

# Secure the Mission. Protect the Data.

For the Department of War (DoW), cyber risk is mission risk. As data, users and applications extend across cloud, edge, and AI, legacy security models fall short. Netskope helps the DoW protect sensitive data, enable zero trust access, and maintain operational advantage without slowing the mission.

## Key Benefits

- Protect mission data across cloud, AI, SaaS, web, private apps, and on-prem environments
- Enforce zero trust access to applications and data without exposing the network
- Gain real time visibility into user activity, data movement, and AI and application usage
- Govern AI usage by controlling access, preventing sensitive data exposure, and enforcing policies in real time
- Reduce risk from unauthorized access, credential compromise, and data exfiltration

Nearly 60% of breaches involve human actions [1], with credential compromise a leading vector, putting warfighter access, mission applications, and sensitive data at risk.

<sup>1</sup>Verizon 2025 Data Breach Investigations Report (DBIR)

## The operational challenge

DoW agencies operate in contested, highly interconnected mission environments where users, data, and applications span cloud, web, private networks, and mission partners. This expanded attack surface is increasingly targeted by nation-state adversaries.

- Legacy controls that struggle with modern access complexity and user behavior
- Mission data distributed across cloud, SaaS, edge, and coalition environments
- Adversaries exploit fragmented visibility and legacy access models
- Growing reliance on remote access, contractors, and mission partners
- Urgent need to operationalize zero trust and enable secure AI adoption
- Legacy VPNs and siloed tools limit consistent enforcement and visibility
- Limited cross-domain visibility reduces mission resilience

Agencies must also enable secure access for warfighters, civilians, contractors, and partners without impacting mission speed or continuity.

## How Netskope supports the Department of War

Netskope helps the DoW secure mission data, enable zero trust access, and govern AI usage across cloud, SaaS, web, AI, and private applications. Our unified platform aligns to the DoW Zero Trust Reference Architecture across its seven pillars and helps agencies address challenges such as secure AI adoption. It delivers adaptive, real-time security controls that protect data and govern AI across all environments, providing visibility into data movement and AI activity, reducing exposure of sensitive information, and accelerating zero trust maturity.

## Protect mission data wherever it moves

DoW mission data moves across cloud, SaaS, web, endpoints, and AI environments, far beyond the traditional network boundary. Netskope provides the visibility and control needed to secure sensitive data wherever it travels, while enforcing consistent protection policies in real time.

- Gain visibility into sensitive data across cloud, SaaS, web, and AI
- Prevent data loss and unauthorized access in real time
- Reduce risk from insider threats and unauthorized access
- Apply consistent protection policies across all users and environments

## Enable zero trust access for a distributed force

Warfighters, contractors, and mission partners require secure access without exposing DoW networks. Netskope enables zero trust access by connecting users directly to applications based on identity and mission context.

- Connect users to applications based on intent with granular user-to-application segmentation
- Enforce least-privilege access based on identity, device, and usage context
- Protect sensitive data during access and use
- Reduce lateral movement and limit impact of compromised credentials
- Support secure access from any location or device

## Secure AI to enable mission innovation

The DoW is a rapid adopter of AI for enhanced decision-making and mission effectiveness. Netskope provides the visibility and controls needed to secure AI usage while protecting sensitive data.

- Discover and govern all AI usage, including shadow AI
- Prevent sensitive data from being entered into or exposed by AI tools

- Get real-time content moderation for every interaction
- Enforce real-time policies to allow, block, or guide AI access and usage
- Automate adversarial simulations to continuously validate systems

## Deliver fast, reliable access

Mission users require fast, reliable access to applications and data, whether on base, remote, or at the tactical edge. Netskope NewEdge provides a globally distributed, cloud-native infrastructure to optimize connectivity and ensure consistent performance without sacrificing security.

- Provide low latency, direct access to mission applications
- Eliminate performance bottlenecks from legacy routing and VPNs
- Ensure consistent performance across bases, remote users, and mission environments
- Monitor and optimize user experience across any location with digital experience monitoring (DEM)

## One platform for visibility, control, and operational efficiency

DoW environments often rely on fragmented security and networking tools that increase costs and slow operations. Netskope consolidates critical security capabilities into a single cloud-native platform to reduce complexity and improve operational efficiency.

- Replace multiple tools with a unified cloud-native platform
- Provide unified visibility across cloud, SaaS, web, and private applications
- Enforce consistent policies from a single control plane across environments
- Accelerate detection, investigation, and response across the enterprise



Interested in learning more?

Request a demo

Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for the AI ecosystem inclusive of agents, applications, tools, LLMs, people, devices, and data. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications – providing security and accelerating performance without trade-offs. Learn more at [netskope.com](https://netskope.com), [Netskope.ai](https://Netskope.ai), on [LinkedIn](#), and [Instagram](#).

©2026 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized "N" logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners.