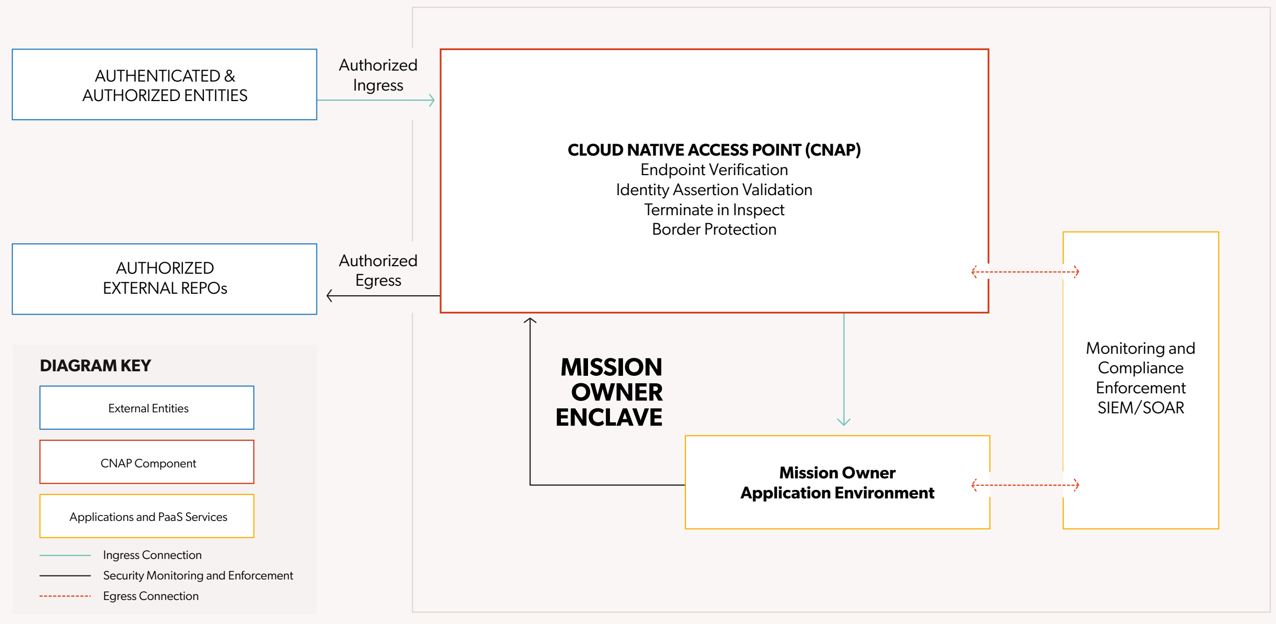
MODERNIZING DOD CLOUD ACCESS WITH PLATFORM ONE’S CNAP POWERED BY APPGATE

Platform One empowers the Department of Defense (DOD) to accelerate innovation and maintain a tactical advantage by delivering secure, cloud-native IT solutions. By integrating Appgate ZTNA’s cloud-native Zero Trust Network Access (ZTNA) capability, built on its software-defined perimeter, into Cloud One, Platform One ensures precise, context-aware, least-privilege access to mission-critical resources. This partnership drives operational excellence, enabling DOD teams to deploy resilient applications and streamline secure workflows in highly dynamic environments.

Introduction

The Department of Defense (DOD) faces significant challenges maintaining security, efficiency, and operational agility across its diverse and complex IT environments. As the pace of innovation accelerates, legacy systems and traditional access methods struggle to keep up with the demands of modern, distributed workforces, cloud adoption and advanced cybersecurity threats. These challenges are compounded by the need to ensure seamless collaboration between developers, operators and mission-critical systems, all while meeting stringent security and compliance requirements.

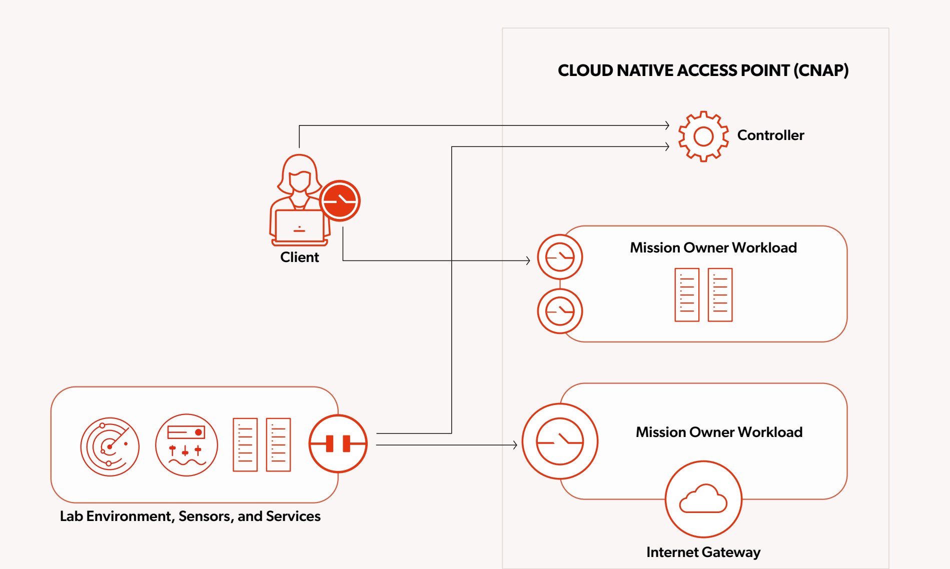
Platform One addresses these challenges by delivering a modern cloud-native platform that combines advanced DevSecOps pipelines, secure Kubernetes environments, and innovative tools like Cloud One’s Cloud Native Access Point (CNAP). CNAP combines capabilities such as Appgate ZTNA, next-generation firewall, DNS management, and Bring Your Own Identity Provider (BYOIdP) to craft a cloud-native ZTNA solution, designed to provide secure, context-aware, least-privilege access to security-critical resources. This design has been codified as the DOD’s CNAP Reference Design and implemented in other service locations, as well. This integration ensures that DOD teams can securely connect to the resources they need, whether operating on or off a non-classified internet protocol router (NIPR) network, enabling faster development cycles, enhanced security and greater mission success.


AUTHENTICATED & AUTHORIZED ENTITIES
Authorized Ingress
CLOUD NATIVE ACCESS POINT (CNAP)
Endpoint Verification
Identity Assertion Validation
Terminate in Inspect
Border Protection
AUTHORIZED EXTERNAL REPOs
Authorized Egress
MISSION OWNER ENCLAVE
Mission Owner Application Environment
Monitoring and Compliance Enforcement SIEM/SOAR
DIAGRAM KEY
External Entities
CNAP Component
Applications and PaaS Services
Ingress Connection
Security Monitoring and Enforcement
Egress Connection

The DOD’s Cloud Native Access Point Vision: Operational Viewpoint (OV-1)

The Solution

Appgate ZTNA is crucial to Cloud One's CNAP ZTNA offering, enabling its Zero Trust strategy and meeting the security demands of modern, distributed environments and emerging DOD Zero Trust compliance requirements. Additionally, Appgate ZTNA's direct-routed model establishes a dynamic, context-aware 1:1 encrypted connection between devices and only the specific resources they are authorized to access. This "segment-of-one" approach ensures robust security, reduces the attack surface, and supports direct routing for optimized performance. Designed for hybrid and cloud infrastructures, Appgate ZTNA also delivers scalable, distributed and highly available Zero Trust access without compromising flexibility and performance.



Appgate ZTNA powers secure, identity-based access in Cloud Ones' Cloud Native Access Point (CNAP) for mission-critical DOD resources.

Use Cases

Expanded Protocol Support

Supports non-standard (80/443) ports and protocols to enable the ever-growing capability set emerging from cloud development practices.

BYOD Alignment and Device Compliance

Aligns with emerging BYOD needs across the DOD through the Zero Trust, "assume breach" mindset, introducing new advancements in device compliance and segmentation practices.

Secure Remote Access

Enables secure access to DOD cloud resources (IL2/4/5/6) from anywhere in the world, regardless of network or environment, from secure government networks such as NIPRNet to untrusted public Wi-Fi connections.

Microservices Hosting

Provides a secure Kubernetes platform for deploying and managing microservices, enabling an enterprise-level Security Information and Event Management (SIEM) capability.

CI/CD Pipeline Security

Integrates security measures into continuous integration and deployment (CI/CD) workflows to ensure code integrity, enabling continuous vulnerability review and SBOM management.

Multi-Cloud Resource Access:

Facilitates secure connections to resources across multiple cloud environments.

Compliance Enforcement

Ensures all access and operations adhere to DOD Zero Trust Strategy v2.0 security policies and standards, aligning with controls before the 2027 implementation deadline.

Bring Your Own Identity Provider (BYOIdP)

Integrates with standard IdPs, such as Microsoft Active Directory, Keycloak, and Okta, allowing CNAP to support evolving identity needs and the DOD's shift toward modern Identity, Credential, and Access Management (ICAM) capabilities.

KEY ASPECTS OF THE JOINT SOLUTION INCLUDE:

Zero Trust Access

Enforces granular, context-aware access to DOD cloud resources, ensuring that users and devices only connect to what they are authorized to access.

Direct-Routed Architecture

Eliminates the inefficiencies of cloud-routed solutions by providing high-performance, low-latency access to critical resources, even in hybrid and distributed environments.

Dynamic Security Posture

Creates "segment-of-one" connections, reducing the attack surface and allowing access only to specifically granted resources.

Seamless DevSecOps Integration

Enables secure, continuous delivery pipelines, accelerating the deployment of mission-critical applications.

Scalability and Resilience

Ensures high availability, due to a distributed architecture, supporting the needs of both DOD operators and developers in rapidly evolving operational landscapes.

Conclusion

Cloud One's CNAP, powered by Appgate ZTNA, represents a cutting-edge integration of Zero Trust principles with modern cloud security frameworks. By embedding Appgate's scalable and performance-driven ZTNA solution, Cloud One ensures secure, seamless and efficient access to critical DOD cloud resources, enabling developers and operators to deliver innovation with confidence. This partnership underscores the importance of strong, context-aware security controls that prioritize performance to achieve mission-critical objectives. Together, Cloud One and Appgate enable Platform One organizations to accelerate application deployment, enhance operational agility, and maintain uncompromising security standards in dynamic and distributed environments.

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.

About Platform One

Platform One (P1) is a modern cloud-era platform that provides valuable tooling, hosts CI/CD DevSecOps pipelines, and offers a secure Kubernetes platform for hosting microservices. Authorization to go live with your application can be achieved faster than ever by using Iron Bank hardened containers and P1 pipeline security tools. The resulting Certificate to Field (CtF) and Continuous Authority to Operate (cATO) provides developers the ability to push validated code into production on an ongoing basis. This results in shorter development cycles, less debugging, and more rapid feature development. Learn more at https://p1.dso.mil/.

BENEFITS

Accelerated Deployment
Achieves faster authorization to deploy applications, resulting in shorter development cycles and more rapid feature development.

Enhanced Security
Ensures that only authenticated and authorized users and devices have access to specific resources, significantly reducing the risk of breaches.

Operational Efficiency
Streamlines secure access and reduces complexity and administrative overhead with the seamless integration of Appgate ZTNA into Platform One's ecosystem.

Compliance Assurance
Aligns with DOD security standards, ensuring that all operations meet necessary regulatory requirements.