netskope

White Paper +

Netskope Security Service Edge (SSE) for Central & Local Government and Healthcare

Four Security Challenges Government and Healthcare Organisations Can Overcome with SSE

+ Government

INTRODUCTION

The UK public sector faces significant data privacy and cybersecurity challenges as it navigates the complexities of digital transformation, a hybrid workforce, cloud adoption, technology consolidation, and evolving cyber threats. Maintaining adequate defences on-prem was already hard enough for government and healthcare services, but now the opportunities for attack and the lack of visibility leave many risks not just unchecked, but unknown..

Yesterday Versus Today

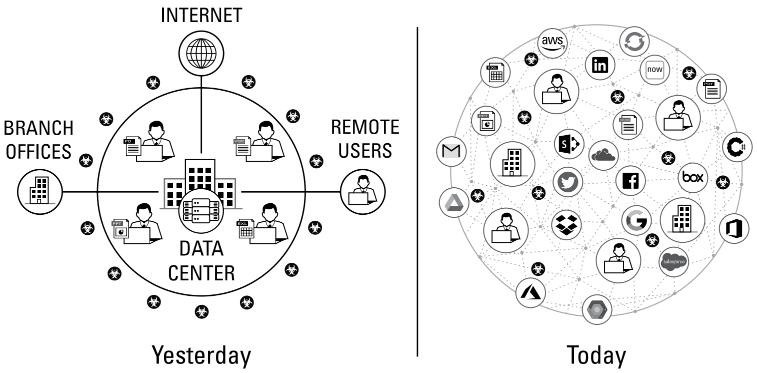


Figure 1. *The old access model was inefficient and ineffective compared to the new model, which enables access from anywhere.*

This deluge of changes and challenges has left many government and healthcare security leaders in a perpetual state of distraction and fear—not just of falling victim to an attack, but of the far-reaching, long-term impacts of an attack on their data, employees, citizens, and patient trust.

A security strategy rooted in an on-prem environment simply won't be effective in an environment where your users and data are being accessed outside the purview of your security team and tools. And, there isn't an "undo" button—the changes to the security landscape aren't elastic and we're not going to just snap back to a time when former security strategies were effective, so it's critical that security leaders take swift, intentional action to retire their legacy tools and strategies and adopt a modern, cloud- and data-centric approach to security.

To address the gaps in security created by this new heavily remote workforce, both local and central government and healthcare are moving toward Secure Access Service Edge (SASE), an architecture that combines several different security and networking elements, at one time siloed, for enhanced security in organisations 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.

Netskope supports the core pillars of the UK Government Cyber Security Strategy with a converged and fully integrated SSE solution that includes SWG, CASB, UEBA, ZTNA, DLP, cloud firewall, and more. This differentiation enables government and healthcare organisations to:

- Gain comprehensive visibility and control over users, devices, and applications with real-time threat protection and data security capabilities.
- Secure access to web, cloud, and private applications for the hybrid public sector workforce.

- Securely enable generative AI applications in sensitive data environments, ensuring compliance and data protection.
- Significantly reduce vendor and tool sprawl, and increase efficiency by deploying and administering fully integrated technologies.
- Benefit from a consistent set of policies on a single management plane located in London providing data residency and sovereignty for log data and API processing.
- Ensure regulatory compliance with a platform accredited to standards including SOC 2, ISO, Cyber Essentials and more.
- Significantly reduce the complexity of integrating legacy technologies and unlock a secure ecosystem of cloud services and third-party applications. This enables the public sector to build stronger partnerships and collaborations with the private sector.

THE FOUR PRINCIPLES OF SSE

Gartner defines Security Service Edge (SSE) as a set of security-focused services delivered through the new SASE cloud-native security architecture, securing access to the web, cloud services, and private applications regardless of the location of the user or the device they are using or where that application is hosted. SSE protects users from malicious and inappropriate content on the web and provides enhanced security and visibility for the SaaS and private applications accessed by end-users.

Much in the way that government and healthcare organisations have realised 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 department data, regardless of where it is. With SSE, organisations can gain context-rich information about what's happening across their environment 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 organise 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, organisations 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 and is critical in our app-centric, risk-accepting, AI-embracing world. 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

Much in the way that government and healthcare organisations have realised 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 data, regardless of where it is.

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 Official-Sensitive or PII information.

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 local and geographically dispersed data centres 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 government and healthcare can overcome by leveraging SSE as part of a data-centric SASE architecture.

1. **Mitigate user-driven cloud adoption risks with cloud data protection**
   While many local and central government departments and healthcare organisations have historically been slow to move to the cloud, the shift to a majority or at least hybrid remote workforce has served as a forcing function for cloud adoption. Unfortunately, however, since end-users are often inclined to choose convenience over security, 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 2024 Netskope Cloud and Threat Report noted that the transition from traditional, on-prem applications to cloud and SaaS apps is far from over, increasing 19% per year. Currently, half of all users now interact with between 11 and 33 apps each month, generating between 600 and 5,000 activities per month. Generative AI (genAI) apps are adding to visibility challenges, as the 2024 Netskope Cloud and Threat Report: AI Apps in the Enterprise shows that 96% of surveyed organisations have users engaging with genAI, with the number of users tripling over the past 12 months. Even for organisations 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

> 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.

scale, efficacy, and automation critical for application discovery, data detection, and classification 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, drivers licences, and other sensitive data types. Netskope also allows organisations to create custom classifications based on training to support unique government and healthcare needs. This model allows detection of images with a higher degree of accuracy and speed without the need to extract all text from images. Netskope's 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.

2. **Performance and security don't have to be mutually exclusive**
Government and healthcare services face the dual challenge of adopting cloud technologies while ensuring security and maintaining IT performance. Many organisations operate in rural areas with limited bandwidth, rely on field workers connecting over VPNs, or continue to support work-from-home arrangements due to pandemic-driven policies. These factors can lead to backhauling and latency, causing significant performance issues that disrupt business operations and mission execution while heightening security risks.

50%

of users now interact with between 11 and 33 apps each month, generating between 600 and 5,000 activities per month[1]

96%

of organisations surveyed have users using genAI, with the number of users tripling over the past 12 months[2]

Modern security solutions, like Netskope's NewEdge Network and private cloud infrastructure, eliminate the traditional trade-off between security and performance. Netskope enhances productivity and agility through fast, optimised user experiences. The NewEdge Network provides comprehensive security without sacrificing application performance, making it a powerful solution for public sector organisations balancing security with operational efficiency.

The Netskope NewEdge Network delivers robust security coverage and resilience with strategically located data centres in over 75 regions, including four UK points of presence (PoPs) in London and Manchester. These local PoPs enable real-time, inline security traffic processing, ensuring government operations remain secure and uninterrupted even during failovers or maintenance. Key features of the NewEdge Network include global access via over 100 data centres, localisation zones covering more than 200 countries and territories, and direct peering with Microsoft, Google, and AWS to minimise latency and optimise performance. Additionally, NewEdge infrastructure meets stringent public sector security requirements through compliance with regulatory frameworks in the US (FedRAMP High), Canada (PBMM), and Australia (IRAP).

Netskope's cloud security services are further strengthened by a management plane in London, which provides policy management, logging, out-of-band services like malware analysis, and ensures data residency and sovereignty for log data and API processing. The data plane, located in

London and Manchester, supports industry-leading SLAs focused on secure traffic processing in the cloud, addressing both decrypted and non-decrypted TLS transactions. With a 99.999% uptime SLA, Netskope guarantees superior performance levels, far surpassing other vendors in speed and reliability.

Netskope's flexible traffic-steering options, including the Netskope Client and integration with existing network investments like SD-WAN, deliver data-centric security without the performance drawbacks common to legacy appliances or competitors relying on public cloud infrastructure. Customers frequently report significant performance improvements, with applications performing up to 50% better, and some experiencing a sixfold improvement for key SaaS applications. Netskope also offers proactive digital experience management (DEM) to monitor and optimise the performance of network and data centre security services.

3. **You can't protect your data if you don't know where it is**

   Many public sector organisations face challenges in maintaining visibility over their assets and data. In the past, files requiring multiple signatures might be uploaded to a shared drive or emailed. However, in today's environment, the same file may pass through several unsecured channels. For example, a file could be sent from a work email to a personal account for signing via an unapproved application like DocuSign, then forwarded through various personal and corporate accounts. This process introduces multiple points of vulnerability, increasing the risk of data loss or the introduction of malicious code into the organisation's network.

   Legacy tools may detect issues upon file return, but often lack real-time mitigation capabilities. With 74% of data theft occurring when corporate data moves to personal instances of approved cloud applications, it's critical to have solutions with instance awareness. This feature allows Netskope's SSE to distinguish between sanctioned and personal instances of the same cloud application. By leveraging this capability, Netskope enforces policies that block access to unauthorised instances or redirect users to approved environments, reducing the risk of data exfiltration and ensuring sensitive data stays within secure, sanctioned applications.

   Netskope SSE provides robust data protection for public sector organisations by securing data across all control points. It prevents accidental or intentional data leakage through comprehensive web protection, real-time cloud traffic inspection, and monitoring of corporate SaaS applications like Microsoft 365, Salesforce, Google Workspace, and Slack, as well as IaaS platforms like AWS, Azure, and Google Cloud. The solution also supports the secure use of generative AI through ML-assisted discovery and risk assessment, while offering advanced DLP capabilities such as file fingerprinting, entity detection, and ML-based classification. It leverages over 3,000 predefined data and personal identifiers to address a variety of use cases and compliance requirements, including GDPR. Additionally, it provides controls to help organisations comply with standards like ISO/IEC 27001:2022, NIST CSF, and NIS2. This ensures comprehensive protection against data leakage, even on personal and unsanctioned platforms.

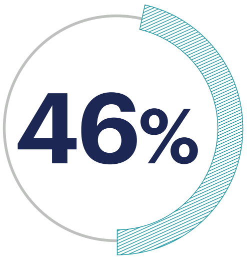
4. **Compliance is static, continuous adaptive trust is dynamic and data-centric**

   The UK government and healthcare must comply with various regulations such as GDPR, Cyber Essentials, NIS2, ISO/IEC 27001:2022, and NCSC guidance. While these compliance frameworks provide essential baselines for cybersecurity, static compliance alone is insufficient to address the constantly evolving cyber threat landscape. To remain resilient, organisations must adopt a continuous, adaptive cybersecurity approach based on zero trust principles. This model assumes no inherent trust, continuously verifying users, devices, and systems at every access point, regardless of their location or previous access history.

   The UK Government's Cyber Security Strategy emphasises the move toward a zero trust approach, minimising access by granting only the least necessary permissions, combined with ongoing verification to reduce risks. This shift is reinforced by the Secure by Design framework, which embeds cybersecurity into every phase of the digital life cycle—from planning and procurement to operation and decommissioning—ensuring security is a foundational consideration rather than an afterthought.

Netskope's Zero Trust Engine, a foundational component of Netskope's SSE solutions, plays a pivotal role in enabling adaptive cybersecurity by continuously gathering and analysing risk telemetry on users, data, devices, and applications. This provides granular, context-aware policy enforcement that dynamically adjusts to the changing risk landscape, moving beyond traditional binary approaches of "block or allow." By employing this adaptive trust model, Netskope ensures sensitive data is safeguarded across all control points, including networks, clouds, endpoints, emails, and even unsanctioned instances of cloud applications. This level of insight helps government and healthcare security teams to maintain secure operations in an environment where data moves fluidly across platforms and devices.

Netskope's user and entity behaviour analytics (UEBA) enhances this adaptive approach by detecting anomalous behaviour that may signal insider threats or compromised accounts. By continuously monitoring activity, Netskope can enforce real-time policy actions, such as blocking risky behaviour or prompting additional verification, to prevent incidents before they escalate.



of malware downloads originate from popular cloud apps[3]

Netskope also provides advanced threat protection against malware, ransomware, and phishing. It decodes cloud traffic and blocks threats across web, SaaS, and IaaS environments, backed by multi-layered defences like anti-malware, intrusion prevention systems, and sandboxing. With tools like User Confidence Index (UCI) risk scoring and remote browser isolation (RBI), it reduces the attack surface and protects networks from compromised users or risky activities.

Cloud Confidence Index (CCI) enables granular control over cloud apps, distinguishing between sanctioned and unsanctioned instances. This reduces the risk of data exfiltration and unauthorised access by automatically blocking or redirecting users to secure, approved instances of applications like Microsoft 365 or Google Workspace.

Netskope also provides advanced data loss prevention (DLP) tools, including inline user coaching, to reduce errors and protect sensitive data across both sanctioned and unsanctioned environments. Its customisable dashboards and seamless integration with SIEMs allow SecOps teams to efficiently detect, investigate, and respond to threats, ensuring organisations stay compliant, and stay prepared for emerging cyber risks.

CONCLUSION

Netskope delivers simplicity with powerful integrated capabilities. At every licence level and in every product configuration, Netskope's differentiated SSE offers local and central government and healthcare customers deep visibility across all traffic, including web and SaaS applications, cloud services, and private applications. Our instance awareness and profiles for more than 75,000 cloud applications provide granular control of activities that enable customers to secure their remote workforce, ensure successful cloud adoption, and sustain critical mission objectives. The Netskope SSE solution delivers these powerful access control and threat and data protection capabilities in simple, straightforward packaging for government and healthcare customers to easily consume, and implement Netskope either in forward proxy or reverse proxy for web, private applications, and SaaS applications (both approved and unapproved), all managed through a single console for greater efficiency.

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 organisation. While the Netskope platform is comprehensive, our SSE solution was engineered as part of our platform to provide simplicity through powerful, integrated capabilities across the policy administration life cycle. With the Netskope SSE solution, government and healthcare leaders can be empowered to move beyond their legacy approaches and tooling and abandon security distractions so they can focus on maintaining a secure organisation for today and tomorrow.

ABOUT NETSKOPE

As enterprises transform their legacy IT infrastructure and move applications and data to the cloud, security needs to transform as well. The Netskope Security Cloud delivers Security Service Edge (SSE) and Secure Access Service Edge (SASE) architecture through a comprehensive, cloud-native platform of technologies that enable secure enterprise digital transformation and secure work-from-anywhere connectivity using integrated cloud access security broker (CASB), secure web gateway (SWG), and Zero Trust Network Access (ZTNA) capabilities. Netskope is fast everywhere, data-centric, and cloud smart, all while enabling good digital citizens and providing a lower total cost of ownership.

1. "Cloud and Threat Report", Netskope, 2024. 2. "Cloud and Threat Report: AI Apps in the Enterprise", Netskope, July 2024. 3. "Cloud and Threat Report", Netskope, 2024.

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.