appgate

The Next Generation of Cybersecurity for Critical Infrastructure: Securing Vital Assets with Universal ZTNA

ZERO TRUST NETWORK ACCESS **WHITE PAPER**

EXECUTIVE SUMMARY

Critical infrastructure faces a growing threat from increasingly sophisticated cyberattacks, exacerbated by the expanding attack surface of IT/OT convergence, cloud adoption and remote work. Traditional security approaches like firewalls and VPNs are no longer sufficient to protect these vital assets. This white paper explores the critical need for modern security solutions in critical infrastructure, focusing on the role of universal Zero Trust Network Access (ZTNA). It examines the challenges faced by different sectors, including energy, utilities, communications, and transportation, and outlines practical Zero Trust strategies to mitigate risks. The paper highlights Appgate Universal ZTNA as a comprehensive solution that enables critical infrastructure organizations to enhance their security posture, improve operational resilience, and ensure the continuity of essential services.

INTRODUCTION

Critical infrastructure encompasses the essential systems and assets that underpin the functioning of modern society. These systems, spanning sectors like energy, utilities, communications, and transportation, are vital for public health, safety, economic stability, and national security. However, these critical sectors face escalating cybersecurity threats that can disrupt operations, cause physical damage, and jeopardize public well-being. For example, a 2023 report by the International Association of Certified ISAOs (IACS) found that reported cyberattacks against critical infrastructure organizations increased by 41% compared to the previous year. Traditional security measures are proving inadequate, necessitating the adoption of modern solutions like ZTNA to safeguard these vital assets.

THE IMPORTANCE OF SECURE ACCESS IN CRITICAL INFRASTRUCTURE

Secure access to critical infrastructure networks is paramount due to:

- **Increasing Cyberthreats:** Attacks against critical infrastructure are rising in frequency and sophistication, with adversaries ranging from nation-states to cybercriminals seeking to disrupt services, steal data, or cause physical damage.
- **Expanding Attack Surface:** Digital transformation initiatives, including cloud adoption, IoT integration, and remote work, have expanded the attack surface of critical infrastructure, creating new entry points for malicious actors.
- **Convergence of IT and OT Networks:** The increasing integration of information technology (IT) and operational technology (OT) networks blurs traditional security perimeters, exposing critical operational systems to cyberattacks. This convergence allows threats to cross over, for example, from an IT network into an industrial control system (ICS) or a physical control system (PCS). A compromised pressure sensor on an oil pipeline could lead to a catastrophic event if not addressed quickly.
- **Potential Consequences of Breaches:** Breaches in critical infrastructure can have severe consequences, including:
  - Disruption of essential services (power outages, communication failures)
  - Physical damage to equipment (e.g., damage to turbines or pipelines)
  - Economic disruption and financial losses
  - Environmental damage
  - Loss of life

CRITICAL INFRASTRUCTURE SECTORS: UNIQUE SECURITY NEEDS

Cyberattacks pose a significant and growing threat to critical infrastructure, with the global average cost of a data breach reaching $4.88 million in 2024. Each critical infrastructure sector has unique security requirements:

- **Energy Sector:** Protecting power generation, transmission and distribution systems from cyberattacks is crucial to prevent blackouts, brownouts, and damage to equipment. Secure access is also vital for managing smart grid technologies and ensuring the reliable delivery of energy. Furthermore, maintaining continuous operations and preventing disruptions is paramount. Secure remote access solutions enable rapid response to emergencies, such as equipment malfunctions or physical breaches, minimizing downtime and ensuring the continued flow of energy. In 2023, the energy sector experienced the highest average cost of a data breach at $5.23 million, highlighting the severe financial repercussions of cyberattacks in this sector.

- **Utilities:** Safeguarding water and wastewater treatment plants, natural gas pipelines, and electricity distribution networks is essential to maintain public health and safety. Secure remote access allows for timely responses to emergencies, such as leaks or equipment malfunctions, ensuring business continuity. Maintaining continuous operations is critical to avoid disruptions in essential services. Secure access solutions enable proactive monitoring and management of critical infrastructure, allowing for rapid response to incidents and minimizing service interruptions. Alarmingly, 45% of industrial organizations, including utilities, experienced a cyberattack in the past 12 months, emphasizing the urgent need for robust security measures.
- **Communications:** Resilient telecommunications networks and emergency communication systems are vital during crises. Secure access to data centers and network operations centers is necessary to prevent disruptions and maintain service availability. Continuous operation of communication networks is crucial, especially during emergencies. Secure access solutions enable real-time monitoring, management, and rapid response to incidents, ensuring uninterrupted communication and information flow. Underscoring the vulnerability of the communications sector, the telecommunications industry had the second-highest number of reported data breaches in 2023.
- **Transportation:** Protecting air traffic control systems, rail infrastructure, and public transportation networks is critical to prevent accidents, delays, and disruptions. Secure access solutions enable efficient management and monitoring of these systems while preventing unauthorized access that could jeopardize public safety. Ensuring the continuous and reliable operation of transportation systems is vital for public safety and economic stability. Secure access solutions enable real-time monitoring, efficient management, and rapid response to incidents, minimizing disruptions and ensuring the safe and efficient movement of people and goods. The transportation sector faces a growing threat from ransomware attacks, which increased by 186% in the first half of 2023.

THE LIMITATIONS OF TRADITIONAL SECURITY APPROACHES

Traditional security approaches, such as static firewalls and VPNs, are ill-equipped to handle the evolving threat landscape:

- **Drawbacks of Static Firewalls and VPNs:** Firewalls offer limited protection against modern threats and often rely on outdated perimeter-based security models. VPNs, while providing remote access, can be vulnerable to compromise and often grant excessive network access, increasing the risk of lateral movement by attackers.
- **Lack of Granular Control and Contextual Awareness:** Traditional security tools lack the granular control and contextual awareness needed to enforce least-privilege access and dynamically adjust security policies based on user behavior, device posture, and location.
- **Challenges with Broad Network Access:** Traditional approaches often grant broad network access, increasing the risk of unauthorized access to critical systems. This lack of segmentation can enable attackers to move laterally within the network and compromise critical assets.

WHY UNIVERSAL ZTNA IS CRITICAL FOR SECURING CRITICAL INFRASTRUCTURE: CHALLENGES AND SOLUTIONS

Universal ZTNA offers a robust framework for securing critical infrastructure by verifying and authenticating every user and device before granting access, regardless of location. Here are some practical strategies and recommendations:

- **Prioritize Isolation:** For highly sensitive systems like ICS/PCS, consider implementing isolated or partially air-gapped networks. This limits the potential for lateral movement even if an attacker gains initial access. ZTNA solutions can then be used to grant access to these isolated segments only when necessary, ensuring that users on and off the network have the required access without compromising security.
- **Implement Microsegmentation:** Divide networks into smaller, isolated zones to contain breaches and prevent lateral movement. This limits the blast radius of an attack.
- **Embrace a Defense-in-Depth Strategy:** Combine universal ZTNA with other security measures like multi-factor authentication (MFA), endpoint detection and response (EDR), and security information and event management (SIEM) to create a layered defense. This ensures that even if one layer is compromised, others are in place to prevent a full-blown breach.

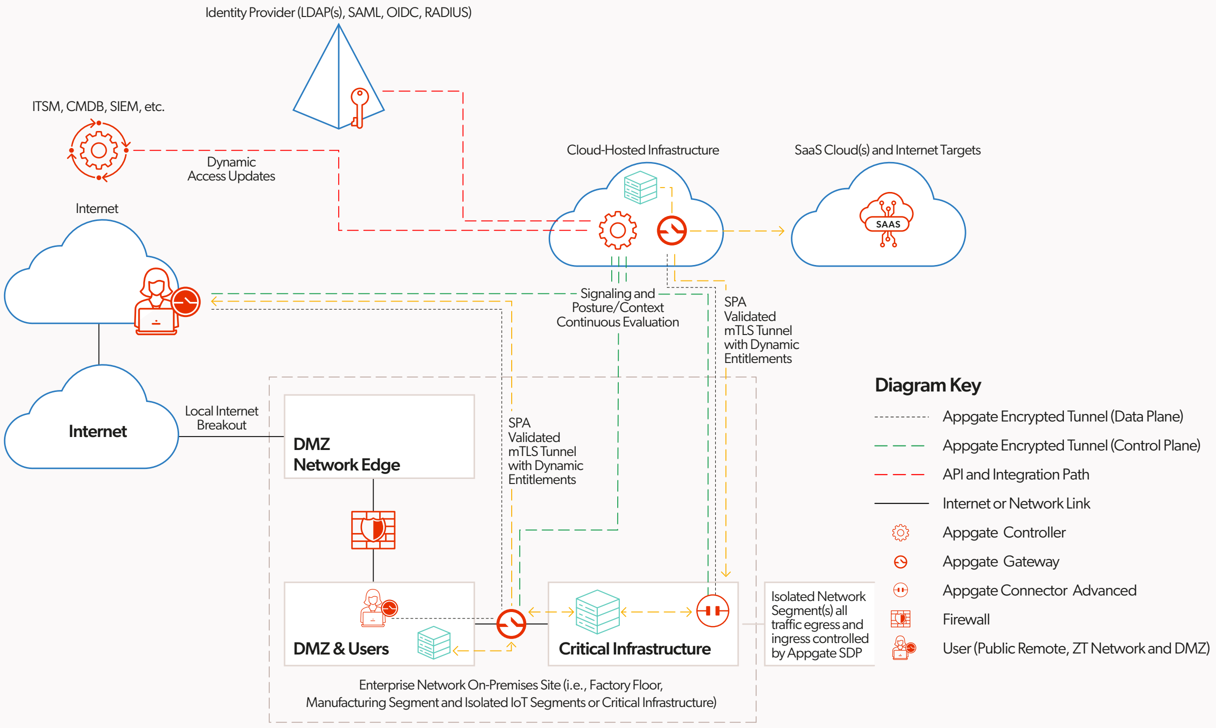
- **Focus on Least Privilege:** Grant users only the necessary access to perform their specific tasks. Regularly review and update access rights to ensure they align with current roles and responsibilities. Leverage ZTNA policies to dynamically enforce least privilege based on contextual factors like user location, device posture and time of day.
- **Continuous Monitoring and Threat Intelligence:** Implement continuous security monitoring and threat intelligence to identify and respond to potential threats in real-time. Integrate ZTNA solutions with your security monitoring tools to gain visibility into access patterns and detect anomalous behavior.

By implementing these strategies, critical infrastructure organizations can significantly enhance their security posture and reduce the risk of cyberattacks.

APPGATE ZTNA: A COMPREHENSIVE SOLUTION FOR CRITICAL INFRASTRUCTURE

Appgate ZTNA is an industry leading solution solution that enables critical infrastructure organizations to secure access to their vital assets. Key capabilities include:

- **Identity-Driven Access Control:** Appgate ZTNA enforces strong authentication and authorization policies, ensuring that only authorized users and devices can access critical resources.
- **Dynamic, Context-Aware Security Policies:** Appgate ZTNA leverages contextual information, such as user location, device posture, and time of day, to dynamically adjust security policies and enforce least-privilege access.
- **Direct-Routed Architecture for Improved Performance:** Appgate ZTNA's unique architecture eliminates the need for network tunnels, providing a seamless and high-performance user experience.
- **Seamless Integration with Existing IT Environments:** Appgate ZTNA integrates with existing technology stacks, including identity providers (IdPs), EDR, SIEM, security orchestration, automation and response (SOAR), IT service management (ITSM) and more to provide a unified security framework.


Identity Provider (LDAP(s), SAML, OIDC, RADIUS)
ITSM, CMDB, SIEM, etc.
Dynamic Access Updates
Cloud-Hosted Infrastructure
SaaS Cloud(s) and Internet Targets
SAAS
Internet
Signaling and Posture/Context Continuous Evaluation
SPA Validated mTLS Tunnel with Dynamic Entitlements
Internet
Local Internet Breakout
DMZ Network Edge
SPA Validated mTLS Tunnel with Dynamic Entitlements
DMZ & Users
Critical Infrastructure
Isolated Network Segment(s) all traffic egress and ingress controlled by Appgate SDP
Enterprise Network On-Premises Site (i.e., Factory Floor, Manufacturing Segment and Isolated IoT Segments or Critical Infrastructure)
Diagram Key
Appgate Encrypted Tunnel (Data Plane)
Appgate Encrypted Tunnel (Control Plane)
API and Integration Path
Internet or Network Link
Appgate Controller
Appgate Gateway
Appgate Connector Advanced
Firewall
User (Public Remote, ZT Network and DMZ)

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

BENEFITS OF IMPLEMENTING APPGATE ZTNA IN CRITICAL INFRASTRUCTURE

- **Enhanced Security Posture and Reduced Risk:** Appgate ZTNA strengthens security posture by enforcing Zero Trust principles, reducing the risk of unauthorized access and lateral movement within critical infrastructure networks.
- **Improved Operational Resilience:** Appgate ZTNA enhances operational resilience by providing secure and reliable access to critical systems, even during disruptions or emergencies. The solution helps maintain business continuity and reduce downtime by enabling authorized personnel to access resources remotely and securely.
- **Simplified Access Management and Reduced IT Overhead:** Appgate ZTNA simplifies access management by providing a centralized platform for defining and enforcing security policies. This reduces IT overhead and streamlines operations.
- **Compliance with Industry Standards:** Appgate ZTNA helps critical infrastructure organizations comply with relevant industry standards and regulations, such as NIST Cybersecurity Framework (CSF) and ISA/IEC 62443.

CASE STUDIES

Sorocaba Refrescos Enables Hundreds of Remote Workers with Appgate ZTNA

Challenge: When the pandemic hit, Sorocaba Refrescos, a leading beverage manufacturer in Brazil, needed to quickly enable remote work for 450 employees. Their existing security infrastructure, reliant on traditional VPNs, wasn't suitable for a large remote workforce and posed security risks.

Solution: To ensure secure remote access and protect critical systems, Sorocaba Refrescos chose Appgate ZTNA. The solution strengthened access controls, ensuring only authorized users could access sensitive data, while also enhancing network segmentation to prevent unauthorized lateral movement.

Results: With Appgate ZTNA, Sorocaba Refrescos saw immediate benefits:

- Improved connection stability and performance for remote employees.
- Enhanced access management, crucial for their lean IT team.
- Reduced risk of unauthorized access through robust security measures.
- Positive user feedback on the solution's reliability and ease of use.
- Stronger internal security by preventing lateral movement within the network.

Elecaustro Transitions to a Secure Remote Workforce and Achieves EGSI Compliance with Appgate ZTNA

Challenge: During the COVID-19 pandemic, Elecaustro S.A., an Ecuadorian energy leader, needed to quickly enable secure remote work for its employees. They needed to maintain access to essential services and internal management systems while ensuring the security of sensitive data and complying with Ecuador's Government Information Security Scheme (Esquema Gubernamental de Seguridad de La Informacion (EGSI).

Solution: Elecaustro implemented Appgate ZTNA to secure critical resources and ensure only authorized users could access the company network. This allowed them to strengthen their remote access security and establish micro-security perimeters based on user identity.

Results: With Appgate ZTNA, Elecaustro realized the following benefits:

- Restricted access from unsecured devices, enhancing overall network security.
- Made critical resources invisible to unauthorized actors, adding another layer of protection.
- Simplified and secured access for employees, improving user experience while maintaining compliance.
- Enabled compliance with EGSI.

CONCLUSION

Modernizing security solutions is an imperative for critical infrastructure organizations facing an increasingly hostile threat landscape. Universal ZTNA is a cornerstone of robust cybersecurity strategies, enabling organizations to secure access to their vital assets and protect against sophisticated attacks. However, ZTNA is just one element of a comprehensive Zero Trust approach.

Zero Trust requires a fundamental shift in security thinking, embracing the principle of "never trust, always verify." This involves continuously verifying users, devices, and applications, regardless of their location or network. It also encompasses data security, ensuring sensitive information is protected through encryption and access controls, and security posture management, which involves continuous assessment and improvement of an organization's overall security posture.

Appgate ZTNA provides a comprehensive solution that empowers critical infrastructure organizations to enhance their security posture, improve operational resilience, and safeguard the essential services they provide. By adopting a holistic Zero Trust approach and leveraging solutions like Appgate ZTNA, critical infrastructure organizations can effectively mitigate risks, maintain operational continuity, and ensure the safety and well-being of the public they serve.

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