CYBERSECURITY PARTNER OF CHOICE

# NPCC Policing Vision 2030: Why zero trust is the cybersecurity strategy UK police forces need

## Table of Contents

## Executive summary

The National Police Chiefs' Council (NPCC) and the Association of Police and Crime Commissioners (APCC)'s Policing Vision 2030 focuses on improving the use of digital technology in UK policing to reduce fragmentation, costs, and complexity, and better manage modern cybersecurity risks.

The National Policing Digital Strategy 2025–2030 provides guidance for UK policing's use of digital technology in line with the *Policing Vision 2030* objectives, including the use of least-privilege controls like zero trust to strengthen cybersecurity defences.

This paper proposes a zero trust SASE platformisation strategy that will help UK police forces meet *Policing Vision 2030* objectives and follow the recommendations of the *National Policing Digital Strategy 2025–2030*. In particular, it will enable UK forces to:

- Share intelligence across forces and with national units more easily – while maintaining strict controls on who can see what.
- Give officers and staff secure access whether at headquarters, on patrol, or working remotely.
- Reduce insider threats and stop cyberattackers moving laterally across their networks.
- Detect and block digital threats in real time, keeping critical policing services online even during cyberattacks.
- Reduce duplication of cybersecurity products, cutting complexity and overlap.

## Introduction

### Why UK policing's digital strategy must change

#### From State of Policing: The Annual Assessment of Policing in England and Wales 2024–25

> **Modern policing depends on the ability to collect, analyse and act on vast amounts of information. Yet outdated technology is holding back many police forces. In our inspections, we frequently find that local and national IT systems are hindering police performance. Science and technology have increasingly advanced over the last few decades. To a large degree, policing hasn't kept up with these advances. Most of the spending on police technology is used to maintain old systems. These are often expensive and rely heavily on adding information manually. They contribute to poor data management and don't allow effective information-sharing within or between forces. Police forces must embrace innovation to meet the policing challenges of the future.**
>
> **In addition, cybersecurity threats against forces need to be managed, and these shouldn't be underestimated.**
>
> **Sir Andy Cooke QPM DL, His Majesty's Chief Inspector of Constabulary[1]**

It's clear that to a large degree, the digital technology used by UK police forces needs to be brought up to date – and that cybersecurity strategy is a key part of that digital technology transformation.

1. HMICFRS, State of Policing 2024–25, licensed under the Open Government Licence v3.0

Taken as a whole, UK policing's current digital strategy is one of fragmentation, overcomplication, and duplication: a patchwork of disjointed systems that often struggle to cooperate effectively. Each force has built its own digital architecture over the years, often in isolation. Many of these systems are based on 15–20-year-old ideas and designs, and are now struggling with the unexpected problems brought about by digital's evolution and the introduction of new technologies such as AI, drones, and wearable devices. The result of all this is duplicated systems and data, repeated manual interventions, high costs, and multiple boundaries and connections that add complexity and increase security risks.

**Key problems with UK policing's current digital approach at force level:**

- **Maintenance burden:** Running piecemeal-created digital infrastructures with duplicated systems is expensive and time-consuming. Around 30%[2] of police forces' technology staff spend is on resources to maintain on-premise infrastructure, and new developments may add even more duplications.
- **Complexity means cost:** With fragmented systems, sharing information and delivering access to national services requires complex processes that increase costs – and can undermine the integrity of the data.
- **Cybersecurity blind spots:** Multiple products, suppliers, and management tools create blind spots in cybersecurity.
- **Cyberthreat intelligence reduced:** Cybersecurity gaps and inconsistencies caused by using multiple products, and a lack of threat intelligence sharing between those products, make cyberthreat intelligence services less effective.
- **Poor user experience:** Digital experience quality varies depending on where officers and staff work. Problems such as weak connectivity, multiple passwords, and no single sign-on make systems frustrating to use and open up new risks.
- **Reactive, not proactive:** Technicians are often focused on short-term fixes to patch current problems rather than building towards a clear future model.
- **Increasing demand:** Each force has a similar infrastructure that requires similar knowledge and skills to maintain, not only duplicating effort across all police organisations but also increasing demand for the same skills, making forces compete in the job market and driving up costs.

## Policing Vision 2030 and National Policing Digital Strategy 2025–2030

*Policing Vision 2030*, the strategic framework recently created to guide the decision making of the police forces of England and Wales, outlines 25 objectives (organised into five pillars of five objectives each) designed to bring about modernisation, increase public trust, and tackle new forms of crime.

As, judiciously, many of those 25 objectives focus on UK policing's use of digital technology, the *National Policing Digital Strategy 2025–2030* was created to show UK police forces how they might use digital tools, data, and modern IT systems more effectively to achieve the *Policing Vision 2030* objectives.

In summary, the *National Policing Digital Strategy 2025–2030* recommends that UK police forces:

- Modernise and unify their digital systems.
- Adopt shared national platforms.
- Strengthen their cybersecurity through approaches like zero trust.

2. National Policing Digital Strategy 2020-2030

## A new digital strategy for UK policing

**This paper proposes a zero trust SASE platformisation strategy to follow the *National Policing Digital Strategy 2025–2030* recommendations.**

- **Zero trust:** Ensures no user, device, or app can gain access to a force's system without verification, even if they're already inside that force's network. Zero trust supports modern work environments and modern business models, simplifies user experience, streamlines cybersecurity, helps forces meet regulatory requirements, and protects critical assets.
- **SASE (secure access service edge):** Moves all security and networking tools into the cloud, so officers and staff can connect safely from anywhere without relying on local systems. SASE reduces digital system complexity, improves performance, supports hybrid work through secure connections, reduces operational costs, and ensures uniform security and compliance across all systems.
- **Platformisation:** Brings all cybersecurity tooling together into one integrated system, making them simpler, more cost-effective, and easier to manage. Platformisation streamlines workflows, enhances system visibility, strengthens cybersecurity while increasing adaptability to new technologies, and helps bridge gaps between digital and executive priorities. This includes additional capabilities to provide AI security and wider cyber operations, and post quantum readiness.

Clearly, the benefits of these digital capabilities extend far beyond improving cybersecurity.

They'll also allow UK police forces to continually access the most up-to-date technologies, helping them meet the objectives of the *Policing Vision 2030*, as follows:

1. **Ensure accountability and strengthen trust** by increasing meaningful, respectful, and effective public engagement across a diverse range of communities.
2. **Collaborate more across policing** and with local authorities, businesses and the voluntary, community, and social enterprise sector **to prevent crime and exploitation**.
3. **Improve the use of multi-agency data**, predictive analytics, and future crime statistics **to inform prevention activity**.
4. **Continue to anticipate and adapt** to the changing nature of crime and criminality.
5. **Increase the use of science, technology, and research** across policing and with partners to support the police in tackling crime.
6. Produce consistent, **high-quality data and use it to inform decision making** and response.
7. Contribute towards Criminal Justice System reform and improvements to **ensure criminals are effectively and efficiently brought to justice**.
8. **Safeguard the workforce** with a strong focus on both their physical and mental health and wellbeing.
9. **Embed a culture of continuous improvement and effective problem solving** across policing and be open to challenge and learning from others.
10. **Develop a learning and evidence-informed culture** and approach, working closely with academia to develop a technology knowledge base.
11. Deliver a more efficient and productive police service, **delivering value for money and balancing opportunity and risk**.

How a zero trust SASE platformisation strategy will help UK police forces to meet these objectives is explained in Section 2.

# 1: The way forward for UK police forces

While it's true that the data a force holds is its most valuable asset – and that any compromise of its security is likely to undermine public trust and confidence – it's equally true that harnessing modern digital, data, and technology capabilities is critical to UK policing's mission to tackle crime and protect the public from harm. To meet many of the overall objectives of *Policing Vision 2030*, it's probable that UK police forces need to make updates to both their cybersecurity strategies and their entire digital architectures in order to deliver efficiency gains through AI and new national capabilities.

Of course, each force's digital architecture needs to be reliable, defendable, and financially viable. It's also vital that it supports current objectives, the objectives outlined by *Policing Vision 2030*, and any changing objectives beyond that. To meet all those criteria, digital architectures must be flexible: agile enough to cope with inevitable changes in the digital, policing, and socio-political landscapes. They also need to be adaptable enough to incorporate necessary new tools and technologies to meet new demands – without expensive delays caused by having to re-establish core foundational infrastructure. In short, UK police forces need a battle-tested, secure, and scalable digital architecture that will support change at pace.

**In answer to those requirements, Palo Alto Networks proposes a zero trust SASE platformisation strategy.**

While the *National Policing Digital Strategy 2025–2030* does not mention any particular cybersecurity architecture by name, it does stress that UK police forces should adopt modern cybersecurity principles, including strong identity and access management, least-privilege controls, and continuous monitoring – all of which are hallmarks of the zero trust SASE platformisation strategy we propose.

## Zero trust, SASE, and platformisation explained

### Zero trust

Zero trust is not a product in itself. It's more of a philosophy, a modern approach to cybersecurity built on the foundational principle of 'never trust, always verify'. In some ways, zero trust is a polar opposite approach to that of traditional cybersecurity, which works on a basis of 'implied trust' – the assumption that any request via a user account must be legitimate because all users are within a static digital security perimeter.

Perhaps the largest issue with implied trust architectures is that a system user needn't be at a desk in an on-site office anymore: the idea of a solely on-premises workforce is long gone. It's most likely that at least some part of every UK police organisation's workforce is now hybrid, and that many other users, applications, technologies, and operational capabilities also now sit outside those traditional digital security perimeters. So UK police forces must now provide digital access from anywhere, to whoever and whatever needs it, with the best possible user experience, to achieve the required operational outcomes. Traditional implied trust architectures struggle to cope with securing these more complex modern parameters – and once inside an implied trust system, cyberattackers can move laterally from one application to another, potentially infiltrating any part of that system's architecture.

It's pretty much inevitable that the 'attack surface' of each UK police force will become even broader as it adopts more and more police applications. Forces can't simply trust that new IT equipment or vendor-supplied hardware or software is secure: any item from any provider could be at risk due to weak security on pre-existing support and partner ecosystems, increasing risk to forces in turn. There are already a number of peripheral devices, such as Body-Worn Video and emergency service communications, that rely upon complex, multi-supplier service models – and physical locations are increasingly run by connected things (such as internet of things-enabled CCTV) that, typically, have more system access than they need. All of this increases opportunities for ever-more-sophisticated threat actors, who see such broad, unevenly protected attack surfaces as ripe for exploitation.

Zero trust counteracts all of these issues, making it the most naturally viable cybersecurity architecture for modern police forces.

With zero trust, it doesn't matter where a request originates. Whether it's from a force-issued laptop, server, corporate or personal smartphone, Body-Worn Video or Emergency Service Network device, the system will assume it's an attempt at a breach. By assuming breach and verifying everything, zero trust eliminates implied trust and any accompanying risk of lateral movement. It doesn't matter if a user, device, or application is already inside the architecture – it's still 'guilty until proven innocent' whenever it makes a request, and must prove its innocence through verification before being granted access to sensitive resources.

A zero trust approach combines fine-grained, least-privileged access with continuous trust verification and deep, ongoing security inspection to protect all users, devices, apps, and data – everywhere.

## SASE: Secure access service edge

SASE is a completely new approach to remote system access that works hand-in-hand with zero trust principles. Embracing zero trust SASE will give UK police forces and their digital systems the agility required to follow *National Policing Digital Strategy 2025–2030* recommendations and meet *Policing Vision 2030* objectives. SASE removes complexity by replacing virtual private networks (VPNs) and point product infrastructure (such as traditional proxy services) with a combination of networking and network security as a service from the cloud.

A SASE solution provides always-on, consistently secure access to applications, data centres, cloud solutions, internet of things services (such as Body-Worn Video, CCTV, vehicle digital solutions, drones, and firearm locker solutions), and partners providing remote support (such as police volunteers, special constables, expert witnesses, platform developers, and product technical support).

As technology develops, platform readiness is key to delivering secure available digital connectivity. Palo Alto Networks post quantum readiness provides peace of mind for policing organisations as they deliver against the NPCC Digital Strategy.

### Components of SASE:

- **Software-defined wide area network (SD-WAN)** ensures sites, officers, and staff can connect and communicate reliably and securely across UK policing networks (such as the Law Enforcement Community Network or the upcoming Emergency Services Network), increasing resilience and enabling smoother collaboration between forces and other organisations.
- **Zero trust network access** continuously checks every access request, no matter where the request might come from. Ensuring systems and data are only within reach of the right users reduces risk, lowers costs, and allows officers and staff to work securely from any location.
- **Firewall as a service (FWaaS)** simplifies operations and saves money by shielding entire forces at a single stroke instead of each site managing its own firewall. This delivers resilient, consistent, next-generation protection for officers, staff, partners, and service providers – however they connect to their force's system.
- **Domain Name System (DNS) Security** ensures forces' trusted domain names – such as 'police.uk' – can't be hijacked or exploited, giving officers and staff confidence that they'll always be connecting to systems that are genuine and safe.

- **Threat Prevention** uses threat intelligence beyond that of any intrusion prevention system to block malware, exploits, and criminal command signals faster, improving mean time to detection and resolution to reduce disruption.
- **Cloud Secure Web Gateway (SWG)** automatically blocks malicious sites through static analysis and machine learning, ensuring officers and staff can browse the web safely without slowing down their daily work.
- **Data loss prevention (DLP)** allows protection of sensitive data according to risk, preventing it from being shared inappropriately without expensive or impractical systems, thus ensuring public trust while managing costs.
- **Cloud access security broker (CASB)** watches over cloud data, governing its access and usage and stopping threats before they can spread, ensuring forces can adopt modern cloud services without losing control of sensitive information.
- **AI-driven security platform** unifies all the above protections into one intelligent system that automates responses, simplifies operations, and strengthens outcomes, reducing the time security and IT teams spend firefighting and enabling them to focus on supporting policing priorities.

## Platformisation

According to a research study[3] published in January 2025 by the IBM Institute for Business Value, the average organisation's cybersecurity relies on a combination of 83 solutions provided to it by 29 vendors. This strategy introduces accountability and responsibility for local teams to integrate, and monitor, collate, and determine action across multiple products without any end-to-end visibility increasing risk and vulnerability hindering operational agility.

The study also revealed that 80% of organisations not using a consolidated platform approach struggle with negative effects from their cybersecurity's fragmentation. The executives surveyed estimate cybersecurity complexity and fragmentation cost their organisations an average of 5% of annual revenue, and 52% of the executives surveyed believe complexity is the biggest impediment to security operations.

In the case of UK police forces, this fragmented approach has the potential to increase risk, introducing vulnerability leading to unintended consequences. Where sensitive data must be protected, inter-agency collaboration demands seamless systems, and public trust depends on operational resilience, the effects of tool sprawl can go beyond damaging a force's efficiency – potentially even to the point of undermining the safety of the public. Knowing this, UK police forces with fragmented digital architectures therefore take extraordinary, reactive, resource-intensive measures to protect their systems and the public trust.

There is, however, a far simpler and more effective solution.

Platformisation integrates all networking, security, and IT management technologies together into one integrated system, reducing Total Cost of Ownership, streamlining workflows, enhancing system visibility, and strengthening cybersecurity. But a platformisation strategy is now even more relevant to UK police forces than those benefits alone might suggest. Using such a strategy will also make it far easier for UK police forces to adopt and manage the zero trust and SASE architectures required to follow the recommendations of the *National Policing Digital Strategy 2025–2030*, meet the objectives of *Policing Vision 2030*, and adapt to any future challenges and new technologies.

3. Capturing the cybersecurity dividend, IBM Institute for Business Value

## 2: How zero trust, SASE, and platformisation will help UK police forces meet the Policing Vision 2030 objectives

A zero trust, SASE platformisation strategy will help UK police forces to meet the *Policing Vision 2030* objectives:

### Public Trust and Accountability

**Ensure accountability and strengthen trust through meaningful public engagement:** Zero trust ensures public-facing systems (e.g. online reporting, community portals) are secure and resistant to impersonation or data breaches, which builds public confidence. Platformisation enables consistent, transparent engagement tools across forces, improving accessibility and responsiveness.

### Prevention and Collaboration

**Collaborate across sectors to prevent crime and exploitation:** SASE enables third-party partners such as local authorities, charities, and businesses to gain secure remote access to shared platforms – without exposing UK police force networks to risk.

**Improve use of multi-agency data and predictive analytics:** Zero trust enables secure operational data sharing between organisations while ensuring only authorised users can access sensitive analytics tools. Platformisation supports unified data environments and analytics dashboards across agencies, improving prevention strategies.

### Tackling Crime and Criminality

**Adapt to the changing nature of crime:** SASE and zero trust are foundational to defending against cybercrime, ransomware, and digital exploitation – and will also support continuing development of operational services with their flexibility and agility. SASE supports rapid deployment of secure access to new tools and intelligence platforms, helping forces respond to emerging threats such as cybercrime and digital fraud.

**Increase use of science, technology, and research:** Platformisation accelerates innovation by integrating research tools, datasets, experimental technologies, and partner systems into a unified ecosystem. The impact of platformisation will be vital to the police officer of the future.

**Produce consistent, high-quality data for decision making:** Zero trust is critical for maintaining data integrity, enforcing access controls and audit trails, and ensuring only authorised personnel can modify or view sensitive data. Platformisation ensures interoperability and standardisation.

**Support Criminal Justice System reform:** SASE enables secure, remote access to justice systems. Platformisation streamlines case management and evidence sharing.

### Workforce Wellbeing

**Safeguard workforce health and wellbeing:** SASE supports flexible, secure remote working, reducing stress and improving work-life balance. It enables officers and staff to securely access systems from multiple operational locations and as required to meet demand or from mobile devices, improving flexibility without compromising security. Platformisation enables access to all applications and digital services across devices and locations.

## Continuous Improvement

**Embed a culture of problem solving and openness:** Platformisation fosters collaboration, experimentation, and feedback loops within forces and across collaborating organisations, enabling scalable innovation by making tools and data accessible across teams securely.

**Develop a learning and evidence-informed culture:** Zero trust protects research environments and shared datasets, enabling safe collaboration between forces and academic institutions to forward education. Platformisation helps forces and their academic partners to connect.

**Deliver a more efficient and productive police service:** SASE reduces infrastructure complexity and associated costs. Platformisation streamlines operations and improves system agility.

# 3: How a zero trust SASE platformisation strategy will benefit UK police forces

Adopting a zero trust SASE platformisation strategy offers UK police forces a number of high-level, strategic, and financial cybersecurity posture, technology architecture, and operational benefits.

## High-level strategic benefits include:

- **Unified digital strategy:** Aligns IT, cybersecurity, and operational priorities under one coherent framework.
- **Digital resilience:** Builds a flexible foundation that adapts to new policing technologies and national initiatives, supporting the police officer of the future.
- **Public trust reinforcement:** Demonstrates proactive leadership in safeguarding sensitive data and public services, reinforcing confidence in digital policing services.
- **Inter-agency collaboration:** Simplifies secure information sharing within forces and between forces and national bodies.

## Financial benefits include:

**Reduced Total Cost of Ownership:** Cuts costs by consolidating multiple overlapping network and security products into one platform, avoiding duplicated spend and supporting operational objectives. This approach has been evidenced through other bluelight organisations. To quantify this, explore the **Forrester** Consulting Total Economic Impact™ study.

- **Lower operational overhead:** Reduces time and cost associated with managing fragmented systems.
- **Predictable budgeting:** Provides transparency with subscription-based models that make costs easier to plan – a move away from capital budget siloed investment planning.
- **Improved ROI:** Ensures investments in platformisation deliver measurable savings compared to capital replacement upgrades.

## Cybersecurity posture benefits include:

- **Zero trust enforcement:** Applies 'never trust, always verify' across all users, devices, and applications.
- **Reduced attack surface:** Eliminates gaps in defences created by disparate, siloed tools.
- **Consistent policy application:** Enforces uniform security rules, regardless of location or device.
- **Cloud-native resilience:** Strengthens protection against modern threats targeting cloud services.

- **Real-time protection against zero-day threats:** Improves threat response times with integrated monitoring.
- **Single-pass inspection:** Checks traffic once, lowering latency and avoiding blind spots.
- **Adaptive security:** Adjusts policies dynamically to user behaviour and risk levels.
- **Compliance alignment:** Assists forces in achieving Police Cyber Assurance Framework, GovAssure, NCSC CAF, and meeting other legislative requirements.
- **Incident response readiness:** Streamlines playbooks and visibility to improve incident response management.
- **Resilience against ransomware:** Limits the spread of attacks with stronger segmentation and access controls underpinned by best-in-class technology.
- **Quantum ready:** Delivers quantum ready confidence to underpin the NPCC strategic objectives.

## Technology architecture benefits include:

- **Simplified cybersecurity and networking landscape:** Replaces legacy systems with one highly available integrated platform.
- **Scalability:** Expands capacity seamlessly as demand increases.
- **Interoperability:** Integrates systems more easily with national policing platforms, third-party applications, or services and partner organisations.
- **Reduced future technical debt:** Moves forces away from patchwork legacy solutions and towards modern architecture.
- **Innovation readiness:** Removes in-point siloed solutions that stifle innovation and delivers core infrastructure not aligned to singular projects, accelerating the delivery of digital objectives to avoid technical sprawl and duplication.
- **Integrated AI:** Security capability to protect UK policing AI objectives that support the integrity of operational decision making.

## Force operational benefits include:

- **Improved frontline mobility:** Enables officers and staff to securely access systems from anywhere, on any device.
- **Faster case handling:** Reduces delays in investigations with streamlined access to data.
- **Secure collaboration:** Allows departments to share intelligence safely across units and with other forces.
- **Operational agility:** Allows forces to deploy new digital policing tools quickly without compromising security.
- **Simplified IT operations:** Frees forces from managing IT complexity, allowing more focus on policing priorities.
- **Agile hybrid workforce support:** Enables forces to operate effectively across office, remote, and frontline environments while maintaining the ability to secure all users, apps, data, and devices – regardless of location or role.

## Conclusion

UK policing digital system capabilities have not fully kept up with the advances of the last few decades. Many are based on ideas and designs that are now two decades old, and consequently are struggling to cope with unexpected aspects of digital's evolution.

UK policing's current digital strategy is one of fragmentation; overcomplication; duplicated systems and data; high costs; poor user experience; and multiple boundaries and connections that add complexity, hinder performance by contributing to poor data management and poor information-sharing, reduce cyberthreat intelligence effectiveness, and create cybersecurity blind spots. This current strategy may be negatively impacting UK policing's mission to tackle crime and protect the public from harm.

Under these circumstances, it's no surprise that many of the 25 objectives of *Policing Vision 2030* focus on improving UK policing's use of digital technology: it's clear that UK police forces **must** embrace modern innovation in digital technology and cybersecurity strategy to meet the policing challenges of the future.

The *National Policing Digital Strategy 2025–2030* was created to show UK police forces how to achieve the digital-connected Policing Vision 2030 objectives. It stresses that UK police forces should adopt modern cybersecurity principles, including strong identity and access management, least-privilege controls, and continuous monitoring – all of which are hallmarks of a zero trust SASE platformisation strategy.

Reliable, defendable, and financially viable, the many benefits of a zero trust SASE platformisation strategy extend far beyond cybersecurity, reaching UK policing high-level strategic and operational areas. The strategy's architecture allows UK police forces to continually access the most up-to-date technologies; helps them meet the 25 objectives of *Policing Vision 2030*; and grants them the agility, flexibility, and adaptability to cope with inevitable changes in the digital, policing, and socio-political landscapes – without expensive delays caused by having to re-establish core foundational infrastructure.

The zero trust SASE platformisation strategy is the battle-tested, secure, scalable, quantum ready digital architecture UK police forces need to help them meet current objectives and support change at pace.

Palo Alto Networks is already working with the UK Ministry of Justice to transform its networks and security. Palo Alto Networks Prisma® SASE and Cortex XSIAM® products are currently strengthening resilience across UK courts, prisons, and probation services, which demonstrates the company's credibility in handling sensitive UK government workloads.

Choosing Palo Alto Networks means partnering with a tested, government-grade zero trust SASE platformisation strategy provider that's already proven in UK ministries and trusted by the UK public sector.

Palo Alto Networks has been named a leader in zero trust edge solutions by Forrester, and its SASE business is one of the world's fastest growing, with over 6,800 clients – including a third of the Fortune 500. Its expertise in reducing tool sprawl by consolidating networking and security into one platform will be of particular value to UK police forces managing diverse IT estates and aiming to follow the recommendations of the *National Policing Digital Strategy 2025–2030*.

For more information about Palo Alto Networks zero trust SASE platformisation solutions, click here.

22 Bishopsgate, Level 55
London, EC2N 4BQ
United Kingdom
0800 028 3904
www.paloaltonetworks.com



parent_ds_NPCC Policing Vision 2030_15.01.26