netskope

White Paper

Reimagining UK Public Sector Cybersecurity with Efficiency and Effectiveness at the Core

Table of Contents

Reimagining UK Public Sector Cybersecurity with Efficiency and Effectiveness at the Core

Navigating the complexities of digital transformation within the UK public sector presents unique challenges for technology leaders. Balancing the drive for innovation and efficiency with stringent compliance requirements, evolving citizen expectations, and the ever-present threat of sophisticated cyberattacks demands a robust and forward-thinking approach. Unlike the environment in the United States, which may be heavily influenced by specific executive orders and federal mandates, the UK landscape is shaped more by established frameworks and guidance issued by national and devolved bodies. This distinction highlights a potentially more decentralised, guidance-driven approach in the UK compared to top-down directives seen elsewhere, suggesting both flexibility and potential challenges in achieving consistent implementation across diverse government departments and public sector organisations.

Underpinning all digital transformation efforts is the critical and non-negotiable need to secure public sector systems against an evolving threat landscape. From opportunistic individuals and organised criminal groups deploying ransomware to state-sponsored actors targeting critical infrastructure, UK government bodies face persistent and increasingly sophisticated cyber risks. The high volume of significant cyber incidents managed by the National Cyber Security Centre (NCSC) that target the public sector underscores that these organisations are primary, not peripheral, targets, likely due to the essential functions they perform and the sensitive data they hold.

To bolster cyber resilience, key frameworks guide UK government departments and public sector organisations. Within Scotland, the Scottish Government has established The Scottish Public Sector Cyber Resilience Framework (PSCRF), providing specific guidance and a common language for organisations to enhance their cyber security posture. At a national level, the National Cyber Security Centre (NCSC) offers comprehensive support and resources, including its widely adopted Cyber Assessment Framework (CAF). The CAF provides a detailed methodology for assessing and improving cyber security practices, particularly for departments and organisations responsible for essential functions or critical national infrastructure across the UK. It is these frameworks and associated guidance, rather than specific executive mandates, that primarily shape the cybersecurity improvement journey for UK public sector bodies, influencing how they assess risk and demonstrate resilience.

Technology leaders in the UK public sector, striving to align with the principles of the PSCRF and leverage the outcome-focused guidance of the NCSC's CAF, are simultaneously grappling with a range of ongoing and evolving issues. These challenges, while specific to how they appear and are regulated within the UK, mirror many of the universal pain points experienced by public sector bodies globally.

Key among these persistent challenges are:

Maintaining legacy systems: Significant portions of IT budgets across the UK public sector are often allocated to maintaining outdated infrastructure, hindering agility and creating security risks.

Managing hybrid IT environments: The coexistence of increasing cloud adoption alongside persistent on-premises solutions introduces complexity in security management and operational efficiency.

Supporting flexible working: The shift towards remote and hybrid models necessitates robust security measures to protect data and ensure secure access for a distributed workforce.

Securing Internet of Things (IoT) devices: The increasing deployment of connected devices in public services introduces new attack vectors requiring careful management and security protocols.

Preparing for emerging technologies, including artificial intelligence (AI): Harnessing the potential of AI requires secure, scalable infrastructure and robust governance frameworks, presenting significant preparatory challenges.

This report aims to explore these critical challenges and examine the role of the PSCRF and NCSC CAF in guiding UK government departments and public sector organisations towards enhanced cyber resilience amidst the ongoing demands of digital transformation.

Zero Trust

Zero trust is a cybersecurity framework based on a “never trust, always verify” approach to network access. A zero trust architecture takes a layered approach to securing data and networks, including all cloud instances, as well as users and devices. Zero trust security models strengthen access controls and protect sensitive data.

Key elements of zero trust security architecture include:

- Identity, credential, and access management (ICAM)
- Endpoint protection
- Continuous monitoring
- Automated detection and response
- Microsegmentation
- Least-privileged access
- Policy enforcement

External Influences That Drive Cybersecurity Technology Choices

Policymakers are putting pressure on CIOs and CISOs to deliver IT solutions that drive rapid, strategic outcomes and meet mission objectives. At the same time, they are integrating zero trust security practices and accelerating the move to secure cloud services to meet UK mandates and guidance. These demands could drive leaders to make quick decisions based on external influences, such as choosing technology that worked for their peers at other agencies or going with a technology brand that they know. They could also choose a solution that solves one issue without taking a holistic view of their overall security needs or that overlaps with existing technologies, potentially duplicating costs.

Consequences of Choosing the Wrong Security Technology

When choosing cybersecurity tools based on external influences, it puts the organisation at risk. It also undermines the confidence technology leaders should have in their technology choices because they were picked without thorough research and alignment with the organisation’s strategy. IT and security leaders may also feel less confident about their ability to guide their organisations to future success in implementing emerging technologies like AI.

A Strategic Approach

To gain the confidence they need in their cybersecurity technology choices and the organisation's ability to scale to meet future innovation demands, IT leaders should take a measured approach to selecting technology tools that consider:

- Where the department or organisation is on their digital transformation roadmap
- What their cybersecurity needs are based on existing tools and alignment to UK frameworks and guidance
- What user experience the organisation wants to provide their teams and citizens
- What lies ahead on the organisation's strategic roadmap
- What mission outcomes the organisation wants to achieve in the future

Here are three things technology leaders should consider when looking for the right cybersecurity tools to achieve zero trust.

1. Balance Legacy Technology with Cloud Migration and Zero Trust Security Practices

UK public sector CIOs are navigating the challenge of maintaining existing legacy systems while strategically transitioning to modern cloud-based infrastructures to align closely with the intent of UK cybersecurity frameworks and guidance. Legacy systems often lack the necessary flexibility to seamlessly integrate advanced security measures. Therefore, public sector IT and security leaders must:

- Assess and align legacy systems with zero trust frameworks and cloud security capabilities
- Implement phased migration strategies to modernise effectively while maintaining operational continuity

To achieve cybersecurity goals, government departments and public sector organisations require a true single platform designed from the ground up with efficiency, effectiveness, and mission readiness at its core. The ideal platform will inherently facilitate an incremental yet continuous improvement in zero trust maturity. By leveraging a unified approach, UK public sector can significantly reduce complexity, eliminate redundancies, and streamline their operations. A single, comprehensive platform eliminates dependency on public cloud infrastructure, providing clear visibility into performance, eliminating hidden costs, and substantially reducing resources required for platform management. This allows leaders to concentrate more resources and attention on mission-critical activities rather than on routine maintenance.

By selecting a unified platform, UK public sector can:

- Consolidate and simplify their technology stacks, minimising software licensing and maintenance expenditures
- Optimize operational efficiency through centralised security policies, controls, and integrated automation capabilities
- Lower administrative overhead via automated compliance reporting, streamlined policy enforcement, and proactive system updates
- Ensure scalability and adaptability to evolving UK mandates and emerging cybersecurity threats

Furthermore, UK IT and security leaders should prioritise platform selections that transparently align with compliance requirements and relevant governmental frameworks, including the NCSC Cyber Assessment Framework (CAF) and the Scottish Public Sector Cyber Resilience Framework (PSCRF). Only through transparency can public sector technology leaders ensure that security tools and platforms support UK government initiatives while identifying and eliminating overlaps to achieve cost-avoidance goals. By embracing this intent-driven, unified platform strategy, the public sector can confidently address both current and future cybersecurity needs, leveraging a secure cloud environment. This type of unified platform delivers exceptional performance, complete visibility, and zero trust-based security and data protection for organisation resources, irrespective of user location.

Key UK Zero Trust Frameworks

The National Cyber Security Centre (NCSC) and the Scottish Government have issued frameworks to guide government departments and public sector organisations on implementing elements of a zero trust architecture.

The NCSC's Cyber Assessment Framework (CAF) provides a systematic and comprehensive approach for assessing and improving cyber security practices, particularly for those responsible for essential functions or critical national infrastructure across the UK.

The Scottish Public Sector Cyber Resilience Framework (PSCRF) provides specific guidance and a common language for the public sector in Scotland to enhance their cyber security posture.

2. Look for a Platform That Supports Integrations

There currently isn't one tool or platform that can achieve full zero trust security across an organisation's enterprise. While many vendors claim to have platforms or solutions that solve all security challenges, they often are just okay at many things while never truly excelling at the key elements of zero trust, leading to gaps in functionality. These gaps can be discovered by attackers, making the UK public sector vulnerable.

A more effective approach is to adopt a platform that supports the seamless integration of multiple key technologies, ensuring the public sector can align with zero trust principles while maximising security effectiveness and cost efficiency. By integrating best-in-class solutions, organisations can create a more resilient cybersecurity framework, leveraging technologies that excel in their respective areas, including:

- **Identity, Credential, and Access Management (ICAM):** Ensures the right individuals have the appropriate access to technology and data resources, reducing insider threats and unauthorised access.
- **Endpoint Detection and Response (EDR):** Protects endpoints and cloud workloads by detecting and preventing threats, minimising the risk of breaches, and enabling rapid incident response by correlating endpoint signals with cloud security policies
- **Automated Threat Detection and Response:** Detects, investigates, and mitigates threats in real time across the organisation's digital ecosystem by enabling teams to automate incident response and threat intelligence sharing
- **Secure Access and Network Visibility:** Monitors and controls user access to networks and data, ensuring compliance with zero trust principles. Integrations with Secure Access Service Edge (SASE) help organisations enforce least-privileged access while securing sensitive government workloads.

By leveraging an open, integrated platform, UK government departments and public sector organisations can:

- Enhance interoperability between security tools without the need for constant rip-and-replace cycles
- Unify security policies across on-premises, hybrid, and cloud environments, ensuring consistency in enforcement
- Reduce operational complexity by automating threat detection, response, and compliance reporting
- Maximise ROI by extending the life cycle and effectiveness of existing security investments

Taking an open platform approach allows the public sector to bridge the gap between legacy and modern security technologies, enabling a scalable, future-ready zero trust architecture without unnecessary disruptions or excessive costs.

Secure Access Service Edge (SASE)

A secure access service edge (SASE) is an architecture first described by Gartner that applies zero trust security standards to protect data wherever it moves. SASE converges multiple security technologies for web, cloud, data, and threat protection along with cloud-edge networking capabilities into a scalable, elastic platform that protects users, data, and applications everywhere. It doesn't matter how many cloud instances, on-premises environments, or remotely connected devices an organisation has—the SASE architecture provides protection and visibility across the enterprise. A SASE platform allows organisations to get the flexibility they need to add zero trust technology tools over time as legacy technology migrates to the cloud. They also optimise the end-user experience.

3. Create a Technology Strategy That Prepares for the Future

While we can't know what technology innovations will happen in the future, prioritising zero trust principles within IT infrastructures that allow for integrations ensures organisations are well-positioned to adapt to future advancements and challenges. When systems are secure in a way that can adapt and scale, leaders can have the confidence to bring on new innovations and adopt new use cases, including integrating AI into their workflows.

Potential use cases include:

- **Improving security by understanding the size and scope of cloud-based apps.** Research has found that employees of large enterprises can access more than 2,400 apps. Many of these apps are cloud-based SaaS applications. 97% are adopted by teams or individual users without the oversight of the IT team. With a platform approach that integrates zero trust security principles, apps can be found, rated, and monitored to reduce risk.
- **Blocking suspicious or risky activity.** If a user attempts to open a risky application or transfer sensitive data to a personal instance of a company-approved application, AI tools can help coach the user in real-time and guide them to safer options and better choices.
- **Securing access to internal apps.** UK public sector has many internally developed apps, which also need to be locked down with zero trust security. This ensures that users are accessing only what they need and not unnecessarily moving laterally through the network.
- **Stopping unapproved data movement.** The right platform tools can help IT and security leaders understand how their organisation collects, transmits, stores, and shares data across applications. With that knowledge, they can strengthen security by stopping unapproved data movement.

By prioritising zero trust through a platform approach, IT and security leaders will be at the forefront of innovation in their organisation, blending technology management with security leadership to guide the enterprise in unlocking new value and staying competitive in the future operational landscape.

Interested in learning more?

Request a demo

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. 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.