MEETING TSA SECURITY DIRECTIVE (SD) PIPELINE-2021-02D REQUIREMENTS

Ensuring Compliance and Securing Critical Pipeline Infrastructure with Appgate Zero Trust Network Access (ZTNA)

Introduction: TSA SD-Pipeline-2021-02D

On July 26, 2023, the Transportation Security Administration (TSA) issued an update to the Pipeline 2021-02 series directives in response to the growing wave of cyber threats targeting the critical energy infrastructure sector. The updated directive, TSA SD-Pipeline-2021-02D, mandates enhanced cybersecurity measures to safeguard pipeline systems against increasingly sophisticated cyberattacks.

This directive builds upon lessons learned from previous years, including the high-profile Colonial Pipeline Company ransomware attack on a major U.S. pipeline operator in 2021, which led to operational downtime, fuel shortages, and widespread economic disruption. That event underscored the devastating impact of cyber threats on both private enterprises and national security, catalyzing the need for stronger collaboration between the Department of Homeland Security (DHS), TSA and the Cybersecurity and Infrastructure Security Agency (CISA).

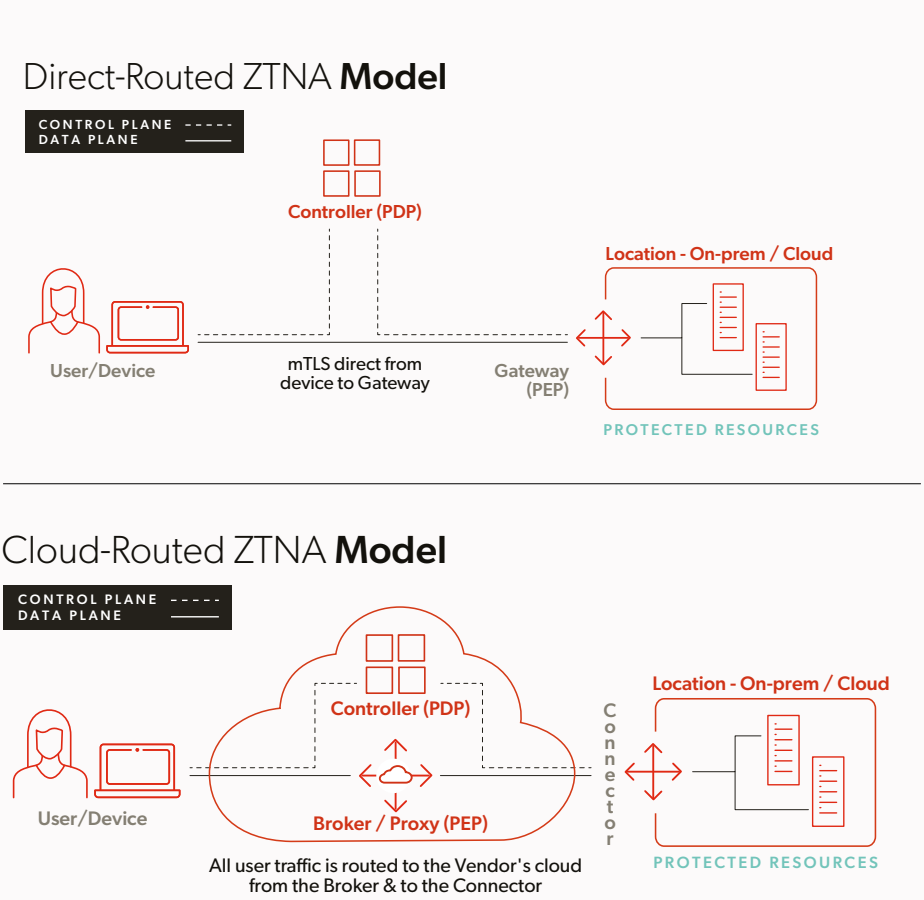
The latest directive introduces performance-based measures that emphasize proactive defenses, including robust access control, continuous monitoring and incident response capabilities. Key requirements such as multi-factor authentication (MFA), implementation of Zero Trust security principles and ongoing network monitoring aim to reduce vulnerabilities, protect critical assets, and ensure operational resilience. The TSA also highlights the importance of aligning with industry standards like the National Institute of Standards and Technology (NIST) cybersecurity framework and ISA/IEC 62443, offering operators flexibility in meeting these stringent cybersecurity objectives.

This evolution of pipeline security directives reflects the heightened need for a dynamic, risk-based approach to defending critical infrastructure in an increasingly interconnected and threat-laden digital landscape.

The Solution: Appgate Zero Trust Network Access (ZTNA)

Appgate delivers a robust ZTNA solution purpose-built to address the unique challenges of securing critical infrastructure, including pipeline systems. By minimizing attack surfaces and enforcing granular, identity-centric access controls, Appgate ensures that only authorized users and devices can access specific resources based on identity, device posture, and contextual factors such as location and time.

Appgate's direct-routed architecture revolutionizes secure access by bypassing the inefficiencies of cloud-routed solutions, which funnel traffic through centralized inspection points. Instead, Appgate establishes secure, direct point-to-point data paths between users and resources, minimizing latency, reducing bandwidth costs and enhancing network performance. For pipeline environments and other critical infrastructure, where uptime and operational efficiency are vital, this model ensures systems remain available, resilient and protected against evolving threats.



Appgate's direct-routed architecture establishes secure, efficient connections between users and resources, avoiding the delays and inefficiencies of cloud-routed solutions that route traffic through centralized inspection points.

Appgate ZTNA is particularly well-suited for securing operational technology (OT) and industrial control systems (ICS) in pipeline environments. Its dynamic access policies adapt in real-time to changes in user behavior or device health, ensuring consistent security for critical systems without disrupting operations. This approach aligns with TSA directives, emphasizing continuous monitoring, rapid response and robust access controls.

Grounded in Zero Trust principles, Appgate ZTNA offers a comprehensive solution for securing critical pipeline infrastructure. The solution ensures compliance readiness, robust protection and operational efficiency, enabling pipeline operators to prioritize resilience and reliability, while entrusting the complexities of cybersecurity to Appgate.

Key features of Appgate ZTNA include:

- **Direct-Routed Architecture:** Secure data paths eliminate unnecessary detours, optimizing performance while ensuring robust protection.
- **Context-Aware Access:** Policies evaluate multiple risk factors before granting access, ensuring that every connection is dynamically verified.
- **Least-Privilege Enforcement:** Access is restricted to only the specific resources required, reducing exposure and minimizing security risks.
- **Scalable Design:** The solution is built to accommodate growing infrastructure and evolving threats, making it ideal for large-scale industrial environments.
- **Seamless Integration:** Appgate provides an enterprise-ready, 100% API-first solution that enhances and integrates with existing technology stacks.

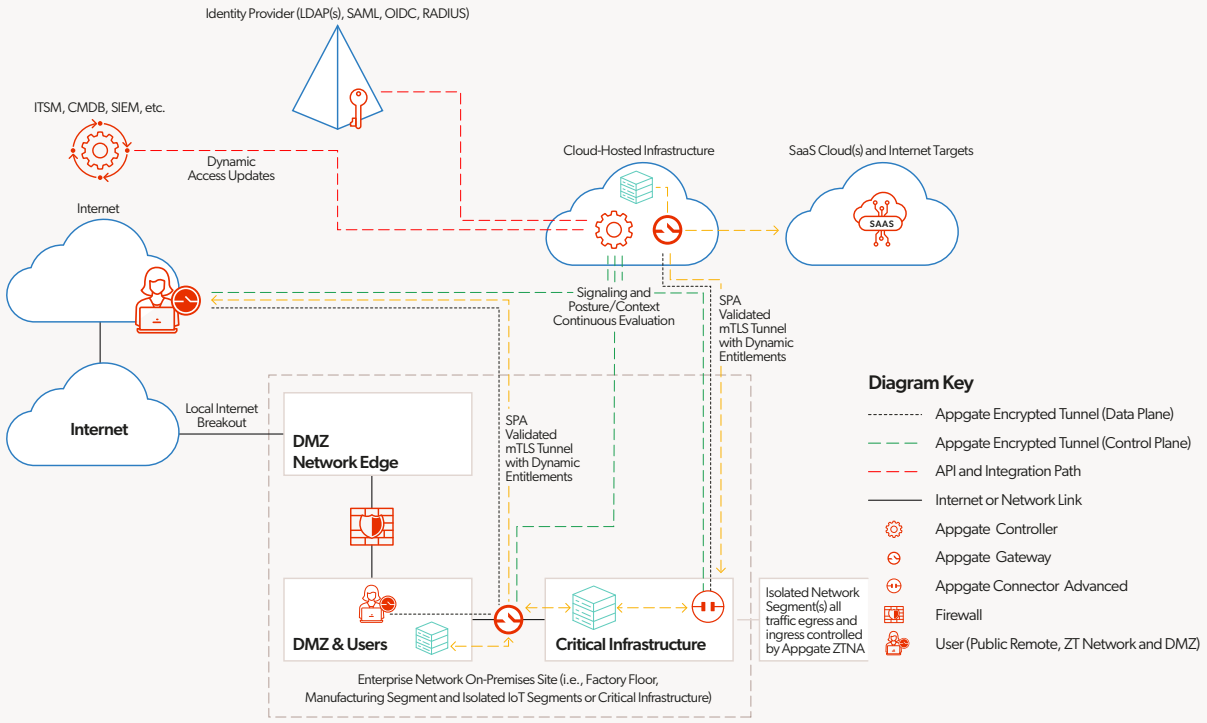
Critical Measures to be Implemented

Section III of the TSA SD-Pipeline-2021-02D focuses on implementing specific cybersecurity measures, including enhanced access control, continuous monitoring, incident detection, and response strategies. Appgate ZTNA directly maps to the following requirements:

SECTION III CYBERSECURITY MEASURES	DESCRIPTION	APPGATE ZTNA
A: Identify Critical Cyber Systems	Requires identifying critical cybersystems and methodologies for doing so	Appgate ZTNA leverages identity-centric security policies to ensure granular visibility into and access control for critical cybersystems. By integrating with existing identity and asset management solutions, it simplifies critical system identification and ensures security measures align with TSA requirements.
B: Network Segmentation	Mandates policies to prevent disruptions between IT and OT systems with clear zone boundaries and secured communications	Appgate ZTNA delivers identity-based north-south segmentation via secure segments of one, ensuring efficient access to critical resources. For east-west segmentation, Appgate integrates with strategic technology alliance partners to contain threats and prevent lateral movement. The combined solution provides broad, 'full-compass' coverage for complex environments.
C: Access Control Measures	Requires multi-factor authentication (MFA), least privilege, and management of shared accounts	Appgate ZTNA integrates with MFA solutions, enforces role-based access control (RBAC), and applies policies based on least privilege and separation of duties. Shared account access is minimized and, when necessary, is managed securely with session-specific credentials. Continuous policy enforcement ensures compliance with access restrictions.
D: Continuous Monitoring and Detection	Mandates capabilities to prevent, detect and respond to cybersecurity threats and anomalies (i.e. malicious IPs/domains, and unauthorized code execution)	Appgate ZTNA provides real-time monitoring and logging of all user activity and enforces strict ingress and egress traffic controls. Integration with security tools (e.g., SIEM, SOAR) ensures proactive threat detection and response. By limiting access to cloaked resources via single packet authorization, it significantly reduces the attack surface exposed to malicious activities.
E: Patch Management	Requires a patch management strategy, prioritization of CISA's Known Exploited Vulnerabilities Catalog, and mitigations for unpatched systems	Appgate ZTNA supports patch management by isolating unpatched systems within secured zones, restricting access only to authorized users. This isolation ensures unpatched vulnerabilities cannot be exploited while enabling controlled access for remediation activities.
F: Cybersecurity Incident Response Plan	Requires a plan to contain, segregate and mitigate cybersecurity incidents, ensuring operational continuity	Appgate ZTNA facilitates rapid containment of infected devices by dynamically adjusting policies to isolate affected systems. Its direct-routed architecture ensures OT systems remain operational even during IT incidents. Integration with incident response tools ensures prompt action and alignment with predefined response objectives.
G: Cybersecurity Assessment Plan	Requires proactive assessments, including architecture reviews, penetration testing, and red/purple team testing	Appgate ZTNA provides detailed audit logs and system telemetry to inform architecture reviews and assessments. Additionally, Appgate's Threat Advisory Services deliver complementary expertise, including advanced penetration testing, malware analysis and many other vulnerability assessments to help identify and remediate risks in critical systems.

Optimized Access for Mission-Critical Systems

Pipeline operators must balance stringent cybersecurity requirements with uninterrupted system performance. Appgate ZTNA achieves this by dynamically provisioning encrypted, one-to-one network connections that enforce strict access policies while optimizing latency-sensitive industrial operations. Unlike legacy solutions that rely on static access lists or broad network permissions, Appgate ZTNA continuously evaluates each connection in real-time, ensuring alignment with Zero Trust principles and the new Directive's access control measures. If a user's risk posture changes—due to device compromise, location shifts, or behavioral anomalies—access is automatically restricted or revalidated. This continuous validation maintains compliance with TSA directives while preserving the availability and integrity of pipeline systems. By extending Zero Trust security across IT and OT environments, Appgate ZTNA adapts to real-world operational demands without disrupting critical workflows.



Appgate's direct-routed approach securely connects users to mission-critical resources without adding unnecessary network complexity.

Conclusion

Appgate ZTNA is the ideal solution for meeting the access control requirements within TSA SD-Pipeline-2021-02D. By securing remote access, enforcing least-privilege access controls, and providing continuous monitoring of user behavior and device health, Appgate ensures pipeline operators can comply with the TSA's stringent cybersecurity measures. Furthermore, the flexibility and scalability of Appgate ZTNA enables pipeline operators to protect both IT and OT environments, ensuring the safety of critical infrastructure while simplifying compliance. With Appgate, pipeline operators can enhance their security posture, reduce risk, and maintain the operational integrity of their networks in the face of emerging cyber threats.

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