Bringing Security and Trust to Public Sector Data

with the Unified Zscaler Data Security Platform

WHITEPAPER

Executive Summary

Public sector agencies handle vast amounts of sensitive and critical information, from healthcare records and tax forms to ID scans and civilian complaints. Unfortunately, many lack the tools or processes to effectively understand, manage, and secure this information, resulting in a chaotic data environment. Unstructured and unclassified data flows across channels, and employees often don't know what constitutes sensitive data or how to properly handle it. This creates fertile ground for data breaches caused by accidental leaks, insider threats, or malicious attacks.

Generative AI (GenAI) tools, now embedded in nearly every aspect of modern work, further complicate this situation by introducing significant risks. Employees using unvetted tools often unknowingly feed sensitive public sector data into shadow AI systems, over which organisations have no visibility or control. Without robust tools to manage these workflows, agencies face enormous compliance, reputational, and operational challenges.

The unified Zscaler Data Security platform is purpose-built to solve these challenges. With advanced capabilities like inline DLP, endpoint DLP, and GenAI protection, Zscaler brings structure to the chaos while securing data in real time. Its advanced capabilities include protection for structured and unstructured data, Optical Character Recognition (OCR) for images and scanned content, and proactive user notifications and coaching to educate employees about data risks. Acting not just as a technical control but as a framework for data governance, Zscaler aligns with key compliance standards such as the NCSC Cyber Assessment Framework (CAF) and Cyber Essentials Plus to ensure that public sector organisations achieve both security and trustworthiness in their operations.

The Problem: Data Chaos in the Public Sector

The Complex Data Landscape

Government agencies manage a wide range of sensitive and regulated data:

- **Healthcare records:** Patient histories, protected health information (PHI), and lab results
- **Tax information:** Financial details containing National Insurance numbers (NIs), banking information, and income filings
- **ID scans:** Images of passports, driver's licenses, and government-issued IDs used for authentication
- **Civilian complaints:** Emails, forms, and submissions that may unintentionally include sensitive (personally identifiable information (PII)

Faced with these diverse datasets, many organisations struggle to classify and manage information effectively. For example, employees may not realise that a scanned ID or an email containing medical details qualifies as sensitive, leading to lax handling. Unstructured and chaotic data flows make traditional security policies insufficient, leaving organisations exposed to significant risks.

Key Risks Without Data Security in Place

1. Accidental Data Leakage

Employees unknowingly share sensitive public sector data on unsecured cloud platforms or by attaching it to email.
Misclassification of sensitive records like ID scans or healthcare files results in inadvertent policy violations.

2. Insider Threats

Trusted insiders may maliciously exfiltrate data for personal or financial gain.
Non-malicious insiders may accidentally mishandle sensitive data because they lack understanding of its importance or risk.

3. Generative AI and "Shadow AI" Risks

GenAI tools are now embedded in everything we do, presenting a double-edged sword of opportunity and risk:

- **Unvetted AI platforms:** Employees experiment with shadow AI tools that are unsanctioned and unmonitored by the organisation.
- **Uncontrolled data flows:** When sensitive data like tax forms, civilian complaints, or patient histories is included in AI prompts, it may be stored indefinitely in AI models outside the organisation's control, both violating compliance requirements and risking public exposure.
- **Data governance blind spots:** Agencies lack visibility into how their data is being shared, analysed, or retained across AI ecosystems.

4. Operational and Personal Impact

Beyond regulatory fines and compliance penalties, data breaches can result in:

- Loss of trust from civilians who rely on public sector organisations to safeguard their personal data
- Identity theft, fraud, and exposure of personal healthcare or financial details, leading to emotional distress and financial harm for the public

5. Cost of Noncompliance

Public sector organisations are subject to frameworks such as the GDPR and the UK's NCSC Cyber Assessment Framework (CAF). Breaches resulting from inadequate data protection bring legal fines, damage public reputation, and disrupt day-to-day operations.

Solution: Zscaler's Approach to Data Security

The unified Zscaler Data Security platform helps public sector organisations mitigate these risks by providing robust and comprehensive data protection. It addresses existing vulnerabilities and brings order to data chaos through proactive organisation, categorisation, and user education.

1. Inline Data Security: Real-Time Protection for Data in Motion

Inline Data Security operates at the network layer, inspecting all data in motion across cloud platforms, email services, and collaboration tools to enforce data security policies in real time.

Key capabilities:

- Structured data protection identifies sensitive information in predefined fields, such as NIs, account numbers, and tax records.
- Unstructured data protection protects freeform information found in scanned forms, emails, and reports.
- Optical character recognition (OCR) extracts and inspects sensitive content in images (e.g., ID scans, handwritten notes, or medical charts).
- Image detection protects information embedded in graphical formats, ensuring scanned images of documents remain secure.
- Data Classification employs advanced techniques to accurately classify sensitive data based on predefined policies and machine learning algorithms.

Impact:

Inline Data Security prevents accidental data leakage in real time, ensures compliance mandates are met, and proactively protects all kinds of public sector datasets, structured and unstructured alike.

2. GenAI Protection: Controlling Risks in an AI World

With GenAI central to workplace productivity, Zscaler provides purpose-built protections to prevent accidental data exposure while allowing agencies to leverage AI responsibly.

Key capabilities:

- Shadow AI usage monitoring detects and blocks user interactions with unsanctioned AI tools that could expose sensitive data.
- AI-specific policies ensure sensitive records or phrases are flagged and protected when employees interact with authorised or unauthorised AI tools.
- Proactive user notifications inform users in real time if an action (e.g., uploading or pasting sensitive data into an AI prompt) poses a security risk, empowering them to act responsibly.
- Real-time coaching provides contextual coaching to educate employees on why their action is risky and how they can better interact with organisational data.

Impact:
GenAI protections from Zscaler empower employees to work securely while preventing unauthorised exposure of sensitive public sector data into external AI systems.

3. Endpoint Data Security: Protecting Data at Rest and Beyond

Endpoint Data Security protects sensitive information stored on or transmitted from employee devices, ensuring security across remote workforces, physical offices, and hybrid environments.

Key capabilities:

- **Removable storage control** blocks sensitive data from being copied to unapproved USB drives or removable media.
- **User behaviour monitoring and alerts** track risky device activities and provide actionable alerts to both users and administrators.

Impact:
Endpoint Data Security closes gaps stemming from remote work and mobile computing, eliminating the risks of data transfer, loss, or physical device theft.

Zscaler Data Security: Alignment with Public Sector Frameworks

Zscaler Data Security aligns with critical regulatory frameworks in the public sector, ensuring compliance while simplifying adherence to industry standards:

- **NCSC Cyber Assessment Framework (CAF):** Zscaler meets principles for Protecting Data and Minimising Incident Impact by providing real-time monitoring, visibility, and mitigations for sensitive data risks.
- **Cyber Essentials Plus:** Zscaler ensures advanced security controls for device protection, data flow monitoring, and secure cloud integrations, supporting organisations in achieving certification.

The Zscaler Advantage

- **Order from chaos:** Automatically classify data, making it easy for agencies to enforce protection policies and meet compliance mandates.
- **End-to-end governance:** Ensure coverage for data in motion, at rest, and in use across networks, endpoints, and cloud platforms.
- **Employee empowerment:** Through user notifications and coaching, provide employees with a clear understanding of their roles in safeguarding data, reducing reliance on IT.
- **Proactive AI management:** Regulate GenAI interactions to maximise innovation while mitigating security risks.
- **Restored trust:** Reinforce trust, accountability, and transparency with civilians by protecting sensitive data.

Conclusion

Public sector agencies are stewards of critical national and personal information. Zscaler Data Security empowers organisations to navigate the future with clear insights, robust protections, and an accountable workforce. Combining world-class technologies like OCR, inline and endpoint data protection, and GenAI protection, Zscaler addresses modern risks while providing the structure agencies need to bring order to their data environments. By adhering to frameworks like NCSC CAF and Cyber Essentials Plus, Zscaler ensures that agencies achieve compliance, operational stability, and public trust.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere