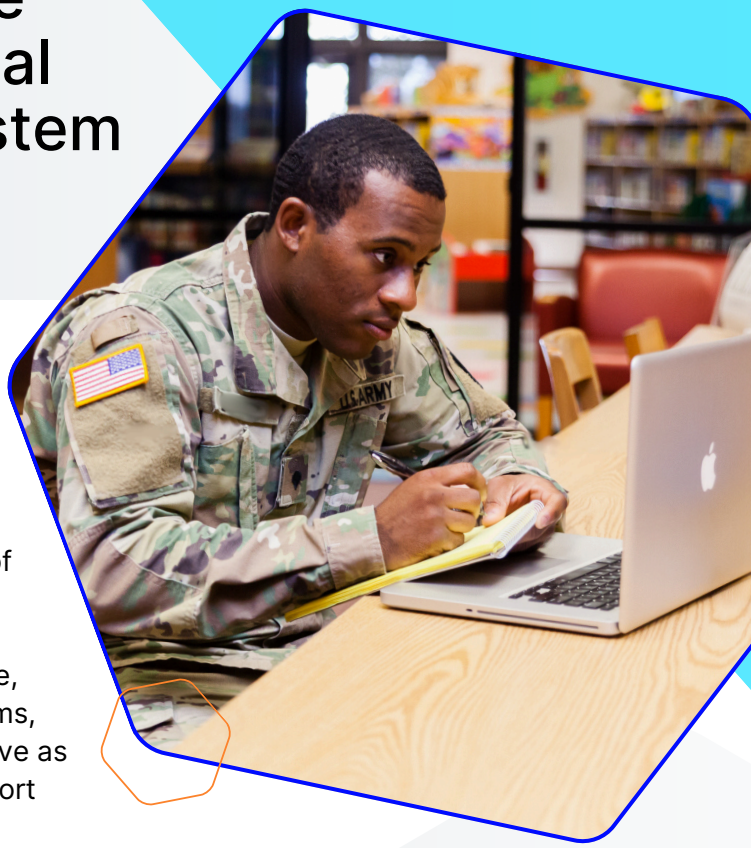
swish CLOUDFLARE

Solution Brief

Optimizing and Securing the Defense Department's Digital Front Door and Support System



Improving Digital Experiences for the Defense Support Structure Network

Across the Department of Defense, also known as the Department of War, millions of service members, families, recruits, civilians, and veterans rely on a broad ecosystem of public-facing digital services every day.

These websites and applications such as Military OneSource, MWR portals, recruiting sites, commissary shopping platforms, education resources, and branch public-affairs domains serve as the digital infrastructure that supports the people who support the mission.

It's important to note that these digital services are not adjunct conveniences, but rather operational enablers.

A military spouse ordering groceries while overseas, a soldier looking for lodging at a military installation in Europe, a sailor accessing recreation services to enjoy hard earned leave, or a veteran looking for healthcare information depend on these sites being fast, reliable, and secure, regardless of where they are in the world.

Yet, most of these properties operate outside of the DODIN. They're often hosted on commercial clouds, legacy platforms, and content-management systems that sit directly on the public Internet and form the digital "front door" to the Defense community.

It's critical that these sites and applications perform flawlessly for legitimate users, while simultaneously stand resilient against constant global cyber pressure. Ensuring their availability and integrity directly contributes to quality of life, readiness, and trust in the DOD's ability to support its people.

> **"These digital services are not adjunct conveniences, but rather operational enablers...**

The Difficulties of Balancing Performance and Security at the Edge

Because these websites and applications operate on the open Internet, they face two persistent challenges:

Performance Limitations

Many of these sites run on aging architectures or unoptimized hosting environments. Users are often stationed abroad or accessing from contested networks and can experience sluggish load times, latency, and periodic outages. Without modern edge distribution, a soldier in Korea or a spouse in Italy may wait three to ten times longer for pages hosted in the U.S. mainland. That delay erodes trust, reduces engagement, and inhibits mission-support services.

Security Exposure

Public-facing Defense websites and applications are also continuously targeted by nation-states, cyber criminals, hacktivists, and automated botnets. These properties face:

- Layer 3–7 DDoS attacks
- Credential stuffing and bot activity
- Application-layer exploits tied to outdated CMS or application vulnerabilities
- Increasing AI-driven attack attempts
- High-value phishing and scraping attempts

Traditional security architectures which are often centralized appliances, bottlenecked tools, and fragmented OSI-layer solutions simply cannot keep pace or scale globally. Many rely on separate web application firewalls (WAFs), load balancers, DNS services, or CDN providers, often stitched together with high cost, operational complexity and limited observability. Worse, every inbound request reaches deep into cloud or hosting infrastructure before being inspected, increasing risk and adding latency.

Bringing a Modern Global Edge Architecture to the Defense Community's Front Door

Swish and Cloudflare deliver a unified, modernized platform that accelerates performance, streamlines operations, reduces costs, and strengthens security for Defense public-facing applications and website without introducing complexity or requiring multi-year modernization cycles.

Cloudflare's global anycast network, spanning 330+ cities across 125 countries, places caching, traffic optimization, and security inspection within milliseconds of 95% of the world's population. Over 40% of the internet is processed by the infrastructure daily, with many of the widest used cloud applications relying upon it. This distributed architecture ensures that performance and protection happen at the edge, not deep within centralized infrastructure.

The Cloudflare Advantage

One global cloud network unlike any other

Only Cloudflare offers an intelligent, global cloud network built from the ground up for security, speed, and reliability.

>40
FedRAMP processing locations, including 8 OCONUS locations

335+
cities in 120+ countries, including 29 NATO countries

13,000+
networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise

405 Tbps
global network edge capacity, consisting of transit connections, peering and private network interconnects

~50 ms
from 95% of the world's Internet-connected population

180+
AI inference locations powered by GPUs

Key Capabilities Include:

- **Ultra-fast CDN and caching** that deliver content locally to global users.
- **Intelligent, real-time traffic routing** that avoids congestion and reduces latency.
- **WAF** with AI-driven detection built on trillions of daily signals.
- **Bot management and API security** to stop automated and application-level threats.
- **Layer 3–7 DDoS mitigation** at massive global scale—absorbing attacks before they reach DoD resources.
- **Global load balancing** for high availability and resilience.
- **Single-pass inspection** combining performance and security without added overhead.

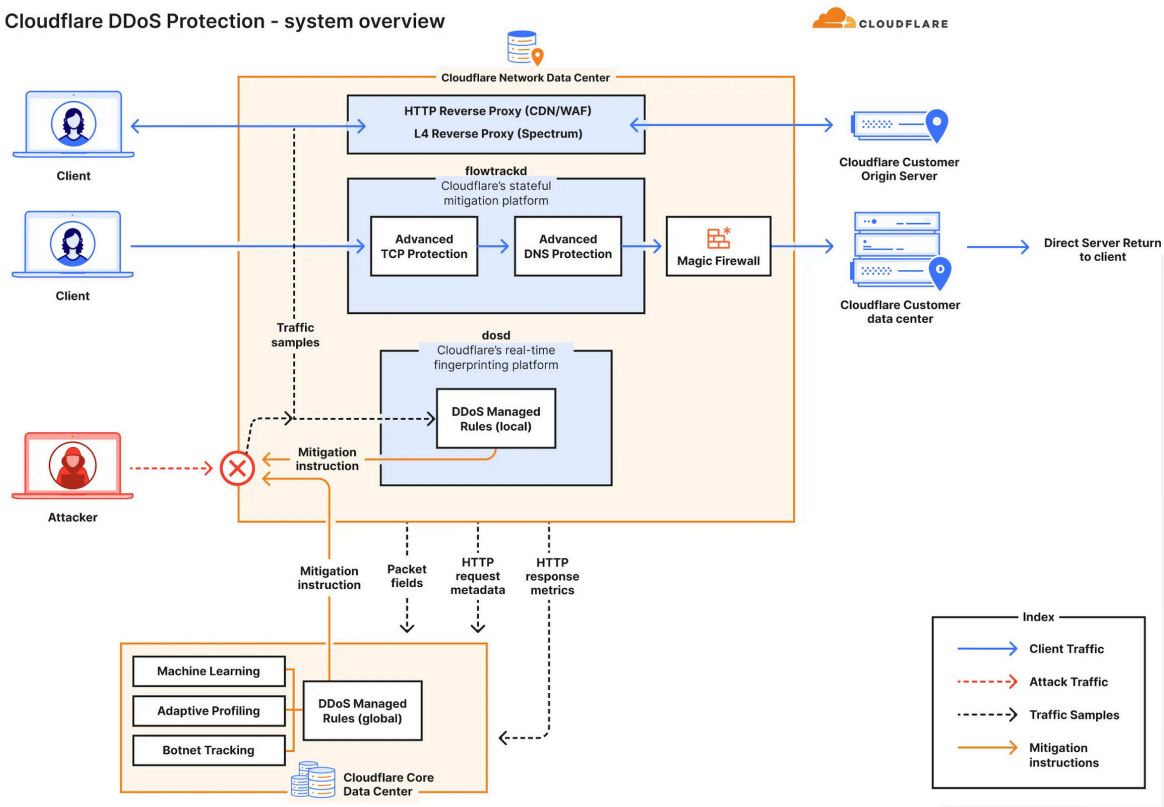
Swish brings deep Defense mission expertise, modernization strategy, and technical integration capability which ensures Cloudflare's platform is aligned to compliance, RMF requirements, CX guidance, and mission outcomes. Together, Swish and Cloudflare offer a simple, scalable, and more cost-effective approach by replacing fragmented legacy tools with a unified platform that performs and protects simultaneously.

Faster Experiences, Stronger Protection, Improved Mission Impact

With Cloudflare operating at the edge and Swish guiding the mission integration, DOD public-facing properties can gain immediate, measurable improvements:

- **Dramatically faster performance** for globally distributed users, including those deployed abroad or connecting from host-nation networks.
- **Higher availability and resiliency**, even during surges tied to recruiting campaigns, PCS seasons, or global events.
- **Reduced cyber risk**, with threats blocked at the edge, far from hosting environments or DOD networks.
- **Lower cost of ownership**, consolidating WAF, CDN, DDoS, routing, and load balancing into a unified platform.
- **Simplified operations**, giving technical owners and ISSMs clear visibility and integrated control.
- **A modernized application posture**, enabling future cloud and digital-service transformation.

For service members, families, recruits, and veterans, the result is simple: reliable, fast, trustworthy digital experiences that support daily life and mission readiness.



Cloudflare offers unrivaled DDoS protection regardless of the location of the user.

A Model for Government-Wide Modernization

The needs of these public-facing DOD websites and applications mirror a broader reality across government: modern public services, require modern digital infrastructure. Swish and Cloudflare's approach of pairing performance and security delivered together at global scale, offers a repeatable, mission-aligned model for government agencies and organizations seeking to modernize without disruption or excessive cost.

Whether supporting military communities, recruiting the next generation of warfighters, or delivering critical public information, government organizations need partners who understands both the mission and technology. Swish and Cloudflare bring the mission-critical combination of deep federal experience, proven edge architecture, and a unified platform that accelerates, protects, and modernizes applications starting on day one.

If you're ready to strengthen your digital front door, and deliver fast, secure, experiences from anywhere in the world, reach out to the Swish and Cloudflare teams by visiting swishdata.com

swish

Swish is a provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for customers. Since 2006, Swish has delivered high-performance solutions and services to the Federal Government market ensuring that customer's digital service capabilities, performance, and security exceed expectations and requirements. Swish is a Service-Disabled, Veteran-Owned and HUBZone certified Small Business.

swishdata.com | info@swishdata.com

The appearance of U.S. Government visual information does not imply or constitute endorsement

CLOUDFLARE

Cloudflare, Inc. (NYSE: NET) is the leading connectivity cloud company on a mission to help build a better Internet. It empowers organizations to make their employees, applications and networks faster and more secure everywhere, while reducing complexity and cost. Cloudflare's connectivity cloud delivers the most full-featured, unified platform of cloud-native products and developer tools, so any organization can gain the control they need to work, develop, and accelerate their business. Powered by one of the world's largest and most interconnected networks, Cloudflare blocks billions of threats online for its customers every day.

cloudflare.com/defense | DOD@cloudflare.com