An analysis of cloud adoption among police forces, the options available to them and why SaaS solutions are the safest, simplest and quickest route to a digital police force.
PoliceBox differentiators ........................................................................... 4
What is included ........................................................................................................ 5

Using the service: Common usage scenarios ........................................... 6
PoliceBox smartphone app: Example usage scenarios ....................... 6
Management Portal: Example usage scenarios ..................................... 11
The PoliceBox App Designer Tool ......................................................... 13
Pricing and subscription models .............................................................. 14
Training ......................................................................................................................... 15
Data Protection ........................................................................................................... 16
Our experience ......................................................................................................... 17
Company Overview .............................................................................................. 17
PoliceBox Service ............................................................................................... 18

About this white paper

This paper is for all police forces who are reviewing their business processes with a view to leveraging digitisation and the cloud. There are pitfalls to jumping straight into the cloud without putting thought into it first, and oftentimes a hybrid cloud/SaaS approach will be more effective. This paper will present the various cloud/SaaS options available to police forces, highlight the benefits and pitfalls to each approach, and demonstrate when a SaaS solution, when available, may offer the best value-for-money, flexibility and performance.

What is the state of cloud adoption in the police today?

The UK public sector has been actively encouraged to move its IT services to the cloud ever since the publication of the government’s first “Cloud First” policy in 2011. With the introduction of the Cloud First policy, the cloud became the default position for all new public sector IT projects. Any new public sector IT project that does not leverage the cloud as its primary strategy must now provide justification for doing so.

“When procuring new or existing services, public sector organisations should consider and fully evaluate potential cloud solutions first before considering any other option. This approach is mandatory for central government and strongly recommended to the wider public sector.” Government Cloud First policy

This policy has resulted in the rapid “cloudification” of the UK public sector. According to figures published by the Cloud Industry Forum (CIF) in 2015, cloud use among the public sector more than doubled in just five years, with the number of public sector organisations saying they were using cloud-based services jumping from 38% in 2010 to 78% in 2015.

However, while the majority of the public sector has been on the cloud bandwagon since the Cloud First policy compelled them to in 2013, the cloud only really became a legitimate option for the police in 2017. This is because cloud providers must have their data centres reviewed by the UK’s National Police Information Risk Management Team to ensure they meet minimum standards for the storing of, and access to, police information. The review, carried out by the National Accreditor for the Police Service, is required by all law enforcement agencies in the UK before they can move data to the cloud, as it ensures that information is held in a Police Approved Secure Facility. While a handful of niche cloud providers gained their accreditation earlier, the UK’s main public cloud providers only gained their police approved status in 2017.

Now that the cloud providers have been granted police approval, the next question is, where do we go from here? What are the options for UK police forces when it comes to moving their IT services to the cloud?

1 https://www.gov.uk/guidance/government-cloud-first-policy
2 https://www.cloudindustryforum.org/content/research-shows-public-sector-cloud-adoption-soaring-care-needed-when-choosing-migration
Why cloud?

It is worth taking a step back to briefly remind ourselves of the benefits of cloud computing. While the cloud may be the default position, a public sector IT project still needs a compelling business case before it can be justified.

What are the benefits police forces can expect from migrating to the cloud?

**Scalability**
A cloud platform can dynamically scale to the needs of the customer by automatically allocating additional compute resource in times of high demand. At the same time, they are often billed in a much more flexible, per-user basis. Combined with the scalability of the underlying architecture, this means another 1,000 users can be added to your service almost instantaneously. No more waiting for new hardware to be delivered, installed and configured before you can add more users to your IT service.

**Cost**
The scalability of the cloud also adds to its cost-effectiveness, since it can be scaled for typical load, then scaled up dynamically for peaks as needed. An on-premise system on the other hand must be scaled for peak loads all of the time, which is inherently more expensive as most of the resources are sitting idle most of the time.

Cloud providers also typically operate on a monthly subscription model, all but eliminating upfront costs. This enables forces to move from a high capex/asset depreciation model to a low monthly opex model. Combined with the scalability to add/remove users when needed, it is also much more efficient since you only pay for the number of users who need the software. No more investing in additional capacity which may never be used.

**Resilience and disaster recovery**
The resilience of cloud computing services significantly reduces the need for “disaster recovery” since the likelihood of disasters are significantly reduced. Cloud services mirror their data across multiple sites both nationally and internationally (in keeping with the data sovereignty requirements of the client), so even a catastrophic hardware failure at one site will not result in data loss. All this being said, in the rare occurrence that a disaster has occurred, cloud computing makes the recovery process easier, faster, and more cost-effective.

**Simplicity**
Cloud services are generally much simpler to manage because many routine processes, such as updating operating systems and software, are handled by the cloud or service provider as an automated service. This means the customer can focus on their own software, safe in the knowledge that the infrastructure is managed for them.

**What are the cloud options for police?**

With the main hurdle now firmly behind them, most police forces are now seriously thinking about the cloud for the very first time. However, given the numerous flavours of cloud to choose from, combined with the challenges and upheaval of transitioning any live IT service from one platform to another, police forces will be wise to proceed with caution and review their options before committing to their cloud path.

While most IT systems can be considered “mission critical” to the smooth operations of a business, they do not directly affect public safety and security. In this regard, the term “mission critical” takes on a much more significant tone in relation to the police. Extra caution and planning isn’t just necessary to avoid an embarrassing IT failure, but it is imperative to maintaining public safety. The police are wise to proceed with caution when it comes to their transition to the cloud.

So, now that there is regulatory approval for the use of cloud datacentres in the UK for Official data, and the major UK cloud providers gained police approval in 2017, forces are now able to press on with cloud adoption. So, what are their options?

**Adopt Office 365**
As a relatively easy first step, forces can start by migrating their office workloads to the Office 365 cloud. This will enable them to begin using the cloud for non-critical workloads, while keeping their own datacentres for more critical data and systems. It will also provide the opportunity for secure interoperation and collaboration between other forces and agencies that are also using Office 365, since collaboration is an integral feature of Office 365. Lastly, because Office 365 uses a cloud-based Active Directory system, forces can begin to leverage a common identity management system for other cloud services. Once a force has adopted Office 365, it makes sense to use these facilities to provide a common identity management solution for other cloud services since users will benefit from one login for all cloud services. Since most police forces require officers to remember multiple login details and passwords to access their different systems, moving towards a “single sign-on” environment would be a dramatic improvement.

**Move datacentre resources to cloud**
Another option being considered by police forces is simply migrating their existing datacentre to the cloud. A so-called “lift and shift” this idea is generally borne out of a misperception that the cloud is “just someone else’s datacentre.” If you manage your own datacentre then the cloud is technically no different – it’s still just a room full of servers, so surely it’s just a matter of lifting the existing code and database to the new environment and letting the cloud provider take over the management of the infrastructure? Unfortunately not. Moving a datacentre to the cloud will provide limited benefits because the virtual machines (VMs) still need to be managed. All you achieve is a change in the cost model of your datacentre from capex to opex. This also raises the issue of writing off your existing datacentre investments and contracts. If you migrate to the cloud before your datacentre has reached its end-of-life, you are effectively throwing money you have already spent down the drain.

**Hybrid cloud**
This is the route many forces will take, and will be the logical next step after migrating office workloads to Office 365. A hybrid cloud will combine some cloud workloads with a base load kept in the datacentre. This is a prudent approach since services can be migrated to the cloud at the most appropriate time (e.g. end-of-life), gives more cost-effective scalability and avoids the risks posed by a “Big Bang” transition since different functions can be migrated over time.
Migrate to IaaS or PaaS

Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) are two routes towards a fully cloud-enabled infrastructure, however both options still require a good amount of management by the customer.

- **IaaS** for example is the closest thing to putting your own datacentre in someone else’s building. You will retain the most control over the hardware but, aside from scalability, you gain the fewest cloud benefits because you still have to manage the hardware. With IaaS, the VMs and other virtual hardware are provided as a service, but much of the maintenance, such as updating operating systems and licensing still has to be managed by the customer. All the major cloud providers (AWS, Azure, Google Cloud, Alibaba Cloud, IBM) offer IaaS.

- **PaaS** is one step above IaaS towards a fully-fledged “cloud” service. This is where the service not only provides the VMs (like IaaS), but also provides the operating system as a managed service. You can then build your applications directly onto the operating system.

Consuming SaaS

Software-as-a-Service goes beyond IaaS and PaaS by providing the application itself as a service. SaaS is typically delivered from outside of the force’s cloud tenancy, secured using HTTPS / TLS1.2 and secured by a cloud-based identity management system as a minimum. SaaS can deliver results to a force more quickly than all of the previous options because it does not automatically require any type of migration. This makes it a very good starting point for the cloud because a force can leverage new technology without having to write-off its existing datacentre investments. While it does need some investment such as integrating with a cloud based identity management system, this is considerably cheaper and lower risk than migrating the force’s entire datacentre to a IaaS or PaaS tenancy.

For many forces, consuming SaaS is the most logical first step to cloud adoption. There is nothing to stop a force from consuming SaaS at any point in their cloud transition. Indeed, a Google search or an Amazon purchase are examples of using SaaS. It is important to remember that the road to the cloud is not a ladder; you do not need to start with on-premise before climbing to IaaS, PaaS and eventually to SaaS. A force can adopt SaaS at any time without migrating anything.

SaaS: Leverage the benefits of the cloud without the hassle

In most instances, when you move your IT services from a self-hosted datacentre to a private cloud provider, you are still using someone else’s software e.g. SAP, Oracle, Microsoft etc. If you are building or buying a cloud infrastructure simply to run someone else’s software, why not use their hardware too? If the supplier offers it, why not adopt a Software-as-a-Service (SaaS) model?

SaaS offers most the benefits of the cloud but with very few drawbacks. With SaaS you can quickly add new capabilities, and users at relatively low risk and cost, there is minimal or zero capital outlay, and SaaS providers practice the highest standards of security and availability. As previously, the major cloud providers have the most sophisticated security protection measures available which are impracticable to implement on-premise or in a private datacentre.

SaaS is often very comparable to the real-world cost of deploying software on your own cloud. Looking at the Digital Marketplace for example, the cost of a two-year software licence installed in your cloud could quite easily cost the same or more than simply using your SaaS provider’s service which uses their own cloud.

The flexible deployment of SaaS can also help to minimise the waste that will occur from mothballing existing datacentres too soon, as deployments can be staggered as and when old assets reach their natural end-of-life. By leveraging a SaaS provider’s service you can stagger the retirement/migration of existing on-premise/cloud infrastructure. This will enable you to either keep or re-purpose assets where you are already committed, preventing you from retiring them before their time.

On-premise, cloud or SaaS: Microsoft Exchange example

The range of options for obtaining Microsoft Exchange is a great example of this scenario. From an entirely self-hosted/self-management model all the way up to a SaaS solution, Exchange can be deployed however you want. On the self-management end you can choose to purchase a licence for Exchange Server 2019 and simply host it on your own datacentre or in a private cloud/IaaS environment. On the SaaS end of the scale you can choose to skip the build process altogether and simply subscribe to hosted Exchange 2019 or Office 365. From a software perspective, the end-user experience is the same in all instances. Every user will have the same synchronised mailbox experience with all the collaboration features that Exchange offers. The difference will be behind the scenes, particularly in the levels of reliability and security offered where the SaaS option is unmatched.
Align with the National Enabling Programme (NEP)

To simplify the choices available to them, particularly when it comes to which of the public cloud platforms to choose from, police forces should align themselves with the recommendations of the NEP.

The NEP was created to underpin the delivery of several outcomes of the Policing Vision 2025. According to the NPCC, it will provide a "modern technology environment that is fundamental to transforming ways of working across policing in the UK." The NEP consists of three inter-related programmes:

1. **Productivity Services**
   - To provide UK forces with a standardised cloud platform and access to collaboration and business tools.

   **Chosen solution: Microsoft Office 365**

2. **Identity and Access Management (IAM)**
   - A standardised platform to IAM across every police force in the country will dramatically improve collaboration and data sharing between forces, enabling officers and staff to get the data they need, when they need it, regardless of location, force, or device. From the end-user perspective, it means an officer can access the appropriate local, regional, and national resources securely and from one single sign-on (SSO).

   **Chosen solution: Microsoft Azure Active Directory (Azure AD)**

3. **National Management Centre**
   - Cybersecurity is a cornerstone of the NEP. The National Management Centre has been devised to secure infrastructure and assets, monitor participating police forces and help mitigate information security risks. It will provide centralised security monitoring and response coordination, so forces are forewarned and able to identify the possibility of cyber-attack, insider threat and data-loss.

   **Chosen solution: Deloitte and BT as delivery partners**

**Which cloud provider to use?**

If you want to host your own resources in the cloud, there are several well-known cloud providers – such as Amazon Web Services, Windows Azure, Google Cloud, UKCloud and many others. Each of these is likely to deliver the performance and resilience that police forces need.

One factor to consider is the ease of interoperability of software, and the ease of achieving inter-force and inter-agency working. For maximum benefit, it is to be hoped that some kind of national ecosystem will evolve to facilitate easier integration between different software services and across forces and agencies. This should be achievable in a manner which is agnostic of cloud provider. For example, the use of a common identity management solution (or an integrated set of solutions) makes sense, to facilitate sharing of data between organisations and to define trust relationships. Where Software-as-a-Service is consumed, the cloud provider is determined by the service provider, and the underlying cloud provider will not normally be an issue as long as it meets the necessary regulatory standards and the data is domiciled in the UK. This also keeps the cloud market competitive as the various cloud providers will be competing to provide specific services which contribute to the overall solution nationally.

4. **Cybersecurity as a cornerstone of the NEP**
   - Cybersecurity is a cornerstone of the NEP. The National Management Centre has been devised to secure infrastructure and assets, monitor participating police forces and help mitigate information security risks. It will provide centralised security monitoring and response.

   **Chosen solution: Deloitte and BT as delivery partners**

**Which cloud provider to use?**

If you want to host your own resources in the cloud, there are several well-known cloud providers – such as Amazon Web Services, Windows Azure, Google Cloud, UKCloud and many others. Each of these is likely to deliver the performance and resilience that police forces need.

Chosen solution: Deloitte and BT as delivery partners

2. **Identity and Access Management (IAM)**
   - A standardised platform to IAM across every police force in the country will dramatically improve collaboration and data sharing between forces, enabling officers and staff to get the data they need, when they need it, regardless of location, force, or device. From the end-user perspective, it means an officer can access the appropriate local, regional, and national resources securely and from one single sign-on (SSO).

   Chosen solution: Microsoft Azure Active Directory (Azure AD)

3. **National Management Centre**
   - Cybersecurity is a cornerstone of the NEP. The National Management Centre has been devised to secure infrastructure and assets, monitor participating police forces and help mitigate information security risks. It will provide centralised security monitoring and response coordination, so forces are forewarned and able to identify the possibility of cyber-attack, insider threat and data-loss.

   Chosen solution: Deloitte and BT as delivery partners

Your place or mine?

The opportunities to leverage SaaS could be right under your nose. Have you looked at your existing supply chain? Do any of your existing software or service providers have their own cloud services? If so, do they have a SaaS solution?

You may be surprised to learn how many of your existing service or software providers have already invested in their own SaaS services, most of which will be based on their own tenancies at the major, well-known cloud providers you may have already deployed or considered (Amazon Web Services, Windows Azure, Google Cloud, UKCloud etc.).

With the right mechanisms in place, it will be cost-effective to leverage your suppliers’ own clouds by adopting their SaaS solutions. Don’t be afraid to put some of your data in your SaaS provider’s cloud as part of a public cloud/SaaS hybrid solution (even if your data is only stored in the SaaS solution for a short period of time as part of your transition, or in transit through your SaaS provider’s solution for data processing before it is passed back to your cloud). This hybrid approach will likely be better from a financial perspective than running everything on your own cloud and does not necessarily mean any compromise in security or reliability. It will also simplify your cloud strategy since that’s one less service to migrate to your cloud, and one less procurement hurdle to jump through since you will already be engaged with this supplier.

Just make sure you check your supplier’s credentials!

- Are they certified against the CyberEssentials scheme?
- Do they adhere to the 14 Cloud Security Principles as defined by the National Cyber Security Centre?
- Are they interoperable with your back-office systems and upcoming national IT initiatives such as NLEDs and the ESN?

- Will they lock you in (e.g. fixed 5-year contracts, do they adhere to the G-Cloud’s requirements for no vendor lock in)?
- Do they align with the NEP?

When it comes to cloud, going “all in” by putting all of your IT services into your own cloud tenancy might not be the right approach. Exploring digitisation and cloud options is an opportunity to review all the solutions out there. It is not simply a matter of lifting everything you already have and putting it into a cloud server, but of finding better ways of doing things which deliver a police force fit for the 21st century.

If a supplier offers you the choice between hosting their solution in your cloud tenancy or theirs (i.e. as a SaaS service), there are very few reasons why you would not choose their tenancy (i.e. consume it as SaaS). The software provider has the expertise to manage their service, and if they can manage that service in real-time they will be able to offer a more cost-effective, responsive and efficient solution than simply providing support for software running in your own cloud. Doing so will not only save you money on the service itself, it will all but eliminate the management overheads, remove the need for a wholesale “lift and shift”, and allow you to stagger your force’s transition to the cloud. If a SaaS solution exists for your chosen service, you can effectively treat it like any other web service. You would not host your own version of Facebook’s software on your server for example. Doing so would be inefficient, a maintenance nightmare and an ongoing security risk. If you can treat any new IT service in the same way (providing they have the necessary security credentials for handling official data) then there is no need to take on more risk than you need to. With SaaS your force can take the fastest, safest and most cost-effective route to digital policing.

https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
