WHITE PAPER

Cloud Adoption in the U.K. Public Sector is Not Matching the Government's Cloud First Policy

solarwinds

Cloud Adoption in the U.K. Public Sector is Not Matching the Government's Cloud First Policy

It's been five years since the U.K. government made it mandatory for central government departments to consider and fully evaluate potential cloud solutions before any other option when procuring new or existing services. It also strongly recommended the policy should be adopted by the wider public sector

In February 2018, the Government Digital Service (GDS) published guidance[1] reiterating its Cloud First policy, which acknowledged departments could "choose an alternative to the cloud but will need to demonstrate that it offers better value for money." It defined value for money as "securing the best mix of quality and effectiveness for the least outlay over the period of the use of the goods or services bought."

The GDS was very clear that Cloud First was intended purely for public cloud and not for community, hybrid, or private cloud deployment models. "There are circumstances where the other deployment models are appropriate but the primary benefits for government come when we embrace the public cloud," it stated. The GDS encouraged departments to consider Software as a Service (SaaS) models, particularly for enterprise IT and back office functions, and to make use of public cloud hosting if bespoke development was necessary.

The GDS added it could help departments "assure the mix of quality and effectiveness of cloud services across their whole life cost (this includes capital, maintenance, management, operating, and exit costs)" as part of the spend control process.

With Cloud First having been in operation for five years, SolarWinds set out to gauge awareness of the policy among a number of government departments and public sector organisations—and to find out how they were adhering to it. To this end, the company submitted a Freedom of Information (FOI) request into cloud adoption in the U.K. government sector.

[1]Government Cloud First policy. *GOV.UK.* Available at: https://www.gov.uk/guidance/government-cloud-first-policy [Published February 3, 2017]

AWARENESS IS HIGH, ADOPTION IS LOWER

Encouragingly, the FOI request revealed that four out of five central government, defence, and NHS organisations were aware of the Cloud First policy. Adoption, however, was much lower. Only 30% of NHS trusts had adopted any level of public cloud in their organisation, while the figure for central government departments was 61%.

The key barriers to public cloud adoption for government organisations were security and compliance, budget, and legacy technology/vendor lock-in. For NHS trusts, security and compliance was the biggest issue (61%), followed by budget (55%) and legacy technology/vendor lock-in (53%). The results for central government were different, with legacy technology/vendor lock-in heading the list of obstacles (50%), followed by security and compliance (39%) and lack of skills to implement public cloud services (25%).

Concerns over security and compliance among NHS trusts may be partly assuaged going forward by the issuing of guidance in January 2018 from the Department of Health over offshoring and the use of public cloud services[2]. The guide states that NHS and social care providers "can safely put health and care data, including non-personal data and confidential patient information, into the public cloud." It argues that cloud services "can mitigate many common risks NHS and social care organisations often face," and believes they "may provide other advantages for NHS and social care organisations including lower IT costs and the ability to develop, test, and deploy services quickly without large capital expense."

However, resistance to making a complete commitment to public cloud persists. The FOI request revealed that 79% of NHS trusts and 41% of central government departments had no plans to fully migrate to the public cloud.

WHAT IS THE PUBLIC CLOUD BEING USED FOR?

Despite the differences in rates of public cloud adoption, NHS trusts and central government departments both identified migrating applications as their primary use for public cloud. Just over three-quarters (76%) of central government respondents indicated they were migrating applications, compared to 68% of NHS trusts.

Another popular use was databases, which accounted for just over 40% for NHS trusts and central government. But there was a divergence between the two in the area of storage: more than half of NHS trusts revealed they used public cloud for storage compared to 32% for central government.

[2]NHS and social care data: off-shoring and the use of public cloud services guidance, NHS Digital. Available at: https://www.digital.nhs.uk/article/8499/NHS-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services-guidance [Published February, 2018].

MONITORING AND MANAGING CHALLENGES

A key issue in the reluctance of government and public sector organisations to migrate to the public cloud is the difficulty they experience monitoring the public cloud as part of their wider data infrastructure. Almost half of NHS trusts (48%) and central government departments (53%) revealed that they used four or more monitoring tools to manage their data infrastructure.

It also emerged from the FOI request that 77% of NHS respondents and 55% of central government respondents were not using the same monitoring tools across their data infrastructure or were unsure if their monitoring and management tools could handle working across on-premises and public cloud environments.

NHS trust challenges: The biggest challenges in monitoring and managing the public cloud were determining suitable workloads for the cloud (49%), lack of control of cloud performance (47%), and protecting and securing the cloud (45%).

Central government challenges: 35% of central government organisations using the public cloud cited challenges in protecting and securing data as their biggest obstacle, with lack of control across the environment, downtime concerns, and identifying suitable workloads (all at 29%) highlighted as significant challenges.

SIGNIFICANT DOUBTS OVER ROI OF PUBLIC CLOUD

Concerns from NHS trusts and central government over how best to use, manage, and monitor public cloud seem to be having a detrimental effect on their views of the potential for an ROI from cloud.

Only 17% of NHS trusts expect to gain any ROI from public cloud adoption, and 6% are already pessimistic enough to believe they won't see any ROI at all. Compared to the NHS, central government is marginally more optimistic, with 18% of departments expecting to get some ROI from the cloud. However, 65% thought it was still too early to determine. Unlike the NHS trusts, no central government department was prepared to categorically rule out the possibility of ROI.

With those figures in mind, it's easy to see why there is still a large measure of reluctance to fully embrace public cloud. But it's also clear that there is a link between their difficulties in monitoring and managing infrastructure (including public cloud) and the problems they are experiencing in trying to achieve the objectives of the government's Cloud First policy.

MANAGING THE CLOUD FIRST CHALLENGE

The results of the FOI suggest government organisations, particularly those handling sensitive data, are still unconvinced that the public cloud is an integral tool that can deliver considerable ROI. The lack of consistency in management tools across the infrastructure is a significant factor in their lack of confidence over the benefits of public cloud.

The government needs tools that combine the monitoring and management of on-premises and cloud infrastructure, including legacy technology, in a way that visualizes global system performance and creates ROI potential. Without them, it will be almost impossible to achieve the cost-efficiency and data fluidity the government is aiming for with the Cloud First policy.

Given the importance the U.K. government has attached to Cloud First, it would be highly regrettable if the initiative was to be undermined by the concerns of public sector organisations over their ability to govern their infrastructure.

HOW CAN SOLARWINDS HELP?

While discrete monitoring tools may cover the basics, the public sector requires a more comprehensive toolset to improve IT efficiency and effectiveness.

By simultaneously monitoring all on-premises and cloud environments, IT professionals in the NHS, central government, and defence can achieve a holistic view across their entire environment, including applications, databases, servers, and the network.

This level of visibility across environments is vital to ensuring public organisations tackle hybrid IT's most pressing challenge: getting the most from the cloud. To maximise the success of public cloud adoption, SolarWinds recommends:

Maintaining visibility across on-premises and cloud environments from one central location

With the vast number of systems in place in organisations such as the NHS, and the rate of change in government technology, a management and monitoring toolset that sits across all platforms is essential. This acts as a single point of truth, and consolidates and correlates data to deliver more depth and breadth of visibility to allow public sector IT professionals to identify problem areas, and keep the organisation focused on helping constituents.

Planning beyond cost efficiency

While the Cloud First policy recommends the cloud based on its cost efficiency and ROI potential, government IT professionals should instead be focused on service delivery, using the cloud to help with scalability and flexibility. While concerns remain around security and compliance, IT professionals will need to ensure they factor these considerations into applications before migrating to cloud services. This will be essential for making the most of the benefits of public cloud while navigating some of the most common concerns.

Cloud-proofing your job

Traditional IT roles are converging, and there is significant hype around automation technology as a way to cut costs. Public sector IT professionals need to focus on improving and cultivating fundamental skillsets that will make them indispensable in the age of the cloud and beyond.

This means being able to look at the Cloud First policy and attaining the skills needed to make this a reality. IT professionals often rank hybrid monitoring/management tools and metrics, application migration, automation, and data analytics as the most important skills and knowledge needed to successfully manage hybrid IT environments. Government IT professionals should look to leverage their peer community to better understand and more quickly put into practice various technology adaptations and abstractions like software-defined constructs, containers, microservices, and serverless architecture. They should establish monitoring as a foundational IT function, also known as monitoring as a discipline, to drive a more proactive, efficient, and effective IT management strategy.

Remaining flexible and plan for future technologies

Every government entity is unique, and the velocity, variety, and volume of new services available is constantly providing new opportunities for innovation. IT professionals must be open to and agile in adopting the best elements of cloud technology, building a roadmap for future proof-of-concepts and migration that will help illustrate ROI and business results for the management teams. A critical part of this will be understanding how to get visibility of the entire infrastructure with hybrid IT monitoring tools, building processes for migration and quality/reliability testing of applications, and learning economic and capacity planning models.

"Trusting but verifying" that cloud is performing as expected

"Trust but verify" will be an essential approach as public sector organisations work to maintain control and visibility of workloads and applications in the cloud. Without this, IT teams will struggle to truly understand how workloads are performing in the cloud, and what is affecting that performance. Building a multi-cloud strategy to avoid downtime from a single point of failure will be critical, and organisations need to implement distributed systems best practices by spreading assets across a variety of regions and managing geographically dispersed workloads.

Learn more about how SolarWinds can help government IT professionals better monitor and manage their infrastructure from on-premises to the cloud here.

About SolarWinds

SolarWinds provides powerful and affordable IT management software to customers worldwide from Fortune 500® enterprises to small businesses, government agencies and educational institutions. We are committed to focusing exclusively on IT pros, and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address all key areas of the infrastructure from on-premises to the cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at www.solarwinds.com.

NATIONAL GOVERNMENT
Phone: +353 21 2330440
Email: nationalgovtsales@solarwinds.com
solarwinds.com/nationalgovernment