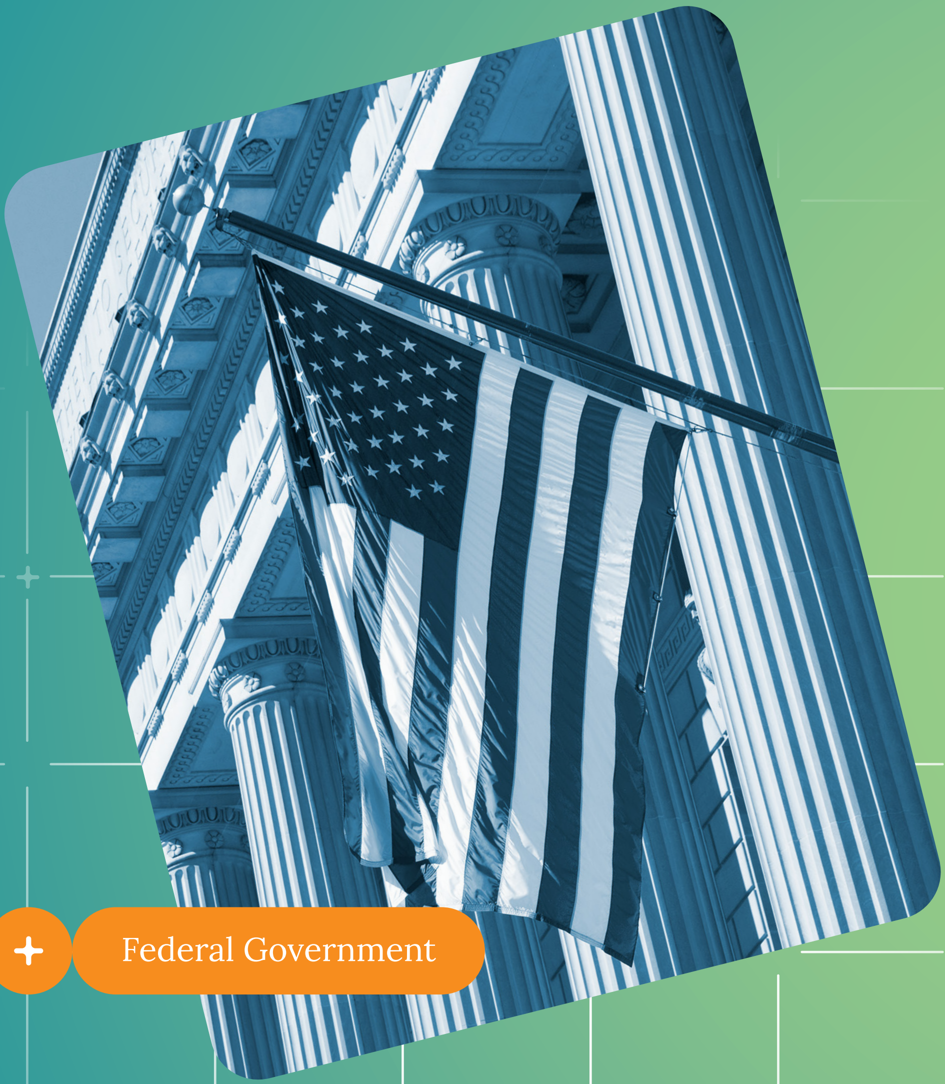
netskope

White Paper

Netskope Intelligent Security Service Edge (SSE) for Federal Government

Four Security Challenges Federal Agencies Can Overcome with Four Principles of SSE



Federal Government

INTRODUCTION: FEDERAL ZERO TRUST ADOPTION REQUIRES SSE

The pandemic in many ways served as the forcing function for zero trust (ZT) adoption, with many agencies realizing the need to move away from a legacy, perimeter-based cybersecurity approach toward a data-centric one with ZT. However, ensuring mission sustainment now requires personnel access to enterprise data and assets from nearly anywhere, not just on-prem, but also in the cloud.

Yesterday Versus Today

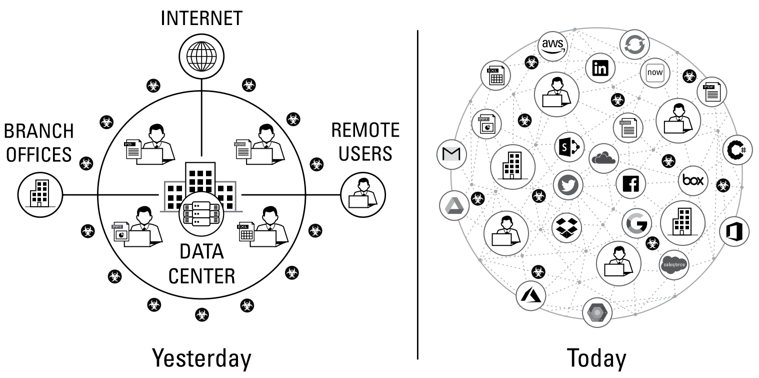


Figure 1. *The old access model was inefficient and ineffective compared to the new model, which enables access from anywhere.*

To address the gaps in security created by this new heavily-remote workforce, agencies are moving towards Secure Access Service Edge (SASE), an architecture that combines several different security and networking elements, at one time siloed, for enhanced security in federal enterprises where cloud access and applications are now ubiquitous. Security Service Edge (SSE), an important concept for understanding the journey to a SASE architecture, represents the evolving security stack needed to successfully achieve a SASE convergence, including technology capabilities such as cloud access security broker (CASB), cloud-native Next-Gen Secure Web Gateway (NG SWG), Firewall-as-a-Service, and Zero Trust Network Access (ZTNA) that are core requirements for that stack.

The Netskope Intelligent Security Service Edge (SSE) solution is integrated on a single platform and includes:

- Cloud-native Next-Gen Secure Web Gateway (NG SWG), multimode cloud access security broker (CASB), and zero trust network access (ZTNA).
- Additional converged capabilities include data loss prevention (DLP), advanced threat protection (ATP), cloud firewall (CFW), remote browser isolation (RBI), user/entity behavior analytics (UEBA), and Advanced Analytics (NAA), all within a single-pass architecture, delivered from a single platform, managed by a single console, and driven by a single policy engine.
- Complete threat and data protection with sensitive data awareness and real-time enforcement and at-rest inspection, with the combination of inline traffic analysis and cloud API interaction.
- Resilience and availability with cloud-hyperscale design, cloud-native infrastructure, and NewEdge, with industry-leading uptime/availability and latency SLAs.

THE FOUR PRINCIPLES OF SSE

SSE, as defined by Gartner in 2021, is a set of security-focused services delivered through the new, SASE cloud-native security architecture for better end-user experiences when securing any user on any device to any service running in public or private clouds. Put simply, SSE describes the evolving security stack that sustains the SASE journey—more specifically, a set of capabilities necessary to achieve the security SASE describes.

Much in the way that federal agencies have realized that Zero Trust is a journey, not a destination, SSE will require a very similar approach. Maintaining a good security posture in today's environment requires the ability to follow agency data, regardless of where it is. With SSE, agencies can gain context-rich information about what's happening across the enterprise with an understanding of the data or object level (e.g., Word document, or Excel sheet). SSE provides distributed points of presence to ensure that the user gets as close as possible to where and how data is accessed, whether it's in the cloud or a private application, ultimately providing agencies with greater visibility and control.

If we usefully organize how SSE solves what security must do in this newer world of keeping data safe in the cloud, four core principles guide our discussion.

Principle #1: Security must follow the data

We now have lots of traffic that a traditional web proxy or firewall can't understand, and can't really even see. We have users who are now everywhere, apps that are in multiple clouds, and data being accessed from anywhere. Given this, organizations must have a security inspection point that follows data everywhere it goes, understanding if the data is sensitive or controlled and limiting the access or export of the data based on where it is accessed from (government system, home system, public system, etc.). According to Gartner, "sensitive-data visibility and control is a critical capability of SASE" and if that inspection point non-negotiably needs to follow the data, that means the inspection point needs to be in the cloud so that its benefits can be delivered to users and delivered to the apps.

Principle #2: Security must be able to decode cloud traffic

Decoding cloud traffic means security must be able to see and interpret API JSON traffic, which web proxies and firewalls can't do. A modern approach to security moves beyond simple allow/block controls and sees what the user is trying to do with the data and understands how they are trying to use it. For example, legacy allow/block controls might bar the upload of files to OneDrive. SSE, on the other hand, could allow more granular controls based on context, meaning that if a user uploads a non-sensitive document to OneDrive, the controls could allow the user to download the file to a home computer for editing if the file doesn't contain PII or CUI information.

> Put simply, SSE describes the evolving security stack that sustains the SASE journey—more specifically, a set of capabilities necessary to achieve the security SASE describes.

According to Gartner, “sensitive-data visibility and control is a critical capability of SASE” and if that inspection point non-negotiably needs to follow the data, that means the inspection point needs to be in the cloud so that its benefits can be delivered to users and delivered to the apps.

Principle #3: Security must be able to understand the context surrounding data access

We must go beyond merely controlling who has access to information and move toward continuous, real-time access and policy controls that adapt on an ongoing basis based on a number of factors, including the users themselves, the devices they're operating, the apps they're accessing, activity, app instance (government vs. personal), data sensitivity, environmental signals like geo-location and time of day, and the threats that are present. All of this is part of understanding, in real time, the context with which they're attempting to access data.

Principle #4: Security can't slow down the network

The user needs to get their data fast, and the network has to be reliable. If security is slowing down access or operability, user experience and productivity suffer, and teams dangerously begin trading off security controls for network speed and reliability. One might think that this is as simple as moving the security controls to the cloud. It's not as simple as that. Ultimately the cloud ends up traversing a dirty place—called the internet—that can cause a whole slew of issues in routing and exposure. This is where private networks come into play so that we can ensure a smooth and efficient path from the end-user to their destination, and back again. Multiple and geographically dispersed POPs enable Netskope to commit to contractual SLAs for high availability and low latency.

With these core SSE principles in mind, there are four security challenges that federal agencies can overcome by leveraging SSE as part of a data-centric SASE architecture.

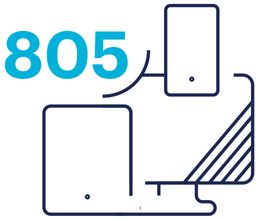
FOUR CHALLENGES FEDERAL AGENCIES CAN OVERCOME WITH SSE

1. **Mitigate user-driven cloud adoption risks with cloud data protection**
   The shift to a majority or at least partial remote workforce over the last few years has served as a forcing function for cloud adoption across federal organizations.

   Unfortunately, however, with traditional perimeters blurring and end users sharing files from corporate machines to personal PCs and cloud-based apps to continue working remotely, this user-driven adoption has created massive security blind spots. The Cloud and Threat Report 2024 from Netskope Research notes that the number of apps used by the average user has increased from 14 to 20 over the past two years, an average 19% increase per year. Even for organizations deploying their own apps, they often lack visibility, let alone the ability to apply adequate controls for cloud data protection.

   Netskope is the gold standard for cloud data protection, as acknowledged by multiple industry analysts and evidenced by adoption in the market. We're pioneering a simple yet powerful approach to modern data protection for multi-cloud and hybrid environments. In contrast to the rigid experience with legacy, appliance-based DLP, Netskope cloud data protection provides the scale, accuracy, and precision needed to deliver security for SASE architectures with agility. Netskope uniquely applies AI/ML to enable scale, efficacy, and automation critical for application discovery, data detection, and classification and access to the data/object with appropriate selective access based on the risk of the device/user in current enterprise environments, where most mission-critical data is processed and stored in cloud applications.

   Corporate traffic today includes approximately 20% image content and image-borne text on average, further complicating data security. Netskope incorporates deep learning models into AI/ML-based image classification for content detection of passports, government IDs, credit cards, social security cards, and other sensitive data types. Netskope also allows federal organizations to create custom classifications based on training to support unique government needs. This model allows detection of images with a higher degree of accuracy and speed without the need to extract all text from images. AI/ML-based image classification also detects screenshots, a highly relevant capability in today's work-from-anywhere environment—especially for controlling screen capture activity by specific groups, such as employees or government contractors who handle sensitive data. The application of AI/ML significantly reduces false positives of image matches at scale. AI/ML-based classifiers can also detect source code, patents, contracts, resumes, and contract-style agreements.



distinct apps are in use by the average 500-2,000 user company

of those distinct apps are unmanaged (i.e. Shadow IT)

2. **Performance and security don’t have to be mutually exclusive**
   In addition to the combination of cloud adoption and security neglect, federal agencies also face the challenge of maintaining IT performance alongside security. At the initial shift to a remote workforce, many agencies leveraged VPNs as a means for remote access to enterprise apps and data. The sheer volume of federal employees connecting via VPN, however, quickly resulted in latency issues and performance degradation, which in turn resulted in employees turning to unmanaged instances of cloud applications for file transfers—connecting to the network by VPN just long enough to get the files and data they needed, then transferring the files to their personal PCs. This challenge not only put agency missions at risk but also significantly increased the attack surface and security risks.

   While legacy approaches to security often mean a degradation in performance, modern approaches and tooling can make security and performance mutually inclusive for federal agencies. Netskope boosts business productivity and agility with the fastest user experience and optimized application performance from its NewEdge security private cloud. Netskope’s extensive peering with web, IaaS, and SaaS providers offers fast, low-latency on-ramps to more than 50 global locations equipped with full compute for real-time, inline security traffic processing close to users. Netskope reinforces its cloud security services with industry-leading service level agreements (SLAs) focused on security traffic processing in the cloud. Addressing both decrypted TLS and non-decrypted transactions, these SLAs build on Netskope’s previously launched five-nines (99.999%) uptime and availability SLA, and ensure customers using the Netskope Security Cloud enjoy network performance at levels of speed and reliability not experienced with other vendors.

   Netskope's flexible traffic-steering options, including the Netskope One Client and integration with existing network investments such as SD-WAN, enable robust data-centric security without the performance trade-offs typical of legacy appliances or competitive alternatives that rely on the unpredictable performance of the public cloud. Customers report that enhancing user experience with the NewEdge network has been one of the most valuable parts of their Netskope journey, with customers typically seeing applications perform 50% better and in one instance a 6x improvement for a customer's top SaaS application. Netskope also offers Proactive Digital Experience Management (P-DEM) to monitor, measure, and investigate the performance of network and data center security services.

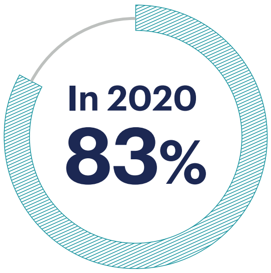
3. **You can’t protect your data if you don’t know where it is**
   Many federal organizations are struggling with how to effectively maintain visibility of their assets and data. In the old world, a file that required signature by three separate users might simply be uploaded to a shared drive, or at worst, emailed several times to each user. In today’s world, however, that same file might originate on the organization’s enterprise network, only to then be sent to a remote user who receives the file at their corporate email address, but then, because DocuSign isn’t an enterprise-approved app, they forward it to a personal email account so they can digitally sign the file with their personal DocuSign account. They then forward the file on to the next user who needs to sign. The second user follows the same procedure, only they accidentally forward it from their personal email account to the third user. The final user signs the file as requested from their corporate address, but is also running Windows XP, and hasn't patched the PC since 2008. In this one, small series of transactions, there are multiple opportunities not just for the data to be lost, but also for malicious code to be embedded within the data when it’s delivered back onto the federal enterprise network.

While some legacy tooling might flag the return file, it likely won't offer a real-time action to mitigate the risks. And, chances are, even if it did, the security team in this scenario would likely be so inundated with other similar flags that this one would just become part of the constant security noise and go unchecked.

Users accessing personal app instances pose a data security threat when users upload sensitive data to them: the organization loses control over access to the data, making it more prone to exposure or misuse. A modern approach to security must be cloud-smart and data-centric—such an approach is the only way to ensure security follows data whenever it goes and maintain real-time, context-rich awareness of your organization's data.

Netskope provides sophisticated cloud security for the deepest visibility and granular context across applications, users, and data with Netskope patented CloudXD as the foundation for our SSE services. Built upon this foundation are unique capabilities that create the structure and attributes that are crucial for effective SSE in action:

- AI/ML-enabled web and cloud application categorization and private application discovery provides the starting point for strong and granular policy enforcement.
- ML-enabled trust scores span cloud applications (the Cloud Confidence Index) and users (the User Confidence Index) to capture anomalies and shifts that in turn can trigger adaptive policy controls and automated workflows for investigations.
- Netskope patented TrueInstance enables dynamic detection of application instances at scale and is critical for data protection and cloud-enabled threat protection.
- Enriched context-based policy with API-based metadata provides the most complete visibility and control between personal, unmanaged, and managed instances for any application or cloud service (i.e., support for 250+ services in AWS including by instance).



of users accessed personal app instances from managed devices each month. Personal app instances pose a data security threat when users upload sensitive data to them: the organization loses control over access to the data, making it more prone to exposure or misuse.

4. **Legacy security approaches are static—Netskope's approach to continuous adaptive trust is dynamic and data-centric**
One of the challenges to Zero Trust adoption that agencies have been wrangling with is the definition. Following Executive Order 14028 to improve the nation's cybersecurity and protect federal government networks, the Office of Management and Budget (OMB) released a Federal strategy in January 2022 to move the U.S. Government toward a Zero Trust approach to cybersecurity. The new strategy states that "a key tenet of a zero trust architecture is that no network is implicitly considered trusted" but it's important to understand that is only the starting point of a long-term zero trust strategy.

When implemented properly and with modern tools to provide proactive controls, improved visibility, and increased points of inspection, Federal agencies can move beyond zero trust. While agencies may be starting with zero trust, the goal should be to create more trust. Traditional security approaches with legacy tooling most often were not designed with zero trust in mind; instead, they focused on perimeter-based security and only protected data that remained within the bounds of that perimeter. In today's environment, agency data no longer only resides within traditional agency perimeters. It's critical that modern approaches and tooling are able to follow the data, regardless of where it resides or the device that's being used to access it.

Netskope's continuous adaptive controls expand zero trust models as part of a SASE, multi-cloud and hybrid architecture to control access, manage threat protection, and monitor data movement. Explicit and granular access controls across applications, application instances, and application activities reduce the attack surface against primary threat vectors such as risky cloud apps, cloud phishing of sanctioned app credentials, and data loss through personal or sanctioned instances of federal government applications, such as M365 or Google Workspace. Netskope's Zero Trust Engine and trust scores for applications and users empower customers to continuously enforce data movement policies and threat protection, with inline behavior coaching and step-up challenges for unintentional or unapproved access or data movement to or between applications.

Netskope leads the way in educating the market about the rise of cloud-enabled threats and data theft which use novel threat tactics emerging in personal and managed use of SaaS applications and public cloud environments. Netskope's Cloud and Threat Report 2024 found that throughout 2023, cloud and SaaS adoption continued to rise in enterprise environments, with users constantly adopting new apps and increasing their use of existing apps. App suites from Microsoft and Google continue to dominate in all industries and geographies worldwide as apps from these vendors become even more ingrained in critical business processes.

According to a public sector-focused survey commissioned by Netskope, 20% of respondents indicated that their organizations' use of cloud solutions increased by 100% or more due to the shift to remote work, more than 30% indicated that it increased by 50% or more, and another 20% indicated that it increased by 25% or more.

Advanced threat protection with Netskope Intelligent SSE prevents malware and threat delivery across web, SaaS, IaaS, and all ports/protocols and is able to identify and thwart a wide array of exploits and identify and remediate anomalous internal (insider) user and entity behavior with real-time policy response options.

Netskope analyzes rich cloud activity metadata from Netskope Zero Trust Engine, plus network and security events and alerts, to create real-time views via pre-built dashboards that are customizable for any audience, from CxO, HR, and BOD, to SecOps and incident response teams. These unique capabilities allow SecOps teams to work with the data that they know best, without reliance on external tools to generate the views they need, and conduct root cause analysis from any perspective—threats, users, data, traffic type (SaaS applications, web, custom applications and services, data). Netskope also provides high-performance log streams to SIEMs, data lakes, and cloud storage to enable SOC and MDR process workflows for incident response and investigations.

Inline user coaching effectively reduces the noise of inadvertent user activities, such as sharing a file to a personal application instance or uploading to the instance of another business unit, which may include third-party users not authorized to access sensitive data placed in those instances. By reducing the attack surface with granular controls and reducing the noise of user errors with inline coaching, advanced data loss prevention can be focused on protecting sensitive and mission-critical data, one of the federal government's most important assets.

CONCLUSION

Netskope delivers simplicity with powerful integrated capabilities. Netskope GovCloud is the government authorized instance of the Netskope Intelligent SSE platform and is powered by the NewEdge network, used by thousands of commercial organizations around the world. Netskope GovCloud is FedRAMP High authorized and provides comprehensive security delivered from the cloud.

At every license level and in every product configuration, Netskope's differentiated SSE offers federal government customers deep visibility across all traffic, including web and SaaS applications, cloud services, and private applications. Our instance awareness and profiles for more than 41,000 cloud applications provide granular control of activities that enable federal government customers to secure their remote workforce, ensure successful cloud adoption, and sustain critical mission objectives.

The Netskope Intelligent SSE solution delivers these powerful access control and threat and data protection capabilities in simple, straightforward packaging for federal government customers to easily consume, and implement Netskope either in forward proxy or reverse proxy for web, private applications, SaaS applications (both approved and unapproved), all managed through a single console.

Navigating the host of security products available on the market today can seem as challenging as identifying and mitigating all the security risks facing your organization. While Netskope's platform is comprehensive, our SSE solution was engineered as part of our platform to provide simplicity through powerful, integrated capabilities across the policy administration lifecycle. With Netskope's SSE solution, federal security leaders can be empowered to move beyond their legacy approaches and tooling and abandon security distractions so they can focus on maintaining a secure organization for today and tomorrow.

WHAT DOES GARTNER SAY ABOUT SSE?

Security Service Edge (SSE) was defined by Gartner in 2021 to capture the evolving security stack necessary to deliver a Secure Access Service Edge (SASE) architecture. The core SSE capabilities can help enable better end-user experience when securing any user on any device to any service running in public or private clouds. SASE converges multiple security technologies for web, cloud, data, and threat protection, plus cloud-edge networking capabilities, into a scalable, elastic platform that protects users, data, and applications everywhere.

Key points:

1. Core capabilities of SSE include cloud-native secure web gateway (SWG), multimode cloud access security broker (CASB), and zero trust network access (ZTNA).

2. Additional converged capabilities include data loss prevention (DLP), advanced threat protection (ATP), firewall-as-a-service (FWaaS), remote browser isolation (RBI), and user/entity behavior analytics (UEBA), all within a single pass architecture, delivered from a single platform, managed by a single console, and driven by a single policy engine.

3. Complete threat and data protection with sensitive data awareness require real-time enforcement and at-rest inspection, possible only with the combination of inline traffic analysis and cloud API interaction.

4. Adaptive policy controls for users, devices, applications, and data permit dynamic balancing of trust against risk that often changes.

5. Strong, actionable SLAs must demonstrate a provider's commitment to ongoing stability of operations and rapid remediations when breaches occur.

ABOUT NETSKOPE

As enterprises transform their legacy IT infrastructure and move applications and data to the cloud, security needs to transform as well. Netskope's SSE is the leader in cloud security helping agencies comply with regulations, protect sensitive information, and defend against the latest emerging threats. Empower your agency today with Netskope's real-time data visibility, defend against the threats of tomorrow, and take advantage of the cloud without sacrificing security. Learn how Netskope helps the Public Sector be ready for anything, visit https://www.netskope.com/solutions/public-sector.

Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.

©2024 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 04/24 WP-524-3