eBook

Securing the UK Roadmap for Modern Digital Government

Delivering modern digital government across central government, defence, the NHS, and frontline services in the UK requires joined up cybersecurity.

netskope

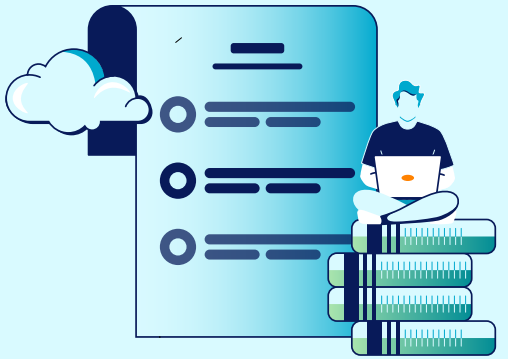

Table of contents

Executive summary

Guided by the Roadmap for Modern Digital Government 2030, the UK public sector is undergoing unprecedented transformation. The new strategy scraps isolated digital pilots in favour of systemic, outcomes-based reform across both central and local government. Central to this vision is unified service delivery and the construction of robust digital public infrastructure, including the National Data Library.

When central government, local authorities and the NHS work to deliver joined-up, AI-enabled services in line with this roadmap, it presents both incredible opportunities and complex security challenges.

This eBook explores how modern network and security platforms such as Netskope One can empower organisations to meet government roadmap objectives. These include the NIST Cyber Security Framework (CSF), NCSC Cyber Assessment Framework (CAF), NHS Data Security and Protection Toolkit (DSPT), and the NHS 10 year plan. We detail how moving from outdated on-premises security stacks delivers true cyber resilience.

Last year, the State of Digital Government Review identified 28% of central government systems as legacy technology: a significant barrier to secure modernisation. The UK's digital strategy relies heavily on collaboration and combined services across departments, local authorities, and private sector contractors. This eBook gives examples of how Netskope's secure access service edge (SASE) platform facilitates these secure integrations, ensuring that shared data and services remain protected under consistent security policies, regardless of where they are accessed.

By adopting the Netskope One platform, organisations can foster shared services, safely harness the National Data Library, and secure the NHS digital front door. The Netskope Zero Trust Engine provides the granular visibility, advanced data loss prevention (DLP), and zero trust network access (ZTNA) required to protect official data and protected private information.

This eBook outlines how the public sector can embrace cloud, SaaS, web, and generative and agentic AI technologies securely, using UK infrastructure, accelerating digital transformation without compromising safety or citizen trust.

Approximately 28% of central government systems are classified as legacy technology.

Source: State of Digital Government Review

Overcoming legacy IT debt in central and local government

Building secure infrastructure that enables modern digital government.

The Roadmap for Modern Digital Government stresses the urgent need to ditch legacy IT to improve citizen services. With around 28% of central government systems classified as legacy, modernisation is critical.

The Netskope One platform acts as a catalyst to meet this goal, consolidating security services and embracing zero trust network access. UK government departments can move from restrictive legacy security to a modern cloud-first security model, with unified threat protection, real-time data protection and access control in one architecture.

This evolution means Official-Sensitive data is no longer exposed by outdated on-premises security. Netskope One Private Access replaces legacy VPNs and grants least-privilege access to internal applications, reducing complexity while defending against state-sponsored threats.

Cyber resilience is powered by the NewEdge network, with UK data centres guaranteeing continuous operational coverage while satisfying strict data protection mandates for government, citizen and patient data.

By consolidating fragmented point solutions—such as standalone VPNs, proxies, and legacy DLP—into a single, UK-sovereign cloud platform, public sector bodies achieve better value for money while modernising security.

Enabling shared services: streamlining frontline services for local authorities

Fostering collaborative council initiatives and AI innovation without adding complexity.

A core pillar of the 2030 Roadmap is joined-up services. As local authorities face increased pressure to deliver value for money while digitising services, managing multiple security point products is unsustainable.

Netskope One is a powerful shared services enabler, supporting local authority mergers and collaborative initiatives without complex hardware or backhauling. Councils consolidate web, cloud, and data security into one unified platform, eliminating the friction of traditional networks. This dramatically improves the cyber posture of local communities, and ensures consistent security across merged or shared entities.

By deploying zero trust network access (ZTNA) with Netskope, councils replace slow, vulnerable legacy VPNs. Civil servants securely access applications from anywhere, fast, boosting productivity.

As frontline staff embrace AI to boost productivity, data risks rise. Netskope provides deep visibility and complete data control for the entire AI ecosystem, empowering IT to protect data without stifling productivity.

Netskope One Security Service Edge (SSE) acts as a powerful shared services enabler, supporting council mergers and collaborative initiatives for local authorities without the need for complex hardware backhauling.

Powering community-focused, integrated care models

Just-right, timely, seamless and secure access to patient data from any device needed to provide the best care.

As NHS Trusts and Integrated Care Boards (ICBs) embrace integrated care models, the risk to patient data grows. A unified digital record requires secure, reliable access. Netskope ensures clinicians access electronic patient record (EPR) systems securely from any location—a GP surgery, hospital ward or in the community—and any device.

Netskope One Private Access provides this connectivity without the friction or performance issues of traditional VPNs. Healthcare professionals can access any applications they need using zero trust principles. As a result, patient data is always protected, aligning with the DSPT and GDPR. With Netskope One Enterprise Browser secure access to these records is possible from any device, so clinicians can deliver more timely, patient-centric care.

Netskope One Data Loss Prevention (DLP) protects patient data from accidental exposure or insider threats, (including preventing well-meaning clinicians from pasting sensitive notes into unapproved AI chatbots), reducing risk.

Netskope One DLP directly supports the NCSC Cyber Assessment Framework (CAF) Objective B (Protecting Against Cyber Attack), by preventing exfiltration of "Official-Sensitive" and "Personally Identifiable/Protected Health Information" (PII/PHI) data across cloud, SaaS, AI, and web.

Harnessing AI and the National Data Library

Securing the AI pipeline for public sector innovation. Moving from the Department of No to the Department of Know.

To support government plans to scale AI and leverage the National Data Library, robust guardrails are essential. AI presents unprecedented opportunities to improve public services, but organic experimentation can expose highly sensitive data.

Netskope secures the entire AI ecosystem including AI applications, copilots with SaaS apps, and agents. Advanced DLP and AI guardrails integrate to identify and block sensitive data from entering AI models, and block adversarial attempts to override system rules or exfiltrate data, by inspecting every request and response.

CASB provides granular visibility into risk and activity in every SaaS and AI tool accessed by remote workers, civil servants, and clinicians, giving a clear view of shadow AI.

Netskope consolidates CASB, next-gen secure web gateway (SWG), and zero trust network access (ZTNA) into one unified platform. This convergence empowers IT to move away from restrictive “block” or “allow” policies for AI, cloud, web, and SaaS.

The boundless potential of AI means new tools frequently arrive unvetted in a user’s browser tab. Organisations face massive application sprawl, with the median enterprise now using 28 distinct AI apps. Netskope shines a light on shadow AI.

Citizen data—always safe—right here in the UK

UK infrastructure with G-Cloud and Cyber Essentials alignment.

Data security is a critical requirement for UK public sector infrastructure. To support this mandate, Netskope traffic is routed directly through UK NewEdge data centres in London and Manchester.

Localised infrastructure ensures all public sector traffic remains strictly UK-resident, satisfying rigorous data security requirements. Crucially, it provides the continuous operational resilience and low-latency performance essential for uninterrupted citizen services and life-saving emergency care.

It's easy to procure Netskope via the G-Cloud framework, and it can assist organisations in meeting and maintaining the necessary controls to achieve Cyber Essentials Certification because it aligns to the five core technical control requirements for IT infrastructure defined by the UK National Cyber Security Centre (NCSC).

With Netskope, the UK public sector can keep highly sensitive information within the country to protect national security and citizen privacy.

Netskope traffic is routed through UK NewEdge data centres in London and Manchester, enabling data residency, low latency, and continuous performance for public sector users.

Delivering secure innovation and cyber resilience for the UK public sector

Transition to a modern digital government and an AI-enabled NHS requires a fundamental shift in cybersecurity architecture. Legacy systems and fragmented point solutions cannot provide the agility, productivity, or protection needed to meet the ambitious goals of the 2030 Roadmap.

By adopting the Netskope One platform, UK public sector organisations can achieve comprehensive visibility and control, directly aligning with NCSC CAF, NHS DSPT and NIST CSF 2.0 requirements.

We equip the public sector to embrace cloud and AI technologies securely, fostering a proactive security mindset that accelerates digital transformation and delivers value for money, all while protecting the nation's most sensitive data.

Start your journey toward a secure, modern digital government today. Request a demonstration to see how the Netskope One platform can consolidate your security stack and protect your sensitive data.
Visit Netskope.com/demo.

About Netskope

Netskope is a leader in modern security and networking for the cloud and AI era. Built on the Netskope One platform, Netskope unifies secure access, data security, and AI security to give organizations real-time visibility and control across cloud, AI, SaaS, web, and private applications. Powered by NewEdge, Netskope helps customers reduce risk, simplify infrastructure, and eliminate trade-offs between security and performance. Learn more at netskope.com.

Interested in learning more?

Request a demo