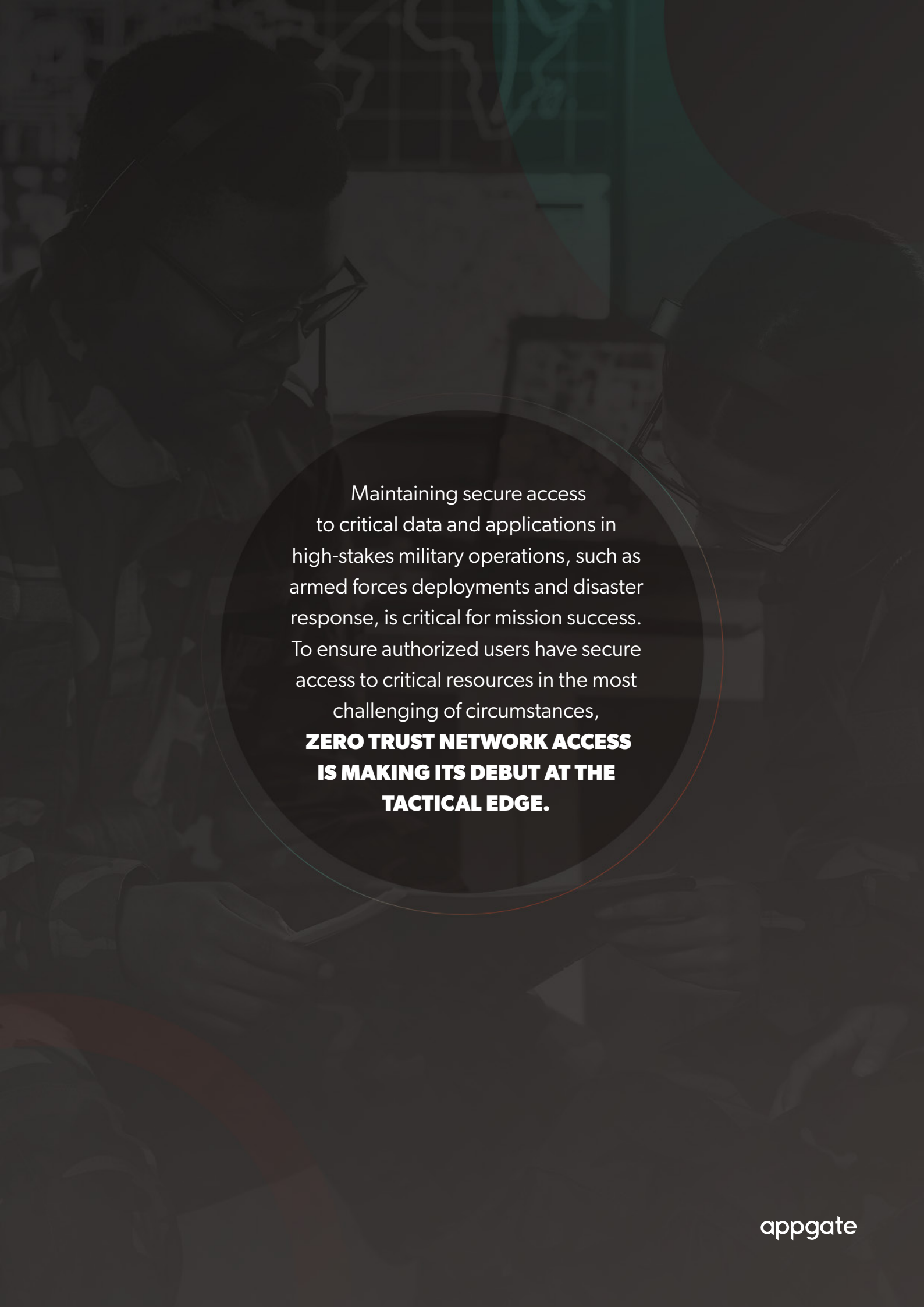
appgate

Securing
the Tactical Edge:

HOW ZTNA SAFEGUARDS MISSION-CRITICAL MILITARY OPERATIONS

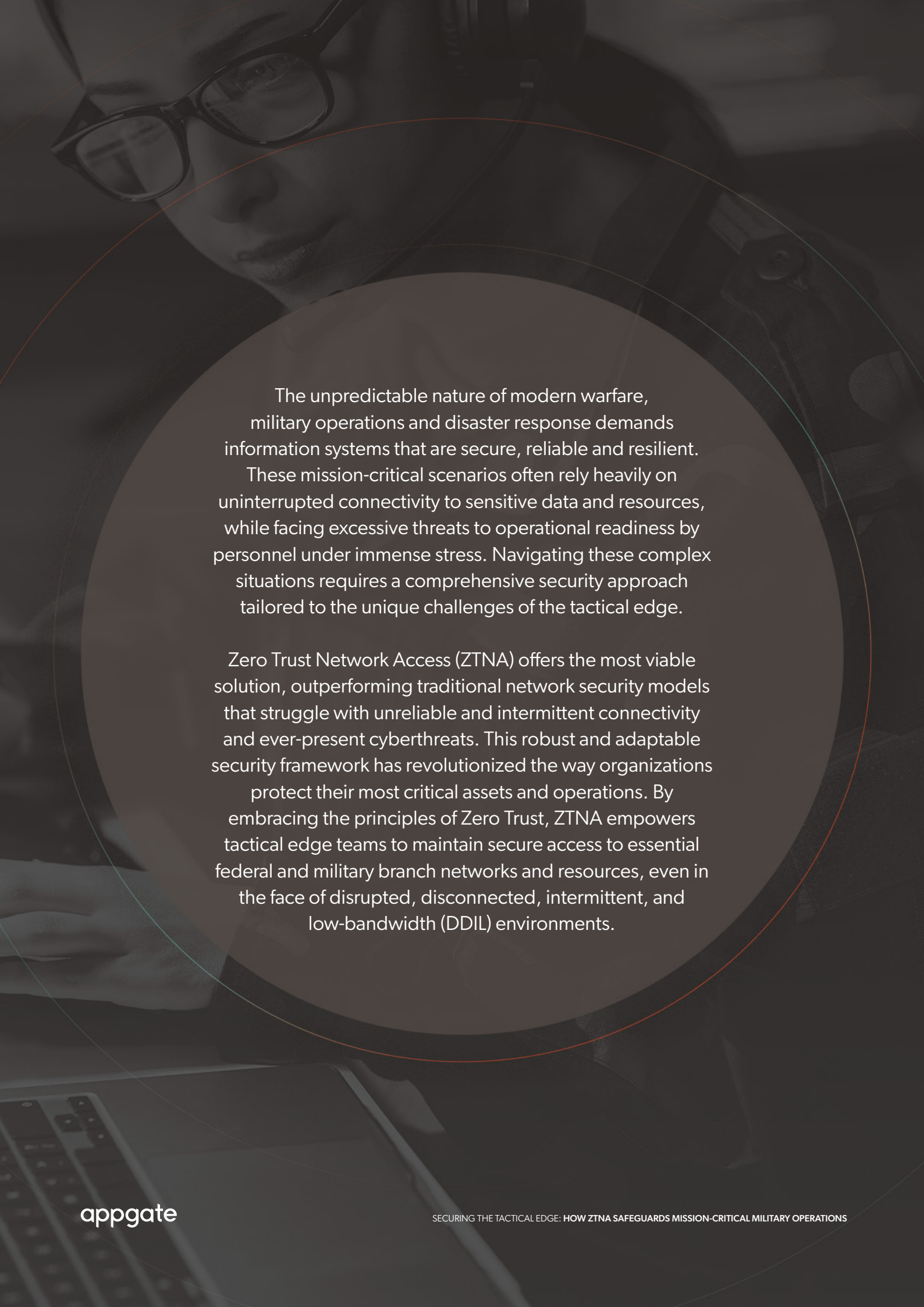


Maintaining secure access to critical data and applications in high-stakes military operations, such as armed forces deployments and disaster response, is critical for mission success. To ensure authorized users have secure access to critical resources in the most challenging of circumstances,

ZERO TRUST NETWORK ACCESS IS MAKING ITS DEBUT AT THE TACTICAL EDGE.

appgate

TABLE OF CONTENTS



The unpredictable nature of modern warfare, military operations and disaster response demands information systems that are secure, reliable and resilient. These mission-critical scenarios often rely heavily on uninterrupted connectivity to sensitive data and resources, while facing excessive threats to operational readiness by personnel under immense stress. Navigating these complex situations requires a comprehensive security approach tailored to the unique challenges of the tactical edge.

Zero Trust Network Access (ZTNA) offers the most viable solution, outperforming traditional network security models that struggle with unreliable and intermittent connectivity and ever-present cyberthreats. This robust and adaptable security framework has revolutionized the way organizations protect their most critical assets and operations. By embracing the principles of Zero Trust, ZTNA empowers tactical edge teams to maintain secure access to essential federal and military branch networks and resources, even in the face of disrupted, disconnected, intermittent, and low-bandwidth (DDIL) environments.

Understanding tactical edge cybersecurity challenges

Vital time-sensitive decisions that are inherent at the tactical edge have immediate and significant consequences, making secure access a top priority. However, rapidly changing and evolving conditions on the operational frontline present a unique set of security challenges. These include:

Connectivity disruptions:

Tactical operations may take place in remote, isolated or contested regions, where internet connectivity and traditional network infrastructure are unreliable or nonexistent. Maintaining secure access to mission-critical resources in these DDIL environments is a constant challenge.

Diverse communication modes:

Tactical teams may need to leverage a variety of communication methods, such as satellite communications, 5G, Wi-Fi meshes and radio over IP. Integrating and securing these diverse communication modes is essential for mission success.

Legacy systems and operational technology:

The tactical edge often includes a mix of modern IT systems, legacy equipment and operational technology used for critical functions. Securing and amalgamating these disparate systems is a difficult undertaking.

Heightened cyberthreats:

The tactical edge is a high-risk environment, where cyber adversaries actively seek to disrupt or compromise systems. Protecting mission-critical data and resources from cyberthreats is a paramount concern.

Mobility and disconnected operations:

Tactical teams often need to operate in a highly mobile, disconnected manner, with users and devices constantly on the move. This dynamic can present obstacles to maintaining secure connections and visibility.

Agile and adaptable security measures are paramount at the tactical edge, as even minor delays or vulnerabilities can have significant consequences for mission success and personnel safety.

Limited resources, such as constrained computing power and storage, necessitate lightweight security solutions that won't compromise effectiveness. However, traditional security solutions, like VPNs, are often ill-equipped to handle volatility like unstable network conditions at the tactical edge.

In addition, VPNs can't quickly scale to support an influx of users and devices or the diverse devices and platforms used to run tactical edge operations.

Traditional security solutions, like VPNs, are often ill-equipped to handle volatility like unstable network conditions at the tactical edge

How ZTNA supports federal cybersecurity frontlines

To address these unique challenges, federal agencies are increasingly adopting Zero Trust Network Access as their solution of choice. ZTNA is a modern security framework that shifts the focus from traditional network-centric security to a user, resource- and data-centric approach that verifies access based on contextual factors, such as user identity, device posture and application behavior. The core "never trust, always verify" principle of ZTNA means that every user, device and application is treated as a potential threat, and access is only granted after a rigorous verification process.

Additionally, it continuously authenticates and authorizes users and devices, regardless of their location or network connection status. This approach is particularly well-suited for the tactical edge, where trust boundaries constantly shift and traditional perimeter-based security models fail to adapt. Zero Trust access solutions employ several key principles to secure disconnected operations:

Identity-, device- and data-centric:

ZTNA prioritizes strong user and device authentication, ensuring that only authorized personnel can access sensitive data and resources. Multi-factor authentication and continuous authentication are often used to maintain the highest level of security.

Principle of least privilege:

ZTNA grants users the minimum level of access users need to perform their tasks. This limits the potential damage an attacker can cause if credentials are compromised.

Microsegmentation:

ZTNA divides the network into small, isolated segments, reducing the attack surface and preventing lateral movement. Even if an attacker gains access to one segment, they are contained and cannot easily move to others.

Continuous monitoring and adaptive access:

ZTNA dynamically assesses user, device and environmental factors to make real-time access decisions. This enables adaptive access controls that respond rapidly to evolving conditions, ensuring that only authorized users have the appropriate level of access at any given moment.

Secure multi-mode connectivity:

ZTNA can integrate with a variety of communication modes, including satellite communications, 5G, Wi-Fi meshes and radio over IP, to provide secure access and data sharing across diverse tactical edge environments.

Secure workload migration:

ZTNA enables the secure migration of containerized workloads and applications between the tactical edge and command centers, allowing for rapid deployment of mission-critical resources where they are needed most.

Seamless disconnected operations:

In the event of network disruptions, ZTNA can maintain secure access to local resources at the tactical edge, ensuring users can continue to perform critical functions without interruption.

ZTNA means that every user, device and application is treated as a potential threat, and access is only granted after a rigorous verification process

Appgate SDP:
Differentiated ZTNA for the tactical edge

Appgate SDP, an industry-leading ZTNA solution, excels in addressing the unique security challenges of the tactical edge, making it an ideal fit for federal agency and military branch use cases. Specifically, Appgate SDP ZTNA is certified and fully operational across many U.S. Department of Defense (DoD) service branches including Space Force, Marine Corps, Navy and the Air Force and is authorized to operate at DoD Impact Level 6. It has undergone rigorous penetration testing by U.S. military command and is the only ZTNA solution to achieve Common Criteria certification.

In addition, **Appgate SDP ZTNA** offers differentiated features to ensure secure and reliable access to critical resources that include:

Direct-routed architecture:

Eliminates the need to route traffic through a central cloud-hosted service or proxy, ensuring low-latency access to resources even when internet connectivity is unavailable.

Single packet authorization (SPA):

Cloaks the network edge, making it difficult for adversaries to identify and attack protected resources.

Mutual TLS (mTLS) technology:

Enhances communication security and mitigates cyberthreats like man-in-the-middle attacks and session hijacking.

Workload migration:

Allows applications to be seamlessly migrated between central command and the tactical edge, ensuring optimal performance and availability.

What is Direct-Routed **ZTNA?**

Direct-routed ZTNA architectures provide a purpose-built and flexible approach to accommodate the unique set of private applications and network infrastructures within an enterprise. This model ensures full control over how data traverses the network; providing secure access to all user-to-resource and resource-to-resource connections from anywhere across hybrid infrastructure located everywhere.

A key advantage is the scalability and performance of direct-routed architectures, allowing enterprises to scale their business while maintaining optimal network performance. The pricing model associated with direct-routed ZTNA is transparent, easily comprehensible and devoid of hidden charges, providing enterprises with a predictable and manageable cost structure.

Zero Trust Network Access (ZTNA) is revolutionizing how federal organizations secure operations in disconnected and tactical edge environments. The evolving landscape of modern warfare, military operations and crisis response demands adaptable security solutions for the unique challenges at the tactical edge.

As the operational landscape evolves, federal agencies embracing ZTNA will be better equipped to protect their assets, ensure mission success and maintain a strategic advantage against emerging cyberthreats.

Appgate SDP, ZTNA revolutionizes network defense with its direct-routed architecture— safeguarding mission-critical operations in the most demanding of environments.

Want to know more about how Appgate SDP, ZTNA secures disconnected and tactical edge operations?
Watch the ZTNA Table Talks replay now.

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