CLOUD GATEWAY

Simplified Networking, Unified Security

FROM FRAGMENTED TOOLS TO TRUSTED CAPABILITY

A perspective on the infrastructure foundations for UK policing reform

Prepared by: Cloud Gateway
Published: April 2026

PUBLIC

Contents

About this paper

Cloud Gateway provides secure network connectivity and zero trust infrastructure to the UK government and public sector. We work with public safety and justice organisations every day, giving us a particular lens of what the infrastructure layer can and cannot do and where it constrains the future of policing.

This paper sets out our view on the current landscape, drawing on the NPCC Policing Problem Book, the government's *From Local to National* white paper, and the Hogan-Howe review, which is expected shortly. We are publishing now because the infrastructure arguments here hold regardless of what Lord Hogan-Howe recommends. A second paper will respond to those structural recommendations directly, once they are known.

This paper does not tell policing what to do. It offers our view of the underlying infrastructure conditions - what they make harder, what they make possible, and where the practical starting points are.

Executive summary

Three major documents, the NPCC Problem Book, From Local to National, and the Hogan-Howe review - are converging on the same underlying questions: interoperability, shared capability, and data standards. That alignment is significant as it creates a stronger mandate for action than policing has had in years.

The infrastructure reality is straightforward: around £590 million of a roughly £2 billion annual IT budget goes on maintaining legacy on-premise systems. Wholesale replacement is neither feasible nor advisable. But incremental, well-sequenced steps toward shared, standards-aligned infrastructure improve the security position now, reduce cost over time, and mean that whatever operational structures are implemented, the technical foundations are in place to support them.

The 2023 supply chain incidents and the PSNI breach, with recovery costs estimated at £174–217 million, show what the current structural exposure means in practice. These were not policing failures, they were a distributed, on-premise model becoming visible as a risk which has a direct impact on operational policing and staff and officer's ability to do their jobs.

Our view is that the near-term priority is sequencing: identify the infrastructure changes that unlock the most across the problem set, and start there, before structures change, not after. Naturally, this sits alongside broader transformational programmes of work which unlock potential within operational policing, both easing wait times, overrun systems and staff.

Victor Holmin

Chief Executive Officer
Cloud Gateway

The moment we're in

UK policing is navigating a convergence of pressures that do not often arrive together. The NPCC Policing Problem Book consolidates over 200 operational problems into 13 underlying challenges and explicitly calls for joint working, intelligent co-investment, and broader collaboration. The government's From Local to National proposes fewer, larger forces, a National Police Service, and stronger national standards in data, technology, and training. And the Hogan-Howe review has interoperability and technology consistency named explicitly in its terms of reference - not as aspirations, but as design requirements for new force structures.

These documents are not saying the same thing in different ways. They are arriving at the same foundational questions from different angles. That convergence matters, because it creates a window for infrastructure decisions that would previously have been harder to make.

The direction of travel is already set. The National Police Capability Environment is on Azure. The NPCC cyber strategy calls for a defend-as-one approach. The National Policing Digital Strategy 2025–2030 is in place. This paper builds on those foundations - it does not argue against the grain of the sector's own direction.

The infrastructure reality

The £590 million legacy maintenance figure is not a failure of planning. It reflects decades of procurement decisions made under genuine operational and financial pressure. But it is money not available for the capability investment everyone knows is needed - and it is money spent defending an estate that is structurally harder to secure than a consolidated one.

Distributed on-premise environments create a larger, less uniformly managed attack surface. The 2023 supply chain incidents illustrated this. So did the PSNI breach, which put officer identities into the hands of people who wanted to use them, at an estimated recovery cost of £174-217 million. The NCA identifies ransomware as the single greatest cyber threat to the UK public sector. Policing is consistently in scope.

The case for moving is not about transformation for its own sake. It is about what shared, standards-aligned cloud infrastructure does to that risk profile - fewer independent supplier relationships, more consistent patching, centralised security governance. Zero trust infrastructure can be layered onto existing environments and extended incrementally. You do not have to move everything to start improving the position.

Forces that make progress now will be in a stronger position when Hogan-Howe's structural recommendations land - because shared cloud works at current force boundaries and survives consolidation without being rebuilt.

Five pressure points where infrastructure shapes outcomes

The NPCC Problem Book names 13 underlying challenges. Read together, five are fundamentally shaped by the infrastructure layer beneath them.

1: Digital evidence and investigative throughput

Digital evidence features in around 90% of investigations, and volumes are doubling roughly every two years. Too much of the work of securing, transferring, and analysing that material remains manual. That creates backlogs, delays justice, and in cases involving the most serious harm - including violence against women and girls - means victims wait longer for outcomes. This is not a forensic tooling problem alone. It is a workflow, storage, and transfer problem.

HMICFRS found more than 25,000 devices awaiting examination, with wait times up to 18 months. The Westminster Commission on Forensic Science reported in June 2025 that more than 30,000 prosecutions collapsed between 2020 and 2024 due to evidence failures. Where automation has been piloted, one force saw a 55 percent reduction in processing time.

2: Public contact and the quality of data

The public contact function is the point at which information enters the policing system. The quality and structure of what is captured there shapes everything downstream: triage, investigative quality, safeguarding referrals. Single Online Home is critical national infrastructure. Keeping it functioning - and improving the data quality it generates - depends on the infrastructure connecting it to force systems. Surface-level modernisation without that layer does not deliver the outcomes forces or the public need.

3: Interoperability across boundaries

Interoperability is named in the Hogan-Howe terms of reference. The national standards programme through Police Digital Service is the right vehicle. But consistent adoption of those standards is what makes interoperability real rather than theoretical. That requires a shared infrastructure layer - common patterns for data exchange, identity, access management, and audit.

4: AI governance before scaling

Responsible AI deployment requires access controls, audit trails, and data lineage. These are infrastructure decisions, not application-layer ones. Getting that layer right before scaling AI is significantly more effective than retrofitting governance onto existing systems. In a constrained budget environment, the governance architecture needs to be built in from the start - rework is not a realistic option.

5: A repeatable path from pilot to scale

One of the clearest frustrations in policing technology is that what works in one force rarely travels. Shared infrastructure directly reduces the cost and complexity of replication. That is the most practical argument for national standards: it makes the next deployment cheaper and faster than the last one.

Our view: common patterns and design principles

We do not yet know what the Hogan-Howe review will recommend. But in our view, the following principles will be relevant to any structural outcome.

Shared foundations over isolated solutions

Common patterns for data exchange, identity and access management, security governance, and audit are what make interoperability and scale achievable. The alternative - parallel investments in incompatible local estates - compounds the maintenance burden and defers the problem.

Evidential integrity built in from day one

As evidence volumes grow and synthetic content becomes more prevalent, the infrastructure layer's ability to preserve provenance and chain of custody becomes as important as the forensic capability sitting above it.

AI governance as infrastructure, not afterthought

Transparency, auditability, and access controls are infrastructure decisions first. Building them in is significantly more effective - and more defensible - than adding them later.

Operational journeys as the design anchor

The infrastructure that serves the officer's workflow, the victim's contact experience, and the analyst's access to relevant data should be designed around those journeys - not around system or organisational boundaries.

A repeatable path from pilot to scale

Shared infrastructure reduces the barrier to deploying what works. That is what makes innovation sustainable rather than episodic.

Where to start: a near-term agenda

The reform context creates a stronger mandate for pace than has existed before. But pace without sequencing reproduces the fragmentation both the NPCC and the government are trying to move beyond.

Our reading is that the near-term agenda should focus on two things in parallel.

Shared data infrastructure and security

The foundational layer. Common standards for data movement, identity, access, and audit need to be in place for cross-force capability to work. This is the starting point. Each step improves the security posture and builds compatibility with whatever structures emerge from reform.

Public contact and service integration

Structured data capture, consistent access governance, and downstream integration. These are the foundations that connect the front door to everything behind it. Modernising the front end without addressing this layer does not deliver the outcomes.

A phased approach is realistic. The question is which changes within current strategy unlock the most across the problem set, and what can be done now, within real budgets, that does not need to be undone when structures change.

What Cloud Gateway brings

We are not a systems integrator and we are not a forensics vendor. Our relevance is specific: we provide the secure connectivity and zero trust infrastructure that sits beneath the capability layer, the foundations that enable data to move safely between systems, teams, and organisations.

In practice, that means three things.

Platform

Government-grade secure network connectivity and zero trust infrastructure, layered onto existing environments. Forces do not need to replace their estate to benefit. We work with what is there and extend incrementally toward a more secure, interoperable position.

Rapid pilots

We can stand up controlled, secure environments quickly - useful for testing cross-force data sharing patterns, AI governance models, or digital contact integrations before committing to scale. This matters in a sector where the gap between proof of concept and operational adoption is where promising ideas most often fail.

Governance templates

Based on our experience across government and public safety, we carry practical patterns for access management, audit, data movement controls, and zero trust policy - the governance scaffolding that enables responsible AI and data sharing rather than blocking it.

Where forces need end-to-end capability, we work with partners who carry complementary depth. Our value is in the infrastructure layer - and in ensuring that layer is built in a way that supports, rather than constrains, everything above it.

What comes next

A second paper will follow the Hogan-Howe review. It will address how the near-term infrastructure agenda maps to the new structural architecture - and where the review's recommendations create specific opportunities or constraints for the capability plays set out here.

The infrastructure arguments in this paper hold regardless of what Hogan-Howe recommends. The sequencing logic - build the foundations before structures change, not after - applies across the range of structural outcomes currently in play.

If you are a CIO, CTO, or transformation lead working on any of the infrastructure or capability challenges described here, we would welcome the conversation.

References and Links

NPCC Policing Problem Book (2025):
https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/ddat/2025/251022-npcc-policing-problem-book-2025.pdf

From Local to National: A New Model for Policing (2026):
https://www.gov.uk/government/publications/from-local-to-national-a-new-model-for-policing

Hogan-Howe Review: Terms of Reference (March 2026):
https://www.gov.uk/government/publications/independent-review-of-police-force-structures-terms-of-reference/independent-review-of-police-force-structures-terms-of-reference

National Policing Digital Strategy 2025-2030 (NPCC/PDS):
https://pds.police.uk/wp-content/uploads/2025/05/250519-NPCC-Digital-Strategy_FINAL.pdf

National Police Capability Environment:
https://pds.police.uk/welcome/pds-service-catalogue/managed-information-technology-services/national-police-capability-environment/

GOV.UK Information Security Review 2023 (source for PSNI and Met Police incidents):
https://www.gov.uk/government/publications/information-security-review-2023-final-report/information-security-review-2023-final-report-html

NCA Cyber Crime Threat Assessment:
https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

techUK National Policing Digital Strategy commentary:
https://www.techuk.org/resource/national-policing-digital-strategy-refresh.html

HMICFRS Digital Forensics Inspection:
https://www.justiceinspectorates.gov.uk/hmicfrs

Westminster Commission on Forensic Science (June 2025):
https://futurejustice.org.uk/wp-content/uploads/2025/06/FS_Digital_latest.pdf

55% automation figure: sourced from Home Office spokesperson quoted in LBC, June 2025:
https://www.lbc.co.uk/article/police-overwhelmed-digital-forensics-25-000-devices-await-checks-DWzNNJ_2/

CLOUD GATEWAY

Simplified Networking, Unified Security

Contact

Cloud Gateway
The Ministry, Borough
79 Borough Rd, London SE1 1DN
+44 (0)20 3870 2444

cloudgateway.co.uk

sales@cloudgateway.co.uk

linkedin.com/company/cloudgateway