Solution Brief

Netskope NewEdge Government (US)

Federal agencies must secure data, users, and AI across distributed environments. Netskope delivers a FedRAMP High platform that protects federal data wherever it moves, across users, applications, and AI services. By converging networking, security, and data protection into a single platform, agencies reduce risk, simplify operations, and accelerate mission outcomes.

Quick Glance

- Reduce complexity and improve mission efficiency with a unified FedRAMP High platform for networking, security, and data protection.
- Protect federal data in motion and at rest across web, SaaS, cloud, and AI environments.
- Prevent lateral movement with zero trust enforcement that inspects all traffic inline for full visibility.
- Govern and secure AI interactions from prompt to output, preventing data leakage in real time.
- Prevent breaches and maintain mission continuity with real-time detection, control, and enforcement across environments.

> "As a federal systems integrator, Netskope was the clear winner for our zero trust solution adoption."

Todd Welsh, Executive Director
of Zero Trust Engineering.
ManTech International

The Challenge

Federal agencies operate in an environment that has outpaced traditional security architectures. Data is constantly moving across SaaS, cloud, and AI environments, while users work from base, remote, and edge locations. At the same time, encrypted traffic, rapid AI adoption, and expanding hybrid missions have erased the traditional network perimeter. Legacy, fragmented security tools create visibility without consistent enforcement, leaving gaps in control, increased risk of data exposure, and limited ability to apply zero trust uniformly. With constrained resources and rising operational complexity, agencies struggle to modernize securely while managing tool sprawl, controlling costs, and protecting sensitive data.

To meet mission demands, agencies need a unified approach that enforces security where activity actually occurs, at the point of access and data interaction.

The Solution

Netskope for federal agencies

Netskope NewEdge Government (US) is a FedRAMP High authorized platform that converges security, networking, and data protection into a single, cloud-native architecture. With real-time, inline enforcement across all traffic, agencies gain consistent visibility and control without added complexity.

By securing data, access, and AI interactions in one platform, Netskope enables federal agencies to reduce risk, simplify operations, and achieve faster, mission-aligned outcomes.

Secure federal data wherever it goes

Federal agencies must secure sensitive data that moves continuously across SaaS, cloud, web, private applications, and emerging AI environments. Each interaction creates risk, and legacy approaches that rely on perimeter controls or after-the-fact inspection leave critical gaps.

Netskope secures data at the point of interaction with a unified, cloud-native enforcement layer that operates inline and in real time. All traffic, including web, SaaS, private apps, and AI, is inspected through a single-pass architecture, enabling consistent policy enforcement across all channels.

Agencies can identify sensitive data, apply granular controls based on context, and prevent unauthorized access or exfiltration before it occurs. Policies follow the data wherever it moves, eliminating blind spots created by disconnected tools.

By combining complete visibility with real-time control, agencies shift from reactive detection to proactive protection, reducing risk, strengthening compliance, and accelerating secure digital transformation.

Move beyond traditional perimeters and protect sensitive federal data anywhere it travels with consistent, real-time enforcement across all applications and infrastructure.

Contextual and granular zero trust enforcement

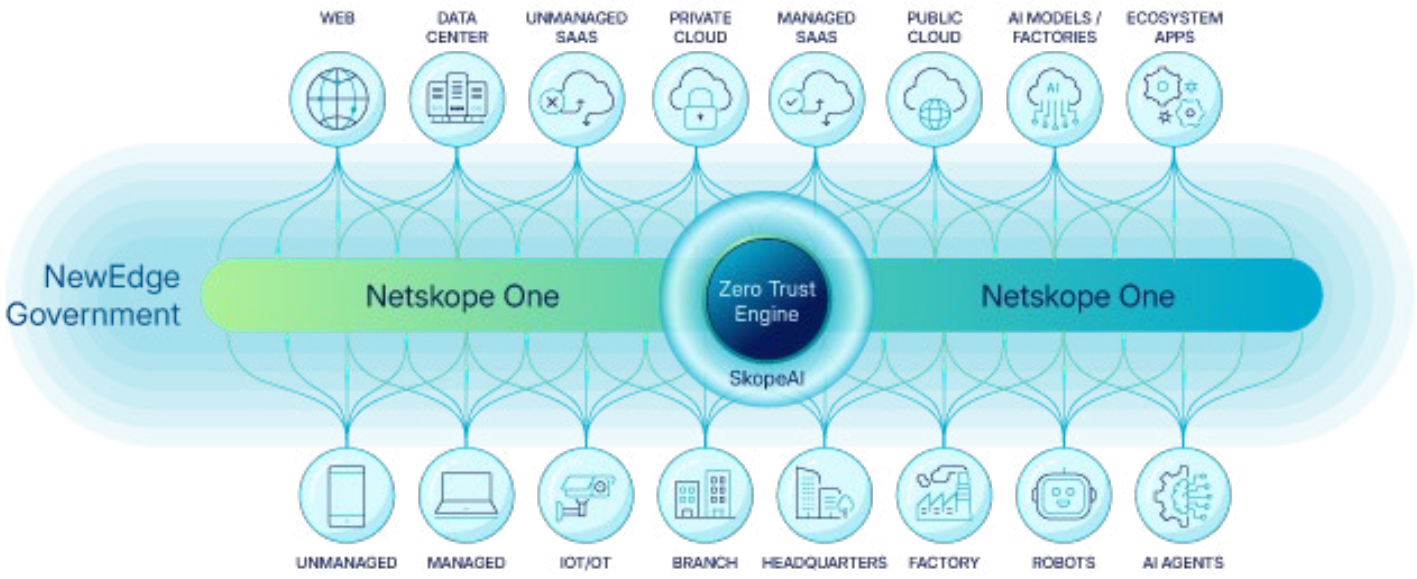
Modern federal environments require access decisions that go beyond static authentication. Users, devices, and applications are constantly changing and trust must be continuously evaluated.

Netskope enforces zero trust by applying real-time, context-aware policies at every access point. Each request is evaluated based on identity, device posture, application risk, location, and session behavior, ensuring access is granted only when conditions are met.

Unlike legacy VPN-based approaches that extend network access, Netskope connects users directly to applications, eliminating implicit trust and reducing the attack surface. Access is continuously monitored and dynamically adjusted throughout the session to prevent misuse or lateral movement.

This approach enables agencies to enforce least privilege at scale, secure remote and third-party access, and deliver consistent, high-performance connectivity for users, whether on base, remote, or at the tactical edge.

Consolidate security tools into a single platform to eliminate complexity, automate reporting, and drastically reduce costs.



Netskope NewEdge Government (US) Architecture

Secure artificial intelligence from prompt to output

AI is rapidly becoming part of daily workflows across federal agencies, but it introduces new risks at the point of interaction. Sensitive data can be unintentionally exposed through prompts, and AI-generated outputs may create downstream security or compliance challenges.

Netskope provides real-time visibility and governance over AI usage across both sanctioned and sanctioned tools. Inline inspection allows agencies to monitor what data is being entered into AI systems and apply policies to prevent sensitive data from being shared.

Controls extend beyond input to govern how AI-generated outputs are handled, enabling agencies to block, allow, or guide user behavior based on context and risk. This ensures that both sides of the interaction, prompt and response, are secure.

By extending unified, real-time enforcement to AI activity, agencies can confidently adopt AI technologies, accelerating innovation while maintaining control, protecting sensitive data, and meeting compliance requirements.

Lower operating costs and complexity

Netskope consolidates security, networking, and data protection into a single cloud-native platform with one enforcement point and a unified management plane. A single client and single-pass inspection architecture reduce infrastructure overhead while improving performance and user experience.

Built-in analytics, automated reporting, and centralized policy management eliminate the need for manual data aggregation and cross-tool correlation. Security teams can quickly understand risk, generate compliance reports, and take action without stitching together insights from multiple systems.

By replacing fragmented workflows with real-time enforcement and unified operations, agencies reduce total cost of ownership, enable faster decision-making, improve efficiency, and free resources to focus on mission priorities instead of tool management.

BENEFITS	DESCRIPTION
Complete visibility across all traffic	Gain unparalleled insights into user activity, sensitive data, and application usage to easily prepare for any operational scenario or emerging threat.
Eliminate legacy virtual private networks	Replace outdated remote access infrastructure with highly secure, context-aware application access that completely removes inherent implicit trust.
Protect data everywhere it travels	Implement robust data-centric security policies that actively follow your sensitive information across the web, cloud applications, and private infrastructure.
Govern artificial intelligence securely	Confidently discover unauthorized artificial intelligence tools and proactively prevent sensitive data exposure during user prompts and large language model interactions.
Reduce total cost of ownership	Consolidate heavily fragmented security and networking tools into a single platform to maximize efficiency and drastically cut operational spending.
Ensure zero trust compliance	Continuously verify every single access request using identity, device health, and rich context to definitively meet strict federal modernization mandates.
Faster incident response	Unified visibility and real-time control enable security teams to detect, investigate, and remediate threats more quickly without relying on manual correlation.
Automate reporting and essential analytics	Utilize built-in analytics to effortlessly generate customized reports, saving countless hours of manual work and instantly improving platform policy tuning.