appgate

Secure DOD Operations in Tactical Edge & Denied, Degraded, Intermittent and Limited Bandwidth (DDIL) Environments with Appgate SDP Zero Trust Network Access

Table of Contents

EXECUTIVE SUMMARY

The Department of Defense (DOD) faces the complex challenge of securing operations across all domains—land, air, sea, space and cyber—while ensuring seamless and resilient communication, even in the most challenging environments. The Joint All-Domain Command and Control (JADC2) initiative reflects this necessity, aiming to integrate warfighting capabilities across military branches to enable faster, more informed responses to emerging threats. To maintain operational superiority, the DOD requires robust and adaptable solutions, particularly in Denied, Degraded, Intermittent and Limited Bandwidth (DDIL) environments where traditional communication methods may be unreliable.

CHALLENGES IN TACTICAL EDGE & DDIL ENVIRONMENTS

DDIL environments pose unique challenges, including:

- **Uninterrupted Command & Control:** Maintaining command and control continuity despite disrupted communication channels.
- **Secure, Resilient Communications:** Protecting sensitive information from cyberthreats while preserving communication integrity.
- **Coalition Interoperability:** Enabling seamless information sharing among coalition partners who may use different tools, technologies and security standards.
- **Operational Flexibility:** Supporting mission success in environments with limited infrastructure and connectivity.

The DOD requires solutions that address these challenges and foster interoperability between U.S. forces and coalition partners, ensuring a unified and secure operational posture.

APPGATE SDP UNIVERSAL ZERO TRUST NETWORK ACCESS

Appgate SDP Universal ZTNA is well-suited to address the specific needs of the DOD. Specifically, it provides a robust, data-centric approach* to security, ensuring that the *right* user gains access to the *right* data at the *right* time, regardless of their operational environment.

Key capabilities include:

- **Dynamic Access Control:** Appgate SDP leverages identity attributes, device telemetry and environmental context to dynamically enforce security policies, even in isolated or contested environments.
- **Resilient Operations:** Built on a distributed direct-routed architecture, Appgate SDP enables seamless access to both enterprise and local tactical resources, ensuring continuous operation and security enforcement even when disconnected from the enterprise network.
- **Unified Access Across Environments:** Users can access both tactical and enterprise resources using the same Zero Trust principles, ensuring a consistent security posture across all levels of operation.
- **Scalable, Lightweight Deployment:** Appgate SDP supports deployment on small form-factor devices and within virtualized environments, enabling flexibility and scalability in forward-deployed and tactical edge scenarios.
- **Cloaked –** Due to its Single Packet Authorization (SPA**), Appgate SDP makes the network invisible. This enables the network edge to be cloaked, making it extremely difficult for adversaries to identify and attack protected resources.

**See 'Appgate SDP Understanding Single Packet Authorization (SPA) White Paper for a further understanding. [https://www.appgate.com/resources/appgate-sdp/single-packet-authorization-whitepaper]

SOLVING INTEROPERABILITY CHALLENGES

Interoperability across DOD branches and coalition partners is a significant challenge due to the diverse tools and technologies used to manage user access. Appgate SDP Universal ZTNA addresses these challenges through a flexible, comprehensive approach that includes:

- **Clientless Access:** Secure access is provided via a standard web browser, which is ideal for rapid onboarding and coalition operations.
- **Secure Browser Access:** Isolating browsing sessions to protect the user's local environment ensures secure data access in less controlled environments.
- **Browser Extension-Based Access:** Enabling secure connections without full client installation provides flexibility for users operating with different security tools, even on headless clients, such as mission computers.
- **Interoperability with Existing Solutions:** Facilitating seamless integration and unified policy enforcement across different environments ensures consistent security postures even with various technologies.

Alignment with JADC2 Objectives

Appgate SDP Universal ZTNA aligns closely with JADC2 objectives by enabling secure, dynamic access control and supporting multi-domain operations. The platform's ability to maintain resilient operations in contested environments and ensure interoperability across various technologies and partners is crucial to JADC2's mission success.

Proven and Tested Security

Appgate SDP Universal ZTNA has been rigorously tested and certified to meet the highest security standards required by the DOD:

- **Multiple Authorizations to Operate (ATOs) (IL2-IL6):** Supporting secure access across all security domains, from unclassified to classified environments.
- **Common Criteria EAL Certification:** Providing an international standard for evaluating and certifying the security of Information Technology (IT) products and systems.
- **NIAP Protection Profile (In Progress):** Appgate is undergoing multiple protection profile certifications to meet U.S. government security requirements, supporting classified and tactical network deployments.
- **DISA Category Assurance List (CAL) Approved:** Meeting the DOD's stringent security and interoperability standards.

As the DOD advances its Zero Trust strategy, Appgate SDP Universal ZTNA offers a powerful, adaptable solution that ensures secure, resilient operations across all domains, even in the most challenging tactical edge and DDIL environments. By facilitating seamless communication, cloaking, dynamic access control and interoperability, Appgate SDP is uniquely positioned to support the DOD's mission success in today's complex and contested global landscape.

ZERO TRUST NETWORK ACCESS IN TACTICAL EDGE & DENIED, DEGRADED, INTERMITTENT AND LIMITED BANDWIDTH (DDIL)ENVIRONMENTS

Modern defense and military operations require secure and resilient communication and information-sharing capabilities, especially in Tactical Edge environments. Engaging adversaries requires Denied, Degraded, Intermittent and Limited Bandwidth (DDIL) capabilities, where traditional communication methods are either compromised or non-existent, necessitates robust and adaptable communication solutions. The Department of Defense (DOD) prioritizes addressing threats from near-peer adversaries, ensuring all operational units—from special operations forces to conventional military branches—can operate effectively in these complex scenarios.

DDIL environments present unique challenges across various military operations. These include ensuring uninterrupted command, control, communications, computer and cyberdefense, as indicated by the DOD's framework for its Command and Control Centers, usually referred to as C2, C4, and C5, based on their specific capabilities.

Additionally, DDIL environments often lead to further complications such as:

- Limited Situational Awareness
- Insecure Communications
- Coalition Interoperability
- Disrupted Data Sharing
- Device and System Incompatibility
- Infrastructure Constraints
- Fragmented Collaboration
- Physical Operating Footprint

A common requirement across various DOD organizations, including the U.S. Special Operations Command (SOCOM) and the U.S. Combatant Commands (COCOMs), is the need for resilient communication solutions that can adapt to the constraints and challenges of DDIL environments.

Interoperability holds special importance in these environments because military operations increasingly involve mission and coalition partners who need to securely share information across diverse platforms, technologies and security protocols. With each partner using different tools, compatibility issues can arise, potentially hindering operational effectiveness. Ensuring seamless communication among these diverse systems and secure information sharing, even in DDIL conditions, is vital for mission success.

Another critical aspect of operating in DDIL environments is the need for secure and resilient infrastructure that can withstand both physical and cyberthreats, adversaries are increasingly targeting military communications and information systems. Consequently, the DOD must deploy solutions that can operate in contested environments and protect against sophisticated cyberthreats. This includes ensuring data encryption, access control, and systems designed to maintain core functionality even under attack.

From CONUS and OCONUS to the tactical edge, the DOD enterprise requires programs like Joint All-Domain Command and Control (JADC2) to integrate warfighting capability from all military branches, including ABMS (Advanced Battle Management System) (U.S. Air Force), Project Convergence (U.S. Army), U.S. Naval Operational Architecture (NOA) and Force Design (U.S. Marine Corps). This integration enables seamless, multi-domain operations and enhances communication and coordination across air, land, sea, space, and cyber domains. However, the success of these programs relies heavily on operational readiness in DDIL environments.

Command and Control Centers

Command and Control Centers are vital, responsible for gathering and processing critical information to support operations, decision-making, and resource management for military and joint operations as well as in cyber security operations.

Here's a breakdown of their individual functions:

- **C2 - Command and Control:** Refers to the authority and coordination a commander exercises over forces to accomplish missions.
- **C4 - Command, Control, Communications and Computers:** Builds on C2 by incorporating communication systems and computer networks to enhance decision-making and situational awareness.
- **C5 - Command, Control, Communications, Computers and Cyber:** Expands C4 by adding cyber operations, emphasizing cybersecurity and leveraging cyber capabilities for defense and offensive operations.

Appgate SDP Capabilities

Appgate SDP Universal Zero Trust Network Access (ZTNA) effectively addresses the specific and evolving needs of the Department of Defense (DOD) across all operational environments, ensuring that the *right* user gains access to the *right* data at the *right* time. By leveraging identity attributes, device telemetry, and contextual factors, Appgate SDP enables real-time, dynamic access decisions that align with operational needs. This capability extends across various environments, including enterprise networks, forward-deployed units, tactical edge operations, OT and IoT devices, air-gapped/classified environments such as the Secret Internet Protocol Router Network (SIPRNet), and the Joint Worldwide Intelligence Communication System (JWICS).

Appgate SDP adopts a data-centric approach, recognizing that improved foundational data management inherently leads to better and more secure user/identity management. This allows Appgate to provide precise and dynamic access control tailored to the specific needs of each user and system. The platform leverages tags and labels to define and enforce granular access policies that adapt to real-time conditions. This capability directly aligns with the DOD's data search and discovery classification strategy, as outlined by the DOD in "Data, Analytics, and Artificial Intelligence Adoption Strategy" dated June 27, 2023. The DOD states, "…data sets targeted for improvement will be founded on metadata to allow for data search and discovery; prioritized for relevance and mission value."

By intertwining these concepts within a robust ZTNA solution, the DOD can achieve operational success across diverse and contested battlespaces, ensuring compliance with the Zero Trust Framework objectives set forth by the DOD CIO in documents such as the "Department of Defense Zero Trust Overlays," (February 2024), and the" DOD Zero Trust Strategy, v1," (October 2022). Appgate SDP ensures that users and systems can only access the data for which they are explicitly authorized, safeguarding critical information across all DOD operations. This adaptability is crucial for maintaining security and operational effectiveness in any scenario, from conventional to highly sensitive missions.

Appgate SDP is the ideal solution for a mission-first approach, as demonstrated by its unique ability to operate effectively in contested environments and its advanced cloaking capabilities, making the entire underlying infrastructure (i.e., resources and applications) undiscoverable to the adversary. By rendering critical resources invisible to unauthorized users, Appgate SDP dramatically reduces the cyberattack surface. This approach is designed to align with the DOD's diverse mission requirements, providing unparalleled security and flexibility across all levels of operations, from the enterprise to tactical edge environments.

Data-Centric Security: How Appgate Enables Zero Trust in the DO

While Appgate SDP's primary function is to provide Zero Trust Network Access (ZTNA), its true strength lies in its data-centric approach used to enforce access policies. Instead of focusing solely on granting access to networks, Appgate SDP's policy engine is designed to make decisions based on how the workload, application, or data is tagged or labeled.

How Appgate SDP Utilizes Tags, Labels, and Metadata

Appgate SDP integrates with a wide array of sources, consuming tags, labels, and other contextually rich metadata to enforce real-time security policies. This approach enables dynamic access controls, providing granular protection for sensitive data and mission-critical systems.

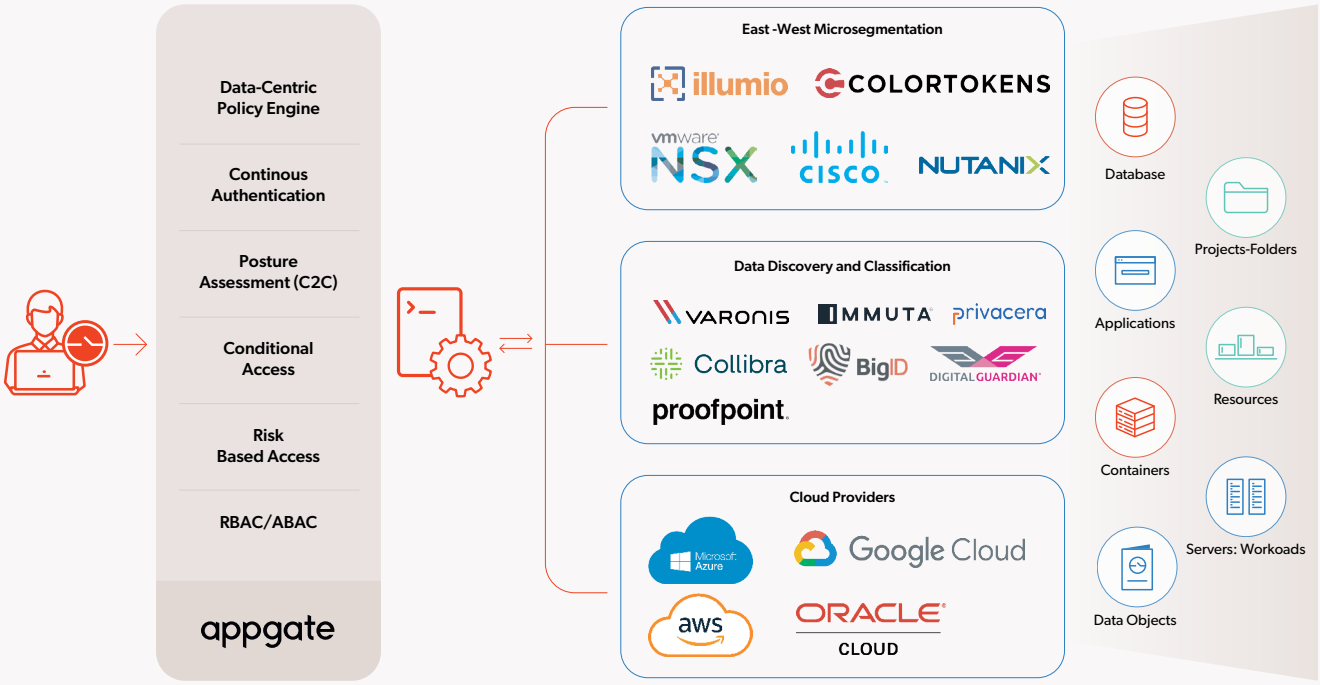
Key capabilities include:

- **Micro-segmentation Overlays/Underlays:** Appgate SDP consumes tags and labels from micro-segmentation tools to enforce dynamic access controls based on the segmentation of traffic within the network.
- **Data Discovery, Classification, and Governance:** Appgate SDP integrates with tools that classify and label data, consuming tags that represent data sensitivity or classification levels; for example, NOFORN, FVEY, CUI, HIPAA and PII.
- **Infrastructure Providers (Cloud and Hypervisors):** Appgate SDP pulls tags from infrastructure providers like cloud platforms (AWS, Azure, GCP) and hypervisors to enforce policies based on workload attributes, such as IL4/IL5 classifications, or environment types like Dev vs. Prod, or to specific projects or programs.
- **Data Loss Prevention (DLP) Tools:** Appgate SDP leverages tags from DLP tools to enforce security policies based on how the data is labeled and its associated risk level.
- **Adaptability in DOD Operations:** Appgate SDP's data-centric approach is designed to meet the unique security challenges faced by the DOD. It provides a flexible, tag- and label-driven system that dynamically responds to evolving mission requirements, security classifications, and operational needs. By continuously adjusting access policies based on metadata, Appgate ensures that the right individuals have access to the right resources at the right time.

Data-Centric Security in a Zero Trust Framework

In traditional security models, access is typically governed by static parameters such as IP address-based Access Control Lists (ACLs). While this approach was once effective, it has become increasingly insufficient for the DOD dynamic and high-stakes operations. The static nature of ACLs makes them difficult to manage, as they are continuously added to over time, but rarely pruned for fear of breaking critical systems. As a result, these lists become stale, bloated with outdated entries, and demand significant manpower to operate and maintain.

Appgate SDP's data-centric model overcomes these challenges by focusing on tags and labels associated with workload, application, and data, thereby enabling the creation of adaptive, context-aware access controls. Rather than relying on static rules, policies are dynamically adjusted in real time based on tags and labels, reducing operational overhead and enhancing security posture.



Data-centric security model.

APPGATE SDP IN TACTICAL EDGE AND DDIL ENVIRONMENTS

Appgate SDP empowers tactical edge users to seamlessly access both enterprise and local/forward-deployed tactical resources, even in environments with DDIL network connectivity to the enterprise. By implementing a Zero Trust approach that is robust and adaptable, Appgate SDP consistently enforces security policies, regardless of connectivity status.

At the tactical edge, Appgate SDP Universal ZTNA enables parallel access to critical resources, both locally and from the enterprise. Its distributed architecture supports direct connections to resources, enabling users to maintain operational efficiency without relying on a centralized, cloud-based network. This demonstrates the consistent application of Zero Trust principles, whether interacting with a local tactical system or an enterprise application.

- **Unified Access Across Environments:** Users can access both tactical and enterprise resources using the same Zero Trust principles, ensuring a consistent security posture across all levels of operation.
- **Autonomous Operation:** Even when disconnected from the enterprise, Appgate SDP continues to enforce Zero Trust policies locally, thereby maintaining security without compromise.
- **Sustain Operations-Local Management:** Onboarding coalition forces, provisioning access, and applying Zero Trust policies can all be managed at the tactical edge, independent of enterprise connectivity.
- **Effortless Synchronization:** Once connectivity is restored, Appgate SDP seamlessly synchronizes local and enterprise environments, applying version control and rollbacks as needed. This is not time dependent.

In a joint operation involving various coalition partners, maintaining a robust security posture becomes even more challenging. Appgate SDP enables the rapid and secure onboarding of these partners, even in a DDIL environment.

For instance, a U.S. Special Operations team working with allied forces in a remote location can use Appgate SDP to grant access to mission-critical systems for a newly arrived allied contingent. Despite being disconnected from the enterprise network, the local instance of Appgate SDP allows for the seamless creation of new user accounts, access provisioning, and the application of stringent Zero Trust controls. This ensures that the security posture remains intact as new users are onboarded, preventing unauthorized access. In addition, these users will be cloaked at the edge effectively making their presence invisible.

It's important to distinguish between true on-prem solutions and cloud-based offerings, even those marketed as 'private cloud.' Any company claiming that their private cloud is equivalent to on-prem in a tactical setting is misleading. While it may offer some benefits, it still fundamentally relies on connectivity to their infrastructure. In contrast, Appgate SDP is purpose built for DDIL operations. Even if all external communication is lost, the local Appgate SDP instance continues to function, ensuring uninterrupted access control and security.

Most importantly, the user experience remains uninterrupted; the team doesn't need to change anything if the enterprise network is unavailable. Appgate SDP automatically adjusts access depending on available resources, ensuring continuous and transparent operation. When the network reconnects, all local changes, including new user onboarding and policy adjustments, are synchronized back to the enterprise environment without a time limit. This synchronization process includes version control, allowing for the review and rollback of changes if necessary. This capability ensures that even in the most challenging operational environments, coalition forces can collaborate securely and efficiently without compromising overall mission integrity.

SOLVING FOR INTEROPERABILITY CHALLENGES ACROSS MILITARY BRANCHES, DOD AGENCIES AND COALITION ENVIRONMENTS

Interoperability remains a significant challenge within the DOD due to the diverse tools, technologies and policies employed by different military branches and Defense agencies to manage user access. This challenge is amplified in coalition environments where partners may have disparate security standards or systems that do not directly align with DOD Zero Trust protocols. Ensuring seamless operations and secure data access across these varied environments is critical for mission success, particularly in complex, forward-deployed tactical scenarios.

Appgate SDP addresses these interoperability challenges with a flexible and comprehensive Zero Trust solution that ensures secure access in DDIL environments:

1. **Clientless Access:** Appgate SDP Universal ZTNA includes a robust clientless access portal that enables users to securely connect to resources via a standard web browser. This is ideal when deploying agents on all devices is impractical, such as in coalition operations or when rapid onboarding is necessary. It ensures secure access without the need for extensive software installation on endpoint devices.
2. **Secure Browser Access:** Appgate SDP provides secure browser-based access and isolation browsing sessions to protect users' local environments from potential threats. This method, based on mTLS, supports a Zero Trust architecture by enforcing security policies directly within the browser, ensuring secure access to sensitive data and that resources are accessed securely even in less controlled environments, such as coalition operations or in-theater operations.
3. **Browser Extension-Based Access:** The browser extensions within Appgate SDP enable secure resource access without a full client installation. This capability is particularly useful when users operate with different security tools or on devices that can't support a full client, such as specialized weapons systems or headless clients. It provides a flexible, yet secure access solution that aligns with the diverse operational needs of various military branches, DOD agencies and coalition partners.

4. **Enabling Interoperability with Existing ZT Solutions:** Appgate SDP Universal ZTNA facilitates interoperability with other Zero Trust solutions already in use by different branches or coalition partners. This capability allows for seamless integration and unified policy enforcement across different environments, ensuring security even with diverse technologies. This approach is vital as mission requirements evolve and new partners join the operational framework, enabling consistent Zero Trust policies to be applied and managed efficiently.
5. **Cloaked –** Due to its single packet authorization, Appgate SDP makes your network invisible. This enables the network edge to be cloaked, making it extremely difficult for adversaries to identify and attack protected resources.

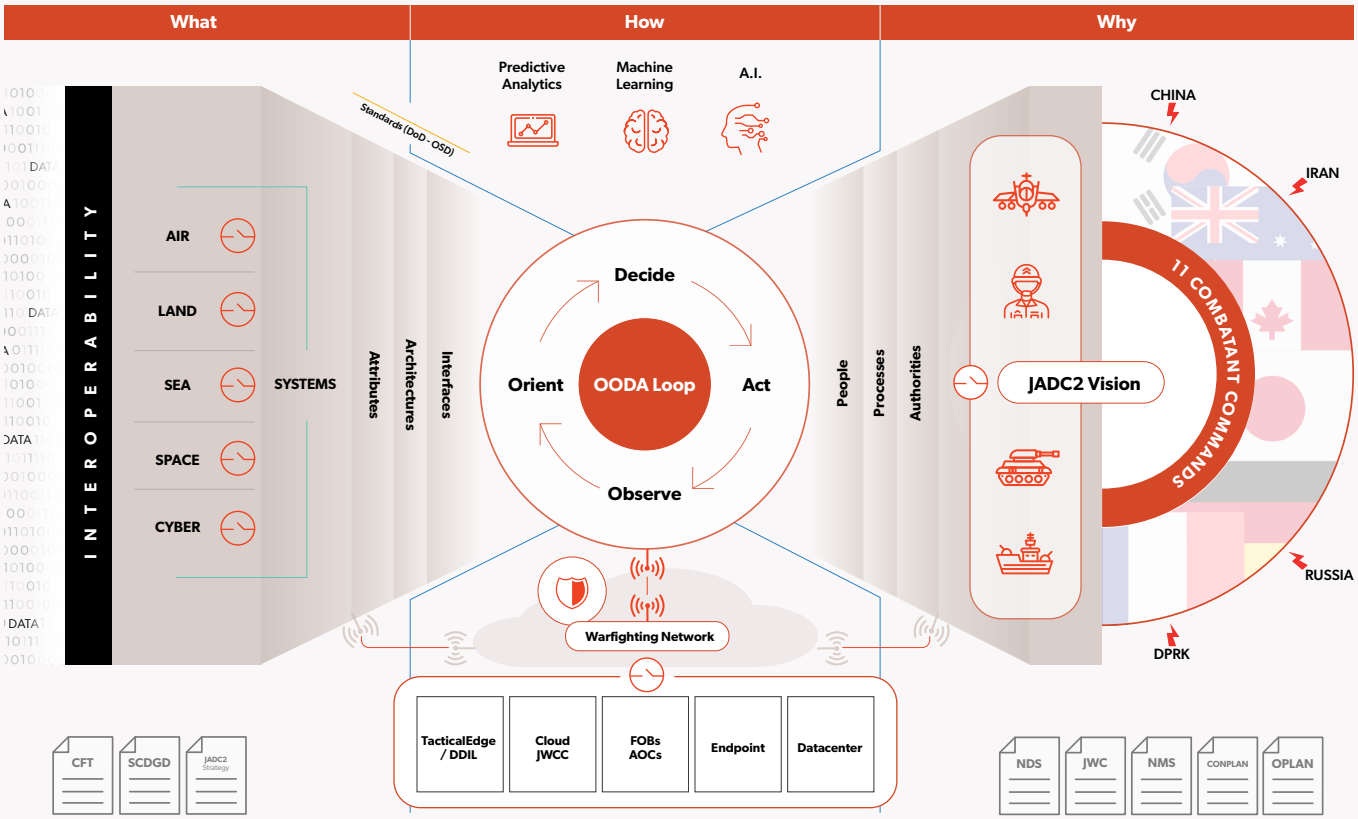
These capabilities underscore Appgate's commitment to providing a versatile and secure Zero Trust solution that meets the DOD's complex and evolving mission requirements. Whether operating in a fully connected enterprise, a tactical edge scenario, or a coalition operation with varied security postures, Appgate SDP ensures robust and adaptable solutions to address interoperability challenges.

ALIGNMENT WITH JADC2

JADC2 integrates and connects sensors, warfighters and command and control nodes across all domains, including air, land, sea, space and cyber. The goal is seamless, real-time communication and decision-making across the entire battlespace, enabling faster and more informed responses to emerging threats.

Appgate SDP closely aligns with JADC2 objectives, particularly in facilitating secure and seamless communication across domains and with coalition partners. Here's how:

1. **Secure and Dynamic Access Control:** Appgate SDP Universal ZTNA ensures that the *right* users can access the *right* data at the *right* time, regardless of their location or operational domain. This is crucial for JADC2, where rapid, secure access to information across all domains is essential for mission success.
2. **Interoperability:** Appgate SDP's ability to integrate with various existing technologies and security frameworks enables it to support JADC2's diverse needs. Whether through its clientless access portal, secure browser-based access, or interoperability with other Zero Trust solutions, Appgate SDP ensures secure communication and information sharing across all branches of the military, DOD agencies and coalition partners.
3. **Resilient Operations in Contested Environments:** In scenarios where communication links are degraded or disconnected, such as DDIL environments, Appgate SDP ensures Zero Trust policies are enforced locally. This maintains operational security and effectiveness in JADC2 operations, where forces may need to operate independently while adhering to strict security protocols.
4. **Support for Multi-Domain Operations:** Appgate SDP's support for the multi-domain operations central to JADC2 is enhanced by its data-centric approach, a recognition that improved foundational data management is key to achieving better and more secure user/identity management. By ensuring data accuracy, centralized control, and proper protection, Appgate SDP enables robust access control, ensuring data protection and accessibility solely by authorized individuals, even within intricate, multi-domain environments.
5. **Secure:** A key tenant of JADC2 is to provide a layered cyberdefense to deter malicious activity. Appgate SDP makes the network invisible using Single Packet Authorization (SPA) to cloak the network and its users. This makes it very difficult for adversaries and nation-state attackers to identify protected resources. Appgate provides the technology necessary to conduct secure C2 (command and control) in contested environments.



Joint All Domain Command and Control (JADC2) is a strategic warfighting concept that connects the data sensors, shooters, and related communications devices of all U.S. military services.

AUTHORIZATIONS AND CERTIFICATIONS

Appgate SDP has been rigorously tested and is certified to meet the high security standards required by the DOD and other federal agencies. Its advanced security posture is demonstrated through:

Multiple ATOs across IL2-IL6: Appgate SDP has achieved multiple Authorizations to Operate (ATOs) across Impact Levels 2 through 6, including environments supporting unclassified to classified data, ensuring secure access across all security domains.

Common Criteria EAL Certification: Appgate SDP is Common Criteria - Evaluation Assurance Level (EAL) certified, providing an internationally recognized standard for computer security certification, critical for systems handling National Security Systems (NSS). This certification ensures that Appgate's ZTNA platform meets stringent security requirements for handling sensitive and classified information.

NIAP Common Criteria Protection Profiles (In Process): Appgate is undergoing certifications to meet Protection Profile Functional Package TLS v1 and Protection Profile Application Software v1.4, both of which are for U.S. government NSS security requirements, supporting classified and tactical network deployments.

DISA Category Assurance List (CAL) Approved: Appgate SDP is included in the Defense Information Systems Agency (DISA) Category Assurance List, confirming it meets the DOD's stringent security and interoperability standards.

CONCLUSION

In today's unpredictable and contested environments, where the Department of Defense (DOD) and its coalition partners must operate across multiple domains and under varying conditions, the need for resilient, adaptive, and secure solutions is paramount. Appgate SDP Universal Zero Trust Network Access is purpose-built to address these challenges, providing robust security, scalability, and flexibility essential for operations at the tactical edge and in DDIL environments.

As the DOD continues to advance its Zero Trust strategy, Appgate is ready to support mission success by securely connecting, managing and protecting resources in the most demanding operational environments. This ensures tactical edge operations are as secure and effective as those in fully connected enterprise settings, contributing to mission success.

To learn more about how Appgate SDP Universal ZTNA can support your federal agency's security needs, visit https://www.appgate.com/federal-division.

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.