networks.

ENABLE UNIFIED IT AND OT SECURITY
Provide multiple collectives and air-gap IT from OT within the same solution.

MAINTAIN COMPLIANCE
Compliance with industry standards and regulations.

Appgate's ZTNA: A Strategic Imperative for the Energy Sector

Zero Trust Network Access (ZTNA) represents a strategic evolution to mitigate these risks, establishing a "never trust, always verify" framework that dynamically validates every access request. By mandating rigorous authentication and authorization for each user and device, ZTNA ensures that access to sensitive systems is granted only to verified and authorized entities. Appgate ZTNA is purpose-built to address these challenges. Key features include:

- **Dynamic 1:1 Network Connections:** Creates one-to-one network connections that are invisible to unauthorized users.
- **Granular Access Control:** Ensures authorized access to resources with policies adapting to risk levels.
- **High-Performance Architecture:** Utilizes direct-routed architecture for low-latency access.
- **Enterprise Readiness:** Integrates with IT/OT infrastructure and security components.
- **Scalability and Flexibility:** Adapts to evolving needs, supporting secure access for growing infrastructure.

Securing the Future of Energy with Zero Trust

To safeguard critical infrastructure and ensure reliable delivery in this evolving landscape, a Zero Trust security model is a necessity. Appgate ZTNA offers a comprehensive approach to securing critical energy systems. As cyber threats evolve, adopting a Zero Trust approach is not just advisable but imperative.

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 ZTNA 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