

REVOLUTIONIZING CLOUD NATIVE ACCESS POINT SOLUTIONS

Highly Secure and Performant ZTNA in the DOD

Marine Corps Community Services' (MCCS) operational success hinges on its ability to rapidly develop and deploy resilient IT solutions. By integrating Appgate ZTNA into its Cloud Native Access Point (CNAP) offering, MCCS significantly transformed its IT operations to deliver cutting-edge, secure and agile software systems that meet both the secure access and performance needs of Department of Defense (DOD) mission owners.

Introduction

Modernizing IT infrastructure to meet evolving mission demands is a significant challenge for the DOD. For MCCS, it was imperative to eliminate prolonged development cycles, streamline Authority to Operate (ATO) certifications, and replace outdated toolchains and legacy practices that hindered agility. MCCS struggled with prolonged IT solution delivery, constrained by outdated waterfall development methods and rigid compliance processes that stretched project timelines to three years or more. These inefficiencies conflicted with MCCS's need to rapidly deliver IT capabilities that would enhance operational readiness and provide a decisive digital advantage to mission owners.

To accelerate the delivery of mission-critical capabilities to the warfighter, MCCS created Operation StormBreaker to implement a streamlined, dual-path approach to cybersecurity authorization, ensuring both speed and security in deploying mission workloads:

1. **Agile ATO:** Designed for traditional workloads, this process delivers an ATO within 30 days, significantly reducing the time required for security approvals.
2. **Rapid Assess and Incorporate Software Engineering (RAISE):** Optimized for containerized applications, RAISE enables same-day authorization by integrating applications into an existing ATO using certified DevSecOps pipelines.

By leveraging these two pathways, Operation StormBreaker reduced time-to-field from over **36 months to under 9 months**, achieving a **\$10M cost avoidance** over the past 18 months by accelerating operational readiness and eliminating unnecessary delays for MCCS.

Operation StormBreaker's digital transformation strategy is comprised of technology, processes and culture initiatives designed to build a digital enterprise consisting of:

- **A central landing zone and platform for the modernization effort:** The platform, hosted on AWS GovCloud, is SCCA compliant and utilizes cloud-native operations/governance, infrastructure as code, and policy as code. The platform also hosts traditional and modern workloads as a service to mission owners.
- **A software factory to industrialize software delivery:** The Operation StormBreaker Software Factory is a virtual assembly plant equipped with tools, process workflows and environments to produce software with minimal human intervention. It automates the development, build, test, assess, and release process, and deploys container workloads with continuous authorization.
- **Digital transformation through DevSecOps, Lean and Agile:** Operation StormBreaker's modernization strategy integrates technology, processes and cultural initiatives to create an operationally aligned digital enterprise. Embedding cybersecurity within the system development lifecycle transforms risk management into a proactive, data-driven and continuous process, aligning operational outcomes with compliance standards.

JOINT BENEFITS

Speed and Agility

Achieve mission capability deployment at the speed of mission, drastically reducing time-to-field critical solutions.

Unified Access for Distributed Teams

Securely connect government, contractors and mission partners to critical resources, while maintaining strict security protocols.

Enhanced Security


Ensure secure, resilient access to mission-critical environments and workloads with Zero Trust principles.

Improved Developer Productivity

Foster collaboration and accelerate software delivery timelines with seamless, secure access.

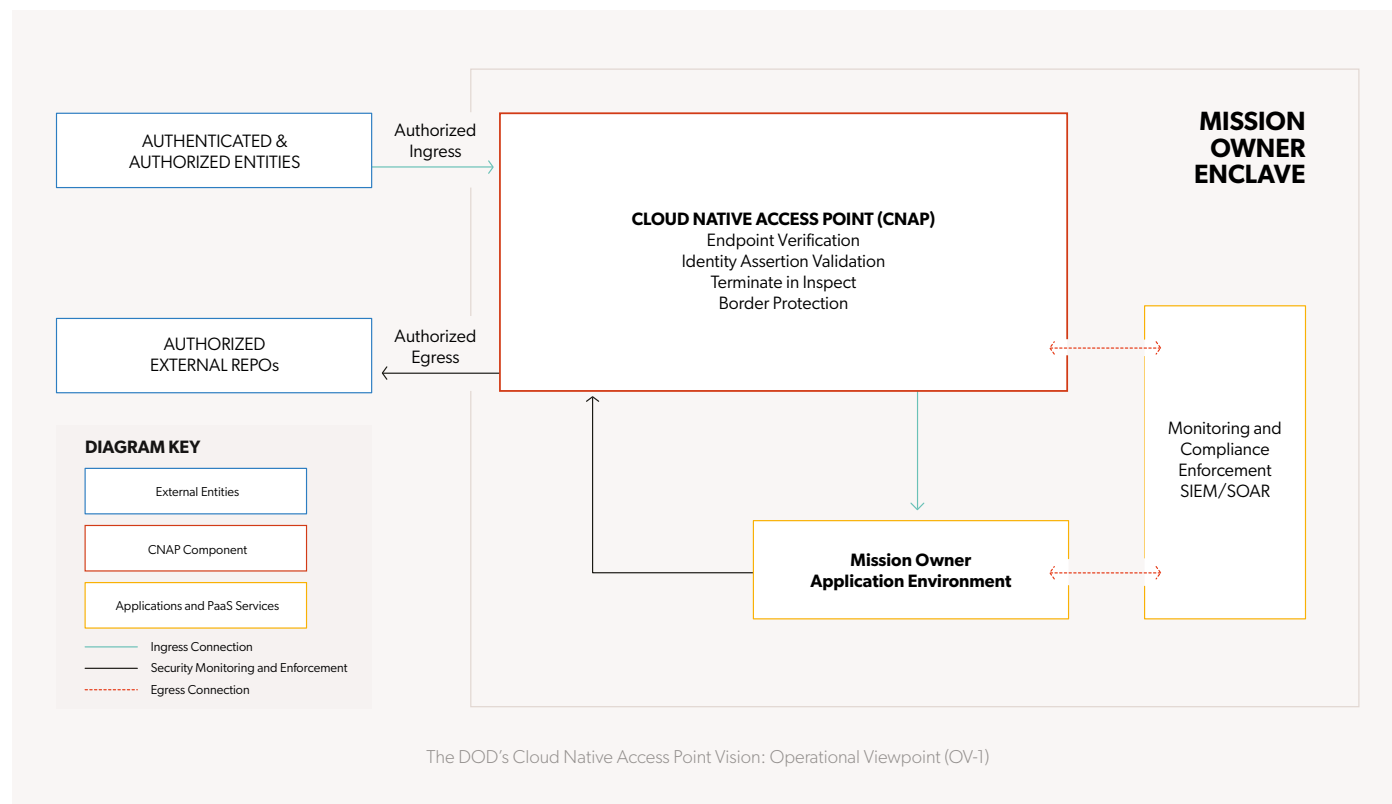
Operational Readiness

Enhance mission effectiveness and warfighter superiority with rapid deployment capabilities.





A key enabler for this transformational approach is the DOD's CNAP framework. CNAP is a Zero Trust architecture that leverages cloud-native security principles to provide secure access to mission-critical resources in cloud environments. This approach ensures that DOD users and devices can securely access resources from anywhere, on any device, while maintaining the highest levels of compliance, encryption and monitoring. In November 2022, Operation StormBreaker set a milestone by being first to the fight, obtaining the first authorized CNAP in the Marine Corps.

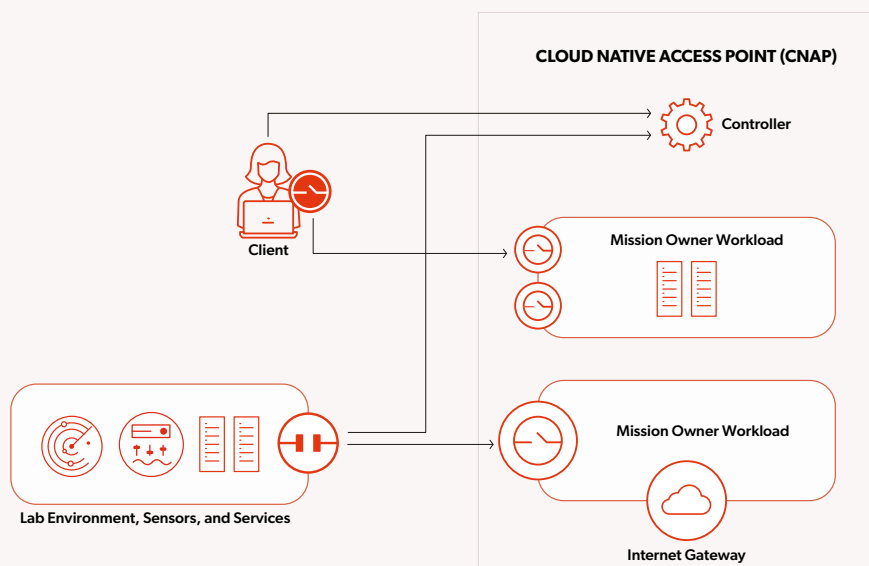


The Solution

Appgate plays a pivotal role in advancing Operation StormBreaker's ZTNA strategy as part of its CNAP framework, delivering a modern security approach tailored to the needs of distributed DOD operations. With Appgate, Operation StormBreaker overcomes legacy security limitations by enabling dynamic, identity-centric access to mission-critical resources. Appgate ZTNA leverages a software-defined, direct-routed model to create highly secure, individualized connections between users, devices, and the specific resources they are authorized to access. This "segment-of-one" approach minimizes the attack surface and provides context-aware, policy-driven access decisions based on real-time conditions, ensuring compliance without sacrificing operational efficiency.

Moreover the integration of Appgate within the CNAP architecture ensures seamless interoperability with Marine Corps Enterprise Networks (MCEN) users by enabling secure, role-based access to mission-critical applications. As a software-defined perimeter solution, Appgate dynamically verifies user identity and device posture before granting access, ensuring that only authorized MCEN users can connect to designated workloads. This approach enhances security while providing a flexible, Zero Trust access model that supports both traditional and cloud-native environments, improving operational efficiency and mission readiness.

Appgate's direct-routed architecture ensures secure, low-latency access by bypassing cloud-based relays and reducing dependency on central chokepoints. This distributed model enhances scalability, availability and resilience, making it ideal for mission owners requiring both agility and security. With Appgate, Operation StormBreaker equips mission owners with the tools to securely innovate at speed, thereby streamlining ATO processes, reducing time-to-field, and ultimately delivering a significant advantage in support of DOD objectives.



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

KEY ASPECTS OF THE JOINT SOLUTION INCLUDE:

Advanced Zero Trust Architecture: Appgate cloaks Operation StormBreaker's infrastructure, allowing only authorized users and devices to access mission-critical environments. This minimizes the attack surface while securing the central landing zone and critical data highways to protect hybrid and cloud environments.

Secure and Distributed Access: Appgate provides secure enclave access for distributed teams, including government, .mil domain, contractors (CTR), and Mission Partner Environments (MPEs), ensuring seamless collaboration while maintaining strict security protocols.

Industrialized Software Delivery: The Operation StormBreaker Software Factory automates development, testing and deployment, accelerating software production and enabling containerized workloads to achieve same-day continuous authorization, with traditional workloads authorized in 30 days.

Agile and Scalable Deployment: The solution supports rapid mission capability deployment while extending secure access to other DOD mission owners, enhancing operational efficiency across the defense ecosystem.

Continuous Security and Compliance: Integrated monitoring and feedback loops ensure real-time visibility, security and alignment with DOD standards to sustain operational readiness.

Conclusion

Operation StormBreaker's CNAP framework demonstrates its commitment to modernizing IT infrastructure to meet the evolving demands of mission-critical operations. By integrating Appgate ZTNA into its CNAP solution, Operation StormBreaker has successfully transformed its approach to secure access, enabling the rapid and reliable deployment of software systems that align with the DOD's stringent security requirements. The reliability and security of the CNAP and fully implemented Advanced ZT was thoroughly tested by Operation StormBreaker's Cyber Security Services Provider (CSSP), Marine Corps Cyber Operation Group (MCCOG) in 2024.

Looking ahead, Operation StormBreaker intends to expand its use of Appgate's advanced capabilities to secure distributed environments, simplify ATO processes, and deliver flexible, context-aware access solutions. This strategic collaboration not only strengthens security and operational effectiveness but also enables Operation StormBreaker to rapidly deploy mission-critical capabilities, giving the Marines they serve a competitive edge.

Operation StormBreaker is offering its platform and capabilities, sharing keys to success, and supporting department-wide transformation so other DOD components can achieve similar positive outcomes. Operation StormBreaker now offers its agile ATO, software factory and landing zone capabilities to other DOD mission owners as a service. For more information or to schedule a discussion, contact MCCSCloudEnclave@usmc-mccs.org.

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 ZTNA 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 Operation StormBreaker

Operation StormBreaker provides a common computing environment for DOD mission owners, offering a full spectrum of commercial cloud services, shared infrastructure, platforms, and active cyber defense. Built for speed, scale, and security, it integrates Zero Trust and modern cloud-native approaches to accelerate mission success in the digital battlespace. Supporting Zone C and Production workloads at Impact Levels 2, 4, and 5, StormBreaker ensures secure, mission-ready compute so you can bring the fight to the cloud with confidence.

About Marine Corps Community Services

MCCS provides commanders with an integrated organization for the development and delivery of Quality-of-Life programs and services. MCCS operates family, fitness and recreation, exchange and business, services and other Quality of Life programs and services for Marines and their families. Learn more at www.usmc-mccs.org.